

A man in a light blue shirt is seen from the side, holding a tablet. The background is a factory floor with various pieces of machinery and a clock. Overlaid on the scene are several futuristic digital elements: a 'NEWS' section with a person icon, a '24/7' icon with a circular arrow, a 'Home' button, and a 'Industry Online Support' text. There are also icons for a folder, a network of people, and a magnifying glass. The overall aesthetic is high-tech and industrial.

SIEMENS

**SIMATIC PCS
myExpert
Data Collector +
SMMC Installation**

SIMATIC PCS myExpert



<https://support.industry.siemens.com/cs/ww/de/view/>

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.



GEFAHR

bedeutet, dass Tod oder schwere Körperverletzung eintreten wird, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.



WARNUNG

bedeutet, dass Tod oder schwere Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.



VORSICHT

bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG

bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung qualifiziertem Personal gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:



VORSICHT

Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z.B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter <https://www.siemens.com/industrialsecurity>.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter <https://www.siemens.com/industrialsecurity>.

In Übereinstimmung mit internationalen Standards und Best Practices des Risikomanagements stuft Siemens die Bedrohungsstufe gegenüber unserem SIMATIC

Produkt PCS myExpert und seinen Health Agents mit einer Skala von 4 (grün, gelb, orange, rot) auf die Stufe "gelb" ein (die deutsche BSI-Nomenklatur lautet "Limited"): Alle in PCS myExpert vorhandenen Maßnahmen sind darauf ausgelegt, mindestens vor dieser Bedrohungsstufe zu schützen.

Nähere Informationen entnehmen Sie bitte:

[BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz](#),
(Datum 07.05.2018)

Download [PDF](#), (Seite 21-22)

Inhaltsverzeichnis

	Rechtliche Hinweise	3
1	Vorwort	7
2	Allgemeine Informationen.....	8
	2.1 Disclaimer	8
	2.2 Zielgruppe	8
3	Voraussetzung	9
	3.1 Maintenance Station (MS Server) prüfen.....	10
	3.2 Benutzerrechte anpassen	12
	3.3 SIMATIC Management Console installieren	13
	3.4 Lizenzen verteilen	14
	3.5 SIMATIC Management Console starten und konfigurieren	14
	3.6 SIMATIC Management Agent Installation:	16
	3.7 Inventardaten in der Anlagensicht ermitteln und exportieren.....	17
	3.8 Inventardaten in der Netzwerksicht ermitteln und exportieren	20
	3.9 myExpert: Inventardaten einlesen.....	22
	3.10 Zusätzliche Funktionen in SMMC	23
	3.11 Datenbestand in myExpert auf Vollständigkeit prüfen	23
	3.12 Daten in myExpert kommentieren und bewerten (2h)	23
4	PCS myExpert Data Collector	25
	4.1 Installation und Konfiguration von Logstash	25
	4.1.1 Voraussetzungen für den Betrieb von Logstash	25
	4.1.2 Installation von Logstash.....	25
	4.1.3 Logstash Konfiguration.....	26
	4.1.4 Logstash als geplanten Task konfigurieren.....	26
	4.2 Installation Metricbeats via msi Installer – Health Agents.....	30
	4.3 Installation Winlogbeats via msi Installer (optional) – Health Agents	30
	4.4 Installation der Health Agents mit Hilfe der SMMC	31

1 Vorwort

Ziel des Handbuchs

In diesem Dokument erfahren Sie, wie Sie den SIMATIC PCS myExpert Data Collector und dessen Data Agenten auf einem Windows basierten Betriebssystem installieren. Weiterhin beschreibt das Dokument die Installation und Konfiguration der Simatic Management Konsole, welche für den Betrieb von SIMATIC PCS myExpert erforderlich ist. Auch die Überprüfung und Konfiguration von Netzwerkgeräten zur Inventarisierung wird in diesem Manual thematisiert.

Kerninhalte

Folgende Kernpunkte werden in diesem Dokument behandelt:

- Installation und Konfiguration der SIMATIC Management Console
- Installation der Data Collector Bestandteile
- Konfiguration der Data Collector Bestandteile

Erforderliche Grundkenntnisse

Über grundlegende Kenntnisse mit Windows basierten Betriebssystemen hinaus sind keine besonderen Kenntnisse erforderlich

2 Allgemeine Informationen

2.1 Disclaimer

Der Inhalt dieses Handbuchs wurde auf Übereinstimmung mit der beschriebenen Hard- und Software überprüft. Da Abweichungen nicht vollständig ausgeschlossen werden können, kann eine vollständige Übereinstimmung nicht garantiert werden. Die Daten in diesem Handbuch werden jedoch regelmäßig überprüft und notwendige Korrekturen werden in späteren Ausgaben berücksichtigt. Verbesserungsvorschläge sind willkommen. Dieses Manual ersetzt nicht die bekannten Manuals zur SIMATIC Management Console, sondern dient lediglich als Ergänzung. Siehe Kapitel 3 – Voraussetzungen.

2.2 Zielgruppe

Dieses Handbuch richtet sich an SIMATIC PCS myExpert Anwender, die die SIMATIC Management Console für den Betrieb in myExpert zu installieren und vorzubereiten. Weiterhin wird die Installation der myExpert Data Collector Komponenten beschrieben.

3 Voraussetzung

Folgende Informationen werden als bekannt vorausgesetzt:

SID ist erzeugt und in die Objekteigenschaften des PCS 7 Multiprojekt eingetragen.

(<https://support.industry.siemens.com/cs/de/de/view/109807363>)

Handbuch SIMATIC Management Console V9.1

<https://support.industry.siemens.com/cs/de/de/view/109805386>

Liesmich SIMATIC Management Console V9.1 SP1

<https://support.industry.siemens.com/cs/de/de/view/109801046>

Gegebener Netzwerkaufbau: abgesichert gemäß PCS 7 Kompendium - Security

3.1 Maintenance Station (MS Server) prüfen

Eine PCS 7 Maintenance Station der in der Anlage vorhandenen PCS 7 Version (Ausprägung Basis oder Standard) wird zum Auslesen der Inventardaten (Online) der projektierten Switche benötigt → Details und Anleitungen siehe z.B.

[Handbuch PCS7 Maintenance Station V9.1 SP1](#) oder

<https://support.industry.siemens.com/cs/de/de/view/27833758>

Switch Projektierung innerhalb des SIMATIC Net OPC Server des MS Servers:
SNMP-Geräteprofil passend zur Hardware eingestellt?

Erreichbare SCALANCE SC600 sind über MIBII Profil zu projektieren.

Wenn nicht erreichbar bzw. nicht projektiert können diese auch nachträglich in myExpert in der Inventar Sicht über ein Template File importiert werden

Hinweis: Unterschiedliche SNMP Profile für SCALANCE X200 und XC200! Die Projektierung soll an den aktuell vorhandenen Switch angepasst sein.

Projektieren der Maintenance Stationen

5.11 Projektieren der Überwachung von Industrie-PCs und Netz-Objekten

Übersicht

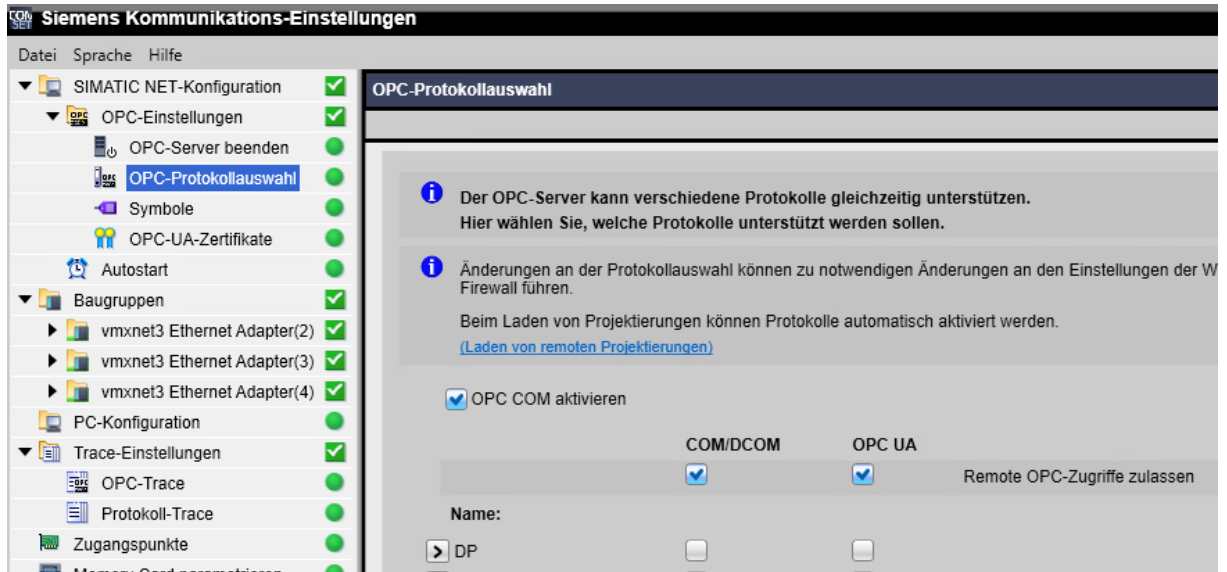
Die folgende Tabelle zeigt die Zuordnung der Community zum Geräteprofil.

