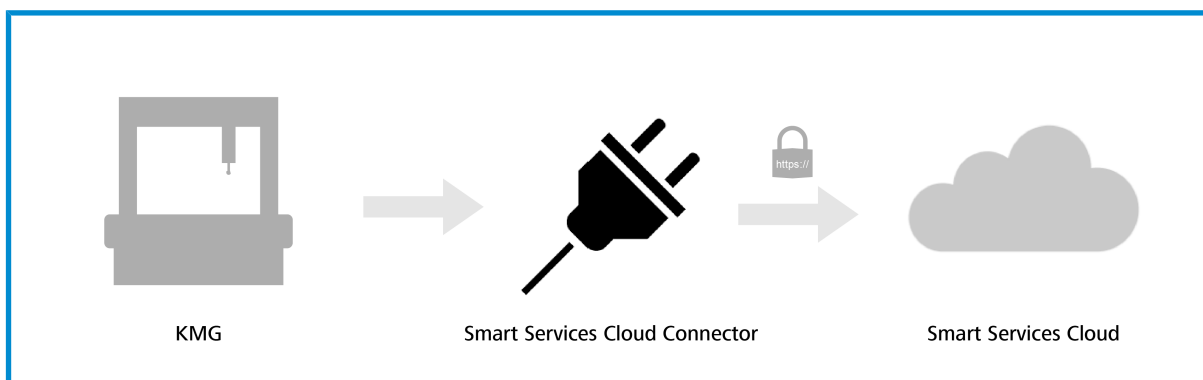


ZEISS Smart Services Cloud Connector



Einleitung

Der **Smart Services Cloud Connector** (im Folgenden auch **Cloud Connector** genannt) ermöglicht die Verwendung des **Smart Services Dashboard** zur Überwachung von ZEISS Koordinatenmessgeräten (KMG). Er stellt eine Verbindung zwischen dem Bedienerrechner der Messmaschine und der **Smart Services Cloud** her:



Der **Cloud Connector** agiert hier als IoT Device-Client, der die Maschine an der **Smart Services Cloud** registriert und die Verbindung herstellt.

Dieses Dokument gibt einen technischen Überblick über den **Cloud Connector** und dessen Arbeitsweise ([↗ Kapitel 1: Architektur & technische Beschreibung \[Seite 6\]](#)) und geht auf Sicherheitsaspekte ein ([↗ Kapitel 2 Sicherheitsbetrachtungen \[Seite 8\]](#)).

Kapitel [↗ 3 \[Seite 9\]](#), [↗ 4 \[Seite 14\]](#) und [↗ 5 \[Seite 17\]](#) beschreiben die notwendigen Schritte zu Installation, Reparatur und Deinstallation des **Cloud Connectors**.

Zudem werden hilfreiche Werkzeuge für die Installation, das Management und die Analyse des **Cloud Connectors** beschrieben ([↗ Kapitel 6: Werkzeuge des Betriebssystems \[Seite 18\]](#)) und in [↗ Kapitel 7 \[Seite 24\]](#) häufig gestellte Fragen beantwortet.

Bei weiteren Fragen finden Sie die notwendigen Kontaktdaten auf der Rückseite/letzten Seite des Dokuments.

Inhaltsverzeichnis

1	Architektur & technische Beschreibung	6		
1.1	Systemübersicht	6		
1.1.1	Kommunikation	6		
1.1.2	Zertifikate	7		
1.1.3	Protokollierung	7		
1.2	Dateispeicherorte	7		
2	Sicherheitsbetrachtungen	8		
2.1	Verschlüsselung	8		
2.2	Minimierte Anforderungen an die Netzwerkinfrastruktur	8		
2.3	Eindeutige Identifikation der Maschinen	8		
2.4	Standards	8		
3	Installation	9		
3.1	Systemvoraussetzungen	9		
3.2	Cloud Connector installieren	10		
4	Reparatur und Deinstallation	14		
5	Migration	17		
6	Werkzeuge des Betriebssystems	18		
6.1	Windows Installer	18		
6.2	Management von Windows Services	18		
6.2.1	Dienste starten/beenden	19		
6.2.2	Zustand des Services ermitteln	19		
6.2.3	Prozess-ID des Dienstes ermitteln	20		
6.2.4	Dienst beenden erzwingen	20		
6.2.5	Dienst deinstallieren	20		
6.3	Verwaltung von Zertifikaten	21		
6.3.1	Übersicht installierter Zertifikate aufrufen	22		
6.3.2	Maschinenzertifikat für Cloud Connector	22		
7	Problembehandlung	24		
7.1	Installationsprobleme	24		
7.2	Fehler nicht in Protokolldatei	25		
7.3	Netzwerkconfiguration	26		
7.4	Cloud Connector lässt sich nicht deinstallieren	26		
7.5	Maschinenzertifikate manuell entfernen	26		
7.6	Dienst lässt sich nicht beenden	26		

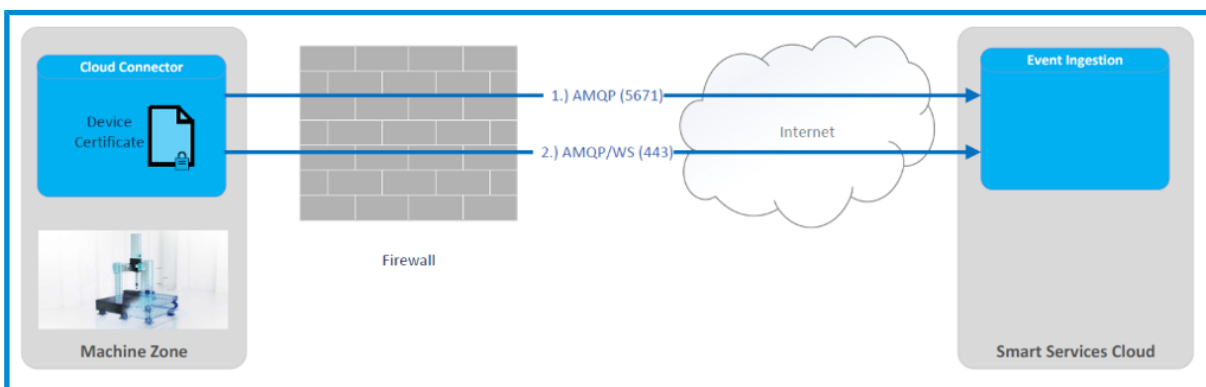
.....

