SIMATIC PCS myExpert SINEC NMS Inventory Export

SIMATIC PCS myExpert

Legal Notices

Warning concept

This manual contains instructions that you must follow for your personal safety as well as to avoid property damage. The information on your personal safety is highlighted by a warning triangle, information about property damage alone is without a warning triangle. Depending on the risk level, the warnings are displayed in decreasing order as follows.

 DANGER	**means that death or serious bodily injury will occur if the appropriate precautions are not taken.**

 WARNING	**means that death or serious bodily injury may occur if the appropriate precautions are not taken.**

 CAUTION	**means that minor bodily injury may occur if the appropriate precautions are not taken.**

ATTENTION	**means that property damage may occur if the appropriate precautions are not taken.**

If more than one hazard level occurs, the warning for the highest level is always used. If a warning with the warning triangle warns of personal injury, then a warning of property damage may also be attached to the same warning.

Qualified staff

The product/system associated with this documentation may only be handled by personnel qualified for the respective task in compliance with the documentation associated with the respective task, in particular the safety and warning instructions contained therein. Due to their training and experience, qualified personnel are qualified to identify risks and avoid possible hazards when handling these products/systems.

Proper use of Siemens products

Keep the following in mind:

 CAUTION	**Siemens products may only be used for the applications specified in the catalog and the associated technical documentation. If third-party products and components are used, they must be recommended or approved by Siemens. The proper and safe operation of the products requires proper transport, proper storage, installation, assembly, installation, commissioning, operation and maintenance. The permissible environmental conditions must be complied with. Instructions in the associated documentation must be observed.**

Siemens AG
Industry Sector
P.O. Box 48 48
90026 Nuremberg
GERMANY

Ⓟ 02/2022 Subject to change

Marches

All designations marked with the intellectual property rights notice ® are registered trademarks of Siemens AG. The other designations in this document may be trademarks, the use of which by third parties for their purposes may infringe the rights of the owners.

Disclaimer

We have checked the content of the brochure for compliance with the hardware and software described. Nevertheless, deviations cannot be ruled out, so that we do not assume any liability for complete conformity. The information in this brochure will be checked regularly, and any necessary corrections will be included in the following editions.

Security Advisories

Siemens offers products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to secure plants, systems, machines and networks against cyber threats, it is necessary to implement (and continuously maintain) a holistic industrial security concept that corresponds to the current state of the art. Siemens' products and solutions are just one component of such a concept.

Customer is responsible for preventing unauthorized access to its facilities, systems, machinery, and networks. Systems, machines and components should only be connected to the corporate network or the Internet if and to the extent necessary and appropriate protective measures (e.g. use of firewalls and network segmentation) have been taken.

In addition, Siemens' recommendations on appropriate protective measures should be observed. For more information about Industrial Security, see https://www.siemens.com/industrialsecurity.

Siemens products and solutions are constantly being developed to make them even safer. Siemens strongly recommends that updates be carried out as soon as the corresponding updates are available and that only the latest product versions are used. Using outdated or unsupported versions can increase the risk of cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS feed at https://www.siemens.com/industrialsecurity.

In accordance with international standards and best practices in risk management, Siemens upgraded the threat level to our SIMATIC PCS myExpert and its Health Agents on a scale of 4 (green, yellow, orange, red) to the "yellow" level (the German BSI nomenclature is "Limited"): All measures present in PCS myExpert are designed to protect against at least this level of threat.

For more information, please refer to:

BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz, (Date: 07.05.2018)

Download PDF, (page 21-22)

Siemens AG
Industry Sector
P.O. Box 48 48
90026 Nuremberg
GERMANY

Ⓟ 02/2022 Subject to change

Table of contents

Table of figures

1 Foreword

Aim of the handbook

In this document, find information and link to instruction for inventory report creation in SINEC NMS to integrate network devices into the inventory of SIMATIC PCS myExpert.

Required basic knowledge

No special knowledge is required .

2 General information

2.1 Disclaimer

The contents of this manual have been checked for compliance with the hardware and software described. Since deviations cannot be completely ruled out, complete compliance cannot be guaranteed. However, the data in this manual will be reviewed regularly and any necessary corrections will be taken into account in later editions. Suggestions for improvement are welcome. This manual does not replace the well-known manuals for the SIMATIC Management Console, but only serves as a supplement. See Chapter 3 – Prerequisites.

