
# SIMATIC PCS myExpert SINEC NMS Inventar Export

SIMATIC PCS myExpert

# Rechtliche Hinweise

### Warnkonzept

Dieses Handbuch enthält Anweisungen, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden befolgen müssen. Die Informationen zu Ihrer persönlichen Sicherheit werden durch ein Warndreieck hervorgehoben, Informationen über Sachschäden allein sind ohne Warndreieck. Je nach Risikostufe werden die Warnungen in absteigender Reihenfolge wie folgt angezeigt.

| | |
|---|---|
|  GEFAHR | **bedeutet, dass es zum Tod oder zu einer schweren Körperverletzung kommt, wenn nicht die entsprechenden Vorsichtsmaßnahmen getroffen werden.** |

| | |
|---|---|
|  WARNUNG | **bedeutet, dass es zum Tod oder zu einer schweren Körperverletzung kommen kann, wenn keine geeigneten Vorsichtsmaßnahmen getroffen werden.** |

| | |
|---|---|
|  VORSICHT | **bedeutet, dass es zu leichten Körperverletzungen kommen kann, wenn nicht die entsprechenden Vorsichtsmaßnahmen getroffen werden.** |

| | |
|---|---|
| AUFMERK SAMKEIT | **bedeutet, dass es zu Sachschäden kommen kann, wenn nicht die entsprechenden Vorkehrungen getroffen werden.** |

Wenn mehr als eine Gefahrenstufe auftritt, wird immer die Warnung für die höchste Stufe verwendet. Warnt eine Warnung mit dem Warndreieck vor Personenschäden, so kann der gleichen Warnung auch eine Warnung vor Sachschäden beigefügt werden.

### Qualifiziertes Personal

Das zu dieser Dokumentation gehörende Produkt/System darf nur von Personal gehandhabt werden, das für die jeweilige Aufgabe qualifiziert ist, und zwar unter Beachtung der mit der jeweiligen Aufgabe verbundenen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist aufgrund seiner Ausbildung und Erfahrung in der Lage, Risiken zu erkennen und mögliche Gefahren im Umgang mit diesen Produkten/Systemen zu vermeiden.

### Richtiger Einsatz von Siemens-Produkten

Beachten Sie Folgendes:



Siemens AG
Branche
Postfach 48 48
90026 Nürnberg
DEUTSCHLAND

(P) 02/2022 Änderungen vorbehalten

| | |
|---|---|
| VORSICHT | **Siemens-Produkte dürfen nur für die im Katalog und der zugehörigen technischen Dokumentation angegebenen Anwendungen verwendet werden. Werden Produkte und Komponenten von Drittanbietern verwendet, müssen diese von Siemens empfohlen oder freigegeben werden. Der ordnungsgemäße und sichere Betrieb der Produkte erfordert den ordnungsgemäßen Transport, die ordnungsgemäße Lagerung, die Installation, die Montage, die Installation, die Inbetriebnahme, den Betrieb und die Wartung. Die zulässigen Umgebungsbedingungen sind einzuhalten. Hinweise in der zugehörigen Dokumentation sind zu beachten.** |

**Marken**

Alle Bezeichnungen, die mit dem Immaterialgüterrechtsvermerk ® gekennzeichnet sind, sind eingetragene Marken der Siemens AG. Bei den anderen Bezeichnungen in diesem Dokument kann es sich um Marken handeln, deren Verwendung durch Dritte für ihre Zwecke die Rechte der Eigentümer verletzen kann.

**Verzichtserklärung**

Wir haben den Inhalt der Broschüre auf Übereinstimmung mit der beschriebenen Hard- und Software überprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir keine Haftung für vollständige Konformität übernehmen. Die Informationen in dieser Broschüre werden regelmäßig überprüft und notwendige Korrekturen in die folgenden Ausgaben aufgenommen.



**Sicherheitshinweise**

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

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyberbedrohungen abzusichern, ist es notwendig, ein ganzheitliches Industrial Security Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens sind nur ein Baustein eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Einrichtungen, Systeme, Maschinen und Netzwerke zu verhindern. Anlagen, Maschinen und Komponenten sollten nur dann mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit erforderliche und angemessene Schutzmaßnahmen (z.B. Einsatz von Firewalls und Netzwerksegmentierung) getroffen wurden.