1 Architektur & technische Beschreibung

Der **Cloud Connector** ist technisch ein lokaler Windows Service auf dem Bedienerrechner, der festgelegte Ereignisse der Messmaschine vom CMM-Agent über Microsoft Message Queuing bekommt und diese gesichert in die **Smart Services Cloud** überträgt. Die Verwendung von Message Queues ermöglicht es auch, kurzzeitige Verbindungsabbrüche ohne Datenverlust zu überbrücken.

Die **Smart Services Cloud** ist das auf Basis von Microsoft Azure implementierte Backend für **ZEISS Smart Services**-Funktionalitäten wie z. B. das **Smart Services Dashboard**. Diese wird nach internationalen Standards (bspw. ISO 27001, HIPAA, FedRAMP, SOC1 und SOC2) zertifizierten und auditierten Microsoft Rechenzentren in Europa betrieben.

1.1 Systemübersicht



1.1.1 Kommunikation

Der **Cloud Connector** verwendet für die Kommunikation mit der **Smart Services Cloud** ausschließlich das AMQP-Protokoll. Jede Kommunikation ist hierbei TLS verschlüsselt. Für die Verwendung in unterschiedlichen Netzwerktopologien verwendet der **Cloud Connector** einen Fallbackmechanismus mit dem maximalen Bedarf von zwei geöffneten Ports an der Firewall:

In einem ersten Schritt versucht sich der **Cloud Connector** über den Port 5671 per AMQP über TCP mit der **Smart Services Cloud** zu verbinden. Sollte hierüber keine Verbindung aufgebaut werden können, verwendet der Cloud Connector den Port 443 mittels AMQP über Secure WebSockets.

Dieses Verhalten ermöglicht die Umsetzung unterschiedlicher Szenarien und gibt dem Nutzer die volle Kontrolle ausschließlich durch entsprechende Konfiguration an der Firewall. Bei Verwendung von Port 5671 ist der Datenverkehr separiert von evtl. anderen Komponenten, die über 443 nach außen kommunizieren und eindeutig dem **Cloud Connector** zuordenbar. Falls dies nicht gewünscht ist, kann durch Verwendung des Ports 443 mit der minimalen Anzahl von genau einer Portfreischaltung der **Cloud Connector** im eigenen Netz betrieben werden.

Der **Cloud Connector** unterstützt auch die Kommunikation über Proxyserver.

1.1.2 Zertifikate

Die Identität der Maschinen wird durch ausgestellte Maschinenzertifikate der Carl Zeiss Industriellen Messtechnik GmbH sichergestellt. Der **Cloud Connector** kann sich nur mit einem gültigen Maschinenzertifikat an der **Smart Services Cloud** registrieren. Die Zertifikate sind eindeutig einer Maschine zugeordnet und stellen daher eine Art Ausweis dar. Technisch hat ein Maschinenzertifikat die Seriennummer des Geräts als Common Name (CN) hinterlegt.

Das Maschinenzertifikat wird hierzu im Microsoft Windows Zertifikatsspeicher des Bedienerrechners hinterlegt und vom **Cloud Connector** für die Registrierung bzw. Provisionierung verwendet.

1.1.3 Protokollierung

Der **Cloud Connector** schreibt detailliert Informationen in Protokolldateien. Hierin können sowohl die übertragenen Ereignisse als auch Informationen zum Zustand des **Cloud Connectors** nachverfolgt werden. Bei einer Standardkonfiguration werden die Protokolldateien am voreingestellten Ablageort in einem rotierenden Verfahren gespeichert. Dieser Pfad kann in der Konfigurationsdatei des **Cloud Connectors** individuell eingestellt werden. Der entsprechende Abschnitt ist:

```
"logger": {  
  "LogLevel": "Info",  
  "FileName": "${specialfolder:folder=CommonDocuments}/ZEISS/Smart Services Cloud  
Connector/logs/log.txt",  
  "Format": "${longdate} | ${level:uppercase=true} | ${logger} | ${message} ${except-  
ion:format=toString,Data:maxInnerExceptionLevel=10}",  
  "AmountOfLogsToKeep": 10  
},
```

Hier kann über das Property `FileName` der Ablageort und über `AmountOfLogsToKeep` die Anzahl der aufbewahrten, nicht überschriebenen alten Protokolldateien eingestellt werden. Das Format der protokollierten Informationen sollte nicht geändert werden, da sonst für Analysen eventuell notwendige Daten fehlen.

1.2 Dateispeicherorte

Der **Cloud Connector** speichert verschiedene Artefakte an den folgenden Stellen des Bedienerrechners:

Verzeichnis	Zweck	Ablageort/Voreinstellung
Installation	Ablage der für den Cloud Connector notwendigen Programmdateien	C:\Program Files (x86)\ZEISS\Smart Services Cloud Connector\
Konfiguration	Ablage von Konfigurationsdateien für den Cloud Connector : <ul style="list-style-type: none">■ preferences.json■ serviceconfig.json	C:\Users\Public\Documents\ZEISS\Smart Services Cloud Connector\
Protokollierung	Ablage der vom Cloud Connector geschriebenen Protokolldateien: <ul style="list-style-type: none">■ log.txt■ log.[0-9].txt	C:\Users\Public\Documents\ZEISS\Smart Services Cloud Connector\logs

2 Sicherheitsbetrachtungen

Der **Cloud Connector** stellt durch unterschiedliche Maßnahmen die Sicherheit des Betriebs sowie die Vertraulichkeit und Integrität der übertragenen Daten sicher. Sicherheitsaspekte werden im Rahmen des Entwicklungsprozesses betrachtet und regelmäßig geprüft. Maßnahmen zur Sicherung des Netzwerks selbst sind allerdings als Mitwirkungspflicht des Nutzers im Rahmen des operativen Betriebs zu sehen.

Die folgenden Punkte sind aus architektonischer Sicht relevant.

2.1 Verschlüsselung

Jede vom **Cloud Connector** genutzte Kommunikationsstrecke (siehe [🔗 Kommunikation \[Seite 6\]](#)) wird auf Transportebene mittels TLS 1.2 mit dem Advanced Encryption Standard (AES) 256 bit verschlüsselt (Secure AMQP Protokoll – AMQPS oder WebSockets).

