

## SIMATIC NET

### Netzwerkmanagement SINEC PNI




#### Betriebsanleitung

<u>Vorwort</u>	<b>1</b>
<u>Installation und Start</u>	<b>2</b>
<u>Bedienung</u>	<b>3</b>
<u>Troubleshooting</u>	<b>4</b>

## 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.

 <b>GEFAHR</b>
bedeutet, dass Tod oder schwere Körperverletzung eintreten <b>wird</b> , wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.
 <b>WARNUNG</b>
bedeutet, dass Tod oder schwere Körperverletzung eintreten <b>kann</b> , wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.
 <b>VORSICHT</b>
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.
<b>ACHTUNG</b>
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:

 <b>WARNUNG</b>
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.

# Inhaltsverzeichnis

<b>1</b>	<b>Vorwort.....</b>	<b>5</b>
1.1	Intended operational environment.....	7
1.2	Netzbelastung durch SINEC PNI.....	7
1.3	Security-Empfehlungen.....	8
<b>2</b>	<b>Installation und Start.....</b>	<b>9</b>
2.1	Systemvoraussetzungen .....	9
2.2	Installation und Start.....	10
2.3	Deinstallation .....	10
2.4	Aufbau der Bedienoberfläche .....	11
2.5	Ports.....	15
<b>3</b>	<b>Bedienung.....</b>	<b>17</b>
3.1	Geräteliste.....	17
3.1.1	Firmware aktualisieren.....	19
3.1.2	Gerätekonfiguration .....	23
3.1.3	Herunterladen und Hochladen .....	28
3.2	Einstellungen.....	31
3.3	Geräteanmeldedaten .....	34
<b>4</b>	<b>Troubleshooting .....</b>	<b>35</b>
4.1	Aktualisieren der Firmware fehlgeschlagen .....	36
	<b>Index.....</b>	<b>39</b>



# Vorwort

## Zweck dieser Software

SINEC PNI (Primary Network Initialization) dient der Erkennung und Initialisierung von PROFINET-Geräten sowie der Basiskonfiguration von SCALANCE-, RUGGEDCOM- und RTLS-Geräten.

Zu den konfigurierbaren Parametern zählen neben IP-Adressinformationen auch PROFINET- und PROFIBUS-Parameter (IE/PB-Link) sowie Geräteanmeldedaten.

## Zweck dieser Dokumentation

Dieses Handbuch unterstützt Sie beim Arbeiten mit SINEC PNI.

## Gültigkeitsbereich

Die Informationen in diesem Dokument gelten für SINEC PNI V1.0 Service Pack 1 Update 1.

## Marken

Folgende und eventuell weitere nicht mit dem Schutzrechtsvermerk<sup>®</sup> gekennzeichnete Bezeichnungen sind eingetragene Marken der Siemens AG:

SINEC, SCALANCE, RUGGEDCOM, RTLS

## Lizenzbedingungen

---

### Hinweis

#### Open Source Software

Das Produkt enthält Open Source Software. Lesen Sie die Lizenzbedingungen zur Open Source Software genau durch, bevor Sie das Produkt nutzen.

---

Sie finden die Lizenzbedingungen in folgendem Dokument, das sich auf dem mitgelieferten Datenträger befindet:

OSS\_SINEC-PNI\_99.pdf

## SIMATIC NET-Glossar

Erklärungen zu vielen Fachbegriffen, die in dieser Dokumentation vorkommen, sind im SIMATIC NET-Glossar enthalten.

Sie finden das SIMATIC NET-Glossar im Internet auf unseren Industry Online Support-Seiten unter folgender Adresse:

Beitrags-ID 50305045 (<https://support.industry.siemens.com/cs/ww/de/view/50305045>)

## Außerbetriebnahme

Beachten Sie, dass auf dem Rechner, auf welchem die Software installiert ist, auch personenbezogene Daten wie Adressen oder Passwörter gespeichert sein können.

Nehmen Sie das Gerät ordnungsgemäß außer Betrieb, um zu verhindern, dass unbefugte Personen an vertrauliche Daten gelangen.

Löschen Sie zur Außerbetriebnahme alle Daten vom Gerät.

## Ciphers

Beachten Sie, dass SINEC PNI aus Gründen der Kompatibilität neben den starken Verschlüsselungsverfahren auch die schwachen unterstützt.

## 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 einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter:

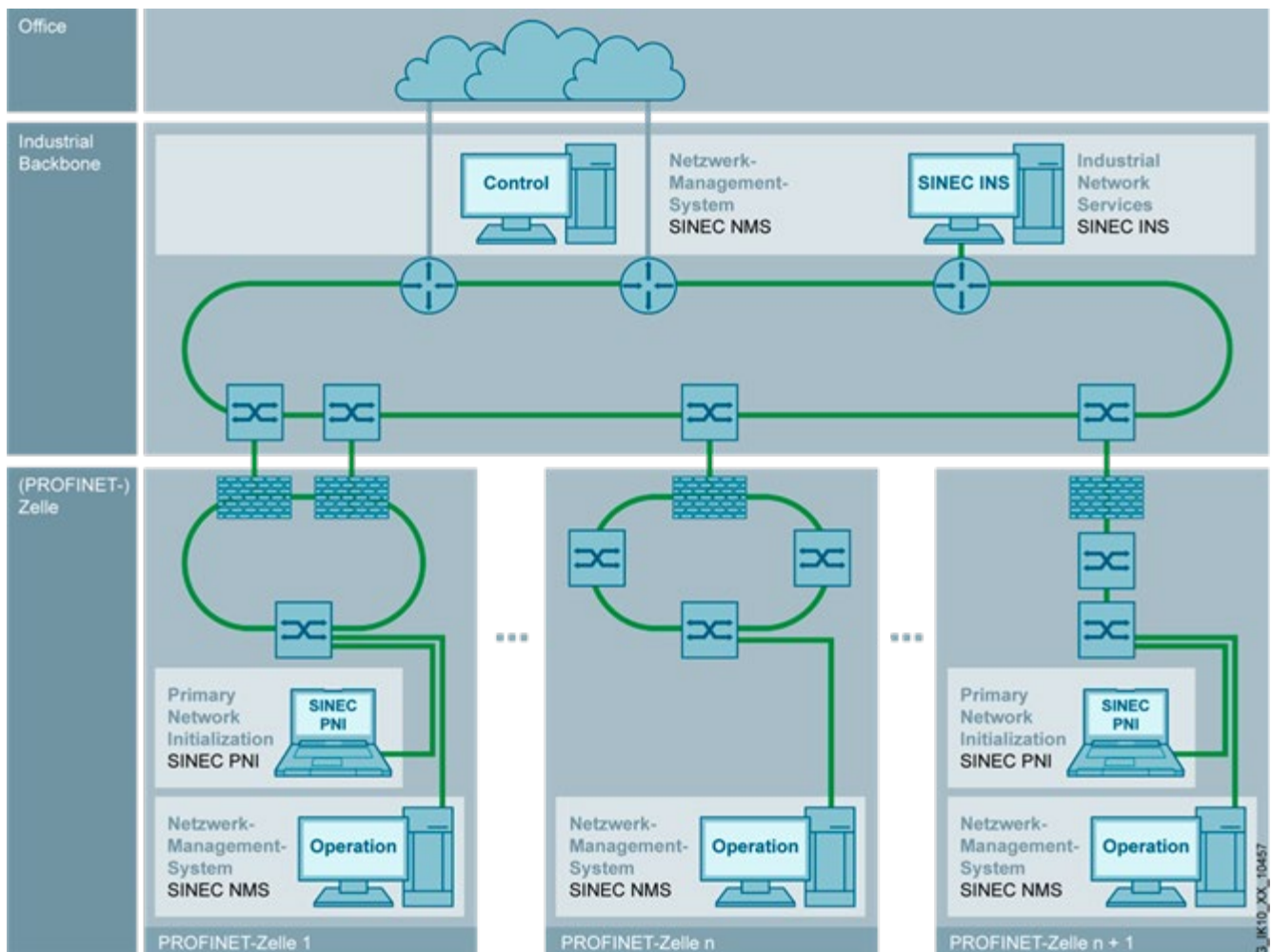
<https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>)

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie 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> (<https://www.siemens.com/industrialsecurity>)

## 1.1 Intended operational environment



## 1.2 Netzbelastung durch SINEC PNI

SINEC PNI beansprucht zur Initialisierung und Inbetriebnahme von Geräten einen Anteil der im Netzwerk verfügbaren Datenübertragungsrate.

