SIEMENS

Vorwort

SCALANCE S615 mit dem WAN verbinden 1

SIMATIC NET

Industrial Ethernet Security SCALANCE S615

Getting Started

01/2019

C79000-G8900-C390-04

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:

⚠WARNUNG
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.

Siemens AG
Global Services Information Technology
80200 MÜNCHEN
DEUTSCHLAND

Dokument-Bestellnummer: C79000-G8900-C390
℗ 01/2019 Änderungen vorbehalten

Copyright © Siemens AG 2015 - 2019.
Alle Rechte vorbehalten

Vorwort

Zweck

Anhand von Beispielen wird die Projektierung des SCALANCE S615 gezeigt.

IP-Einstellungen der Beispiele

Hinweis

Die in den Beispielen verwendeten IP-Einstellungen sind frei gewählt.

Im realen Netzverbund müssen Sie diese IP-Einstellungen der Netzwerkumgebung anpassen, um eventuelle Adresskonflikte zu vermeiden.

Allgemeine Benennung

Die Bezeichnung . . .	steht für . . .
SCT	Security Configuration Tool
PST	Primary Setup Tool
Gerät	M87x M81x M826 S615
M87x	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4
M81x	SCALANCE M812-1 SCALANCE M816-1
M826	SCALANCE M826-2
M804PB	SCALANCE M804PB
S615	SCALANCE S615
M-800	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4 SCALANCE M812-1 SCALANCE M816-1 SCALANCE M826-2 SCALANCE M804PB
SINEMA RC	SINEMA Remote Connect

Weiterführende Dokumentation

- Betriebsanleitung

  Diese Dokumente enthalten Informationen zu Montage, Anschließen und Zulassungen der Geräte. Die Konfiguration sowie die Einbindung der Geräte in ein Netzwerk ist nicht Gegenstand dieser Anleitung

  – SCALANCE M874, M876

    Beitrags-ID: 74518712
    (https://support.industry.siemens.com/cs/ww/de/view/109475909)

  – SCALANCE M812, M816

    Beitrags-ID: 90316607
    (https://support.industry.siemens.com/cs/ww/de/view/90316607)

  – SCALANCE M804PB:

    Beitrags-ID: 109759601
    (https://support.industry.siemens.com/cs/ww/de/view/109759601)

  – SCALANCE M826:

    Beitrags-ID: 99450800
    (https://support.industry.siemens.com/cs/ww/de/view/99450800)

  – SCALANCE S615:

    Beitrags-ID: 109475909
    (https://support.industry.siemens.com/cs/ww/de/view/109475909)

- Projektierungshandbuch Web Based Management

  Dieses Dokument soll Sie in die Lage versetzen, Geräte über das Web Based Management in Betrieb zu nehmen und zu projektieren.

  – SCALANCE M-800:

    Beitrags-ID: 109751635
    (https://support.industry.siemens.com/cs/ww/de/view/109751635)

  – SCALANCE S615:

    Beitrags-ID: 109751632
    (https://support.industry.siemens.com/cs/ww/de/view/109751632)

- Projektierungshandbuch Command Line Interface

  Dieses Dokument enthält die CLI-Befehle, die von den Geräten unterstützt werden.

  – SCALANCE M-800

    Beitrags-ID: 109751634
    (https://support.industry.siemens.com/cs/ww/de/view/109751634)

  – SCALANCE S615

    Beitrags-ID: 109751633
    (https://support.industry.siemens.com/cs/ww/de/view/109751633)

- Industrial Ethernet Security – Grundlagen und Anwendung

  Dieses Dokument enthält Informationen zum Arbeiten mit dem SCT (Security Configuration Tool).

  Beitrags-ID: 56577508 (https://support.industry.siemens.com/cs/ww/de/view/56577508)

- SIMATIC NET Industrial Ethernet Netzhandbuch

  Dieses Dokument enthält Informationen zu weiteren SIMATIC NET-Produkten, die Sie gemeinsam mit den Geräten dieser Produktlinie in einem Industrial Ethernet Netzwerk betreiben können

  Beitrags-ID: 27069465 (https://support.industry.siemens.com/cs/ww/de/view/27069465)

SIMATIC NET-Handbücher

Die SIMATIC NET-Handbücher finden Sie auf den Internetseiten des Siemens Industry Online Support:

- über die Suchfunktion:

  Link zum Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/de/ps)

  Geben Sie die Beitrags-ID des jeweiligen Handbuchs oder die Artikelnummer des Geräts als Suchbegriff ein.

