SIEMENS

QUICK START GUIDE

SINEC NMS V2.0

Up and scanning in less than 15 minutes

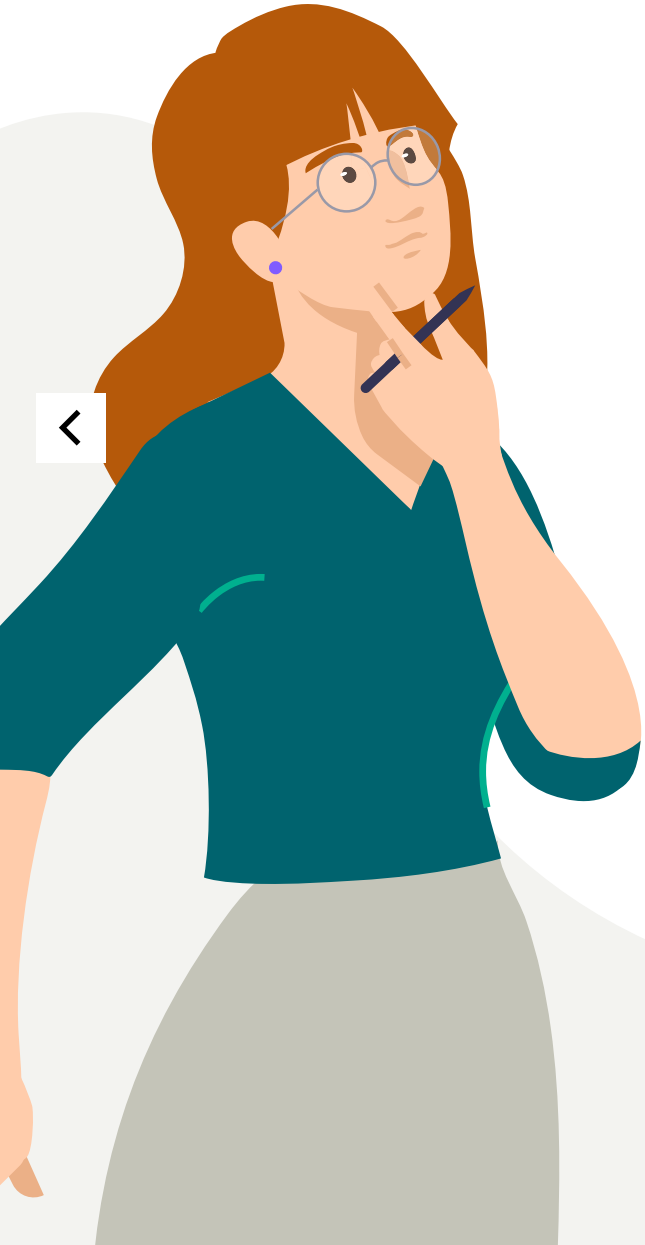


Table of **Contents**

CHAPTER 1

Preparation

Checklist before SINEC NMS installation

Hardware- and software requirements checked (see manual chapter 1.9)?

- Security recommendations checked (see manual chapter A.1)?
- Current user is a local Windows admin and not an Active Directory user?
- Does PC name not contain spaces or special characters?
- At least one network card (NIC) has an active link?
- PC time settings correct?
  - For multi-node: Do both machines have the same time source (e.g., NTP-Server) and time zone?
- Is the installation file version the latest one?
- Is the installation file copied directly to the PC (e.g., Download folder)?
- Do you have a valid licence and licence key ?

CHAPTER 2

Download & Installation

Download

Download the latest SINEC NMS version from the Siemens Industry Online Support Portal: https://support.industry.siemens.com/cs/ww/en/ps/25518/dl

Alternatively, you can purchase SINEC NMS with Online Software Delivery (OSD).

CHAPTER 2

Download & Installation

Installation

Installation as a Single Node system: The Control and Operation is installed on the same PC.