Dies muss bei der Planung von Netzwerken, in denen SINEC PNI eingesetzt werden soll, berücksichtigt werden.

## 1.3 Security-Empfehlungen

Um nicht autorisierten Zugriff zu unterbinden, beachten Sie folgende Security-Empfehlungen.

### Allgemein

- Stellen Sie regelmäßig sicher, dass dieses Produkt diese Empfehlungen und/oder andere interne Security-Richtlinien erfüllt.
- Bewerten Sie Ihre Anlage ganzheitlich im Hinblick auf Sicherheit. Nutzen Sie ein Zellenschutzkonzept mit entsprechenden Produkten.
- Halten Sie die verwendete Software aktuell. Informieren Sie sich regelmäßig über Sicherheitsupdates des Produkts.  
Informationen hierzu finden Sie unter <https://www.siemens.com/industrialsecurity> (<https://www.siemens.com/industrialsecurity>).
- Aktivieren Sie ausschließlich Protokolle, die Sie zur Überwachung und Administration der Geräte benötigen.
- Verwenden Sie nach Möglichkeit stets diejenigen Varianten von Protokollen, die mehr Sicherheit bieten (z.B. SNMPv3).
- Verbindungen über ungesicherte Netzwerkbereiche müssen durch Security-Mechanismen wie SSL-VPN gesichert werden.
- Beschränken Sie den Zugriff auf SINEC PNI auf qualifiziertes Personal.

### Training, Service & Support

Informationen zu Training, Service & Support finden Sie in dem mehrsprachigen Dokument "DC\_support\_99.pdf" auf den Internet-Seiten des Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/de/view/38652101>)



# Installation und Start

## 2.1 Systemvoraussetzungen

### Hardware-Voraussetzungen

Folgende Mindestvoraussetzungen gelten im Hinblick auf die zu verwendende Hardware:

- Arbeitsspeicher: 2 GB
- Festplattenspeicher: 1 GB
- Netzwerkkadapter: 1

### Software-Voraussetzungen

Folgende Voraussetzungen gelten im Hinblick auf das zu verwendende Betriebssystem:

- Microsoft Windows 7 (Pro / Enterprise) SP1
- Microsoft Windows 10 (Enterprise LTSC) Version 1607
- Microsoft Windows 10 (Enterprise LTSC) Version 1809
- Microsoft Windows 10 (Professional / Enterprise) Version 1903
- Microsoft Windows 10 (Professional / Enterprise) Version 1909
- Microsoft Windows Server 2016 Standard (LTSC) Version 1607
- Microsoft Windows Server 2019 Standard (LTSC) Version 1809

Auf jedem Betriebssystem ist die Installation der folgenden Software erforderlich. Beim Start prüft SINEC PNI, ob diese Software installiert ist. Wenn die Software nicht installiert ist, können Sie sie über das SINEC PNI Setup installieren:

- PCap-Treiber: WinPcap/Win10Pcap/NpCap (Programmierschnittstelle, um Netzwerkverkehr auf Layer 2 mitzuschneiden)  
Von SINEC PNI wird die aktuelle Win10Pcap-Version installiert. Mit den folgenden Versionen ist SINEC PNI kompatibel:
  - WinPcap: ab 4.13
  - Win10Pcap: ab 10.2-5002
  - NpCap: ab 0.9983  
Wenn der Treiber NpCap bereits installiert ist, muss dieser die Version 0.9983 oder höher haben. Wenn die Version älter als 0.9983 ist, funktioniert SINEC PNI nicht ordnungsgemäß.
- Visual C++ Redistributable 2015-2019

### Nicht unterstützte Geräte

RUGGEDCOM ROS Non controlled Geräte werden von SINEC PNI nicht unterstützt.

## 2.2 Installation und Start

### Installation und Start

Entpacken Sie das ZIP-Archiv von SINEC PNI. Für das dabei erstellte Verzeichnis benötigen Sie Lese- und Schreibrechte.

Um SINEC PNI zu starten, klicken Sie auf die Datei "SinecPni.exe". Beim Start prüft SINEC PNI, ob der PCap-Treiber und Visual C++ Redistributable installiert sind, siehe Kapitel Systemvoraussetzungen (Seite 9). Wenn diese nicht installiert sind, können diese über SINEC PNI installiert werden.

Für den mitgelieferten TFTP-Server wird das Verzeichnis "temp" erstellt, für dieses Verzeichnis benötigen Sie Lese- und Schreibrechte.

Beim ersten Start wird die Seite "Einstellungen" geöffnet. Auf dieser Seite können Sie die Einstellungen für den Netzwerk-Scan konfigurieren, siehe Kapitel Einstellungen (Seite 31).

Aus Geschwindigkeits- und Ressourcengründen wird empfohlen, nur die Protokolle zu aktivieren, die wirklich benötigt werden.

Nach erfolgter initialer Konfiguration können Sie SINEC PNI über die Datei "SinecPni.exe" im entpackten Dateiordner starten.

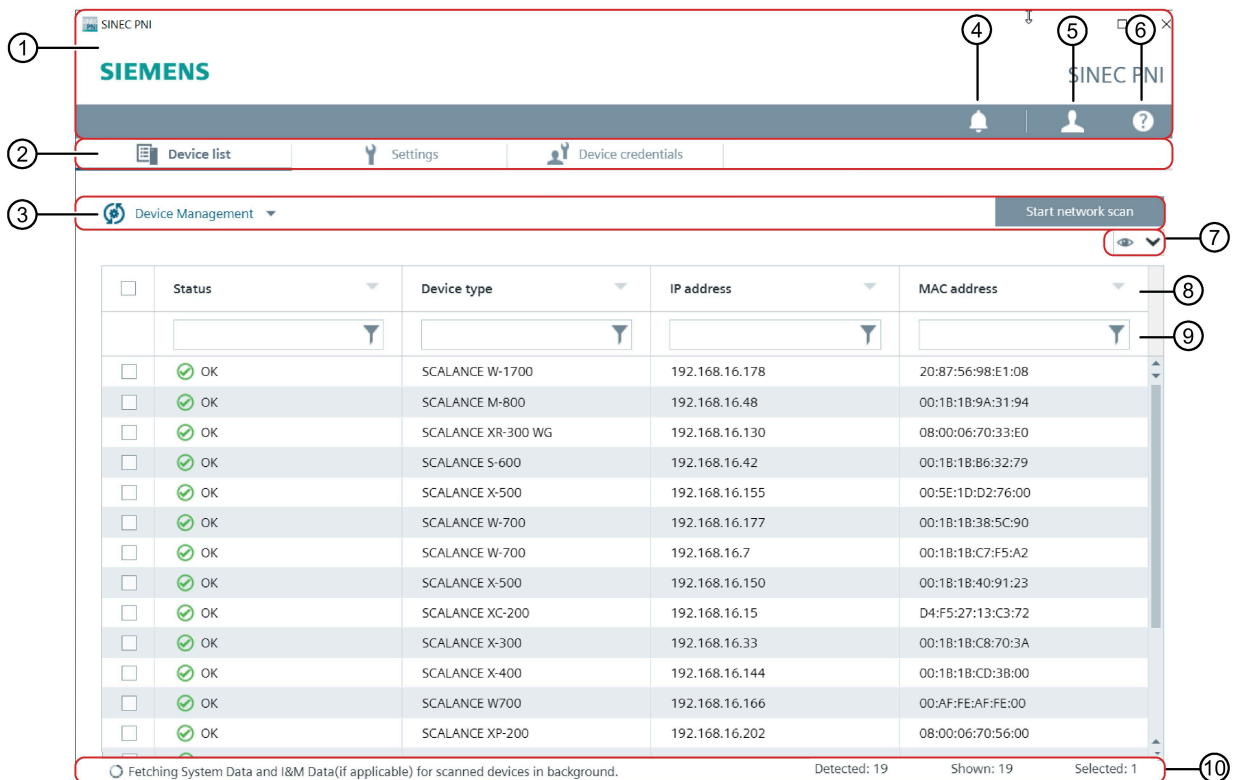
Es kann nur eine SINEC PNI Instanz gestartet werden.

## 2.3 Deinstallation

Zum Deinstallieren löschen Sie den entpackten Dateiordner.