2.2 Minimierte Anforderungen an die Netzwerkinfrastruktur

Eine unnötige Komplexität erhöht das Sicherheitsrisiko in Softwarekomponenten. Daher und um in unterschiedlich ausgestatteten Umgebungen bei den nutzenden Firmen lauffähig zu sein, wurde bei der Architektur des **Cloud Connectors** auf unnötige Komplexität verzichtet. Die Anforderungen an die Netzwerkinfrastruktur wurden minimiert. So ist im Extremfall genau ein Port für die Kommunikation mit der **Smart Services Cloud** an der Firewall zu öffnen. Da es sich hierbei um den für externe Kommunikation schon geöffneten Standardport für verschlüsseltes http (443) handelt, sind in vielen Fällen keine Änderungen an Firewall Einstellungen notwendig. Es werden vom **Cloud Connector** ausschließlich ausgehende Verbindungen aufgebaut. Für eingehende Kommunikation sind keine Ports zu öffnen.

2.3 Eindeutige Identifikation der Maschinen

Um die Integrität und die gesicherte Herkunft der Daten zu gewährleisten, werden die Maschinen durch von **ZEISS** ausgestellte Maschinenzertifikate eindeutig identifiziert. Dies verhindert Angriffsszenarien zum Verschmutzen der Maschinendaten mit falschen Daten. Somit lassen sich nur mit einem gültigen Maschinenzertifikat Daten zu dieser Maschine an die **Smart Services Cloud** übertragen.

Die Zertifikate werden über die **ZEISS** interne Private Key Infrastructure generiert und dem Nutzer zur Verfügung gestellt. Auf Nutzerseite sind diese Maschinenzertifikate mit der entsprechenden Sorgfalt und Vertraulichkeit zu behandeln.

2.4 Standards

Ein weiterer Punkt zur Minimierung von Sicherheitslücken ist die Vermeidung eigener Implementierungen sicherheitsrelevanter Teile. Hierzu wird vom **Cloud Connector** für die Kommunikation ausschließlich das von Microsoft zur Verfügung gestellte Device SDK im Standard verwendet.

3 Installation

Für die Installation des **Cloud Connectors** wird dieser als Windows Installer Paket (msi) zur Verfügung gestellt und muss mit Administratorrechten ausgeführt werden, da der **Cloud Connector** als lokaler Windowsservice installiert wird und das Management des Maschinenzertifikats ebenso erhöhte Rechte benötigt.

3.1 Systemvoraussetzungen

Die aktuelle Version des **Cloud Connectors** kann über das Downloadportal heruntergeladen werden:

<https://portal.zeiss.com/download-center/software/imt>

Die Aufgabe des **Cloud Connectors** ist ausschließlich die Herstellung der Kommunikationsstrecke zwischen dem Bedienerrechner der Messmaschine und der **Smart Services Cloud**. Die entsprechenden Daten bekommt der **Cloud Connector** vom CMM-Agent über Windows Message Queuing. Daher müssen die folgenden Systemanforderungen erfüllt sein:

Kategorie	Bedingung
Maschinensteuerung	C99 N/S/L/L2/M
Steuerungsfirmware	FW ≥ 25.00
Hardware	<p>Vorhandene Netzwerkverbindung über Port 5671 oder Port 443 zu *.azure-devices-provisioning.net und *.azure-devices.net</p> <p>Sollte eine spezifischere Konfiguration benötigt werden, können diese eingeschränkt werden auf zeiss-imt-cmmiot-dps-prod.azure-devices-provisioning.net, zeiss-imt-cmmiot-iot-hub-prod.azure-devices.net und global.azure-devices-provisioning.net. Diese könnten sich allerdings zukünftig ändern.</p>
Betriebssystem	Windows 10 Build 1607 (Anniversary Update) .NET Framework 4.8
Software	Calypso ≥ 6.4.08 (2017) CMM-Agent MSMQ (siehe https://docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/ms711472(v=vs.85) und https://docs.microsoft.com/de-de/dotnet/framework/wcf/samples/installing-message-queuing-msmq zur Installation)
Zertifikat	Ein von ZEISS IMT ausgestelltes Maschinenzertifikat inkl. Passwort für den Private Key

HINWEIS:

Bitte stellen Sie vor der Installation sicher, dass die Einstellungen der lokalen Zeit und Zeitzone auf dem Bedienerrechner der Messmaschine korrekt sind.

3.2 Cloud Connector installieren

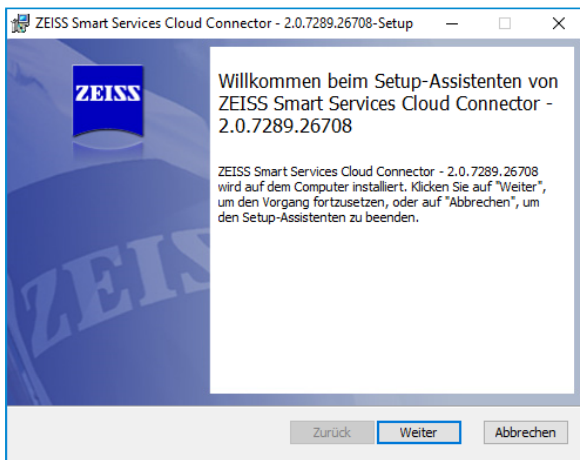
Beachten Sie die Installationshinweise, bevor Sie den **Cloud Connector** installieren.

Vorgehensweise

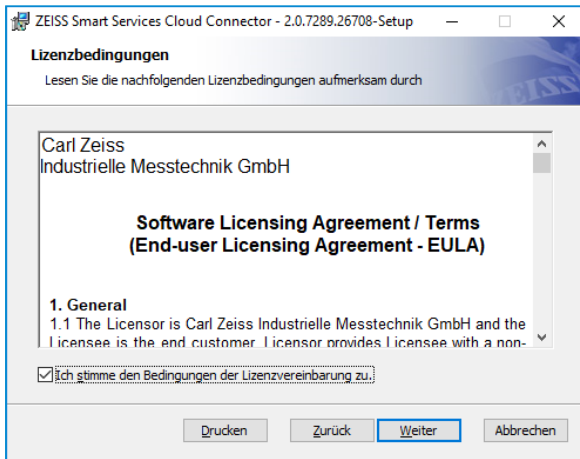
- 1 Starten Sie das Setup des **Cloud Connectors**.