- über die Navigation auf der linken Seite im Bereich "Industrielle Kommunikation":

  Link zum Bereich "Industrielle Kommunikation" (https://support.industry.siemens.com/cs/ww/de/ps/15247/man)

  Navigieren Sie zu der gewünschten Produktgruppe und nehmen Sie folgende Einstellungen vor:
  Register "Beitragsliste", Beitragstyp "Handbuch"

Training, Service & Support

Informationen zu Training, Service & Support finden Sie in dem mehrsprachigen Dokument "DC_support_99.pdf", welches sich auf dem mitgelieferten Datenträger mit Dokumentation befindet.

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 unter folgender Adresse:

50305045 (https://support.industry.siemens.com/cs/ww/de/view/50305045)

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.

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.

Firmware

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

Marken

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

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

Inhaltsverzeichnis

Vorwort 3

1 SCALANCE S615 mit dem WAN verbinden 9

1.1 Prinzipielles Vorgehen 9

1.2 SCALANCE S615 und Netzwerk einrichten 11

1.3 Das Web Based Management starten 12

1.4 Am Web Based Management anmelden 15

1.5 IP-Einstellungen des S615 ändern 17

1.6 Geräteinformationen festlegen 19

1.7 Uhrzeit einstellen 20

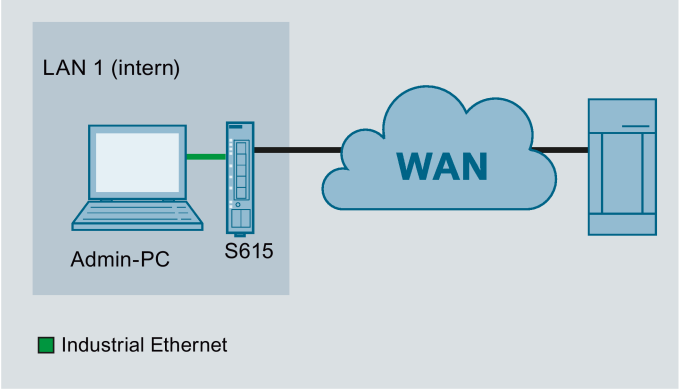
1.8 IP-Subnetz anlegen 23

SCALANCE S615 mit dem WAN verbinden 1

1.1 Prinzipielles Vorgehen

In diesem Beispiel wird dem SCALANCE S615, das sich im Zustand der Werkseinstellungen befindet, eine IP-Adresse zugewiesen. Im Anschluss wird das Gerät über das Web Based Management (WBM) konfiguriert. Der Zugriff auf das WAN über die Ethernet-Schnittstelle P5 des S615 angeschlossen wird.

Aufbau



Erforderliche Geräte/Komponenten

- 1x S615 (zusätzlich optional: eine entsprechend montierte Profilschiene mit Montagematerial)
- 1x 24V-Stromversorgung mit Kabelverbindung und Klemmblockstecker
- 1x PC zum Konfigurieren des S615
- die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet

Verwendete Einstellungen

Die Geräte erhalten für die Beispielkonfiguration die folgenden IP-Adresseinstellungen:

		Interface	IP-Adresse
LAN1	S615	LAN-Port P1 (vlan1)	192.168.100.1 255.255.255.0
		WAN-Port P5 (vlan2)	192.168.50.1 255.255.255.0
	PC1	LAN-Port	192.168.100.20 255.255.255.0 Gateway: IP-Adresse vlan1

Hinweis

Die im Beispiel verwendeten IP-Einstellungen sind frei gewählt.

Im realen Netzverbund müssen Sie diese IP-Einstellungen der Netzwerkumgebung anpassen, um eventuelle Adresskonflikte zu vermeiden.

Projektierungsschritte

1. SCALANCE S615 und Netzwerk einrichten (Seite 11)
2. Das Web Based Management starten (Seite 12)
3. Am Web Based Management anmelden (Seite 15)
4. IP-Einstellungen des SCALANCE S615 ändern (Seite 17)
5. SCALANCE S615 konfigurieren
   - Geräteinformationen festlegen (Seite 19)
   - Uhrzeit einstellen (Seite 20)
   - IP-Subnetz anlegen (Seite 23)

1.2 SCALANCE S615 und Netzwerk einrichten

Hinweis

Machen Sie sich mit den Sicherheitshinweisen vertraut, bevor Sie das Gerät in Betrieb nehmen. Die Sicherheitshinweise finden Sie in der Betriebsanleitung.

Vorgehensweise

1. Packen Sie zunächst das S615 aus und überprüfen Sie den unbeschädigten Zustand.
2. Montieren Sie die Spannungsversorgung.

> ⚠ **WARNUNG**
>
> **Nur Sicherheitskleinspannung verwenden**
>
> Das Gerät SCALANCE S615 ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden.
>
> Das Netzteil für die Versorgung des SCALANCE S615 muss NEC Class 2 gemäß National Electrical Code (r) (ANSI / NFPA 70) entsprechen.