Darüber hinaus sollten die Empfehlungen von Siemens zu geeigneten Schutzmaßnahmen beachtet werden. Weitere Informationen zu Industrial Security finden Sie unter https://www.siemens.com/industrialsecurity.

Siemens-Produkte und -Lösungen werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt dringend, Updates durchzuführen, sobald die entsprechenden Updates verfügbar sind, und nur die neuesten Produktversionen zu verwenden. Die Verwendung veralteter oder nicht unterstützter Versionen kann das Risiko von Cyberbedrohungen erhöhen.

Um über Produktaktualisierungen auf dem Laufenden zu bleiben, abonnieren Sie den RSS-Feed von Siemens Industrial Security unter https://www.siemens.com/industrialsecurity.

In Übereinstimmung mit internationalen Standards und Best Practices im Risikomanagement

Siemens AG
Branche
Postfach 48 48
90026 Nürnberg
DEUTSCHLAND

(P) 02/2022 Änderungen vorbehalten

hat Siemens die Bedrohungsstufe auf einer Skala von 4 (grün, gelb, orange, rot) auf die Stufe "gelb" (die deutsche BSI-Nomenklatur lautet "eingeschränkt") auf unser SIMATIC PCS myExpert und seine Health Agents hochgestuft: Alle in PCS myExpert vorhandenen Maßnahmen sind darauf ausgelegt, mindestens vor dieser Bedrohungsstufe zu schützen.

Weitere Informationen finden Sie unter:

BSI-Standard 200-3: Risikoanalyse auf Basis des IT-Grundschutzes, (Datum: 07.05.2018)

Herunterladen PDF, (Seite 21-22)

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# 1 Vorwort

## Ziel des Handbuchs

In diesem Dokument finden Sie Informationen und Links zur Anleitung zur Erstellung von Inventarisierungsberichten in SINEC NMS, um Netzwerkgeräte in die Inventarisierung von SIMATIC PCS myExpert zu integrieren.

## Erforderliche Grundkenntnisse

Es sind keine besonderen Kenntnisse erforderlich.

# 2 Allgemeine Informationen

## 2.1 Verzichtserklärung

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

## 2.2 Zielgruppe

Dieses Handbuch richtet sich an Anwender von SIMATIC PCS myExpert,

das Sie möchten Netzwerkkomponenten in die Netzwerkkomponenten Ihres Systems einbinden und diese über den gesamten Lebenszyklus und die Nutzung gemäß dem Mehrwert von SIMATIC PCS myExpert begleiten und warten.



## 2.3 Voraussetzung

Um den Mehrwert von SIMATIC PCS myExpert für die Netzwerkkomponenten Ihrer Anlage nutzen zu können, wird der Inventarimport aus SINEC NMS unterstützt. Sie benötigen eine entsprechende Installation in ihrem System.

# 3 Export Erzeugung

Bitte lesen Sie die folgende Anleitung zur SINEC-Berichtserstellung (Inventarisierung):

Es gibt zwei verschiedene Möglichkeiten, mit SINEC NMS einen Inventurbericht zu erstellen

1) Betriebsart und
2) Steuerungsmodus.

Für die Verwendung in SIMATIC PCS myExpert verwenden sie lediglich den "Steuerungsmodus", um einen Inventarexport zu erzeugen.

Der resultierende Bericht enthält alle Daten zu den im Netzwerk verfügbaren Komponenten mit ihren Attributen.

Eine entsprechende Beschreibung und weitere Details finden Sie ab Kapitel 3.2

*Manueller BA_SINEC-NMS_0.pdf*. (Deutsch).



**SIMATIC NET**
**Netzwerk-Verwaltung**
**SINEC NMS**

**Bedienungsanleitung**

Das Handbuch steht unter folgendem Link zum Download bereit.
https://support.industry.siemens.com/cs/document/109762749/simatic-net-netzwerkmanagement-sinec-nms?dti=0&lc=de-WW

*Manueller BA_SINEC-NMS_0.pdf*. (Deutsch).