HINWEIS:

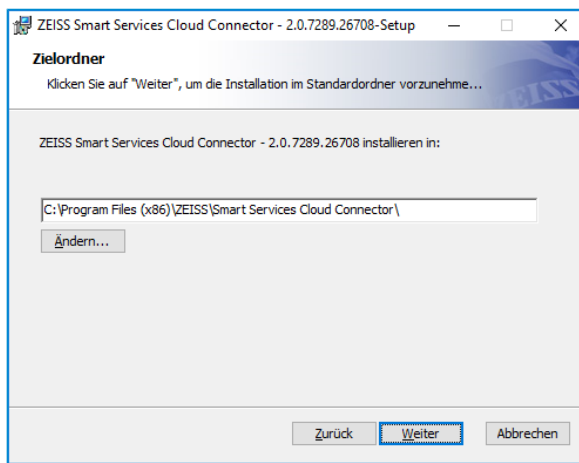
Die aktuelle Version des Cloud Connectors wird auf der Willkommenseite angezeigt.



- 2 Akzeptieren Sie die Lizenzbedingungen des **Cloud Connector**.



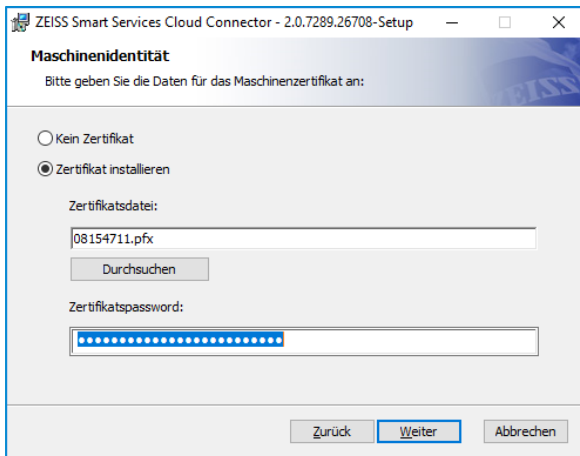
- 3 Wählen Sie den gewünschten Installationspfad für den **Cloud Connector**.



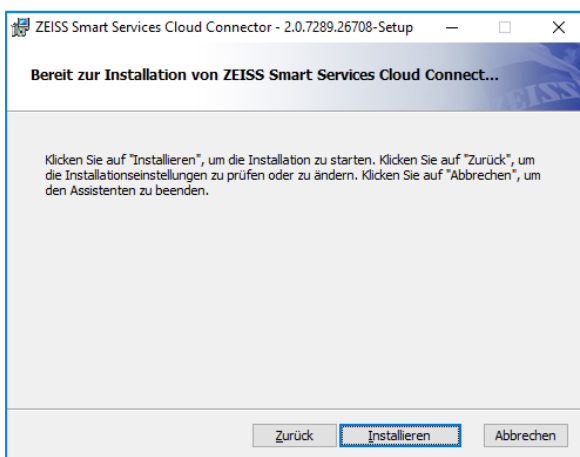
- 4 Optional: Laden Sie bei Bedarf das Maschinenzertifikat als .pfx-Datei hoch. Zusätzlich zur Zertifikatsdatei wird das Passwort für den Private Key benötigt.

HINWEIS:

Das Zertifikat wird während des Installationsvorgangs in den Zertifikatsspeicher importiert.



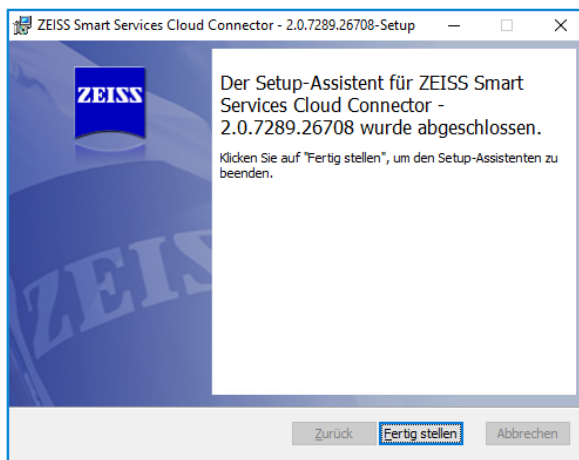
- 5 Wählen Sie **Installieren**, um den Installationsprozess zu starten.



- 6 Nach erfolgreich abgeschlossener Installation erscheint die folgende Meldung.

HINWEIS:

Wurde die Installation nicht erfolgreich ausgeführt, dann wird die Installation automatisch zurückgerollt.

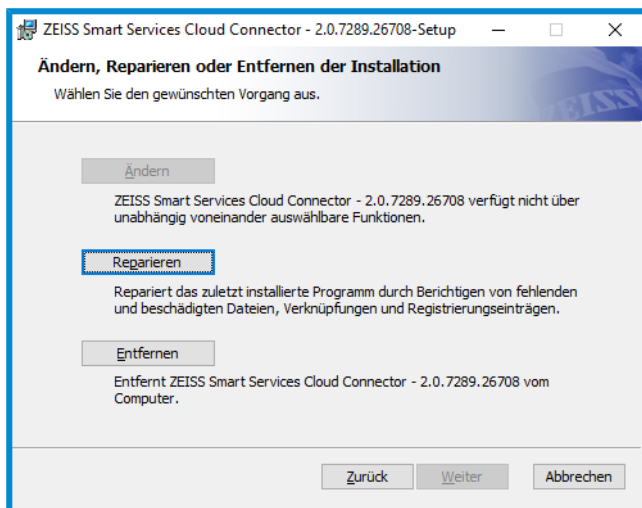


7 Beenden Sie die Installation.

⇒ Der Installationsvorgang ist abgeschlossen.

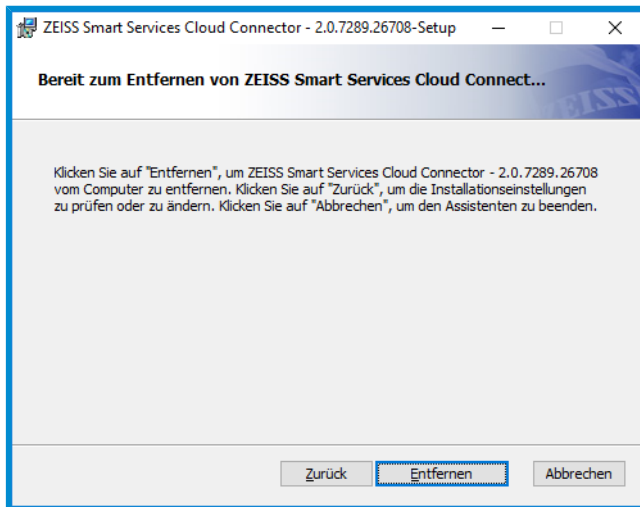
4 Reparatur und Deinstallation

Das **Smart Services Cloud Connector Installer**-Paket kann auch zur Reparatur oder Deinstallation verwendet werden. Bereits beim Start erkennt der Installer, dass der Dienst schon installiert ist und öffnet die Ansicht zur Auswahl von Reparatur der Installation oder Deinstallation.