3. Verdrahten Sie die S615, siehe Aufbau (Seite 9).
4. Schließen Sie das Gerät über die Ethernet-Ports an das lokale Netz an.
5. Schalten Sie das Gerät an. Nachdem Anschließen leuchtet die Fehler-LED (F) rot.
6. Schalten Sie jetzt den PC ein.

1.3 Das Web Based Management starten

Werkseitig ist das SCALANCE S615 unter der folgenden IP-Adresse erreichbar:

- IP-Adresse: 192.168.1.1
- Subnetzmaske: 255.255.255.0

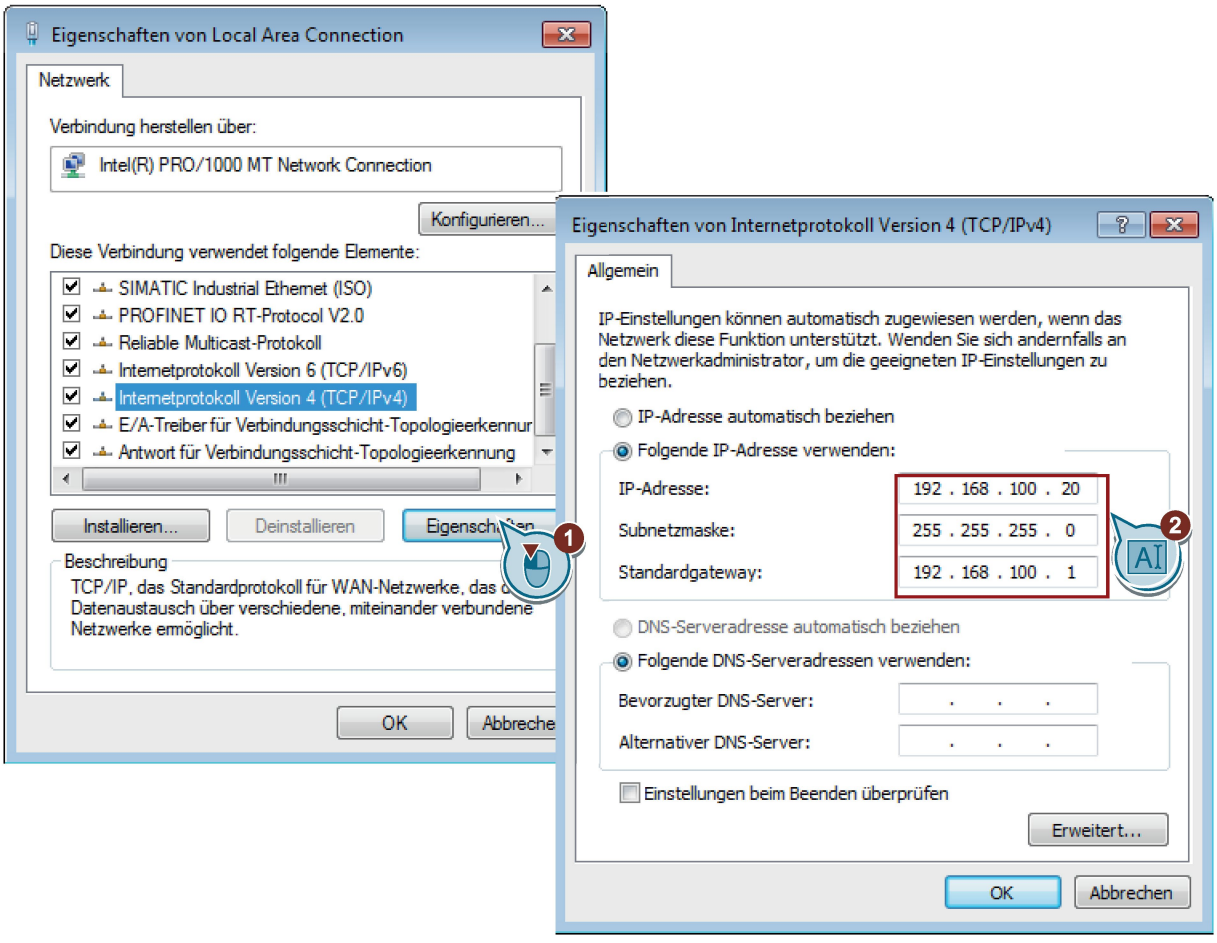
Der Admin-PC erhält in dieser Beispielkonfiguration folgende IP-Adresseinstellung, um auf das Web Based Management des S615 zu zugreifen.