Objekte	Geräteprofil	Community
SCALANCE Reihe X200	Profile_SCALANCE_X200_Vxy.txt	public
SCALANCE Reihe X200 RNA	Profile_SCALANCE_X200RNA_Vxy.txt	
SCALANCE Reihe XB200	Profil_SCALANCE_XB200_Vxy.txt	
SCALANCE Reihe XC200	Profil_SCALANCE_XB200_Vxy.txt	
SCALANCE Reihe XF200	Profil_SCALANCE_XB200_Vxy.txt	
SCALANCE Reihe XP200	Profil_SCALANCE_XB200_Vxy.txt	
SCALANCE Reihe X300	Profil_SCALANCE_X300X400_Vxy.txt	
SCALANCE Reihe X400		
SCALANCE Reihe XM400	Profil_SCALANCE_XM400_Vxy.txt	
SCALANCE Reihe X500	Profil_SCALANCE_X500_Vxy.txt	
SCALANCE Reihe W700	Profil_SCALANCE_W700_Vxy.txt (xy =13)	
SCALANCE Reihe W700 ab Firmware 6.1	Profil_SCALANCE_W700_Vxy.txt (xy >= 61)	
SCALANCE Reihe W1700	Profil_SCALANCE_W700_Vxy.txt	
ESM/OSM	Profil_OSM_Vxy.txt	
Siemens IPC (Industrie-PC)	Profil_IPC_Vxy.txt	SOL
Sonstige Geräte z. B. PCs von Drittanbietern, Premium Server for SIMATIC PCS 7, Netzwerkkarten, Switches	MIB-II_V10.txt	Ermitteln Sie die im Gerät projektierte Community.
Alle Geräte, die durch das Importieren aufgenommen wurden, aber nicht angezeigt werden sollen	Kein SNMP	-

Hinweis

Wenn nicht explizit genannt, steht "xy" jeweils für die neueste Version des Geräteprofils.

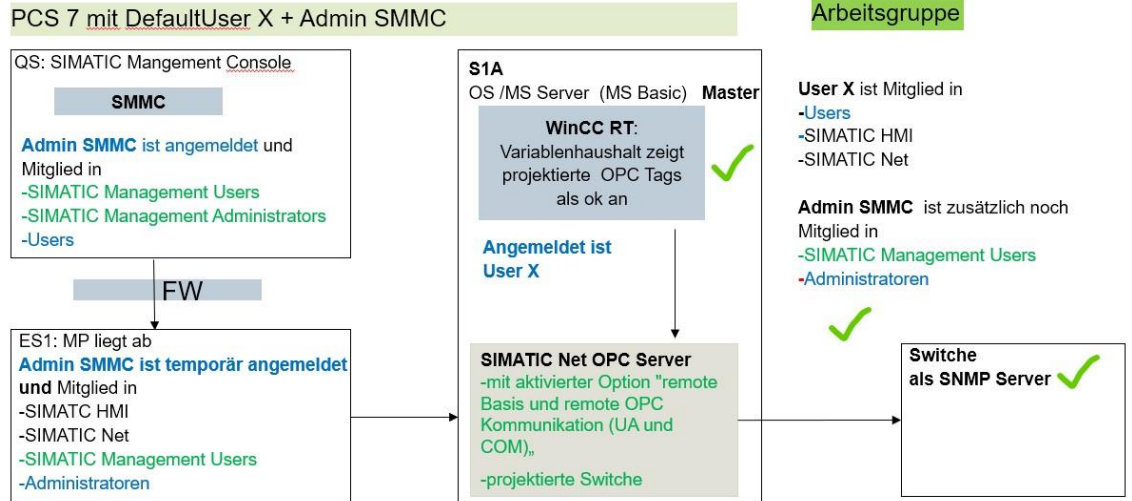
Hinweis für den SIMATIC Net OPC Server: Remote OPC Zugriffe zulassen innerhalb des Programms „Siemens Kommunikationseinstellungen“:



Das Bild zeigt die Kommunikations-Einstellungen ab PCS7 V9.1. In älteren Versionen kann sich der Name für den Remote OPC-Zugriff unterscheiden.

3.2 Benutzerrechte anpassen

Der ausführende Benutzer an der SMMC-Station - typischerweise die Quarantäne Station im Perimeternetz - braucht gemäß SMMC Handbuch Kap 4.1 folgende Rechte im System:



Benutzer SMMC an den jeweiligen Stationen anlegen und in den genannten Gruppen berechtigen.

Die Hinweise im SMMC Handbuch Kap 4.1 bzgl. „Windows Benutzerverwaltung ändern“ sind zu beachten

Station	Username	Users	Administratoren	Mgmt User	Mgmt Admin	SIMATIC NET	SIMATIC HMI
ES	DefaultUser	x		x		x	x
ES	SMMC	X	X	X		X	X
OS Client	DefaultUser	x		x			x
OS/MS Server	DefaultUser	x		x		x	x
OS/MS Server	SMMC		X	X		X	
Quarantaene(SMMC)	SMMC		X	X	X		

3.3 SIMATIC Management Console installieren

Je nach zu installierender SIMATIC Management Console / SIMATIC Management Agent Version ist die dazu gehörende aktuelle Liesmich Beschreibung zu beachten.

SIMATIC Management Console Liesmich V9.1 SP1 Update 2 (online)

<https://support.industry.siemens.com/cs/de/de/view/109815703>

SIMATIC Management Console Liesmich V9.0 SP1 Update 4 (online)

<https://support.industry.siemens.com/cs/de/de/view/109780528>

SIMATIC Management Console Liesmich V9.0 Update 2 (online)

<https://support.industry.siemens.com/cs/de/de/view/109759825>

3.4 Lizenzen verteilen

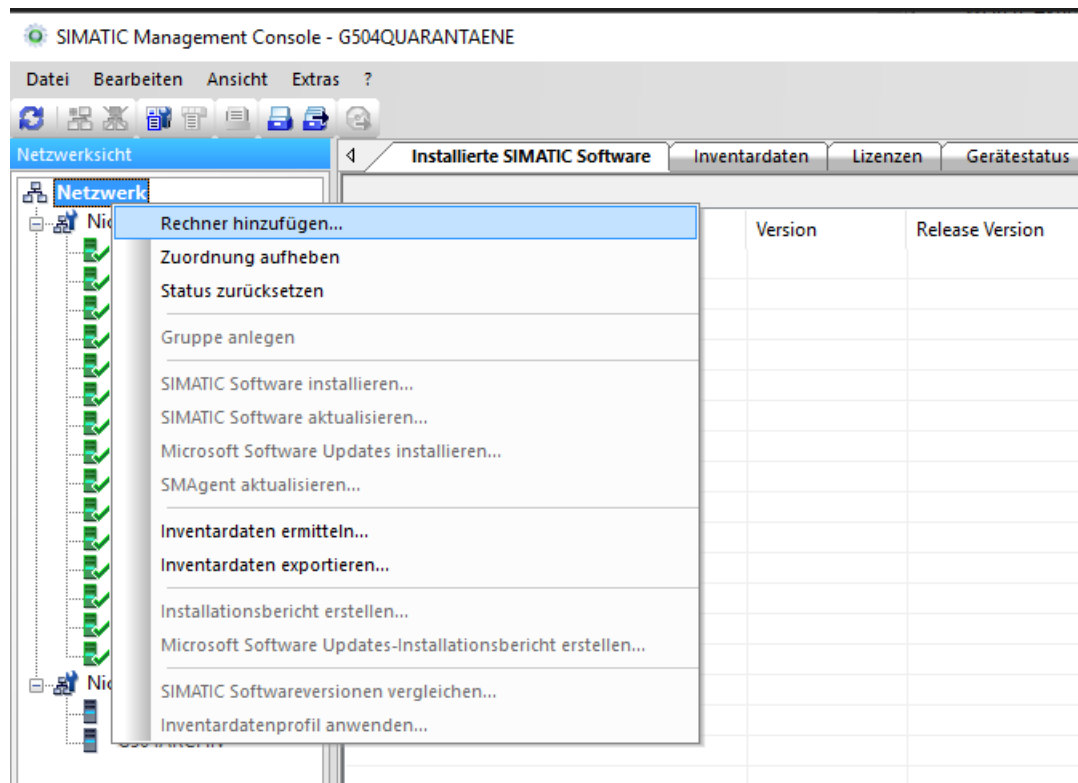
Hinweis

"Ein reduzierter Leistungsumfang der Management Console, welche die Inventarisierung ermöglicht, kann ohne Lizenzen genutzt werden. Die Nutzung des vollen Leistungsumfangs der Management Console erfordert neben einer Lizenz "SIMATIC PCS 7 Management Console" jeweils eine weitere Lizenz "Management Console Agent" für jede per Management Console verwaltete SIMATIC PCS 7 Industrial Workstation. Die Management Console Agents sind in Form kumulierbarer 10er-, 50er- und 100er-Lizenzen beziehbar. Die Funktion Systeminventarisierung kann eingeschränkt auch ohne Lizenzen genutzt werden." Quelle PCS 7 Katalog)