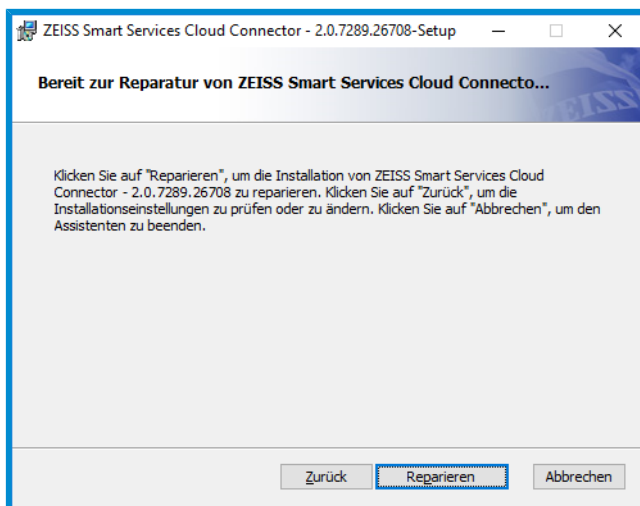


Auswahl von Reparatur/Deinstallation

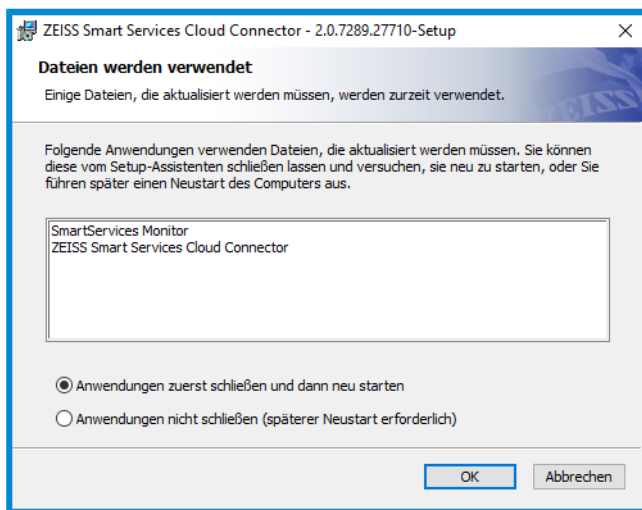
Je nach Auswahl der gewünschten Aktion (Deinstallation oder Reparatur) erscheint eine der folgenden Ansichten. Nach dem Bestätigen mit Remove/Repair werden Änderungen am System vorgenommen.



Auswahl von Deinstallation



Auswahl von Reparatur



Rückfrage zum Schließen betroffener Applikationen

5 Migration

Wenn die Maschine schon mittels **MasterConnect System** angeschlossen war, sollte der installierte Smart Services Service zuerst deinstalliert werden und der **Cloud Connector** dann neu installiert werden (siehe [☛ Cloud Connector installieren \[Seite 10\]](#)).

Zusätzlich können optional weitere Aufräumarbeiten durchgeführt werden:

Der Smart Services Service benötigte für die Kommunikation mit dem **MasterConnect System** noch einen Eintrag in der Hosts-Datei des Betriebssystems:

192.168.168.168 ckconnector.io

Diese werden vom **Cloud Connector** nicht mehr benötigt und können entfernt werden.

In einer Standardinstallation liegen die Konfigurations- und Protokolldateien für den alten Smart Services Service im Pfad:

C:\Users\Public\Documents\ZEISS\Smart Services Service

Diese werden nicht mehr benötigt und können entfernt werden. Eventuell vorhandene alte Zertifikate im Zertifikatsspeicher können entfernt werden (siehe [☛ Verwaltung von Zertifikaten \[Seite 21\]](#)).

6 Werkzeuge des Betriebssystems

Dieses Kapitel listet einige in Windows vorhandene Werkzeuge, die für die Analyse bei Problemfällen oder manueller Korrekturen benutzt werden können. Die Verwendung der meisten Werkzeuge sollte aber im Allgemeinen nicht notwendig sein, da der **Cloud Connector** Installer den **Cloud Connector** in einem sofort benutzbaren Zustand installiert.

6.1 Windows Installer

Das ausgelieferte Windows Installer Paket lässt sich einfach wie im Microsoft Windows Umfeld üblich durch einen Doppelklick im Modus mit graphischer Benutzeroberfläche starten. Die Installation lässt sich durch die Verwendung des Kommandozeilenwerkzeugs `msiexec` aber noch entsprechend den eigenen Bedürfnissen anpassen.

Um Probleme bei der Installation zu identifizieren, kann bei der Installation zusätzlich eine Protokolldatei geschrieben werden:

```
msiexec /i SmartServices.Installer.msi //v install.log
```

Die notwendigen Angaben der Datei zum Maschinenzertifikat und Zertifikatspasswort lassen sich als Kommandozeilenparameter übergeben:

```
msiexec /i SmartServices.Installer.msi /l*v install.log CERT_FILEPATH="[Dateipfad des Zertifikates]" CERT_PASSWORD="[Passwort des Zertifikates]"
```

Zudem unterstützt der Installer auch die Installation im Hintergrund (silent mode). Hier ist es umso wichtiger für entsprechende Rückmeldungen eine Protokolldatei schreiben zu lassen und die Parameter zu übergeben:

```
msiexec /qn /i SmartServices.Installer.msi /l*v install.log CERT_FILEPATH="[Dateipfad des Zertifikates]" CERT_PASSWORD="[Passwort des Zertifikates]"
```

6.2 Management von Windows Services

Durch die Integration des **Cloud Connectors** als Windows Dienst, lassen sich auch alle vorhandenen Werkzeuge zur Verwaltung nutzen.




Die Management-Konsole für Dienste bietet eine grafische Benutzeroberfläche für Windows Dienste:

6.2.1 Dienste starten/beenden

Um Dienste zu starten/beenden, gehen Sie wie folgt vor:

Vorgehensweise

- 1 Drücken Sie *Windows + R*.
→ Es öffnet sich das Fenster **Ausführen**.
- 2 Geben Sie `services.msc` ein.
→ Es öffnet sich das Fenster **Dienste** in dem der Dienst **ZEISS Smart Services Cloud Connector** angezeigt wird.