IP-Adresse	Subnetzmaske
192.168.1.20	255.255.255.0

Vorgehensweise

1. Öffnen Sie auf dem Admin-PC mit dem Menübefehl "Start" > "Systemsteuerung" die Systemsteuerung.
2. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
3. Klicken Sie mit der rechten Maustaste auf das Symbol "LAN-Verbindung" und wählen Sie den Menübefehl "Eigenschaften".
4. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4 (TCP/IPv4)".

5. Geben Sie die Werte nach der obigen Tabelle ein.



6. Bestätigen Sie die Dialoge mit "OK" und schließen Sie die Systemsteuerung.

7. Geben Sie im Adressfeld des Internet-Browsers die IP-Adresse "192.168.1.1" ein.

   Standardmäßig ist der Zugriff über HTTPS aktiviert. Wenn Sie über HTTP auf das Gerät zugreifen, wird die Adresse automatisch auf HTTPS umgeleitet.

   Eine Meldung zum Sicherheitszertifikat erscheint. Quittieren Sie diese Meldung und setzen Sie das Laden der Seite fort.

   Hinweis

   Informationen zum Sicherheitszertifikat

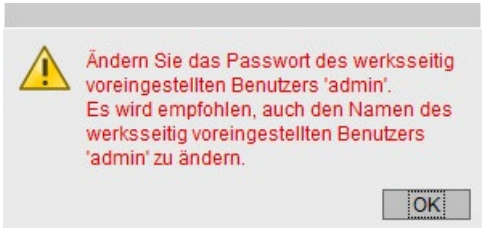
   Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbst unterzeichneten Zertifikat ausgeliefert. Bei Zertifikaten mit Unterschriften, die dem Betriebssystem nicht bekannt sind, erscheint ein Sicherheitshinweis. Sie können sich das Zertifikat anzeigen lassen.

8. Wenn eine einwandfreie Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).

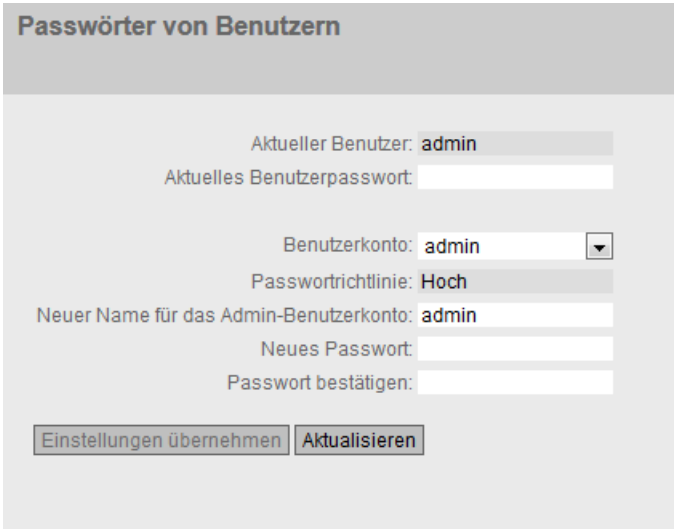
1.4 Am Web Based Management anmelden

Vorgehensweise

1. Melden Sie sich mit dem Benutzernamen "admin" und dem Passwort "admin" an. Sie werden aufgefordert, das Passwort zu ändern. Zusätzlich können Sie einmalig den werksseitig voreingestellten Benutzer "admin" umbenennen. Danach ist ein Umbenennen von "admin" nicht mehr möglich.

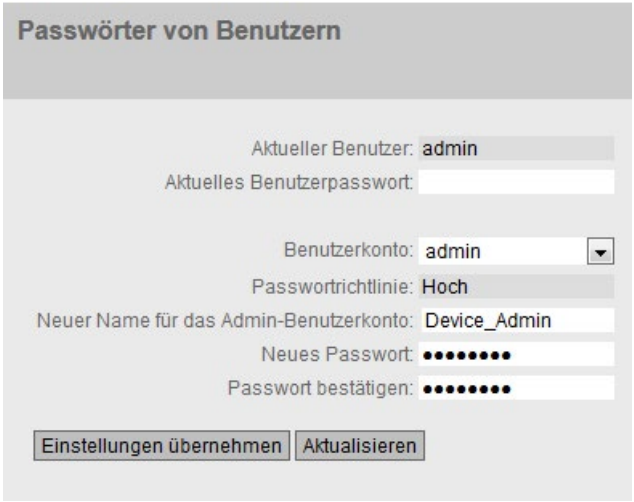


2. Bestätigen Sie den Dialog. Automatisch wird die WBM-Seite "Passwörter von Benutzern" geöffnet.



3. Geben Sie bei "Aktuelles Benutzerpasswort" das Default-Passwort "admin" ein.
4. Ändern Sie bei "Neuer Name für das Admin-Benutzerkonto" den Benutzernamen.
5. Geben Sie bei "Neues Passwort" das neue Passwort ein. Das neue Passwort muss mindestens 8 Zeichen lang sein und Großbuchstaben, Kleinbuchstaben, Zahlen sowie Sonderzeichen enthalten.