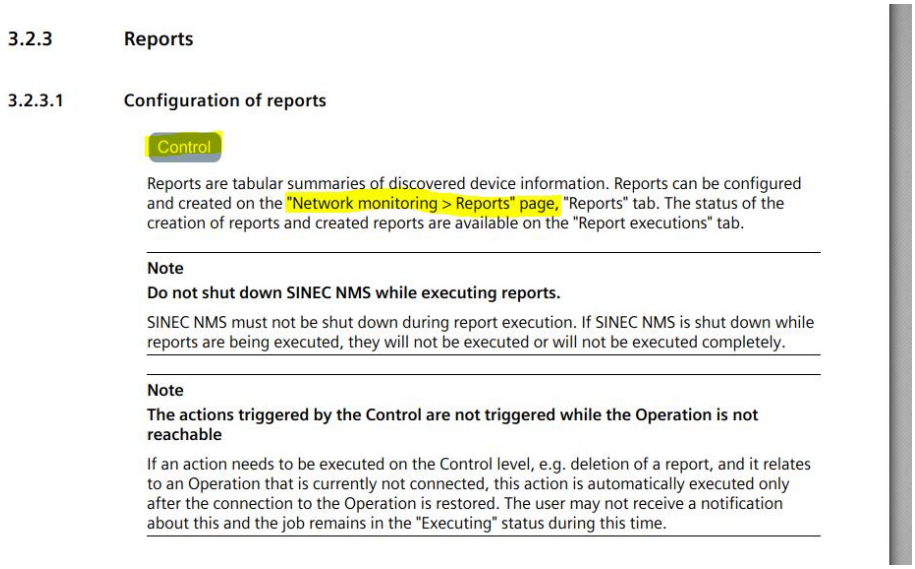
*Manueller BA_SINEC-NMS_76.pdf*. (Englisch).

### 3.1.1 Schnell Info

Um einen Inventurbericht zu erstellen, folgen Sie bitte der Anleitung in
***Kapitel 3.2.3 Berichte.***

Wählen Sie beim Erstellen des Berichts den Typ des Bestandsberichts aus. Das Generieren eines Berichts kann einige Zeit in Anspruch nehmen. Bitte halten Sie SINEC NMS offen.

Die beigefügten Abbildungen dienen der inhaltlichen Orientierung und ersetzen in keiner Weise die Notwendigkeit, das aktuelle Handbuch von SINEC NMS zu verwenden.



### 3.2.3 Reports

#### 3.2.3.1 Configuration of reports

Control

Reports are tabular summaries of discovered device information. Reports can be configured and created on the "Network monitoring > Reports" page, "Reports" tab. The status of the creation of reports and created reports are available on the "Report executions" tab.

**Note**

**Do not shut down SINEC NMS while executing reports.**

SINEC NMS must not be shut down during report execution. If SINEC NMS is shut down while reports are being executed, they will not be executed or will not be executed completely.

**Note**

**The actions triggered by the Control are not triggered while the Operation is not reachable**

If an action needs to be executed on the Control level, e.g. deletion of a report, and it relates to an Operation that is currently not connected, this action is automatically executed only after the connection to the Operation is restored. The user may not receive a notification about this and the job remains in the "Executing" status during this time.

*Abbildung 1 - SINEC NMS Kapitel 3.2.3*

**Editor for creating reports**

Reports can be configured using the following settings:

- Type

  Selection of the type for the report to be created:

  – Inventory: Report with detailed information on all devices discovered by Operations.

  – Availability: Report with information on how long the devices were reachable in a specified time period.

- Name

  The name of the report is formed by SINEC NMS based on the selected report type and the current time stamp.

- Created by

  User who created the report.

- Send notification

*Abbildung 2 - SINEC NMS – Control Mode*

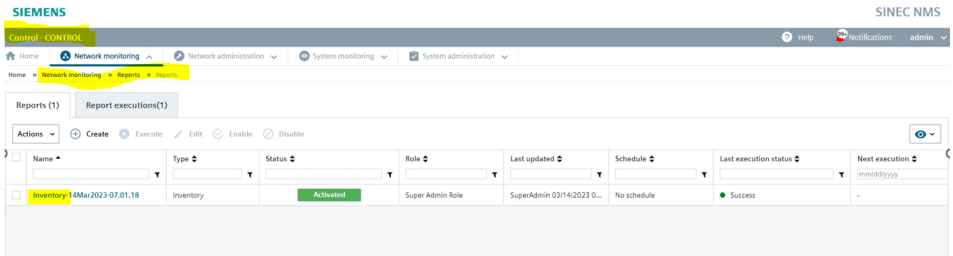



*Abbildung 3 - SINEC NMS – Control Mode – Benutzeroberfläche.*