	Zahlungs- und NFC/SE-Manager	Verwaltet Zahl...	Wird au...	Manuell...	Lokaler Dienst
	ZEISS Smart Services Cloud Connector	Sends messag...	Wird au...	Automa...	Lokaler Dienst
	Zeitbroker	Koordiniert di...	Wird au...	Manuell...	Lokaler Dienst

- 3 Starten/Beenden Sie den Dienst.

Optionale Vorgehensweise

- 1 Drücken Sie *Windows + R*.
→ Es öffnet sich das Fenster **Ausführen**.
- 2 Geben Sie `cmd` ein.
- 3 Geben Sie `net start "Zeiss Smart Services Cloud Connector"` in die Kommandozeile ein.

```
C:\>net start "Zeiss Smart Services Cloud Connector"
ZEISS Smart Services Cloud Connector wird gestartet.
ZEISS Smart Services Cloud Connector wurde erfolgreich gestartet.
```

- 4 Optional: Geben Sie `net stop "Zeiss Smart Services Cloud Connector"` in die Kommandozeile ein.

```
C:\>net stop "Zeiss Smart Services Cloud Connector"
ZEISS Smart Services Cloud Connector wird beendet.
ZEISS Smart Services Cloud Connector wurde erfolgreich beendet.
```

6.2.2 Zustand des Services ermitteln

Um den aktuellen Zustand des Services zu ermitteln, gehen Sie wie folgt vor:

Vorgehensweise

- 1 Öffnen Sie Windows PowerShell.
- 2 Geben Sie `Get-Service -name 'Zeiss Smart Services Cloud Connector'` ein.
→ Es wird der aktuelle Zustand des Services angezeigt.

```
PS C:\> Get-Service -name 'Zeiss Smart Services Cloud Connector'

Status   Name                DisplayName
-----
Stopped  ZEISS Smart Ser...  Zeiss Smart Services Cloud Connector
```

6.2.3 Prozess-ID des Dienstes ermitteln

Um die Prozess ID des Dienstes ermitteln, gehen Sie wie folgt vor:

Vorgehensweise

- 1 Drücken Sie *Windows + R*.
→ Es öffnet sich das Fenster **Ausführen**.
- 2 Geben Sie `cmd` ein.
- 3 Geben Sie `sc queryex "Zeiss Smart Services Cloud Connector"` in die Kommandozeile ein.
→ Es wird die Prozess-ID des Dienstes angezeigt.

```
C:\>sc queryex "Zeiss Smart Services Cloud Connector"

SERVICE_NAME: Zeiss Smart Services Cloud Connector
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
        PID                 : 31992
        FLAGS                 :
```

6.2.4 Dienst beenden erzwingen

Lässt sich ein Dienst nicht mehr stoppen, gehen Sie wie folgt vor:

HINWEIS

Es ist nicht gewährleistet, dass sich der Dienst nach dem harten Beenden in einem konsistenten Zustand befindet!

Vorgehensweise

- 1 Drücken Sie *Windows + R*.
→ Es öffnet sich das Fenster **Ausführen**.
- 2 Geben Sie `cmd` ein.
- 3 Geben Sie `taskkill /pid 31992 /f` in die Kommandozeile ein.
→ Der Dienst wird gestoppt.

```
C:\>taskkill /pid 31992 /f
ERFOLGREICH: Der Prozess mit PID 31992 wurde beendet.
```

6.2.5 Dienst deinstallieren

Lässt sich ein Dienst nicht mehr mit dem Installer Paket deinstallieren, gehen Sie wie folgt vor:

HINWEIS

Diese Vorgehensweise nur im äußersten Notfall anwenden, falls z. B. die Deinstallation mittels Installer Paket nicht mehr funktioniert.

Vorgehensweise

- 1 Drücken Sie *Windows + R*.
→ Es öffnet sich das Fenster **Ausführen**.
- 2 Geben Sie `cmd` ein.
- 3 Geben Sie `sc delete "Zeiss Smart Services Cloud Connector"` in die Kommandozeile ein.
→ Der Dienst wird deinstalliert.

```
C:\>sc delete "Zeiss Smart Services Cloud Connector"  
[SC] DeleteService ERFOLG
```

6.3 Verwaltung von Zertifikaten

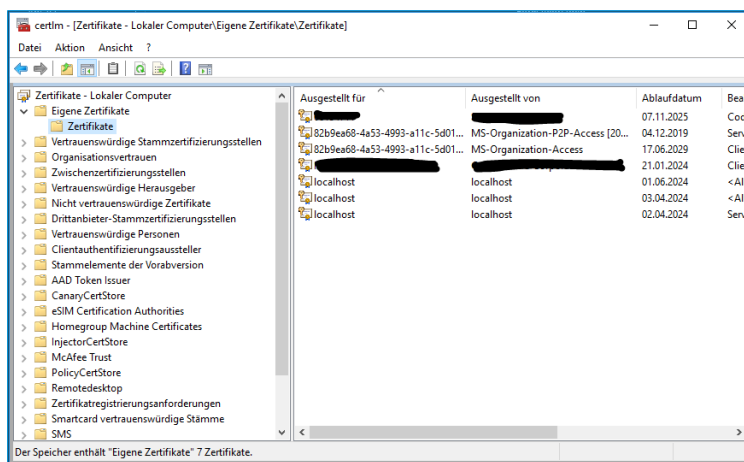
Zur Verwaltung von Zertifikaten im Windows Zertifikatsspeicher existieren unter Windows 10 sowohl Kommandozeilentools wie auch Werkzeuge mit grafischer Oberfläche. Die Verwendung dieser Werkzeuge sollte im Allgemeinen nicht notwendig sein, da der **Smart Services Cloud Connector Installer** sowohl das Maschinenzertifikat in den Zertifikatsspeicher importiert als auch die notwendigen Rechte setzt.