1. Launch the downloaded file “SINECNMS_V2.0.exe” with administrator privileges, extract it, start the installation wizard, and define the installation language.
2. Select which components of SINEC NMS should be installed. In this example:
   - Single-node: Control and Operation
   - User-management component (UMC): Install UMC locally →Needed for central user-management, Web-Single Sign On, and Active Directory Integration
   - Win10 Pcap
3. Click “Next” and choose either to create a new UMC domain or to use an existing UMC domain. Define a name and password for the UMC administrator to be added to this domain. To complete the configuration of UMC, click “Next. “
4. Select the desired trap service (recommended: SINEC NMS trap service because it can handle SNMPv3 traps.)
5. Follow the instructions of the installation wizard and restart the PC after the installation is complete.

CHAPTER 3

First-Time Log-On – set new password for local user

Sign into the Web interface

1. SINEC NMS starts automatically with Windows → Log on with your Web browser to the SINEC NMS Webserver using either the Desktop shortcuts or these URLs:
   - SINEC NMS Control: https://<IP-address / hostname SINEC-NMS-Control>:443
   - SINEC NMS Operation: https://<IP-address / hostname SINEC-NMS-Operation>:8443
2. The very first log-on can only be done by the default local user “superadmin”:
   - Enter a new, secure password for the “superadmin”
   - Log on as a “superadmin” user and use the previously set secure password
   - Now, you can log on as the UMC user that was created during the installation

SINEC NMS log-on options

A) Login as a local user:

- During first log-on, a password must be set for the default user “superadmin”

B) Login as a UMC user:

- UMC user that was created automatically during the installation

CHAPTER 4

Adapt the Operation Parameter Profile for Scanning

Now, adjust the most important parameters of the default parameter profile “Starter Set”

1. What are the **initial device credentials** for the network devices?
   - Parameter group: **Initial device credentials** (SNMP, SSH/NETCONF, HTTPS)
2. What are the **SNMP versions** and **credentials** used for the network devices?
   - Parameter group: SNMP settings for discovery
     – For example, add SNMPv3 profiles for discovery & monitoring here
   - Note: SNMP discovery, based on the version, uses this order: SNMPv3 → SNMPv2c → SNMPv1
3. What **type of devices** are you expecting? Are you expecting **“old” firmware versions?**
   - For “older” devices such as SCALANCE X200/X300 or RUGGEDCOM ROS devices or “old” firmware versions:
     – Parameter group: Monitoring settings → Permit device communication with legacy ciphers
   - Note: If legacy ciphers are not allowed, no policy-based configurations are possible for the above mentioned “older” devices