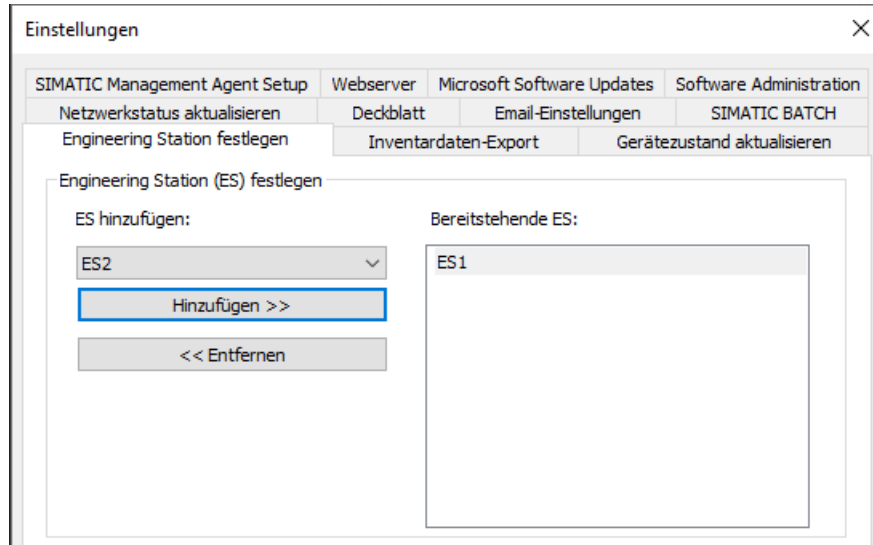
3.5 SIMATIC Management Console starten und konfigurieren

Nachdem die Management Console gestartet wurde, versuchen sich die Rechner bei der Management Console zu melden, auf denen der "SIMATIC Management Agent" aktiviert ist.

Rechner zuordnen

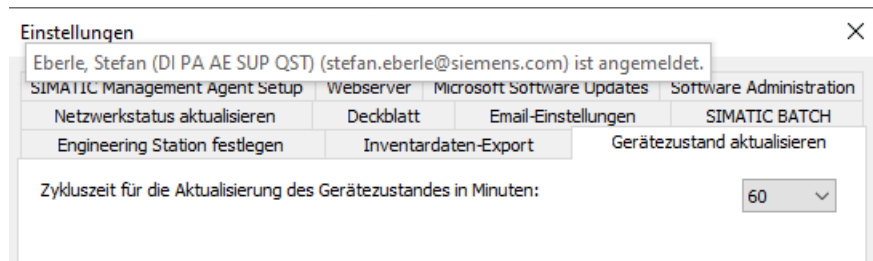


Menü "Extras > Einstellungen":
Register "Engineering Station festlegen").



Register „SIMATIC Management Agent Setup“
 → Verweis auf lokalen Ordner mit SM Agent Setup

Register "Gerätezustand aktualisieren"

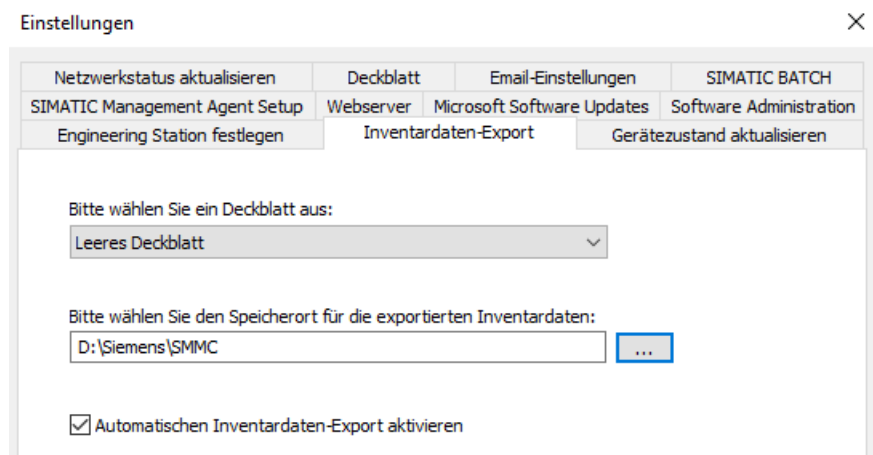


→ Vom Standardwert 1 Minute auf 60 Minuten einstellen

Register "Netzwerkstatus aktualisieren"

Standardwert 5 Minuten

Register "Inventardatenexport"



→ Speicherort auf eigens erstellten Ordner auf D-Partition festlegen
 → Option „Automatischen Inventardatenexport aktivieren“

Kommunikation: PreSharedKey: Passwort vergeben und dokumentieren

3.6 SIMATIC Management Agent Installation:

Dieser Schritt muss für jede PC-Station ausgeführt werden, die inventarisiert werden soll.

Wenn schon eine Version am Zielrechner installiert ist, kann an der SMMC die Funktion „SM Agent aktualisieren...“ genutzt werden

Falls die Software McAfee ApplicationControl aktiviert ist, sind entsprechende temporäre Schritte notwendig.

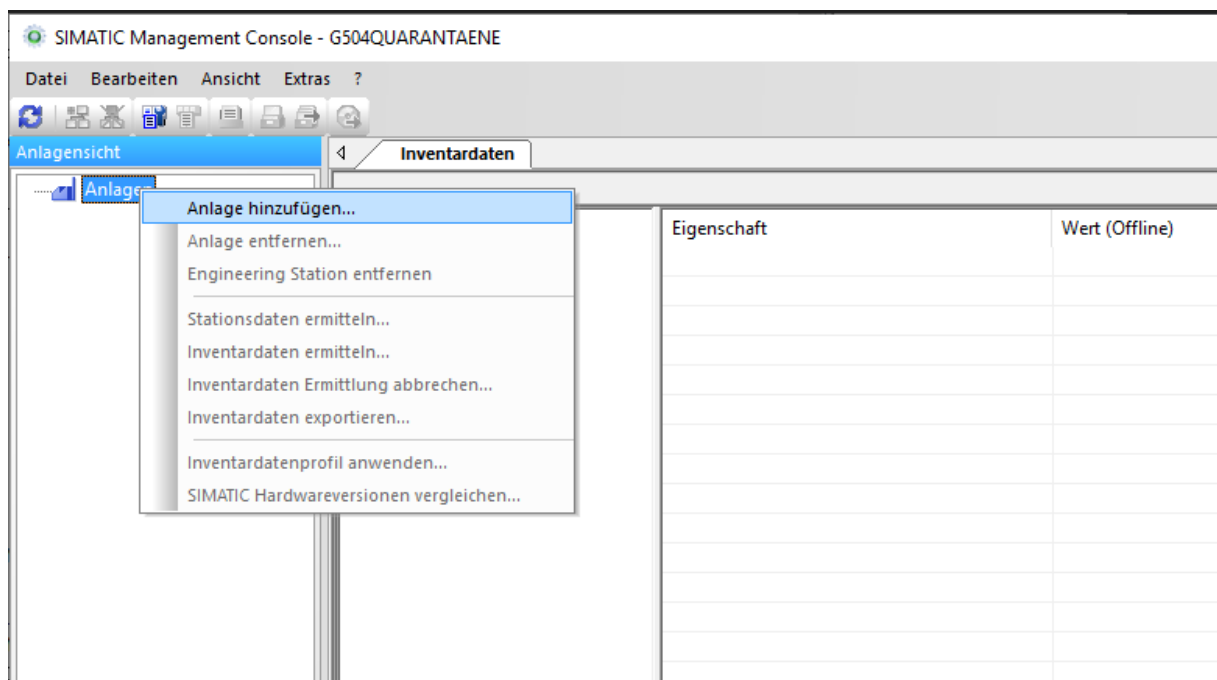
Art der Installation: lokal (Handbuch SMMC Kap 4.3) oder über Remotedesktopverbindung (nur bei deaktivierter OS Runtime. Handbuch SMMC Kap 4.4)