6.3.1 Übersicht installierter Zertifikate aufrufen

Um eine Übersicht der installierten Zertifikate aufzurufen, gehen Sie wie folgt vor:

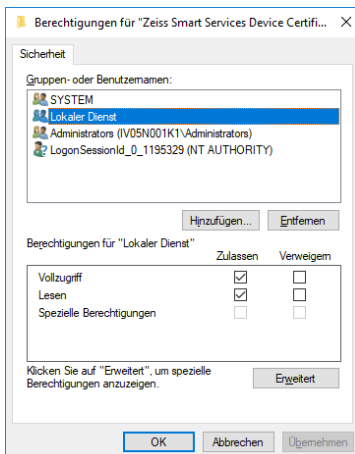
Vorgehensweise

- 1 Drücken Sie *Windows + R*.
→ Es öffnet sich das Fenster **Ausführen**.
- 2 Geben Sie `certlm.msc` ein.
→ Es wird der lokale Zertifikatsspeicher angezeigt.



6.3.2 Maschinenzertifikat für Cloud Connector

Das Maschinenzertifikat für den **Cloud Connector** wird im Zertifikatsspeicher der lokalen Maschine hinterlegt. Mit der Management-Konsole (siehe [Übersicht installierter Zertifikate aufrufen \[Seite 22\]](#)) lassen sich sowohl Zertifikate importieren (*rechte Maustaste - Alle Aufgaben - Importieren*), die Zertifikatsdetails eines Zertifikats einsehen (*rechte Maustaste - Öffnen*) oder auch Zertifikate löschen (*rechte Maustaste - Löschen*), wobei dies nur als Administrator möglich ist. Mit diesem Tool lassen sich auch die Zugriffsrechte auf den Private Key des Zertifikats prüfen und ändern (*rechte Maustaste - Alle Aufgaben - Private Schlüssel verwalten*). Wichtig ist hier, dass lokale Dienste Vollzugriff auf das **Cloud Connector**-Maschinenzertifikat haben.



Das Importieren und die Ausgabe der Zertifikatsdetails lassen sich alternativ auch über die Kommandozeile mittels `certutil` durchführen. Um eine Übersicht der entsprechenden Zertifikate zu bekommen ist noch der entsprechende Name des Zertifikatspeichers (`my`) anzugeben:

```
certutil -store my
```

Die Ausgabe listet dann die installierten Zertifikate in der folgenden Form:

```
Anbieter = Microsoft RSA SChannel Cryptographic Provider
Der private Schlüssel ist NICHT exportierbar
Verschlüsselungstest wurde durchgeführt

===== Zertifikat 1 =====
Seriennummer: 01
Aussteller: CN=SmartServices DEV
  Nicht vor: 07.11.2019 06:27
  Nicht nach: 07.11.2025 08:27
Antragsteller: CN=08154711
Kein Stammzertifikat
Zertifikathash(sha1): c1de191b5cf4a44beb70623b71d417801c74dd91
  Schlüsselcontainer = {B039423C-8058-44B5-ABC5-6CAAE0FF0880}
  Eindeutiger Containername: 09bd0f9fa592e71016d7a242d901c2cf_cf96acf0-fc2d-4f7e-96b7-453f0d1fd74a
  Anbieter = Microsoft Strong Cryptographic Provider
Das Testen der Signature wurde erfolgreich abgeschlossen

===== Zertifikat 2 =====
Seriennummer: 43a7b019ad19b38e45390d2954d5ebab
Aussteller: CN=localhost
  Nicht vor: 03.06.2019 09:26
  Nicht nach: 01.06.2024 09:26
Antragsteller: CN=localhost
Signatur stimmt mit dem öffentlichen Schlüssel überein.
Stammzertifikat: Antragsteller stimmt mit Aussteller überein
Zertifikathash(sha1): a800e12e19ab2badf72235c7c9656b9a3b2b21f8
```

Um spezifische Gerätezertifikate zu einem gegebenen Common-Name (entspricht in diesem Kontext der Seriennummer des KMGs) anzuzeigen, muss nur noch der entsprechende CN angegeben werden:

```
certutil -store my 08154711
```

```
C:\>certutil -store my 08154711
my "Eigene Zertifikate"
===== Zertifikat 1 =====
Seriennummer: 01
Aussteller: CN=SmartServices DEV
  Nicht vor: 07.11.2019 06:27
  Nicht nach: 07.11.2025 08:27
Antragsteller: CN=08154711
Kein Stammzertifikat
Zertifikathash(sha1): c1de191b5cf4a44beb70623b71d417801c74dd91
  Schlüsselcontainer = {B039423C-8058-44B5-ABC5-6CAAE0FF0880}
  Eindeutiger Containername: 09bd0f9fa592e71016d7a242d901c2cf_cf96acf0-fc2d-4f7e-96b7-453f0d1fd74a
  Anbieter = Microsoft Strong Cryptographic Provider
Das Testen der Signature wurde erfolgreich abgeschlossen
CertUtil: -store-Befehl wurde erfolgreich ausgeführt.
```

Zum Löschen eines spezifischen Zertifikates, muss der Name des Zertifikatspeichers und der Common-Name (CN) des zu löschenden Zertifikates angegeben werden:

```
certutil -delstore my a7584d23-8b12-4ef7-a980-84134a1fbd4e
```

```
C:\>certutil -delstore my a7584d23-8b12-4ef7-a980-84134a1fbd4e
my "Eigene Zertifikate"
CertUtil: -delstore-Befehl wurde erfolgreich ausgeführt.
```

7 Problembehandlung

7.1 Installationsprobleme

Falls es beim Installationsprozess zu Problemen kommt und die Installation abbricht, lassen sich detaillierte Informationen durch das Starten des Installationspakets mit eingeschalteter Protokollierung sammeln:

Vorgehensweise

- 1 Drücken Sie *Windows* + *R*.
→ Es öffnet sich das Fenster **Ausführen**.
- 2 Geben Sie `cmd` ein.
- 3 Navigieren Sie zum Verzeichnis in welchem das Installationspaket abgelegt ist.
- 4 Starten Sie die Installation mit Protokollierung: `msiexec /i SmartServices.Installer.msi /l*v install.log`

⇒ Alle Installationsaktivitäten werden dann in die Datei `install.log` im entsprechenden Verzeichnis protokolliert. Diese Datei ist bei Bedarf dem ZEISS Service zu Analyse Zwecken zu übergeben.

HINWEIS:

Sollte es zu einem Abbruch bzw. Rollback der Installation kommen ohne, dass im Installationsprotokoll eine Ursache erkenntlich ist, kann dies an einem zu langen Pfad der Zertifikatsdatei liegen. Daher sollte das Zertifikat möglichst nicht zu tief im Verzeichnisbaum abgelegt sein.