CHAPTER 4

Adapt the Operation Parameter Profile for Scanning

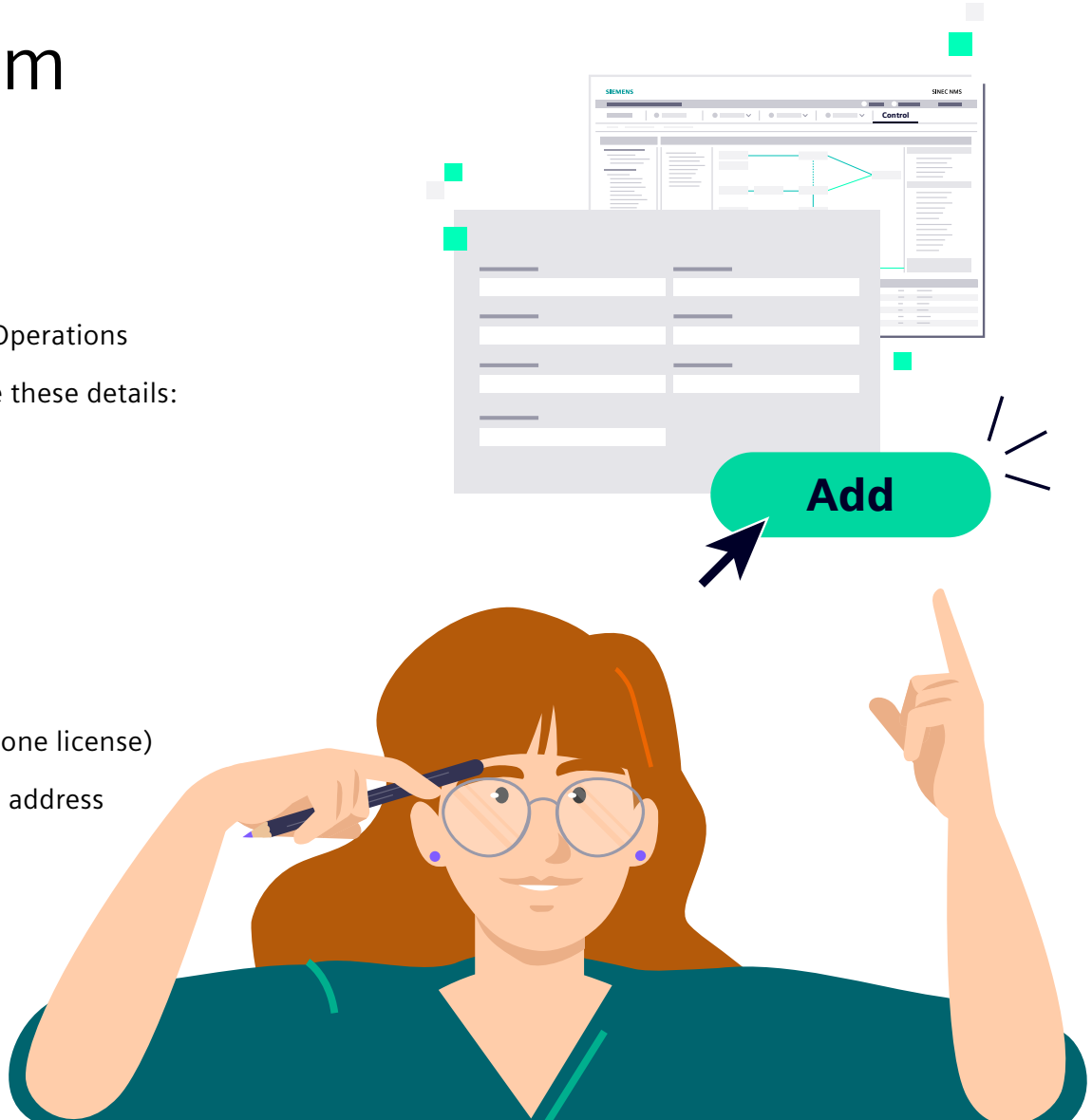
Good to know about the SINEC NMS parameter profile:

- Configure all parameters, e.g., discovery settings, device credentials ...
- For each operation, one parameter profile can be assigned with a specific set of parameters.
- By default, the “Start Set” profile is available with all default settings for all parameters.

Further information for parameter profiles can be found in the manual, chapter 6.3.

CHAPTER 5

Add the Operation to the Control System



Now, add the SINEC NMS Operation to the Control

1. Navigate to Control → System Administration → Operations
2. Click on the button “Add Operation” and provide these details:
   - IP address/host name of the operation
   - Certificate password
   - Parameter profile “Starter Set”
   - Position in folder hierarchy
   - Operation name
   - Number of devices (one device will consume one license)
   - Name of scan range + first IP address + last IP address
3. To finish, click on the button “Add.”

CHAPTER 6

Network Scan, Device List, Topology & Credentials

Scan the network

Wait, until the SINEC NMS operation is added to the control system and all the parameters are synced (System Status: "OK").

When OK, click on the action "Start network scan" and wait until the network scan is finished (depends on the number of devices in the scan range and network quality).

Check the scan results – asset list

Once the network scan is completed, you can find the discovered network devices in the automatically generated asset-/inventory list either in the Control system or Operation:

Device list in the Control:

1. Navigate to Control → Network monitoring → Devices

Asset list in the Operation:

2. Navigate to Operation → Network monitoring → Devices

Good to know about the asset list:

If an expected device ...