6. Wiederholen Sie das neue Passwort bei "Passwort bestätigen" zur Bestätigung. Beide Einträge müssen übereinstimmen.



7. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Ergebnis

Die Änderungen sind sofort wirksam und der Zugriff über DCP ist schreibgeschützt.

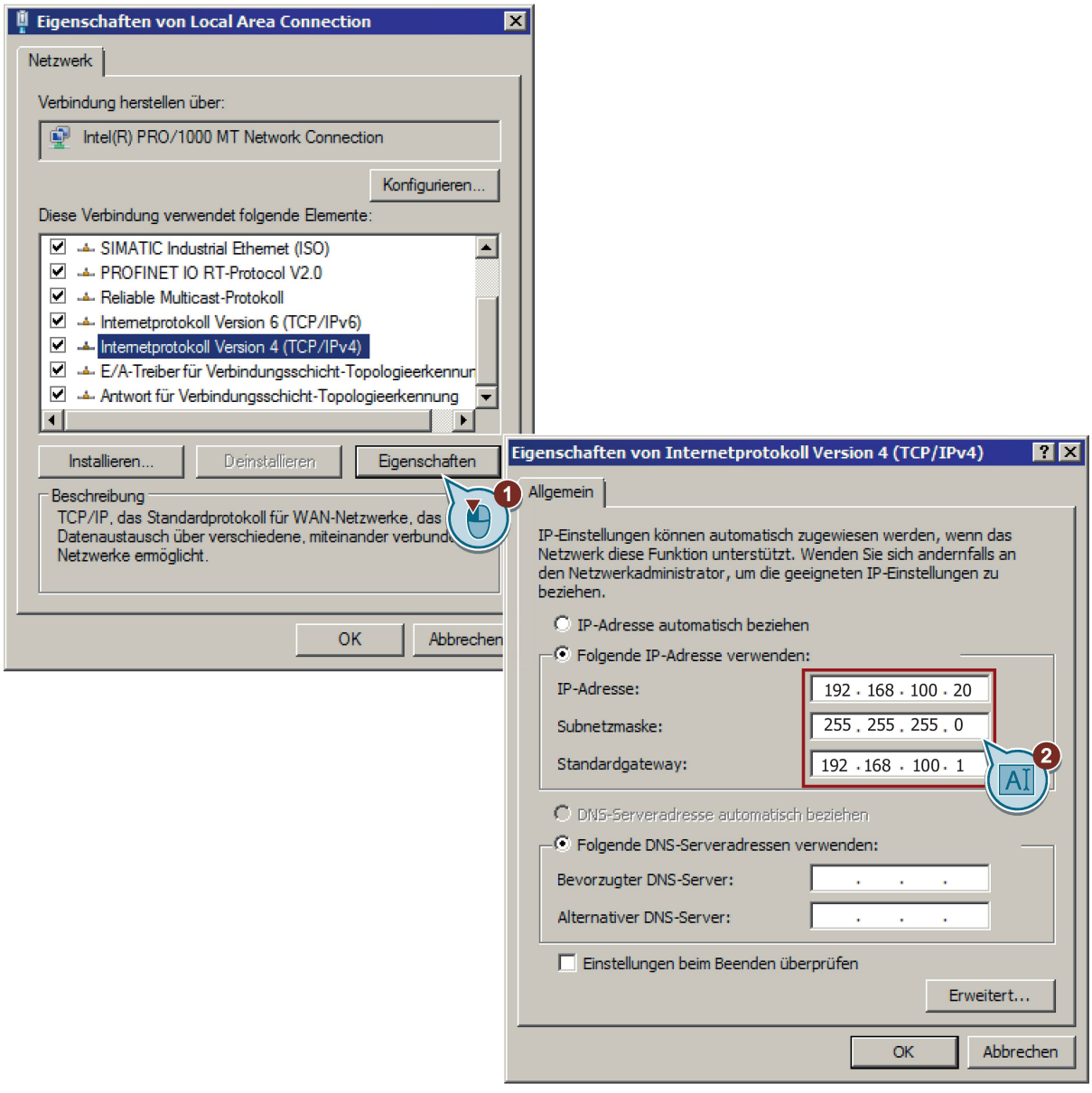
Der Basic Wizard startet, um Sie bei der Konfiguration der Geräteparameter zu unterstützen.

1.5 IP-Einstellungen des S615 ändern

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Layer 3 > Subnetze" und im Inhaltsbereich auf das Register "Konfiguration".
2. Geben Sie die IP-Adresse für vlan1 nach der Tabelle "Verwendete Einstellungen (Seite 9)" ein.
3. Klicken Sie auf "Einstellungen übernehmen".