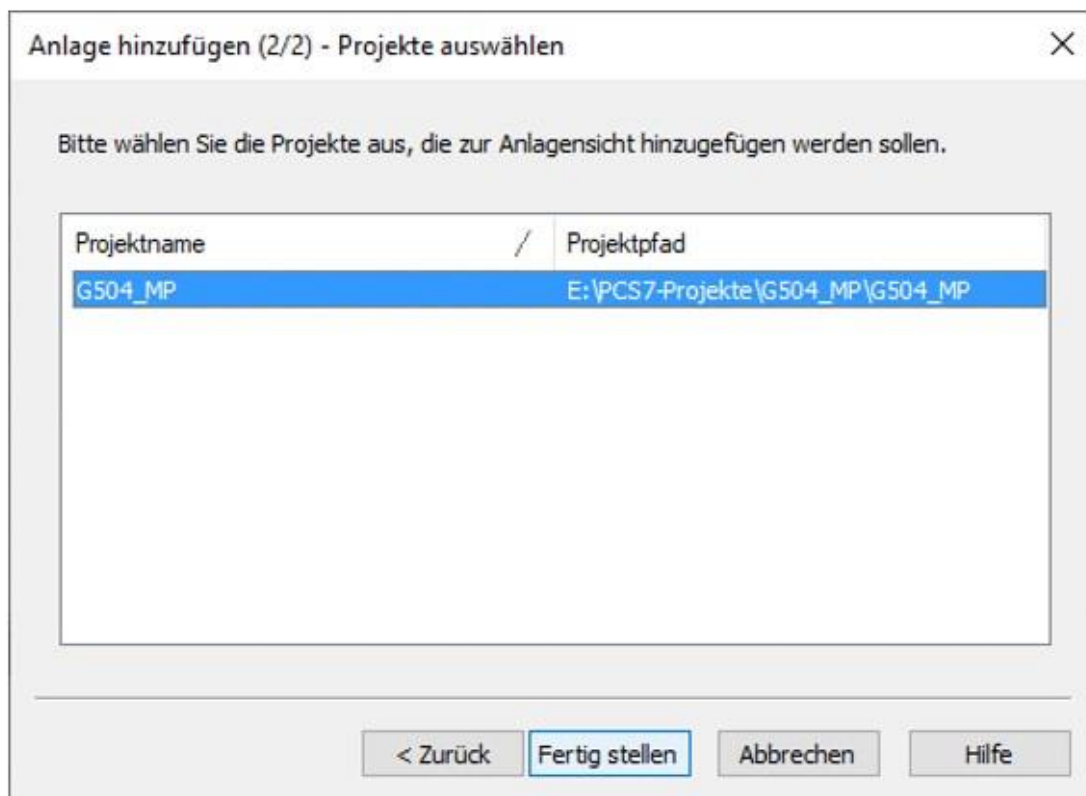
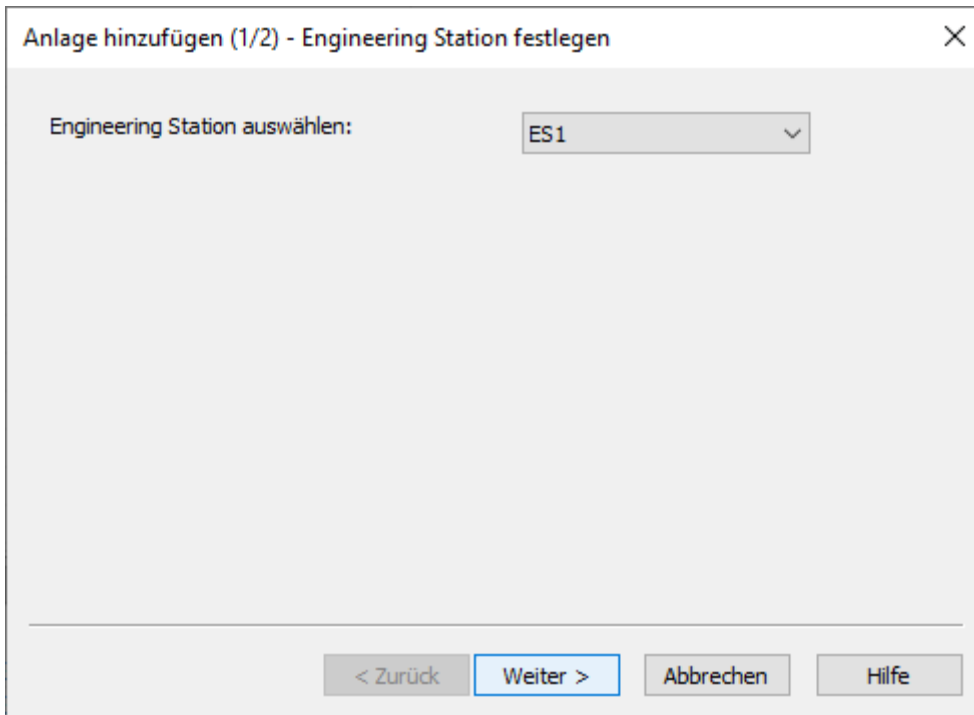
Wenn Kommunikation über unterschiedliche Subnetze: Handbuch SMMC Kap 4.5
→lokale Windows FW + Externe FW einstellen (**Portfreigabe beachten**)

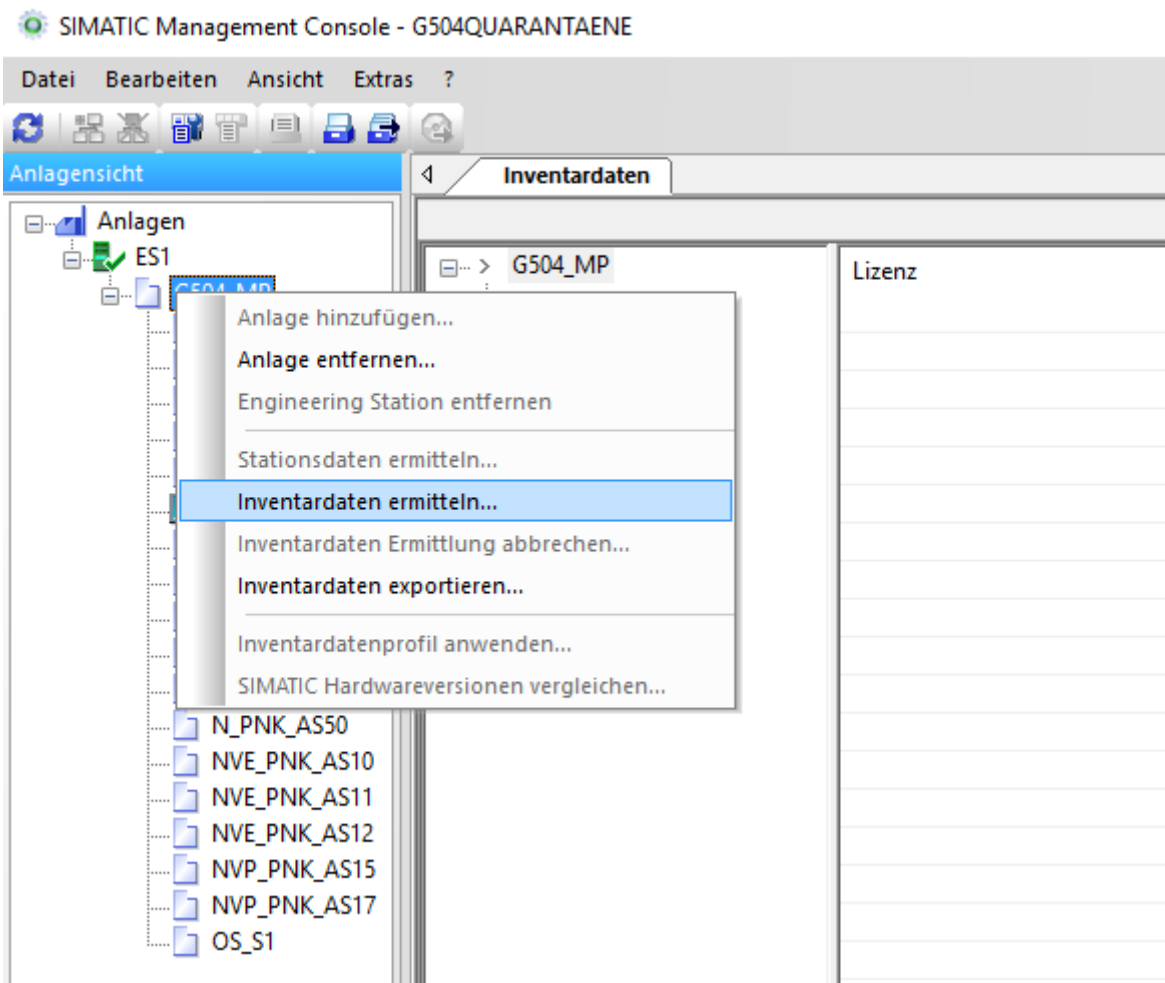
Hinweis: kurzzeitig Stopp der OS Runtime notwendig

3.7 Inventardaten in der Anlagensicht ermitteln und exportieren

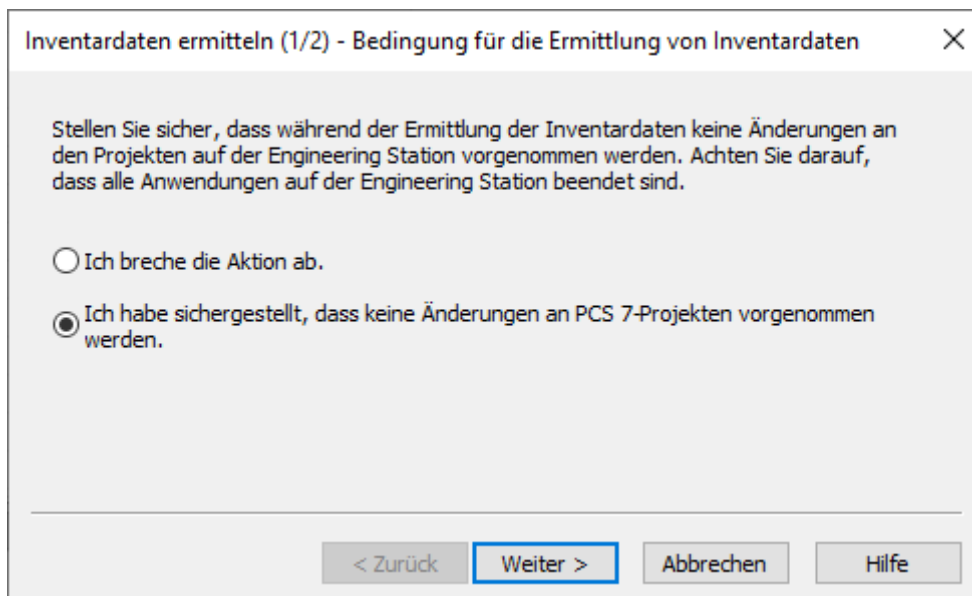
- Inventardaten in der Anlagensicht einmalig über das komplette MP ermitteln
- Nach Änderungen in der Anlage: Inventardaten in der Anlagensicht bei Bedarf über ein Teilprojekt zum Aktualisieren ermitteln
- Inventardaten in der Anlagensicht über das komplette MP exportieren (**Notwendige Daten für myExpert**)
 - Gemäß Handbuch Kap 5.6.3 ff