## 2.4 Aufbau der Bedienoberfläche

Die folgende Abbildung zeigt wesentliche Bedienelemente von SINEC PNI. Die Bedienelemente der Kopfzeile sind unabhängig vom gewählten Navigationseintrag verfügbar.



- ① Kopfzeile
- ② Navigation
- ③ Aktionsmenü und Schaltflächen für den Schnellzugriff, siehe Abschnitt unten
- ④ Benachrichtigungsmenü mit Anzahl der ungelesenen Benachrichtigungen, siehe Abschnitt unten
- ⑤ Benutzermenü, siehe Abschnitt unten
- ⑥ Menü zum Aufruf der Online-Hilfe und zur Anzeige der installierten SINEC PNI Version
- ⑦ Klappliste für die Auswahl der anzuzeigenden Spalten
- ⑧ Symbole zum aufsteigenden / absteigenden Sortieren von Spalteninhalten
- ⑨ Eingabefeld zum textuellen Filtern von Spalteninhalten
- ⑩ Statuszeile mit Informationen zum Holen der Systemdaten

Bild 2-1 Bedienoberfläche von SINEC PNI

### Aktionsmenü und Schaltflächen für den Schnellzugriff

Das Aktionsmenü enthält alle auf einer Seite zur Verfügung stehenden Funktionen. Mithilfe der Stern-Symbole können Sie häufig verwendete Aktionen definieren, die für den Schnellzugriff neben dem Aktionsmenü angezeigt werden.

## Benachrichtigungsmenü

Über das Symbol können Sie die Benachrichtigungsliste aufklappen. Die Zahl gibt die Anzahl ungelesener Benachrichtigungen. Die Benachrichtigungen enthalten Warnungen, Fehlermeldungen und Benachrichtigungen, die über abgeschlossene Aktionen informieren. Die Benachrichtigungen werden nach der MAC-Adresse des Geräts gruppiert. Wenn Sie auf die Benachrichtigung klicken, werden die Details sichtbar.

Um den gesuchten Inhalt zu filtern, geben Sie in das Eingabefeld einen Suchtext ein und mit der <ENTER>-Taste bestätigen.

Einzelne Benachrichtigungen können Sie über die Schaltfläche "Löschen" aus dem Benachrichtigungsmenü entfernen. Über die Schaltfläche "Alle löschen" werden alle Benachrichtigungen entfernt.

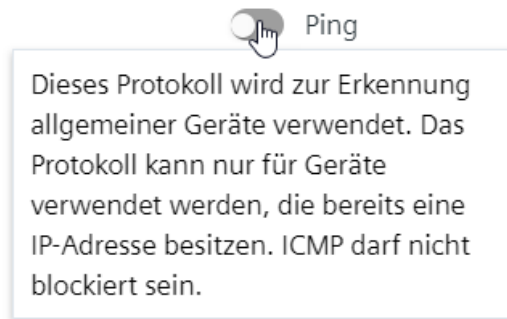


## Benutzermenü

Das Benutzermenü enthält Schaltflächen zur Umstellung der Sprache. Es werden die Sprachen Deutsch und Englisch unterstützt.




## Tooltip

Ist an dem Parameter ein Tooltip verfügbar, erscheint dieser wenn Sie mit der Maus auf der Stelle verweilen.



## Tastaturbedienung

Einige Funktionen lassen sich über das Menü ausführen oder über Tastenkombinationen.

Funktion		Tastenkombination
Benachrichtigungsmenü 		F3
Benutzermenü 	Sprache	ALT + A
Hilfemenü 	Online-Hilfe	F1
	Über SINEC PNI	F11
Netzwerk-Scan starten		F5
Geräteliste		STRG + ALT + L
Einstellungen		STRG + ALT + S
Geräteanmeldedaten		STRG + ALT + C

Funktion		Tastenkombination
Geräteverwaltung	Gerätekfiguration ändern	ALT + C
	Gerät zurücksetzen	-
	WBM öffnen	ALT + O oder F2
	Auswahl exportieren	-
	Geräteverfügbarkeit	LED blinken
		Gerät anpingen
	Firmware aktualisieren	-
	Gerät neu starten	ALT + R
	Herunterladen und Hochladen	Auf den PC herunterladen
		Auf das Gerät hochladen

## Tabellen

Die Geräteliste ist eine tabellarische Zusammenfassung der ermittelten Geräteinformationen.

### Einträge in Tabellen auswählen

In der ersten Spalte jeder Tabelle befinden sich Optionskästchen. Die Optionskästchen befinden sich in der Kopfzeile und in jeder Tabellenzeile.

Gehen Sie wie folgt beschrieben vor, um Tabelleneinträge zu selektieren.

- Einzelnen Eintrag wählen

Klicken Sie in eine Tabellenzeile. Damit selektieren Sie einen einzelnen Eintrag und deselektieren andere selektierte Einträge.

- Mehrere Einträge wählen

Aktivieren Sie bei gedrückter Shift-Taste das Optionskästchen des ersten und letzten Eintrags im gewünschten Tabellenbereich.

Die Ausführung startet mit dem zuerst ausgewählten Gerät.

- Mehrere Einträge beliebig verteilt wählen


Klicken Sie in die Tabellenzeilen der gewünschten Einträge. Damit selektieren Sie die gewünschten Einträge und deselektieren andere selektierte Einträge.

Die Konfiguration wird in der Reihenfolge zugewiesen, in der die Geräte in der Geräteliste ausgewählt sind.

- Alle Einträge derselben Seite wählen

Aktivieren Sie das Optionskästchen in der Kopfzeile.

### Spalten ein-/ausblenden

Durch Klicken auf das Auge-Symbol  rechts oberhalb einer Tabelle öffnet sich die Klappliste mit den verfügbaren Spalten. Durch Aktivierung der Optionskästchen können Sie die Spalten auswählen, die in der Tabelle angezeigt werden sollen.

**Tabelle sortieren**

Durch Klicken auf einen Tabellenkopf können Sie die Tabelle nach den Werten dieser Spalte auf- oder absteigend sortieren.

**Einträge filtern**

In die Eingabefelder der Kopfzeilen kann ein Suchtext eingegeben werden, um den gesuchten Inhalt zu filtern.

## 2.5 Ports

SINEC PNI verwendet die folgenden Ports für die Kommunikation mit Geräten. Standardmäßig sind diese Ports in der Windows-Firewall für ausgehenden Datenverkehr nicht blockiert. Wenn während des Betriebs von SINEC PNI Probleme auftreten, überprüfen Sie die entsprechenden Ports in der Windows-Firewall-Konfiguration.

Dienst	Protokoll/ Portnr.	Vorein- gestellter Portstatus	Konfi- gurierbar	Authenti- fizierung	Verschlüsse- lung	Hinweis zum Verhalten, wenn Port blockiert
Secure Shell (SSH)	UDP/22	Offen	--	✓	✓	Konfiguration lesen und schreiben auf Geräten nicht möglich
SNMPv1/v2c	UDP/161	Offen	--	--	--	Konfiguration lesen und schreiben auf Geräten nicht möglich
SNMPv3	UDP/161	Offen	--	Optional	Optional	Konfiguration lesen und schreiben auf Geräten nicht möglich
HTTP	TCP/80	Offen	✓	✓ <sup>1)</sup>	--	Standard-Browser kann Webseiten des Geräts nicht anzeigen
HTTPS	TCP/443	Offen	✓	✓	✓	Standard-Browser kann Webseiten des Geräts nicht anzeigen
TFTP	UDP/69	Offen	✓	--	--	Folgendes ist nicht möglich: <ul style="list-style-type: none"> <li>• Aktualisierung der Firmware auf Geräten</li> <li>• Herunterladen von Dateien auf den PC</li> <li>• Hochladen von Dateien auf das Gerät</li> </ul>

<sup>1)</sup> Nur beim externen HTTP-Server






# Bedienung

## 3.1 Geräteliste

Auf der Seite "Geräteliste" können Sie das Netzwerk über die Schaltfläche "Netzwerk-Scan starten" nach Geräten durchsuchen. Dabei werden die Scan-Einstellungen verwendet, die auf der Seite "Einstellungen" konfiguriert sind, siehe Kapitel Einstellungen (Seite 31).

Die gefundenen Geräte können Sie über die "Geräteverwaltung" konfigurieren, LED- sowie ICMP-Erreichbarkeitstests (PING) durchführen und die Geräte auf PROFINET-Standard-einstellungen oder auf Werkseinstellungen zurücksetzen.