   In der Adresszeile des Webbrowsers wird die IP-Adresse automatisch angepasst. Der Webbrowser auf dem Admin-PC kann nicht mehr auf das Web Based Management zugreifen, da seine IP-Einstellungen nicht mehr passen.
4. Öffnen Sie auf dem Admin-PC mit dem Menübefehl "Start" > "Systemsteuerung" die Systemsteuerung.
5. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
6. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4 (TCP/IPv4)".
7. Geben Sie die Werte für den PC nach der Tabelle "Verwendete Einstellungen (Seite 9)" ein.



8. Bestätigen Sie die Dialoge mit "OK" und schließen Sie die Systemsteuerung.
9. Geben Sie im Adressfeld des Webbrowsers die IP-Adresse für vlan 1 ein, siehe Tabelle "Verwendete Einstellungen (Seite 9)". Wenn eine einwandfreie Verbindung zum Gerät besteht, erscheint die Anmeldeseite des Web Based Managements (WBM).
10. Melden Sie sich mit dem Benutzernamen "admin" und dem geänderten Passwort an.

1.6 Geräteinformationen festlegen

Zur besseren Identifikation der SCALANCE S615 legen Sie allgemeine Geräteinformationen fest.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "System > Allgemein" und im Inhaltsbereich auf das Register "Gerät".
2. Tragen Sie bei "Systemname" einen Namen für das Gerät ein.
3. Tragen Sie bei "Systemkontakt" den für das Gerät zuständigen Ansprechpartner ein.
4. Tragen Sie bei "Gerätestandort" die Ortsbezeichnung des Aufstellungsorts ein, z.B. die Raumnummer.

5. Klicken Sie auf die Schaltfläche "Einstellungen übernehmen".

Ergebnis

Die allgemeinen Geräteinformationen der SCALANCE S615 sind festgelegt.

1.7 Uhrzeit einstellen

Zur Überprüfung der zeitlichen Gültigkeit von Zertifikaten und für die Zeitstempel von Logbuch-Einträgen werden auf dem SCALANCE S615 Datum und Uhrzeit geführt. Sie können die Systemzeit selbst manuell einstellen, oder Sie lassen sie mit einem Zeitserver automatisch synchronisieren. Für dieses Beispiel wird der Zeitserver über NTP konfiguriert.

Hinweis

Manuelle Zeiteinstellung - Verhalten nach Unterbrechung der Spannungsversorgung

Beachten Sie, dass die Uhrzeit auf Werkseinstellung zurückgesetzt wird, wenn die Spannungsversorgung unterbrochen wird. Nach Wiederkehr der Spannungsversorgung müssen Sie erneut die Systemzeit einstellen. Dadurch können Zertifikate ihre Gültigkeit verlieren.

Synchronisation über Zeitserver

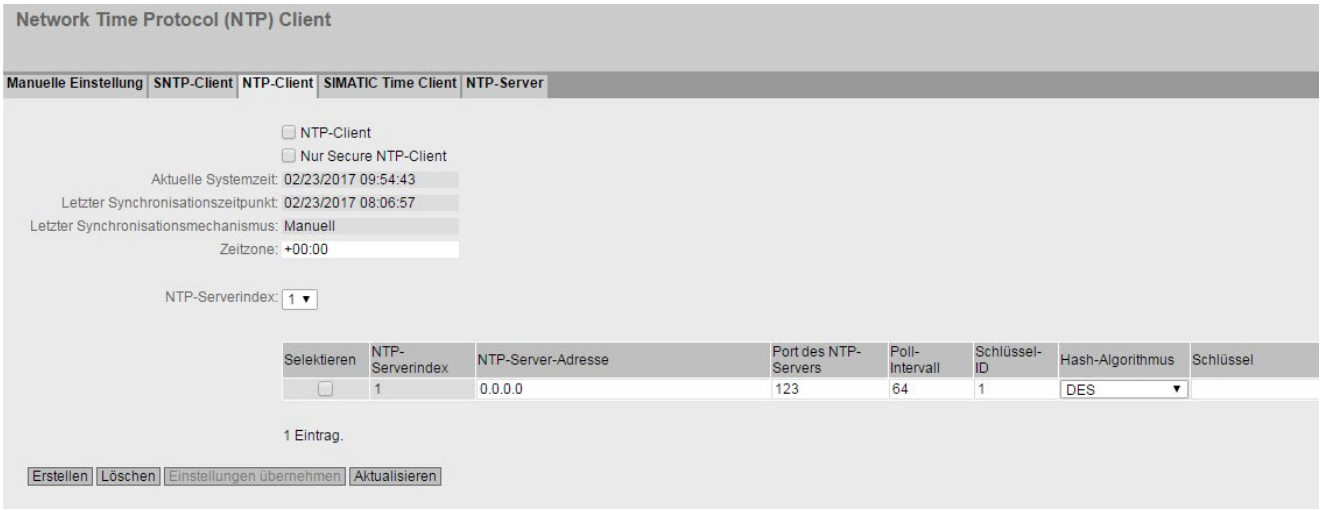
Die Synchronisation der Systemzeit über einen öffentlichen Zeitserver verursacht ein zusätzliches Datenaufkommen auf der Verbindung. Je nach Teilnehmervertrag sind damit erhöhte Kosten verbunden.