... is not discovered at all:

- Check whether it's reachable via one of the discovery protocols, e.g., ICMP
- Check if a firewall is between the Operation and device

... is discovered as "DEFAULT_ICMP_Device":

- Check, if SNMP is enabled on the device or allowed through the firewall
- Check, if a suitable SNMP profile for discovery is available
- Check, that SINEC NMS is not blocked by a brute-force-mechanism on the device...

... is discovered as "DEFAULT_SNMP_Device":

- A proper device profile was not found in the SINEC NMS database → If needed, you can create your own SNMP-based device profile (see FAQ "3rd party device integration")

CHAPTER 6

Network Scan, Device List, Topology & Credentials

Check the scan results – network topology

During the scan, the network topology is identified using a standardized mechanism and displayed in the SINEC NMS Operation:

Good to know about network topology:

If a network connection is not automatically discovered:

- Check whether SNMP is reachable for the device(s)
- Check whether LLDP is enabled on the device(s)
- Workaround: Draw the network connection between the devices manually

The network topology can be directly integrated into the overlaying HMI/SCADA system via URL call

Topology in Operation:

1. Navigate to Operation → Topology.

Using the green/gray button (orange frame) in the left navigation bar, you can change between the:

- **Online mode** (monitoring of device and connection status and network load), and
- **Offline mode** (add and arrange devices, draw connections, change topology settings, add background pictures, create a reference topology)

Now, create a **reference topology** (green frame) in offline mode and start 24/7 monitoring by changing back to the online mode (orange frame).

CHAPTER 6

Network Scan, Device List, Topology & Credentials

Check the scan results – event list

During the 24/7 monitoring, all network and system events are collected in the Operations event list:
Navigate to Operation → Devices

The event list can be found at the bottom of the User Interface. The event list can be hidden, filtered and additional columns can be added via the wrench icon.

Check the scan results – device credentials

In case not all devices share the same credentials (as provided in the “Starter Profile”), you can simply adjust them for each device in the credential repository:

Navigate to Operation → Network Administration → Credential repository

Good to know about device credentials:

In the device credential repository, you can:

- Copy and paste credentials from one device to multiple other devices
- Trust or untrust one or more devices

CHAPTER 7

Further SINEC NMS Use-Cases, & Features

Do you also have to solve some of these challenges?

1. How can I diagnose and troubleshoot my network devices?
   Use the SINEC NMS inventory list, network topology, and event list: Link
2. How can I update the firmware of my SCALANCE, RUGGEDCOM, and RFID devices?
   Use SINEC NMS firmware-management: Link
3. How can I disable unused ports or unsecure protocols of my network devices?
   Use the SINEC NMS configuration cockpit: Link
4. How can I easily and graphically configure my SCALANCE SC-600, M-800 and RUGEDDCOM ROX 2 firewalls?
   Use SINEC NMS firewall management and create communication relations: Link
5. How can I reuse my existing users from my company's Active Directory domain?
   Use the SINEC NMS user-management component (UMC): Link
6. How can I integrate third-party devices into SINEC NMS?
   Use the SINEC NMS device profile concept and extend it easily: Link
7. How can I roll out Web server certificates to my SCALANCE or RUGGEDCOM devices?
   Use the SINEC NMS certificate management feature: Link
8. How can I transfer network information from SINEC NMS to overlaying HMI/SCADA systems?
   Use the standardized SINEC NMS northbound interfaces: Link

CHAPTER 7

Further SINEC NMS Use Cases & Features

Further SINEC NMS information such as FAQ, downloads, manual, readme files can be found in our Siemens Online Portal:

https://support.industry.siemens.com/cs/ww/en/ps/25518

Publisher
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe
Deutschland

Article No. DIPA-B10418-00-7600
HL 23070983 WS 10230.0

Security information

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

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a

holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
siemens.com/industrialsecurity