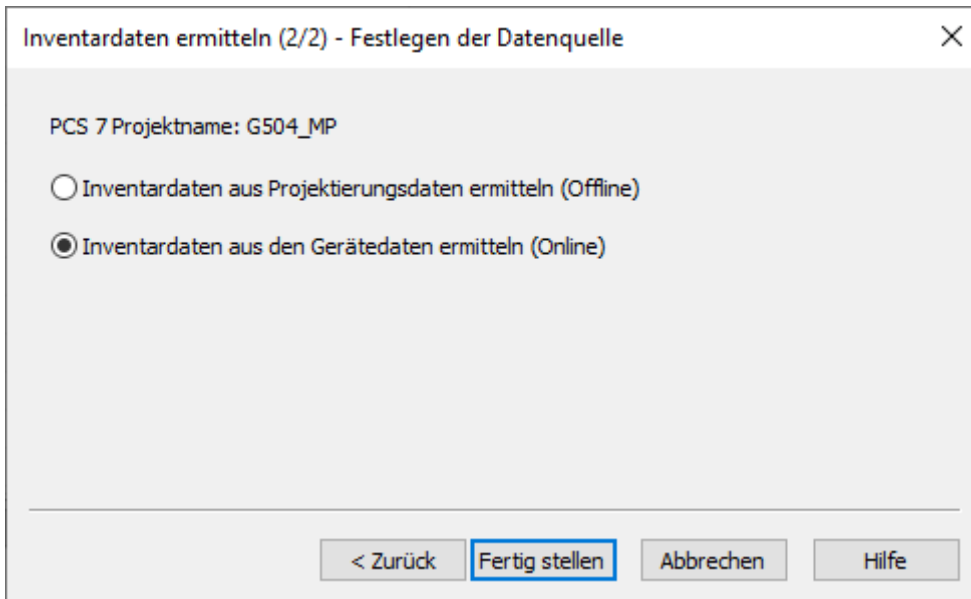






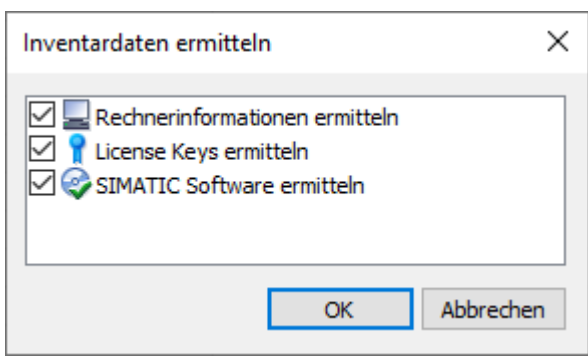
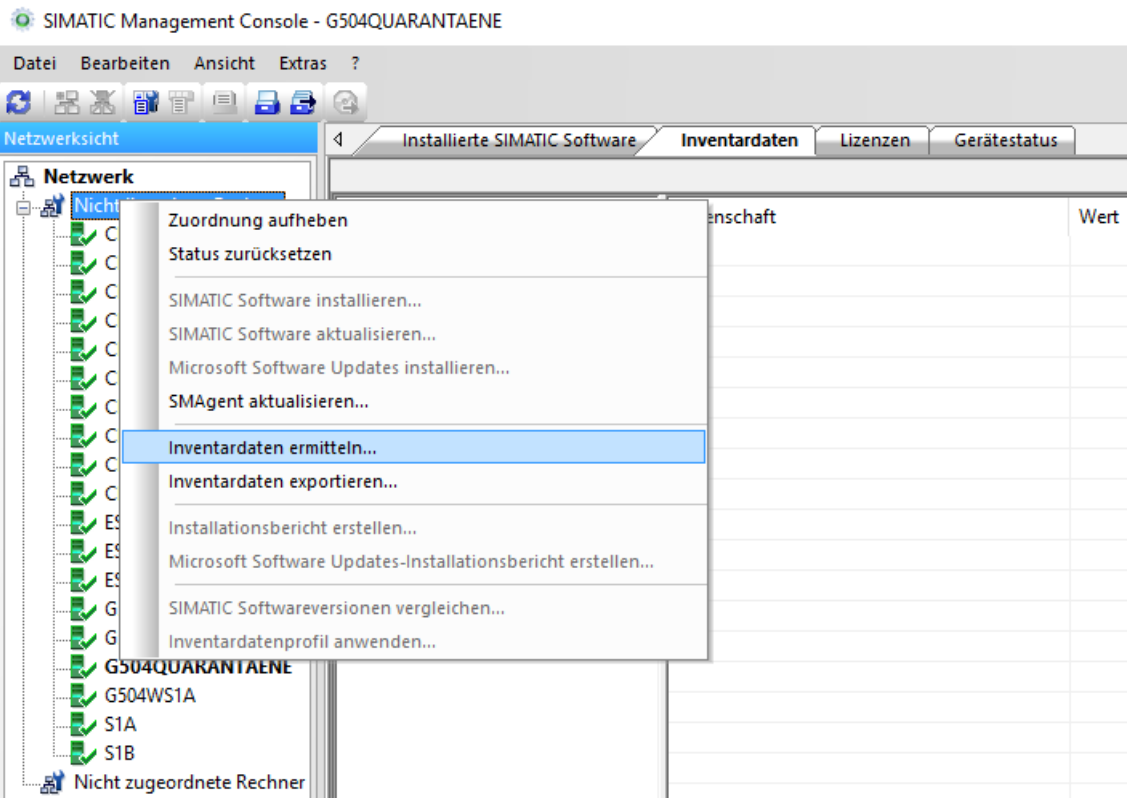
© Siemens AG 2022 All rights reserved



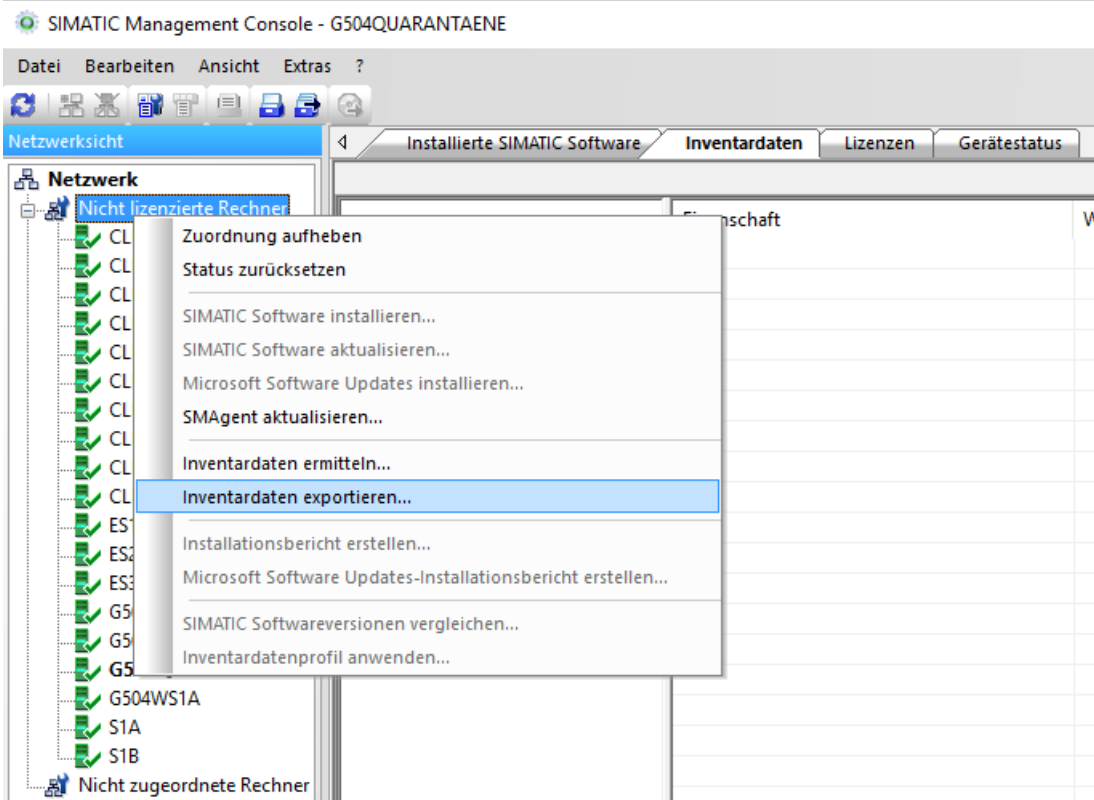


3.8 Inventardaten in der Netzwerksicht ermitteln und exportieren

- Gruppe anlegen und Rechner zuordnen
- Rechner manuell hinzufügen, wenn SMMC auf Quarantäne
„Die automatische Erkennung von Rechnern ist auf das jeweilige Subnetz begrenzt, um die Netzwerklast zu begrenzen. Deshalb müssen die Rechner, die nicht Teil des Subnetzes sind, der SIMATIC Management Console manuell zugeordnet werden, indem Sie mit der rechten Maustaste auf "Netzwerk" klicken und die Option "Rechner hinzufügen" wählen.“
- Inventardaten in der Netzwerksicht ermitteln und exportieren
(Notwendige Daten für myExpert)
 - Gemäß Handbuch Kap 5.6.2 ff
 - Wichtig: myExpert braucht einen Gesamtexport (siehe Hinweis nächste Seite)