Über die Schaltfläche  können Sie in der Geräteliste Spalten ein- oder ausblenden und die Reihenfolge der Spalten ändern.

## Bedienung

Im Menü "Geräteverwaltung" gibt es folgende Menüeinträge:

- Geräte-Konfiguration ändern  
Ruft den Editor zur Konfiguration der ausgewählten Geräte auf, siehe Kapitel Gerätekonfiguration (Seite 23).
- Gerät zurücksetzen  
Ruft einen Dialog auf, in dem Sie eine der folgenden Optionen auswählen können:
  - Auf PROFINET-StandardEinstellungen zurücksetzen: Setzt die ausgewählten PROFINET-Geräte auf die jeweiligen StandardEinstellungen des PROFINET IO-Profiles zurück. Welche Einstellungen zurückgesetzt werden, hängt vom Funktionsumfang des jeweiligen Geräts ab. Diese Funktion ist nur für Geräte verfügbar, die den aktuellen PROFINET-Standard unterstützen.
  - Auf Werkseinstellungen zurücksetzen: Setzt die ausgewählten Geräte auf Werkseinstellungen zurück und entfernt diese aus der Geräteliste. Nach dem Zurücksetzen ist ein neuer Netzwerk-Scan notwendig.

---

### Hinweis

#### Verlust der IP-Adresse

Durch das Zurücksetzen auf die PROFINET- StandardEinstellungen oder auf die Werkseinstellungen des Geräts geht auch die IP-Adresse verloren. Das Gerät ist danach nur über eine ggf. vorhandene serielle Schnittstelle, SINEC PNI (via PN-DCP), DHCP oder über RCDP ansprechbar.

#### SCALANCE M800 & S -Geräte

Nach dem Zurücksetzen auf Werkseinstellungen verliert das Gerät seine projektierte IP-Adresse und ist wieder über die werkseitig eingestellte IP-Adresse 192.168.1.1 (außer M826, SC-600) zu erreichen. Führen Sie einen Netzwerk-Scan durch und passen Sie die IP-Adresse an. Nach dem Ändern müssen Sie erneut einen Netzwerk-Scan durchführen.

Bei M826, SC-600 geht auch die IP-Adresse verloren. Das Gerät ist danach nur über eine ggf. vorhandene serielle Schnittstelle, SINEC PNI (via PN-DCP) oder DHCP ansprechbar.

---

- WBM öffnen  
Ruft das WBM (Web Based Management) der ausgewählten Geräte im Webbrowser auf. Auf der Seite "Einstellungen" konfigurieren Sie das Protokoll und den Port, die für den Aufruf des WBMs verwendet werden.
- Auswahl exportieren  
Exportiert die ausgewählten Einträge der Geräteliste in eine CSV-Datei.

- Geräteverfügbarkeit
  - LED blinken

Führt einen LED-Blinktest (via PN-DCP oder via RCDP) auf den ausgewählten Geräten durch, wenn dies von den Geräten unterstützt wird.

Die LEDs der Geräte blinken so lange, bis Sie auf die Schaltfläche "Stopp" klicken.
  - Gerät anpingen

Führt eine ICMP-Erreichbarkeitsabfrage (PING) für die ausgewählten Geräte aus.
- Firmware aktualisieren

Ruft den Dialog auf, in dem Sie eine der folgenden Optionen auswählen können, siehe Kapitel Firmware aktualisieren (Seite 19).
- Gerät neu starten

Führt auf dem ausgewählten Gerät einen Neustart durch.
- Herunterladen und Hochladen

Über dieses Menü können Sie Dateien des Geräts herunter- oder hochladen, siehe Kapitel "Herunterladen und Hochladen (Seite 28)".

  - Für SCALANCE-Geräte sind die SNMP-Geräteanmeldedaten (Seite 34) erforderlich.
  - Für ROS und ROX2-Geräte sind die SSH-Geräteanmeldedaten (Seite 34) erforderlich.

## **Eigenschaften**

Für Geräte, die im Rahmen des Netzwerk-Scans gefunden wurden, werden Eigenschaften wie deren Gerätestatus und IP-Adresse in der Tabelle unterhalb der Schaltflächen angezeigt.

Folgende Gerätestatus sind möglich:

- OK
- Warnung

Das Gerät hat die IP-Adresse 0.0.0.0.
- Fehler

Es besteht ein IP-/MAC-Adress- oder Namenskonflikt mit einem anderen Gerät.

### **3.1.1 Firmware aktualisieren**

Über den Dialog können Sie Firmware-Versionen auf den Geräten aktualisieren. Um die Firmware auf das Gerät zu laden, sind korrekte Geräteanmeldedaten erforderlich.

Die Einstellungen sind abhängig von der gewählten Gerätefamilie.

Die gesamte Pfadlänge des Zielverzeichnis einschließlich des Unterordners und des Dateinamens (inklusive Dateiendung) kann maximal 255 Zeichen lang sein. Systembedingt unterstützen einige Geräte nur maximal 32 Zeichen.

**Einstellungen bei SCALANCE**

Legen Sie fest, ob Sie die Firmware-Datei von einem mitgelieferten oder externen TFTP-Server auf das Gerät übertragen.

- Einstellungen für den mitgelieferten TFTP-Server
  - NIC-IP-Adresse wählen  
Bei mehreren IP-Adressen wählen Sie die IP-Adresse des Netzwerkadapters (NIC) aus, über die die Übertragung abläuft.
  - Pfad zur Firmware-Datei  
Navigieren Sie in das Verzeichnis, in dem die Firmware-Datei \*.sfw / \*.lad abgelegt ist.
  - Portnummer  
Geben Sie die Portnummer an, die für die Übertragung genutzt wird.
- Einstellungen für den externen TFTP-Server
  - Externer Server-Pfad  
Geben Sie die URL an, z. B. :192.168.1.10\Ordner\SCALANCEX400.sfw
  - Portnummer  
Geben Sie die Portnummer an, die für die Übertragung genutzt wird.
- Firmware aktualisieren  
Klicken Sie auf die Schaltfläche, um die Firmware auf das Gerät zu laden. Ein Dialog mit Aufforderung zum Bestätigen wird geöffnet. Nach dem Bestätigen wird der Statusdialog aufgerufen. In diesem Dialog werden der Status der Übertragung, die IP-Adresse und die MAC-Adresse angezeigt.

**Einstellungen bei RUGGEDCOM (ROS)**

- Dateipfad  
Navigieren Sie in das Verzeichnis, in dem die Zielformatdatei abgelegt ist.
- Zielnamen  
Geben Sie den Namen der Zielformatdatei an.
  - main.bin – Das Firmware-Image der RUGGEDCOM ROS-Hauptanwendung
  - boot.bin – Bootloader-Firmware-Image
  - fpga.xsvf – Das binäre FPGA-Firmware-Image
- Firmware aktualisieren  
Wählen Sie die Datei aus, die auf das Gerät geladen wird und klicken Sie auf die Schaltfläche "Firmware aktualisieren". Um die ausgewählte Datei zu entfernen, klicken Sie auf die Schaltfläche "Auswahl entfernen".  
Wenn keine Dateien ausgewählt sind, werden alle übertragen.  
Ein Dialog mit Aufforderung zum Bestätigen wird geöffnet. Nach dem Bestätigen wird der Statusdialog aufgerufen. In diesem Dialog werden der Status der Übertragung, die IP-Adresse und die MAC-Adresse angezeigt.

### **Einstellungen bei RFID**

- Pfad zur Firmware-Datei

Navigieren Sie in das Verzeichnis, in dem die Firmware-Datei \*.sfw abgelegt ist.

- Firmware aktualisieren

Beachten Sie, dass Sie als "Benutzer" ein Firmware-Update nur durchführen können, wenn sich das Kommunikationsmodul im Zustand "Bereit" befindet.

Klicken Sie auf die Schaltfläche, um die Firmware auf das Gerät zu laden. Ein Dialog mit Aufforderung zum Bestätigen wird geöffnet. Nach dem Bestätigen wird der Statusdialog aufgerufen. In diesem Dialog wird der Status der Übertragung, die IP-Adresse und die MAC-Adresse angezeigt.

### **Einstellungen bei RUGGEDCOM (ROX)**

Legen Sie fest, ob Sie die Firmware-Datei von einem mitgelieferten oder externen HTTP-Server auf das Gerät übertragen.