7.2 Fehler nicht in Protokolldatei

Zur Analyse von Fehlern, die nicht in den Protokolldateien auftauchen, lassen sich Hinweise auf die Ursache oft auch aus der Ereignisanzeige bekommen.

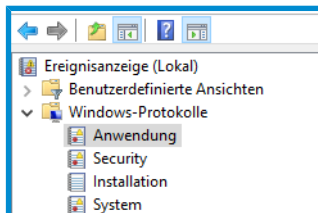
Vorgehensweise

- 1 Drücken Sie **Windows + R**.

→ Es öffnet sich das Fenster **Ausführen**.

- 2 Geben Sie **eventvwr** ein.

⇒ Es werden die entsprechenden Warnungen und Fehler unter **Windows-Protokolle** in der Kategorie **Anwendung** aufgelistet.



Über die Details der Ereignisse können die Fehlerursachen analysiert werden.

Anwendung Anzahl von Ereignissen: 46.019 (!) Neue Ereignisse sind verfügbar				
Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	04.12.2019 16:00:04	RestartManager	10000	Keine
Informationen	04.12.2019 15:49:39	RestartManager	10001	Keine
Informationen	04.12.2019 15:49:39	MsInstaller	1035	Keine
Informationen	04.12.2019 15:49:39	MsInstaller	11728	Keine
Informationen	04.12.2019 15:49:37	RestartManager	10001	Keine
Fehler	04.12.2019 15:49:37	RestartManager	10007	Keine
Informationen	04.12.2019 15:49:37	MsInstaller	1042	Keine
Informationen	04.12.2019 15:49:31	RestartManager	10002	Keine
Informationen	04.12.2019 15:49:31	RestartManager	10002	Keine
Informationen	04.12.2019 15:49:30	ZeissSmartServicesCloudConnector	0	Keine
Informationen	04.12.2019 15:49:23	RestartManager	10000	Keine

Ereignis 10007, RestartManager	
Allgemein	Details
Die Anwendung oder der Dienst "ZEISS Smart Services Cloud Connector" konnte nicht neu gestartet werden.	

7.3 Netzwerkkonfiguration

Sollte trotz evtl. notwendiger Firewallfreischaltungen keine erfolgreiche Verbindung des Smart Services Cloud Connectors mit der Cloud aufgebaut werden können, kann dies möglicherweise daran liegen, dass eine Namensauflösung (DNS) auf dem entsprechenden PC nicht möglich ist. Dies lässt sich über den Befehl `nslookup` prüfen.

Vorgehensweise

1 Drücken Sie *Windows + R*.

→ Es öffnet sich das Fenster **Ausführen**.

2 Geben Sie `nslookup global.azure-devices-provisioning.net` ein.

⇒ Die Adresse sollte erfolgreich aufgelöst werden können und es wird eine Ausgabe ähnlich der folgenden angezeigt:

Nicht autorisierende Antwort:

Name: idsu-prod-am-001-su.westeurope.cloudapp.azure.com

Address: 23.100.8.130

Aliases: global.azure-devices-provisioning.net; id-prod-global-endpoint.trafficmanager.net

Derselbe Test ist für die beiden Adressen `zeiss-imt-cmmiot-iothub-prod.azure-devices.net` und `zeiss-imt-cmmiot-dps-prod.azure-devices-provisioning.net` durchzuführen.

7.4 Cloud Connector lässt sich nicht deinstallieren

Ein abgebrochener Installationsvorgang oder das nicht mehr im Betriebssystem vorhandene ursprüngliche msi-Paket kann dazu führen, dass der **Cloud Connector** sich nicht mehr deinstallieren lässt. In diesem Fall kann mit dem von Microsoft zur Verfügung gestellten Tool zur Problembehandlung versucht werden den **Cloud Connector** trotzdem zu deinstallieren. Anschließend kann durch die Neuinstallation wieder ein konsistenter Zustand hergestellt werden. Das Tool ist unter folgendem Link verfügbar:




↳ <https://support.microsoft.com/de-de/help/17588/windows-fix-problems-that-block-programs-being-installed-or-removed>

7.5 Maschinenzertifikate manuell entfernen

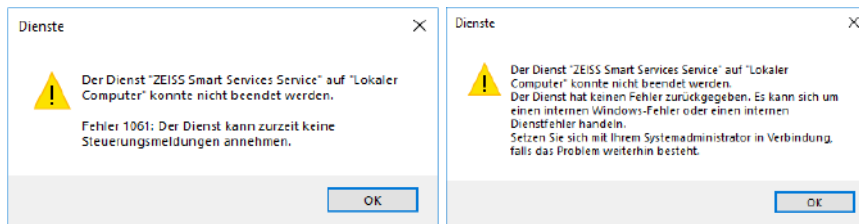
Die **Cloud Connector**-Zertifikate werden im Microsoft Windows Zertifikatsspeicher gespeichert und können dort auch wieder entfernt werden (siehe ↳ *Verwaltung von Zertifikaten [Seite 21]*).

7.6 Dienst lässt sich nicht beenden

Im Normalzustand kann der **Cloud Connector**-Dienst über den Smart Services Monitor oder in der Dienste-Verwaltung (`services.msc`) über das Kontextmenü beendet werden (siehe ↳ *Dienste starten/beenden [Seite 19]*):

 Zahlungs- und NFC/SE-Manager	Verwaltet Zahl...	Wird au...	Manuell...	Lokaler Dienst
 ZEISS Smart Services Cloud Connector	Sends messag...	Wird au...	Automa...	Lokaler Dienst
 Zeitbroker	Koordiniert di...	Wird au...	Manuell...	Lokaler Dienst

Sollte sich bei der Auswahl von Beenden im Kontextmenü der Dienst nicht beenden lassen und tritt z. B. eine der folgenden Fehlermeldungen auf, dann muss das Beenden des Dienstes erzwungen werden (siehe ↳ *Dienst beenden erzwingen [Seite 20]*)



```
sc queryex "Zeiss Smart Services Service"
```

```
SERVICE_NAME: Zeiss Smart Services Service
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
PID : 3932
FLAGS :
```

```
taskkill /PID 3932 /F
```

Carl Zeiss
Industrielle Messtechnik GmbH
73447 Oberkochen
Germany

Vertrieb: +49 7364 20-6336
Service: +49 7364 20-6337
Fax: +49 7364 20-3870

info.metrology.de@zeiss.com
www.zeiss.de/imt