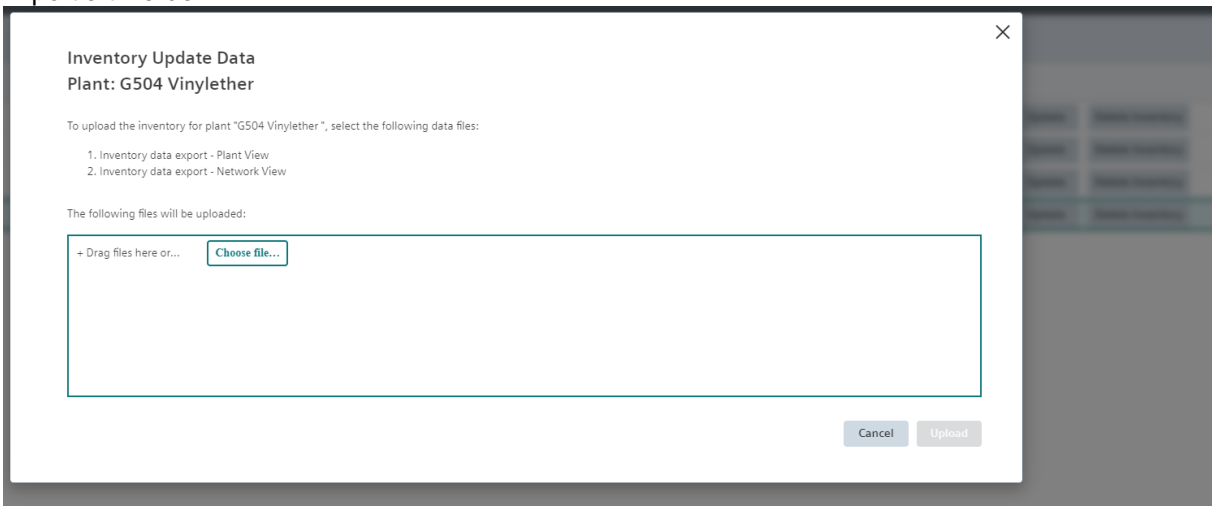


© Siemens AG 2022 All rights reserved



3.9 myExpert: Inventardaten einlesen

Die beiden Exportdateien können bei entsprechender Berechtigung für die Anlage in myExpert importiert werden:



Hinweis:

myExpert kann mehrere Plant View Dateien zusammenführen, **aber** eine Anlage kann immer nur eine Network View als gesamtes verwalten.

- SMMC Anlagensicht/Plant View Export:
Diese Datei enthält eine Auflistung der projizierten HW Komponenten aufführt (Steuerung, CP's, IM's, Netzwerkkomponenten inkl. Seriennummer und FW Version)

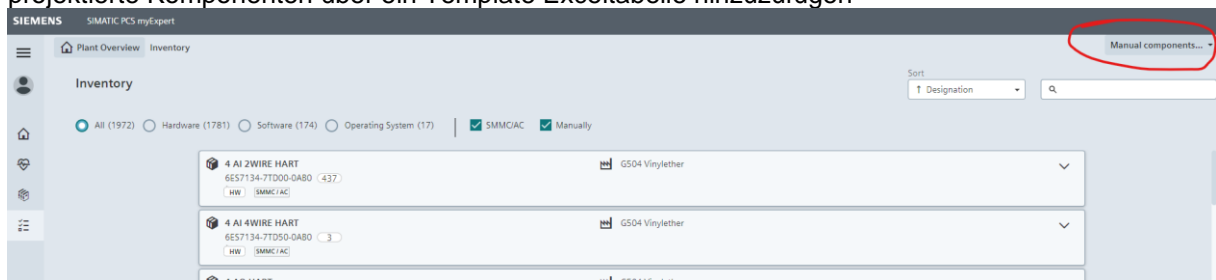
- SMMC Netzwerksicht /Network View:
Diese Datei enthält die Inventardaten der Rechner mit installiertem SM Agent.

3.10 Zusätzliche Funktionen in SMMC

- Menü Datei > Daten sichern
- Optional: Inventardatenprofil Assistent ausführen (für spätere Vergleich über SMMC) – Kap 5.6.5
- Optional: Vergleich der SIMATIC SW Versionen über Versionsreferenzdatei – Kap 5.6.6
- Optional: SW installieren und aktualisieren – Kap 5.5

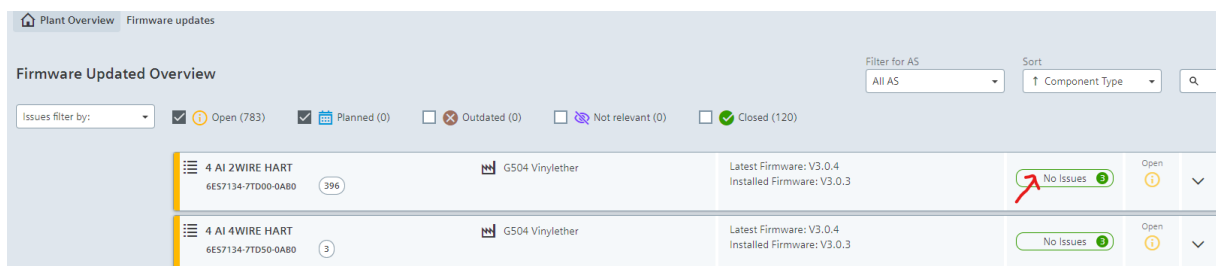
3.11 Datenbestand in myExpert auf Vollständigkeit prüfen

Über den Button „Manual components...“ besteht die Möglichkeit nicht erreichbare, nicht projektierte Komponenten über ein Template Exceltabelle hinzuzufügen



3.12 Daten in myExpert kommentieren und bewerten (2h)

- Beispiel Support Request: Offene SRs prüfen
- Beispiel FW Updates



Change priority group: 4 AI 2WIRE HART



- Immediate **1**
- Suggested **2**
- No Issues **3**
- N.A. **4**

Legend: **1** Action required, as soon as possible **2** Action required at the next opportunity **3** No action required **4** Not rated

Advised Recommendation* (21/1000 Characters)

kein FW-Update nötig.

Cancel Apply

4 PCS myExpert Data Collector

Der SIMATIC PCS myExpert Data Collector besteht aus zwei Teilen.

- Logstash - Der zentrale Teil des myExpert Data Collectors der die Daten in die Cloud überträgt.
- Metricbeats – lokale Data Agents die PC Metriken oder Windows Defender Events an Logstash übertragen.

4.1 Installation und Konfiguration von Logstash

4.1.1 Voraussetzungen für den Betrieb von Logstash

Für den Betrieb von Logstash ist Java erforderlich.

Java 11 oder Java 17 wird unterstützt. Sowohl offizielle Oracle Versionen als auch Open Source Versionen wie OpenJDK sind kompatibel.

Bitte überprüfen Sie, ob Java bereits installiert ist.

Hierzu öffnen Sie bitte eine Kommandozeile und setzen folgenden Befehl ab:

```
java -version
```

Die Ausgabe kann je nach installierter Version unterschiedlich aussehen.

```
PS C:\> Java -version
java version "11.0.3" 2019-04-16 LTS
Java(TM) SE Runtime Environment 18.9 (build 11.0.3+12-LTS)
Java HotSpot(TM) 64-Bit Server VM 18.9 (build 11.0.3+12-LTS, mixed mode)
```

Falls keine Java Installation gefunden werden kann, installieren sie bitte Java. Nach erfolgreicher Installation prüfen sie erneut, mit dem obigen Befehl, ob Java richtig installiert ist.

4.1.2 Installation von Logstash

Logstash wird als Zip-Datei geliefert.

Entpacken Sie die Zip-Datei nach `C:\temp\myExpert_Health\`

Hinweis: Aufgrund der tiefen Ordnerstruktur der Logstash Zip-Datei, kann es passieren, dass das Entpacken fehlschlägt. Falls dies der Fall ist, die Datei z.B. nach C:/ entpacken und anschließend an den Zielordner kopieren.