Einstellungen für den mitgelieferten HTTP-Server

- NIC-IP-Adresse wählen

Bei mehreren IP-Adressen wählen Sie die IP-Adresse des Netzwerkkadapters (NIC) aus, über die die Übertragung abläuft.

- Pfad zur Firmware-Datei

Navigieren Sie in das Verzeichnis, in dem die Firmware-Datei \*.zip abgelegt ist.

Nachdem die zip-Datei ausgewählt wurde, wird versucht, die Ziel ROX-Version aus der Firmware-Datei zu ermitteln. Wenn dies nicht gelingt, müssen Sie die Ziel ROX-Version eingeben.

- Ziel ROX-Version

Das Format ist abhängig von der Firmware-Version, die aktuell auf dem Gerät verwendet wird.

- Firmware-Version < 2.14.0

Die Dateinamen haben die Form rrX.Y.Z.zip, wobei X für die Hauptversionsnummer, Y für die Zwischenversionsnummer und Z für die Patch-Nummer steht, z. B. rr2.14 .0.

Geben Sie die Version im Format 'rrX.Y.Z' an.

- Firmware-Version >= 2.14.0

Geben Sie Folgendes an: "image.tar.bz2".

- Portnummer

Geben Sie die Portnummer an, die für die Übertragung genutzt wird.

Einstellungen für den externen HTTP-Server

- Externer Server-Pfad

Die Einstellung ist abhängig von der Firmware-Version, die aktuell auf dem Gerät verwendet wird.

- Firmware-Version < 2.14.0

`http://(hostname)/(Verzeichnis, in dem die Zielformat abgelegt ist).`

- Firmware-Version > = 2.14.0

`http://(hostname)/(Verzeichnis, in dem die image.tar.bz2 abgelegt ist)`

- Ziel ROX-Version (nur bei ROX-Version < 2.1.4 notwendig)

Die Dateinamen haben die Form `rrX.Y.Z.zip`, wobei X für die Hauptversionsnummer, Y für die Zwischenversionsnummer und Z für die Patch-Nummer steht, z. B. `rr2.14 .0`.

Geben Sie die Version im Format '`rrX.Y.Z`' an oder geben Sie '`current`' ein, um auf die neueste auf dem Upgrade-Server verfügbare Firmware-Version zu aktualisieren.

Portnummer

Geben Sie die Portnummer an, die für die Übertragung genutzt wird.

Firmware aktualisieren

Klicken Sie auf die Schaltfläche, um die Firmware auf das Gerät zu laden. Ein Dialog mit Aufforderung zum Bestätigen wird geöffnet. Nach dem Bestätigen wird der Statusdialog aufgerufen. In diesem Dialog werden der Status der Übertragung, die IP-Adresse und die MAC-Adresse angezeigt.

### **3.1.2      Gerätekonfiguration**

Das Fenster "Gerätekonfiguration" öffnet sich, nachdem Sie ein oder mehrere Geräte aus der Geräteliste auswählen und danach im Menü "Geräteverwaltung" den Eintrag "Gerät konfigurieren" auswählen.

Nach dem Öffnen der "Gerätekonfiguration" versucht SINEC PNI die Daten vom Gerät auszulesen und zeigt dieses durch das "Spinner Icon" an.

Danach können Sie die Parameter in den im Folgenden beschriebenen Registern konfigurieren. Um die geänderten Parameter auf das Gerät zuladen, gibt es folgende Schaltflächen:

- Alles laden

Die Parameter aller Register werden auf das Gerät geladen.

- Laden

Nur die Parameter des aktuell geöffneten Registers werden auf das Gerät geladen.

Geänderte Parameter eines Registers bleiben nach dem Wechsel in ein anderes Register erhalten.

Für den Zugriff auf die Geräte verwendet SINEC PNI die ab Werk eingestellten HTTPS-/SSH- und SNMPv1/v2c-Anmeldedaten. Wenn die Authentifizierung an einem Gerät mit diesen Anmeldedaten nicht möglich ist, verwendet SINEC PNI die Anmeldedaten, die auf der Seite "Geräteanmeldedaten" konfiguriert sind, siehe Kapitel Geräteanmeldedaten (Seite 34).

Wenn SNMPv3 für das Lesen und Schreiben von Werten verwendet werden soll, müssen die dafür zu verwendenden Daten auf der Seite "Geräteanmeldedaten" angegeben werden.

## IP-Konfiguration

In diesem Register können folgende IP-Adressparameter für die ausgewählten Geräte konfiguriert werden:

- IP-Adresse

IPv4-Adresse des Geräts.

Wenn Sie in der Geräteliste mehrere Geräte ausgewählt haben, können Sie im Eingabefeld "Start-IP-Adresse" die erste IP-Adresse eines IP-Adressbereichs angeben, der den ausgewählten Geräten beim Laden zugeordnet wird.

Dabei erhält das zuerst ausgewählte Gerät die Start-IP-Adresse als IP-Adresse.

Der IP-Adressbereich reicht maximal bis zum Ende des vierten Oktetts der angegebenen IP-Adresse. Wenn die Option "DHCP" aktiviert ist, kann der Parameter nicht konfiguriert werden.

---

### Hinweis

#### Massenkonfiguration IP-Adresse

Nach der IP-Massenkonfiguration von Geräten mit gleicher IP-Adresse ändert sich die Reihenfolge der in der Geräteliste angezeigten IP-Adressen nach dem Scan-Vorgang. Bei RUGGEDCOM ROS-Geräte werden die IP-Adressen eventuell nicht in der Reihenfolge zugewiesen, in der die Geräte in der Geräteliste ausgewählt sind. Es hängt davon ab, welches Gerät zuerst antwortet.

---

- Subnetzmaske

Subnetzmaske des Geräts.

Wenn die Option "DHCP" aktiviert ist, kann der Parameter nicht konfiguriert werden.

- Router verwenden

Bei aktiviertem Optionskästchen verwendet das Gerät einen Router zur Adressierung von Teilnehmern eines anderen Subnetzes. Für den zu verwendenden Router kann eine IPv4-Adresse angegeben werden.

Wenn die Option "DHCP" aktiviert ist, kann der Parameter nicht konfiguriert werden.



- DHCP

Wenn diese Option aktiviert ist, erfolgt die IP-Adresskonfiguration des Geräts durch einen DHCP-Server. Der DHCP-Modus legt fest, anhand welchen Parameters die IP-Adresse für das Gerät beim DHCP-Server reserviert wird.

- MAC-Adresse

Die Reservierung der IP-Adresse beim DHCP-Server erfolgt anhand der MAC-Adresse des Geräts.

- Client-ID

Die Reservierung der IP-Adresse beim DHCP-Server erfolgt anhand der angegebenen Client-ID des Geräts. Wenn Sie in der Geräteliste mehrere Geräte ausgewählt haben, können Sie zusätzlich zur Client-ID eine Zahl im Feld Zähler angeben, die als Suffix der Client-ID verwendet wird und beim Laden dem ersten Gerät zugewiesen wird. Für jedes weitere Gerät wird der Zähler um 1 hochgezählt.

- Gerätename

Die Reservierung der IP-Adresse beim DHCP-Server erfolgt anhand des Gerätenamens.

Wenn diese Option zusammen mit anderen Daten auf dem Gerät eingestellt wird, kann das Setzen dieser Daten fehlschlagen, wenn das Gerät nicht rechtzeitig eine IP-Adresse vom DHCP-Server erhält.

Nach der Vergabe über DHCP ist ein neuer Netzwerk-Scan notwendig, um die aktuell durch den DHCP-Server verteilten Adressen für das Gerät anzuzeigen.

## System

In diesem Register können folgende Systemparameter für die ausgewählten Geräte konfiguriert werden:

- Systemname

Beschreibung des Geräts. Wenn Sie in der Geräteliste mehrere Geräte ausgewählt haben, können Sie aus der Klappliste einen der folgenden Werte auswählen:

- Sequenz: Geben Sie eine Zahl an, die als Suffix des Systemnamens verwendet wird und beim Laden dem ersten Gerät zugewiesen wird. Für jedes weitere Gerät wird der Zähler um 1 hochgezählt.
  - Letztes Oktett von IP-Adresse: Die Zahl des letzten IP-Oketts, die die IP-Adresse des jeweiligen Geräts hat, wird als Suffix des Systemnamens verwendet.

- Gerätestandort

Ortsangabe für das Gerät, z. B. eine Raumnummer.