Voraussetzung

- Im lokalen Netz ist ein NTP-Server erreichbar.
- Die IP-Adresse des NTP-Servers ist bekannt.
  Für dieses Beispiel wird ein lokaler Zeitserver mit der IP-Adresse 192.168.100.87 verwendet.

Vorgehensweise

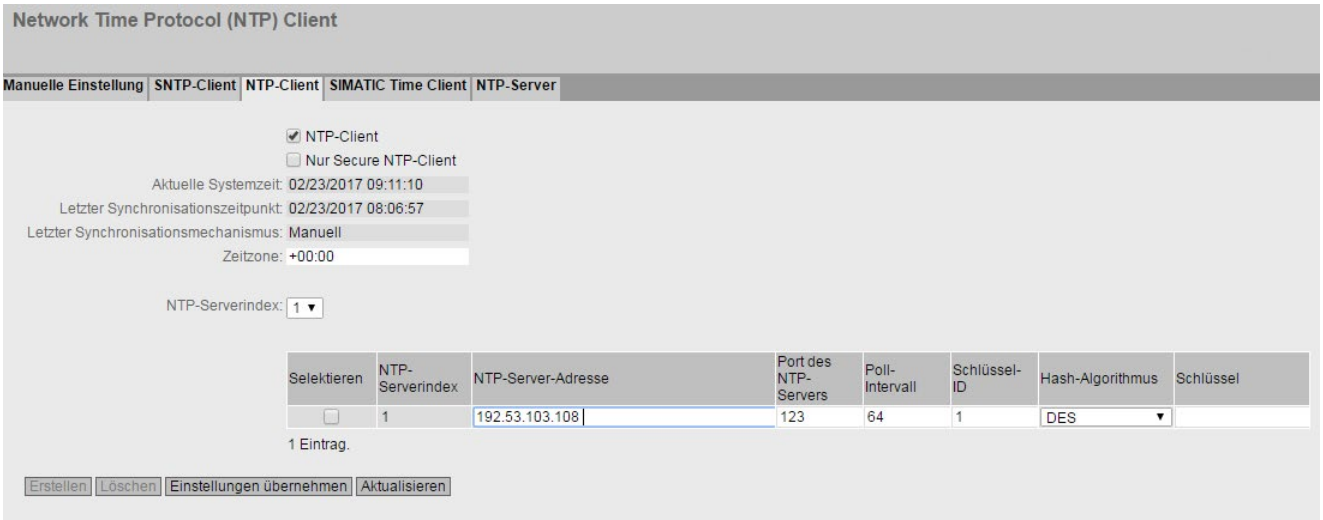
1. Klicken Sie im Navigationsbereich auf "System > Systemzeit" und im Inhaltsbereich auf das Register "NTP-Client".



2. Tragen Sie bei "Zeitzone" die lokale Zeitdifferenz zur Weltzeit (UTC) ein. Für mitteleuropäische Sommerzeit (MESZ) +02:00.
3. Klicken Sie auf "Erstellen". In der Tabelle wird ein neuer Eintrag erstellt.
4. Tragen Sie bei "NTP-Server-Adresse" die IP-Adresse 192.53.103.108 ein.
5. Ändern Sie bei Bedarf den Port bei "Port des NTP-Servers". Standardmäßig ist 123 eingestellt.
6. Tragen Sie bei "Poll-Intervall" den Zeitabstand für die Synchronisation ein. Standardmäßig ist 64 eingestellt.
7. Aktivieren Sie "NTP-Client".
8. Klicken Sie auf "Einstellungen übernehmen".

Ergebnis

Die Systemzeit über NTP ist eingestellt. Klicken Sie auf "Aktualisieren", um die WBM-Seite zu aktualisieren.