Kopieren Sie die entpackte Zip-Datei nach `C:\Program Files\Siemens\myExpert_Health\`

4.1.3 Logstash Konfiguration

1. Kopieren der Zertifikate:

- Quarantäne Host: Kopieren Sie *lumberjack.cert* nach
C:\Program Files\Siemens\myExpert_Health\logstash-8.2.3\cert\
- Lvl 3 Server: Kopieren Sie *lumberjack.cert* und *lumberjack.key* nach
C:\Program Files\Siemens\myExpert_Health\logstash-8.2.3\cert\

*Hinweis: Die Zertifikate erhalten Sie vom myExpert Operations Team
simatic_pcs_myexpert.support.industry@siemens.com*

2. Kopieren der Logstash Konfiguration:

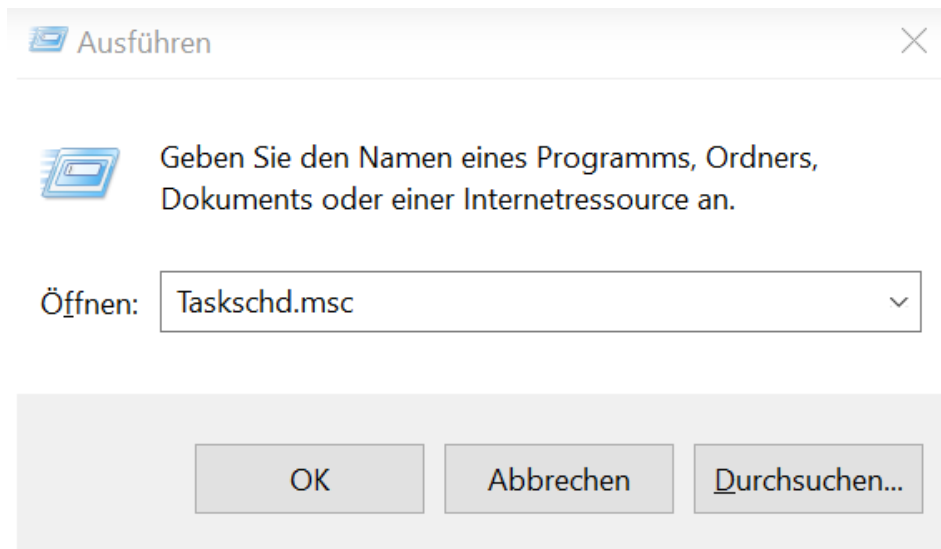
Kopieren Sie *pipelines.yml* nach

C:\Program Files\Siemens\myExpert_Health\logstash-8.2.3\config\

4.1.4 Logstash als geplanten Task konfigurieren

Damit sichergestellt ist, dass Logstash zu dauerhaft läuft, muss es im MS Windows Taskplaner registriert werden. Hierzu wie folgt vorgehen:

1. Windows + R → Es öffnet sich das Ausführen Dialog Fenster
2. Tippen sie Taskschd.msc ein und bestätigen Sie mit Ok.



3. Im neuen Dialog Fenster *Aufgabenplanung* Menüpunkt *Aktion* → *Aufgabe erstellen* auswählen
4. Füllen Sie die Felder im Tab *Allgemein* wie folgt aus

Aufgabe erstellen

Allgemein | Trigger | Aktionen | Bedingungen | Einstellungen

Name: Logstash

Speicherort: \

Autor: [redacted]

Beschreibung: myExpert Data Collector | Logstash

Sicherheitsoptionen

Beim Ausführen der Aufgaben folgendes Benutzerkonto verwenden:
 [redacted] Benutzer oder Gruppe ändern...

Nur ausführen, wenn der Benutzer angemeldet ist

Unabhängig von der Benutzeranmeldung ausführen

Kennwort nicht speichern. Die Aufgabe greift nur auf lokale Computerressourcen zu.

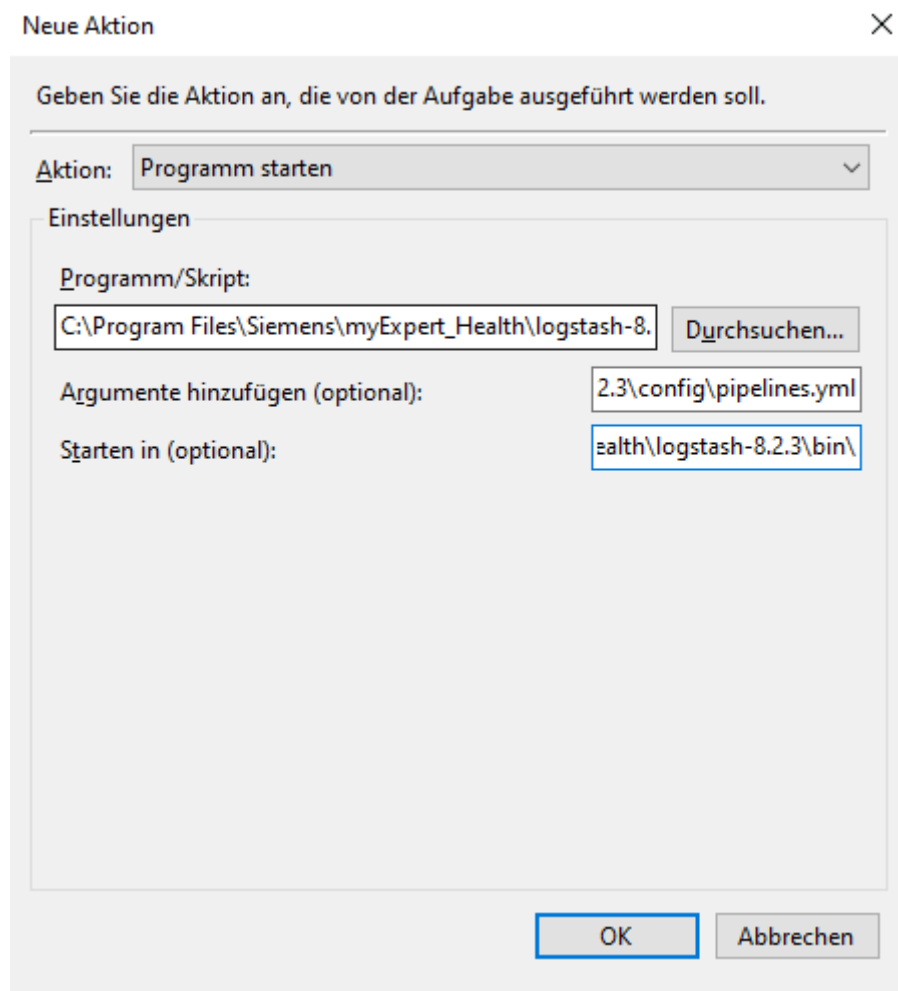
Mit höchsten Privilegien ausführen

Ausgeblendet Konfigurieren für: Windows Vista™, Windows Server™ 2008

OK Abbrechen

5. Wechseln Sie in den Tab *Aktionen* und klicken Sie auf *Neu*

6. Im neuen Dialogfenster die Felder wie folgt ausfüllen



Program/Script: *C:\Program Files\Siemens\myExpert_Health\logstash-8.2.3\bin\logstash.bat*

Argumente hinzufügen: *-f C:\Program Files\Siemens\myExpert_Health\logstash-8.2.3\config\pipelines.yml*

Starten in: *C:\Program Files\Siemens\myExpert_Health\logstash-8.2.3\bin*

7. Bestätigen Sie mit *Ok*

8. Wechseln Sie in den Tab *Trigger*

9. Füllen Sie die Felder wie folgt aus:

Aufgabe Starten: *Beim Start*

Verzögern für: *5 Minuten*

Neuer Trigger

Aufgabe starten: **Beim Start**

Einstellungen

Es sind keine weiteren Einstellungen erforderlich.

Erweiterte Einstellungen

Verzögern für: **5 Minuten**

Wiederholen jede: **1 Stunde** für die Dauer von: **1 Tag**

Alle ausgeführten Aufgaben am Ende der Wiederholungsdauer beenden

Aufgabe beenden nach: **3 Tage**

Aktivieren: **27.06.2022** **09:26:21** Zeitzoneübergreifende Synch.

Ablaufen: **27.06.2023** **09:26:21** Zeitzoneübergreifende Synch.

Aktiviert

OK **Abbrechen**

4.2 Installation Metricbeats via msi Installer – Health Agents

Installieren Sie die Metricbeats mit dem mitgelieferten Installer auf allen PC-Station für die PC Metriken erfasst werden sollen.

Nach der Installation über den Installer öffnet sich automatisch der Metricbeat Data Folder

C:\ProgramData\Elastic\Beats\metricbeat

Kopieren Sie die mitgelieferte *metricbeat.yml* in den Ordner

C:\ProgramData\Elastic\Beats\metricbeat

Kopieren Sie die mitgelieferte *system.yml* in den Ordner

C:\ProgramData\Elastic\Beats\metricbeat\modules.d

Starten Sie Metricbeat über den Windows Service *Elastic Metricbeat 8.2.3*

4.3 Installation Winlogbeats via msi Installer (optional) – Health Agents

Die Winlogbeats werden benötigt, falls die Windows Defender Features von myExpert genutzt werden sollen.

Installieren Sie die Winlogbeats mit dem mitgelieferten Installer auf allen PC-Station für die Windows Defender Metriken erfasst werden sollen.