- Kontaktperson

Name einer Kontaktperson, die für die Verwaltung des Geräts zuständig ist.

## PROFINET

In diesem Register können folgende PROFINET-Parameter für die ausgewählten Geräte konfiguriert werden:

- PROFINET-Gerätename

PROFINET-Gerätename, der für das Gerät angegeben werden kann. Wenn Sie in der Geräteliste mehrere Geräte ausgewählt haben, können Sie aus der Klappliste einen der folgenden Werte auswählen:

- Sequenz: Geben Sie eine Zahl an, die als Suffix des PROFINET-Gerätenamens verwendet wird und beim Laden dem ersten Gerät zugewiesen wird. Für jedes weitere Gerät wird der Zähler um 1 hochgezählt.
- Letztes Oktett von IP-Adresse: Die Zahl des letzten IP-Oktetts, die die IP-Adresse des jeweiligen Geräts hat, wird als Suffix des PROFINET-Gerätenamens verwendet.

- Konvertierter Name

PROFINET-Gerätename, der von SINEC PNI aus dem angegebenen Namen erzeugt wird, wenn er nicht den Regeln von IEC 61158-6-10 entspricht. In diesem Fall wird der konvertierte Gerätename auf das Gerät geladen.

- Anlagenkennzeichen

Eindeutige Kennzeichnung des Geräts innerhalb der Anlage.

- Ortskennzeichen

Eindeutige Kennzeichnung des Geräteorts.

- Einbaudatum

Datum, an welchem das Gerät eingebaut wurde.

- Zusatzinformation

Eingabe von Zusatzinformationen.

## Geräteanmeldedaten

In diesem Register kann das Passwort eines bestehenden Benutzers geändert werden.

- Benutzername

Benutzername, dessen Passwort geändert werden soll.

- Aktuelles Passwort

Passwort, das aktuell vom Benutzer zur Anmeldung am Gerät verwendet wird. Über die Schaltfläche neben dem Eingabefeld kann die Anzeige des Passworts im Klartext aktiviert und deaktiviert werden.

- Neues Passwort

Neues Passwort, das vom Benutzer zur Anmeldung am Gerät verwendet werden soll. Über die Schaltfläche neben dem Eingabefeld kann die Anzeige des Passworts im Klartext aktiviert und deaktiviert werden.

- Passwort bestätigen

Bestätigung des angegebenen Passworts. Beide Passwort-Eingaben müssen übereinstimmen, ansonsten wird eine Meldung angezeigt. Über die Schaltfläche neben dem Eingabefeld kann die Anzeige des Passworts im Klartext aktiviert und deaktiviert werden.

---

### **Hinweis**

#### **Geräteanmeldedaten**

Die Geräte übernehmen die Anmeldedaten, die auf der Seite "Geräteanmeldedaten" konfiguriert sind. Wenn die Authentifizierung an einem Gerät mit diesen Anmeldedaten nicht möglich ist, können Sie hier die Anmeldedaten anpassen.

---

## **PROFIBUS**

In diesem Register können Sie PROFIBUS-Parameter für IE/PB-Link-Geräte konfigurieren.

## **RTLS**

In diesem Register können Sie die IP-Adresse des Locating Manager-Servers konfigurieren.

### 3.1.3 Herunterladen und Hochladen

Nachdem Sie ein oder mehrere Geräte aus der Geräteliste ausgewählt haben und dann im Menü "Geräteverwaltung" den Eintrag "Herunterladen und Hochladen" auswählen, können Sie Dateien hoch- und herunterladen.

Die gesamte Pfadlänge des Zielverzeichnisses einschließlich des Unterordners und des Dateinamens (inklusive Dateiendung) kann maximal 255 Zeichen lang sein. Systembedingt unterstützen einige Geräte nur maximal 32 Zeichen. Bei sehr langen Ordnernamen oder tief verschachtelten Ordnerstrukturen können Dateien nicht mehr umbenannt, bearbeitet oder verschoben werden.

#### Auf den PC herunterladen

Wenn Sie auf "Auf den PC herunterladen" klicken, wird der Dialog "Herunterladen" mit den folgenden Optionen aufgerufen:

- Gerätefamilie

Abhängig davon ist der Umfang der Dateiliste.

- Externer oder interner TFTP-Server (nur bei SCALANCE verfügbar)

Legen Sie fest, ob Sie die Dateien auf einen mitgelieferten oder externen TFTP-Server übertragen.

Einstellungen für den mitgelieferten TFTP-Server

- NIC-IP-Adresse wählen

Bei mehreren IP-Adressen wählen Sie die IP-Adresse des Netzwerkadapters (NIC) aus, über die die Übertragung abläuft.

- Portnummer

Geben Sie die Portnummer an, die für die Übertragung genutzt wird.

- Zielverzeichnis

Geben Sie das Zielverzeichnis an, indem die Datei gespeichert wird.

Einstellungen für den externen TFTP-Server

- Externer Server-Pfad

Geben Sie das Verzeichnis an, in dem die Dateien abgelegt werden. Die Angabe ist wie folgt: IP-Adresse\

- Portnummer

Geben Sie die Portnummer an, die für die Übertragung genutzt wird.

- Ordner/Dateiname

Der Dateiname wird um die gewählte Option erweitert, getrennt durch einen Unterstrich (\_). Der Dateiname ist dann wie folgt aufgebaut:

<Option>\_<Datei> z. B. 192.168.16.1\_config.conf

Beim mitgelieferten TFTP-Server gibt es die Einstellung "Unterordner erstellen". Wenn die Einstellung aktiviert ist, wird die gewählte Option als Namen für den Unterordner verwendet und der Dateiname nicht erweitert.

Kann die Option nicht abgerufen werden, wird als Name "Unknown" verwendet.

Wenn sich im Zielordner bereits eine Datei mit dem gleichen Namen befindet, wird der Dateiname erweitert um den Zusatz "(1)". Das gilt auch für den Namen des Unterordners.

Beim externen TFTP-Server ist das abhängig von den Einstellungen des TFTP-Servers. Wenn die Einstellung nicht unterstützt wird, wird die vorhandene Datei überschrieben und der Dateiname gekürzt, wenn der generierte Dateiname die Zeichengrenze überschreitet.

Der Name des Unterordners und der Dateiname sind abhängig von den folgenden Optionen:

- IP-Adresse
- MAC-Adresse
- Systemname
- PROFINET-Gerätename (nur bei SCALANCE verfügbar)

Wenn bei mehreren ausgewählten Geräten die PROFINET-Gerätenamen leer sind oder die Systemnamen gleich sind, dann wird die Datei überschrieben.

- Datum und Uhrzeit ergänzen

Das Datum und die Uhrzeit werden dem Dateinamen angehängt, getrennt durch einen Unterstrich (\_).

- Dateiliste

Der Umfang ist abhängig von der gewählten Gerätefamilie.

- Schaltfläche "Schließen"

Schließt den Dialog.

- Schaltfläche "Herunterladen"

Klicken Sie auf die Schaltfläche, um die gewünschte Datei herunterzuladen. Der Statusdialog wird geöffnet. In diesem Dialog werden der Status der Übertragung, die IP-Adresse und die MAC-Adresse angezeigt.

Nach Abschluss aller Downloads können Sie entweder den Dialog schließen oder Sie springen über die Schaltfläche "Ordner öffnen" direkt in das Zielverzeichnis.

## Auf das Gerät hochladen

Über den Dialog können Sie z. B. eine zuvor gesicherte Konfiguration wiederherstellen. Das Gerät übernimmt die Konfiguration der ausgewählten Datei und arbeitet mit diesen Einstellungen weiter. Dabei gehen alle bis dahin vorgenommenen und nicht in einer Datei gespeicherten Einstellungen verloren.

### Einstellung bei SCALANCE

- Externer oder interner TFTP-Server

Legen Sie fest, ob Sie die Dateien auf einen mitgelieferten oder externen TFTP-Server übertragen.

Einstellungen für den mitgelieferten TFTP-Server

- NIC-IP-Adresse wählen

Bei mehreren IP-Adressen wählen Sie die IP-Adresse des Netzwerkkadapters (NIC) aus, über die die Übertragung abläuft.

- Pfad der Konfig-Datei

Navigieren Sie in das Verzeichnis, in dem die Konfigurations-Datei abgelegt ist.

- Portnummer

Geben Sie die Portnummer an, die für die Übertragung genutzt wird.