2.2 Target group

This manual is intended for SIMATIC PCS myExpert users,

the You would like to include network components in the network components of your system and accompany and maintain them throughout their life cycle and use in accordance with the added value of SIMATIC PCS myExpert.

2.3 Prerequisite

In order to use the added value of SIMATIC PCS myExpert for the network components of your system, inventory import from SINEC NMS is supported. They need an appropriate installation in their system.

3 Export Generation

Please read the following guide to SINEC-Report Generation (Inventory):

There are two different ways to generate an inventory report with SINEC NMS

1) Operation Mode and
2) control mode.

For use in SIMATIC PCS myExpert, they only use "control mode" to generate an inventory export.

The resulting report contains all data on the components available in the network with their attributes.

You will find a corresponding description and further details from chapter 3.2 onwards

Manual BA_SINEC-NMS_0.pdf. (German).

SIMATIC NET
Network management
SINEC NMS

Operating Instructions

The manual is available for download at the following link.
https://support.industry.siemens.com/cs/document/109762749/simatic-net-netzwerkmanagement-sinec-nms?dti=0&lc=de-WW

Manual BA_SINEC-NMS_0.pdf. (German).

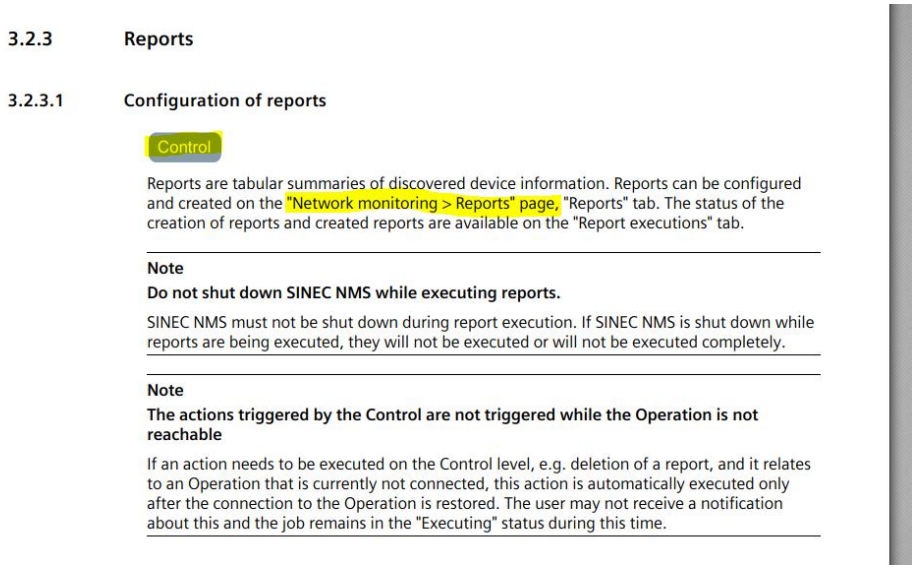
Manual BA_SINEC-NMS_76.pdf. (English).

3.1.1 Quick Info

To generate an inventory report, please follow the listed manual in
Chapter 3.2.3 Reports.

When creating the report, select the inventory report type.
It may take some time to generate a report. Please keep SINEC NMS open.

The attached illustrations are intended for orientation in terms of content and in no way replace the need to use the current manual of SINEC NMS.



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.

Illustration 1 - SINEC NMS Chapter 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

Illustration 2 - SINEC NMS Control Mode

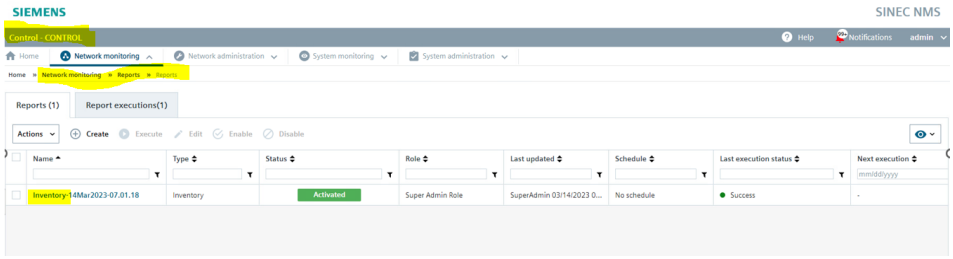


Illustration 3 - SINEC NMS Control mode UI .