Nach der Installation über den Installer öffnet sich automatisch der Winlogbeat Data Folder

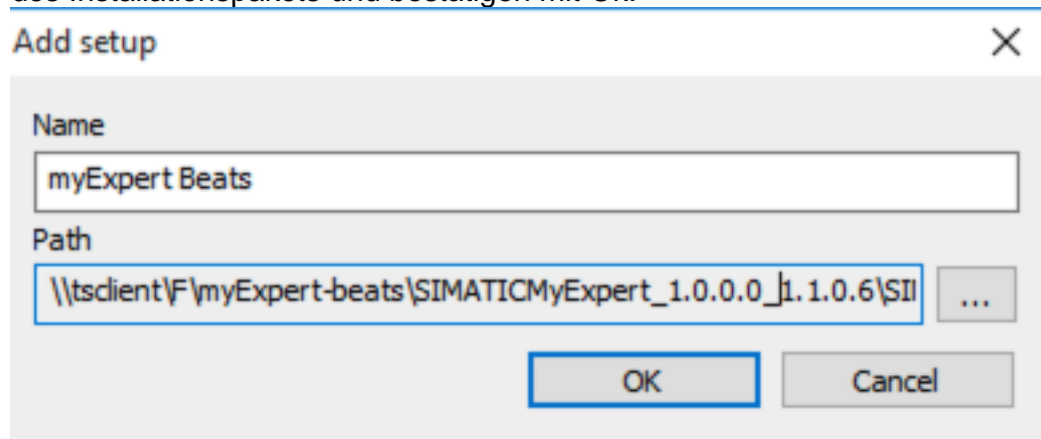
C:\ProgramData\Elastic\Beats\winlogbeat

Kopieren Sie die mitgelieferte *winlogbeat.yml* in den Ordner

C:\ProgramData\Elastic\Beats\metricbeat

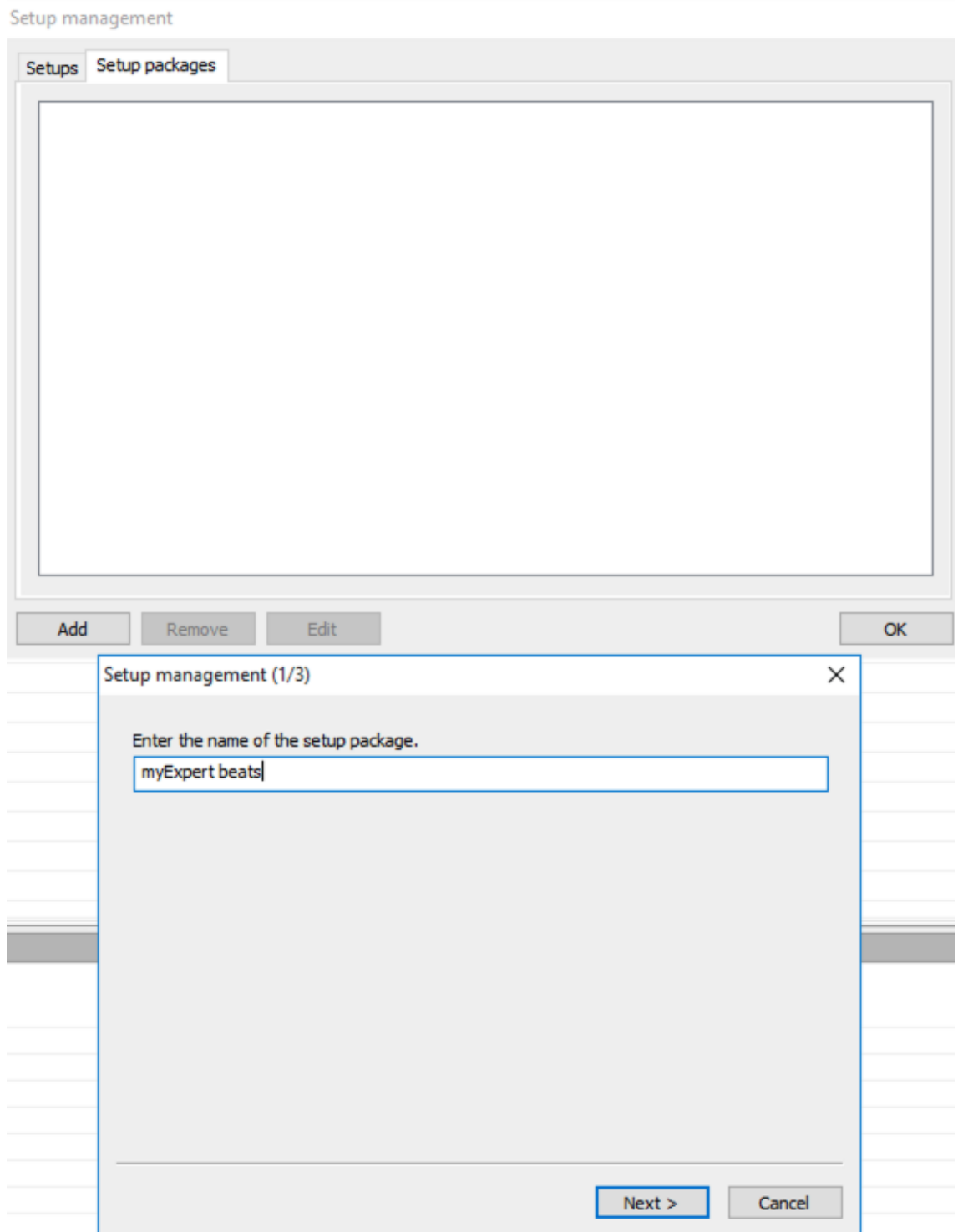
Starten Sie Winlogbeat über den Windows Service *Elastic Winlogbeat 8.2.3*

3. Im neuen Fenster vergeben Sie einen Namen sowie den Pfad zur setup.exe des Installationspakets und bestätigen mit Ok:



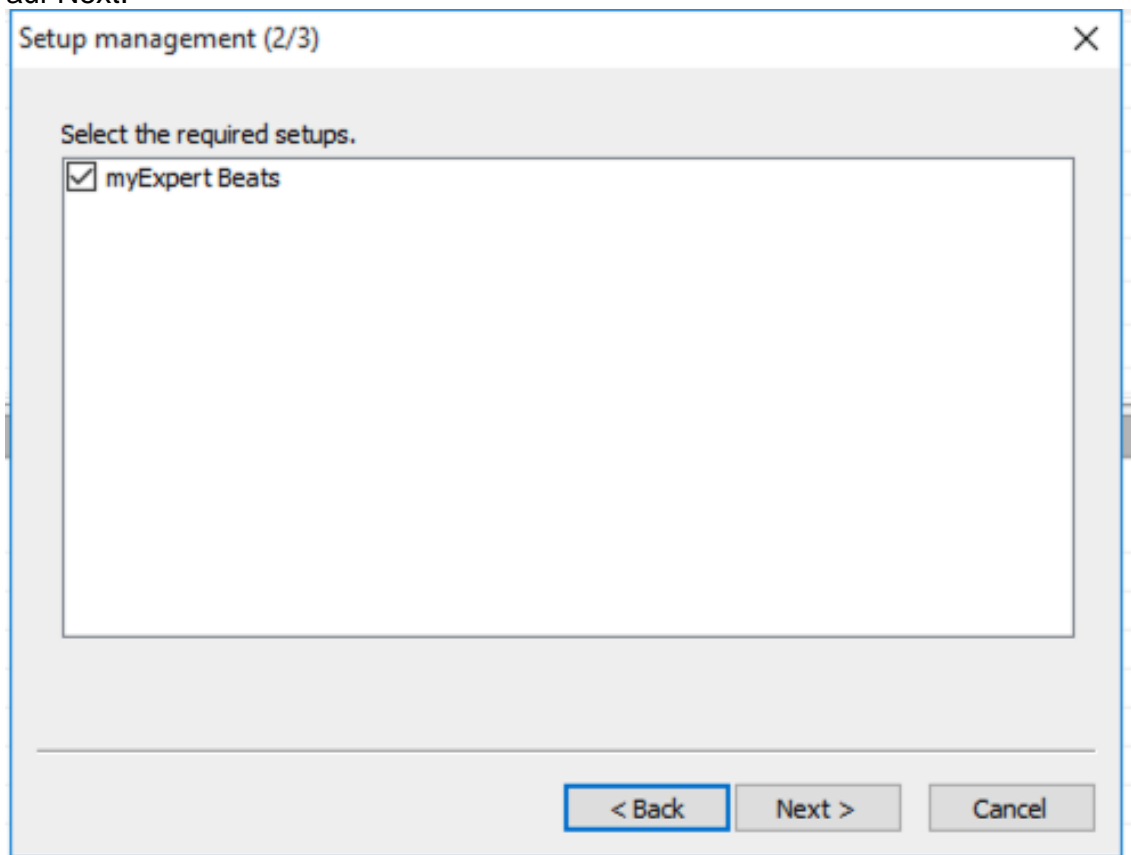
The screenshot shows a dialog box titled "Add setup" with a close button (X) in the top right corner. It contains two input fields: "Name" and "Path". The "Name" field is filled with the text "myExpert Beats". The "Path" field is filled with the text "\\tsclient\F\myExpert-beats\SIMATICMyExpert_1.0.0.0_1.1.0.6\SI". To the right of the "Path" field is a button with three dots "...". At the bottom of the dialog box are two buttons: "OK" and "Cancel".

4. Wechseln Sie in den Tab Setup Pakete und klicken Add



Vergeben Sie einen Namen für das Setup Paket und klicken Sie auf Next.

5. Wählen Sie das Setup, welches unter Schritt 3 erstellt wurde und klicken Sie auf Next.



6. Die Setup Routine startet einmalig.
Führen Sie alle geforderten Schritte der Installationsroutine durch.
7. Das Setup kann nun über die SMMC-Funktion „SIMATIC Software installieren“ durchgeführt werden.