Einstellungen für den externen TFTP-Server

- Dateipfad

Geben Sie das Verzeichnis an, in dem die Datei abgelegt ist.

Die Angabe ist wie folgt: IP-Adresse\Verzeichnis\Datei z. B.  
192.168.16.1\ordner\config\_Scalance\_700.conf

- Portnummer

Geben Sie die Portnummer an, die für die Übertragung genutzt wird.

- Schaltfläche "Schließen"

Schließt den Dialog.

- Schaltfläche "Hochladen"

Klicken Sie auf die Schaltfläche, um die Konfigurationsdatei auf das Gerät zu laden. Der Statusdialog wird geöffnet. In diesem Dialog werden der Status der Übertragung, die IP-Adresse und die MAC-Adresse angezeigt.

Die Geräte, bei denen die "Wiederherstellung" erfolgreich war, aber nicht neu gestartet wurden sieht der Benutzer im Statusdialog die Meldung "Neustart ausstehend".

### Einstellungen bei RUGGEDCOM (ROS)

- Pfad der Konfig-Datei

Geben Sie das Verzeichnis an, in dem die Datei abgelegt ist.

- Pfad der Banner-Datei

Wählen Sie die bannert.txt aus, die hochgeladen werden soll.

- Schaltfläche "Schließen"

Schließt den Dialog.

- Schaltfläche "Hochladen"

Klicken Sie auf die Schaltfläche, um die Konfigurationsdatei auf das Gerät zu laden. Der Statusdialog wird geöffnet. In diesem Dialog werden der Status der Übertragung, die IP-Adresse und die MAC-Adresse angezeigt.

## Statusdialog

Folgende Status sind möglich:

- In Bearbeitung
- Fertig  
Die Datei wurde erfolgreich heruntergeladen.
- Verbindung verloren
- Nicht unterstützt  
Das ausgewählte Gerät wird nicht unterstützt.
- Ungültige-Anmeldedaten (Nur bei RUGGEDCOM ROS / ROX)
- Anmeldefehler
- Neustart ausstehend

Gerät muss neu gestartet werden. Wenn kein Neustart durchgeführt und Sie führen eine andere Aktion durch, wird der Status überschrieben.

## 3.2 Einstellungen

Nach dem ersten Start von SINEC PNI wird die Seite "Einstellungen" angezeigt. Auf dieser Seite legen Sie die Einstellungen fest, die für den Netzwerk-Scan verwendet werden. Stellen Sie vor der Konfiguration dieser Einstellungen sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der zu verwendende Netzwerkadapter ist aktiv.
- Dem zu verwendenden Netzwerkadapter ist eine IP-Adresse zugewiesen.
- Die für SINEC PNI erforderliche Software ist installiert, siehe Kapitel Systemvoraussetzungen (Seite 9).

Folgende Parameter sind verfügbar:

### Netzwerkadapter

Netzwerkadapter, der für den Netzwerk-Scan verwendet wird.

---

### Hinweis

#### Netzwerkadapterkonfiguration nicht zur Laufzeit von SINEC PNI ändern

Der verwendete Netzwerkadapter darf zur Laufzeit von SINEC PNI nicht im verwendeten Betriebssystem deaktiviert oder in seiner Konfiguration geändert werden.

#### Neustart von SINEC PNI

Auf dieser Seite konfigurierte Werte werden nach jedem Neustart von SINEC PNI zurückgesetzt. Davon ausgenommen die Einstellung des Netzwerkadapters.

#### Mehrere Netzwerkadapter

Die ICMP-Erreichbarkeitsabfrage (PING) geht über alle Netzwerkadapter.

---

**Discovery**

Konfigurierbare Geräte im Netzwerk auffinden.

- PROFINET-Geräte (DCP)

Protokoll DCP (Discovery Configuration Protocol) zur Erkennung von PROFINET-Geräten.

- Zusätzliche Informationen auslesen (nicht für S7-1200 V2.2 CPUs empfohlen)

Wenn Sie dieses Optionskästchen aktivieren, werden zusätzlich I&M-Daten (z.B. Artikelnummer, Firmwareversion und Seriennummer) von erkannten Geräten ausgelesen. Die Erkennung von I&M-Daten kann beim Netzwerk-Scan einige Zeit in Anspruch nehmen. Zudem können bei aktiviertem Optionskästchen I&M-Daten (z.B. Anlagenkennzeichen und Ortskennzeichen) im Dialog zur Gerätekonfiguration bearbeitet werden.

- RUGGEDCOM ROS-Geräte (RCDP)

Protokoll RCDP (RUGGEDCOM Discovery Protocol) zur Erkennung von RUGGEDCOM ROS-Geräten.

- RTLS

Zur Erkennung von RTLS-Geräten.

- Ping

Protokoll ICMP echo zur Erreichbarkeitsabfrage von Geräten in dem unten konfigurierten IP-Adressbereich.

Zusätzlich sind die Parameter Timeout und Wiederholversuche konfigurierbar.

Ohne Geräteauswahl können Sie nur das WBM auf dem Gerät öffnen, aber nicht das Gerät konfigurieren. Verwenden Sie das Protokoll nur, wenn die Geräte über keines der anderen Protokolle erreichbar sind.

Mit Geräteauswahl können Sie zusätzlich das Gerät konfigurieren. Folgende Geräte sind auswählbar:

- SCALANCE-Geräte

Protokoll ICMP echo zur Erkennung von SCALANCE-Geräten.

- RUGGEDCOM ROS-Geräte

Protokoll ROS ICMP zur Erkennung von RUGGEDCOM ROS-Geräten.

- RUGGEDCOM ROX2 & WIN-Geräte

Protokolle ICMP echo und SSH zur Erkennung von RUGGEDCOM ROX2- und WIN-Geräten.

- Timeout

Angabe der Zeitdauer in Sekunden, nach welcher eine ICMP-Erreichbarkeitsabfrage (PING) als fehlgeschlagen eingestuft wird.

- Wiederholversuche

Anzahl der Wiederholversuche für ICMP-Erreichbarkeitsabfragen (PING), nachdem ein Gerät nicht auf die erste ICMP-Abfrage geantwortet hat.



- IP-Adressbereiche  
IP-Adressbereiche, in denen nach Geräten gesucht wird. Die Angabe der IP-Adressbereiche ist anhand folgender Notationen möglich.

192.168.11.12 - 192.168.11.120

172.16.2.2

192.168.3.0/24

192.168.6.34 - \*

Mehrere Einträge werden durch ein Komma (,) oder einen Strichpunkt (;) voneinander getrennt. Die Dauer des Netzwerk-Scans ist von der Anzahl der zu erkennenden Geräte abhängig.

- IP-Adressbereiche importieren

Importiert die IP-Adressbereiche, die in einer csv- oder txt-Datei definiert sind.

Mehrere Einträge werden durch ein Komma (,) oder einen Strichpunkt (;) voneinander getrennt. Die Dauer des Netzwerk-Scans ist von der Anzahl der zu erkennenden Geräte abhängig.

Beispiel: 192.168.16.50,192.168.16.52;192.168.1.1 - 192.168.1.20

- WBM öffnen

Protokoll und Port, die für den Aufruf des WBMs von Geräten im Webbrowser verwendet werden.

Nach der Konfiguration der oben genannten Einstellungen können Sie auf der Seite "Geräteliste" Netzwerk-Scans durchführen, siehe Kapitel Geräteliste (Seite 17).

## 3.3 Geräteanmeldedaten

---

### Hinweis

#### Neustart von SINEC PNI

Auf dieser Seite konfigurierte Werte werden nach jedem Neustart von SINEC PNI zurückgesetzt.

---

Für den Zugriff auf die Geräte verwendet SINEC PNI die ab Werk eingestellten HTTPS-/SSH- und SNMPv1/v2c-Anmeldedaten. Wenn die Authentifizierung an einem Gerät mit diesen Anmeldedaten nicht möglich ist, verwendet SINEC PNI die Anmeldedaten, die auf der Seite "Geräteanmeldedaten" konfiguriert sind. Wenn SNMPv3 für das Lesen und Schreiben von Werten verwendet werden soll, müssen die dafür zu verwendenden Daten auf dieser Seite angegeben werden.

- Benutzername

Benutzername, mit dem sich SINEC PNI am Gerät anmeldet. Der Benutzername wird für das Erstellen neuer Benutzer auf Geräten benötigt.