1.8 IP-Subnetz anlegen

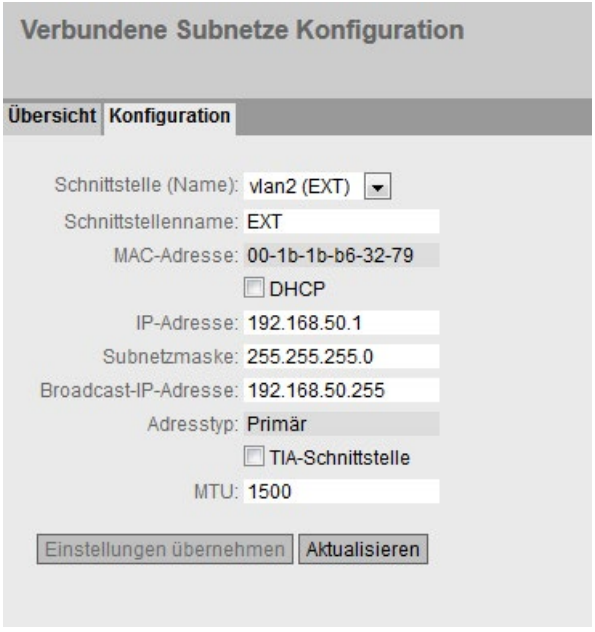
Die Schnittstellen werden unterschiedlich behandelt.

- Ethernet-Schnittstelle P1 (vlan1): Anbindung an LAN
- Ethernet-Schnittstelle P5 (vlan 2): Anbindung an WAN

Für dieses Konfigurationsbeispiel ist nur das IP-Subnetz für die Ethernet-Schnittstelle P5 zu konfigurieren. Das IP-Subnetz für die Ethernet-Schnittstelle P1 ist bereits konfiguriert.

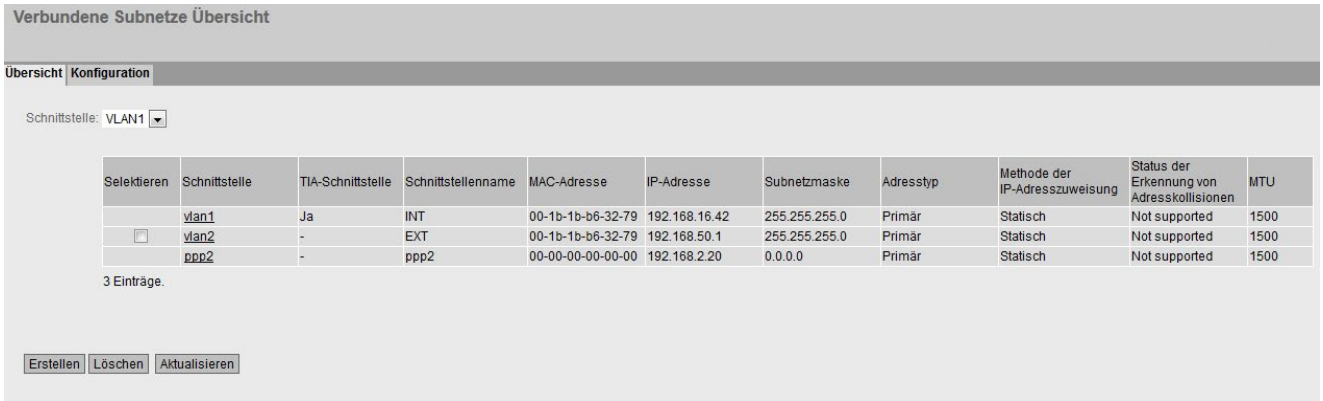
Vorgehensweise

1. Klicken Sie im Navigationsbereich auf "Layer 3 > Subnetze" und im Inhaltsbereich auf das Register "Konfiguration".
2. Wählen Sie bei "Schnittstellen" die "vlan2" aus.
3. Bei "Schnittstellenname" können Sie einen Namen eingeben.
4. Tragen Sie die IP-Adresse für vlan2 ein, siehe Tabelle "Verwendete Einstellungen (Seite 9)"
5. Klicken Sie auf "Einstellungen übernehmen".



Ergebnis

Die IP-Subnetze sind angelegt. Die IP-Subnetze werden im Register "Übersicht" angezeigt.



Selektieren	Schnittstelle	TIA-Schnittstelle	Schnittstellenname	MAC-Adresse	IP-Adresse	Subnetzmaske	Adresstyp	Methode der IP-Adresszuweisung	Status der Erkennung von Adresskollisionen	MTU
	vlan1	Ja	INT	00-1b-1b-b6-32-79	192.168.16.42	255.255.255.0	Primär	Statisch	Not supported	1500
	vlan2	-	EXT	00-1b-1b-b6-32-79	192.168.50.1	255.255.255.0	Primär	Statisch	Not supported	1500
	ppp2	-	ppp2	00-00-00-00-00-00	192.168.2.20	0.0.0.0	Primär	Statisch	Not supported	1500

3 Einträge.