Standardmäßig verwendeter Wert: admin

- Passwort

Passwort, mit dem sich SINEC PNI am Gerät anmeldet. Das Passwort wird für das Erstellen neuer Benutzer auf Geräten benötigt.

Standardmäßig verwendeter Wert: admin

- SNMP-Version

Auswahl der SNMP-Version, deren Anmeldedaten Sie angeben wollen.

- SNMPv1/v2c Community String Lesen

Passwort, das SINEC PNI für den lesenden SNMPv1/v2c-Zugriff auf Geräte verwendet.

Standardmäßig verwendeter Wert: public

- SNMPv1/v2c Community String Lesen/Schreiben

Passwort, das SINEC PNI für den lesenden und schreibenden SNMPv1/v2c-Zugriff auf Geräte verwendet.

Standardmäßig verwendeter Wert: private

- SNMPv3 Benutzername

Benutzername, den SINEC PNI für den lesenden und schreibenden SNMPv3-Zugriff auf Geräte verwendet.

- SNMPv3 Authentifizierung

Auswahl des Hash-Algorithmus und Passwort zur Authentifizierung des verwendeten SNMPv3-Benutzers.

- SNMPv3 Verschlüsselung

Auswahl des Verschlüsselungsalgorithmus und Passwort zur Verschlüsselung der SNMPv3-Kommunikation.

# Troubleshooting

## Das Setzen von Parametern schlägt fehl

Wenn die IP-Adresse zusammen mit anderen Parametern auf dem Gerät konfiguriert wird, kann das Setzen dieser Parameter fehlschlagen, wenn das Gerät nicht rechtzeitig mit der neuen IP-Adresse erreichbar ist. Konfigurieren Sie die Parameter in diesem Fall separat von der IP-Adresse.

Wenn der Systemnamen zusammen mit dem PROFINET-Gerätenamen auf dem Gerät konfiguriert wird, kann das Setzen dieser Parameter fehlschlagen, wenn das Gerät nicht rechtzeitig erreichbar ist. Konfigurieren Sie den Systemnamen in diesem Fall separat von dem PROFINET-Gerätenamen.

## SINEC PNI kann nicht mehr gestartet werden

Wenn während der Ausführung von SINEC PNI Fehlermeldungen wie "Die Aktion kann nicht ausgeführt werden.", "Starten Sie die Anwendung neu." oder "Es ist ein unerwarteter Fehler aufgetreten." erscheinen, dann sind Systemdateien von SINEC PNI möglicherweise korumpiert. Starten Sie SINEC PNI in diesem Fall neu. Wenn SINEC PNI danach noch immer nicht gestartet werden kann, dann laden Sie SINEC PNI von der zugehörigen Siemens-Webseite erneut herunter und verwenden Sie ab sofort diese SINEC PNI Version.

## RUGGEDCOM ROX2: Gleiche/kleinere Firmware-Version

Wenn beim Aktualisieren der Firmware die Fehlermeldung "In der Zielversion wurden keine Unterschiede festgestellt. Nichts zu aktualisieren." erscheint, kann das auch bedeuten, dass das Gerät keine Verbindung zum Server herstellen kann. Ein Downgrade der Firmware für RUGGEDCOM ROX2-Geräte wird nicht unterstützt. Ab der Firmware-Version  $\geq 2.14.0$  wird stattdessen die Fehlermeldung "Datei nicht erfolgreich übertragen" angezeigt.

## RUGGEDCOM ROS: Massenkongfiguration IP-Adresse

Bei der IP-Massenkonfiguration von Geräten mit gleicher IP-Adresse ändert sich die Reihenfolge der in der Geräteliste angezeigten IP-Adressen nach dem Scan-Vorgang. Bei RUGGEDCOM ROS-Geräte werden die IP-Adressen eventuell nicht in der Reihenfolge zugewiesen, in der die Geräte in der Geräteliste ausgewählt sind. Es hängt davon ab, welches Gerät zuerst antwortet.

## RUGGEDCOM ROS: Nach Import der banner.txt schlägt ssh fehl

Die Größenbereich der Bannerdatei:  $< 4 \text{ kBytes} \leq 8 \text{ kBytes}$ .

Nachdem Hochladen einer Datei aus diesem Größenbereich sind Zugriffe über SSH nicht mehr möglich. Laden Sie über Telnet eine leere Version der banner.txt Datei in das Gerät, um die vorhandene Datei zu ersetzen.

## Schutz vor Brute-Force-Angriffen auf Geräten

Wenn die in SINEC PNI hinterlegten Geräteanmeldedaten z. B für SNMP oder HTTPS/SSH nicht zum Gerät passen und SINEC PNI versucht damit auf das Gerät zu zugreifen, wird nach mehreren fehlgeschlagenen Anmeldungen das betreffende Benutzerkonto oder die IP-Adresse vom PNI-Host für einen bestimmten Zeitraum gesperrt. Nach Ablauf kann wieder auf das Gerät zugegriffen werden.

In der Regel ist die Zahl der fehlgeschlagenen Anmeldeversuche, nach denen das Benutzerkonto gesperrt wird, über HTTPS/SSH auf 10 und bei SNMP auf 3 voreingestellt.

## 4.1 Aktualisieren der Firmware fehlgeschlagen

Wenn das Aktualisieren der Firmware fehlschlägt, kann das verschiedene Ursachen haben.

### Firmware-Datei

- Die Firmware-Datei ist nicht gültig.
- Die konfigurierte Ordnerstruktur ist falsch oder ungültig.  
Prüfen Sie nach, ob der Ordner existiert. Passen Sie die Konfiguration entsprechend an.
- In dem Ordner liegt keine Firmware-Datei  
Kopieren Sie in den Ordner die entsprechende Firmware-Datei.

### Gerät

Gerät ist nicht erreichbar.

- Die IP-Adresse hat sich geändert.  
Prüfen Sie mit der der PING-Funktion, ob das Gerät erreichbar ist.  
Führen Sie einen Netzwerk-Scan durch.
- Kabelbruch, Netzkabel gezogen  
Prüfen Sie die Kabelverbindung
- Netzwerkprobleme  
Das Gerät ist erreichbar, aber die Firmware konnte aufgrund geringer Bandbreite nicht vollständig übertragen werden.  
Versuchen Sie es später nochmal. Wenn das Problem weiterhin besteht, wenden Sie sich an den Netzwerkadministrator.
- Netconf-Sperre  
Im Gerät ist die Netconf-Sperre aktiviert.

### **SNMP**

Zugriff über SNMP ist nicht möglich:

- Die hinterlegten Geräteanmeldedaten für SNMP passen nicht zum Gerät.  
Passen Sie Geräteanmeldedaten an.
- Auf dem Gerät ist SNMP deaktiviert oder schreibgeschützt.  
Prüfen Sie auf dem Gerät die SNMP-Konfiguration.
- Auf dem Gerät wird der Zugriff über SNMP durch eine Firewall verhindert.  
Konfigurieren Sie auf dem Gerät eine entsprechende Firewall-Regel.

### **TFTP/HTTP-Server**

Kommunikation zwischen Gerät und TFTP/HTTP-Server ist nicht möglich:

- Der in SINEC PNI konfigurierte Port und der Port des externen TFTP/HTTP-Servers sind unterschiedlich.
- Auf dem PC ist keine Firewall-Regel für den TFTP/HTTP-Port konfiguriert.  
Konfigurieren Sie auf dem PC eine entsprechende Firewallregel.
- Der externe TFTP/HTTP-Server ist nicht gestartet.
- Die Adresse des TFTP/HTTP-Servers ist nicht korrekt.
- Auf dem Gerät wird der Zugriff über TFTP/HTTP durch eine Firewall verhindert.  
Konfigurieren Sie auf dem Gerät eine entsprechende Firewall-Regel.

### **SSH**

Der Zugriff über SSH ist nicht möglich:

- Die hinterlegten Geräteanmeldedaten für SSH passen nicht zum Gerät.  
Passen Sie Geräteanmeldedaten an.
- SINEC PNI unterstützt keine TLS-Version < 1.2  
Prüfen Sie die auf dem Gerät verwendete TLS-Version.
- Auf dem Gerät wird der Zugriff über SSH durch eine Firewall verhindert.  
Konfigurieren Sie auf dem Gerät eine entsprechende Firewall-Regel.



# Index

## G

Glossar, 6

## S

Service & Support, 8  
SIMATIC NET-Glossar, 6

## T

Training, 8