SIEMENS

Lern-/Lehrunterlagen

Siemens Automation Cooperates with Education (SCE) | Ab Version V15.1

TIA Portal Modul 142-200
Industrial Security mit SIMATIC S7-1500 und SCALANCE S615

siemens.de/sce

SIEMENS
Global Industry Partner of WorldSkills International

worldskills

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

Passende SCE Trainer Pakete zu dieser Lern-/Lehrunterlage

Industrielle Kommunikation SIMATIC NET

- **IE SCALANCE S615 mit Software SINEMA RC Basis**
  Bestellnr.: 6GK1950-0BB13
- **IE SCALANCE S615 LAN-Router**
  Bestellnr.: 6GK1950-0BB23

SIMATIC Steuerungen

- **SIMATIC CPU 1516F PN/DP Safety**
  Bestellnr.: 6ES7516-3FN00-4AB2
- **SIMATIC ET 200SP Open Controller CPU 1515SP PC F und HMI RT SW**
  Bestellnr.: 6ES7677-2SB42-4AB1
- **SIMATIC ET 200SP Distributed Controller CPU 1512SP F-1 PN Safety**
  Bestellnr.: 6ES7512-1SK00-4AB2
- **SIMATIC S7 CPU 1516-3 PN/DP**
  Bestellnr.: 6ES7516-3AN00-4AB3
- **SIMATIC CPU 1512C PN mit Software und PM 1507**
  Bestellnr.: 6ES7512-1CK00-4AB1
- **SIMATIC CPU 1512C PN mit Software, PM 1507 und CP 1542-5 (PROFIBUS)**
  Bestellnr.: 6ES7512-1CK00-4AB2
- **SIMATIC CPU 1512C PN mit Software**
  Bestellnr.: 6ES7512-1CK00-4AB6
- **SIMATIC CPU 1512C PN mit Software und CP 1542-5 (PROFIBUS)**
  Bestellnr.: 6ES7512-1CK00-4AB7

SIMATIC STEP 7 Software for Training

- **SIMATIC STEP 7 Professional V15.1 – Einzel-Lizenz**
  Bestellnr.: 6ES7822-1AA05-4YA5
- **SIMATIC STEP 7 Professional V15.1 – 6+20er Klassenraum-Lizenz**
  Bestellnr.: 6ES7822-1BA05-4YA5
- **SIMATIC STEP 7 Professional V15.1 – 6+20er Upgrade-Lizenz**
  Bestellnr.: 6ES7822-1AA05-4YE5
- **SIMATIC STEP 7 Professional V15.1 – 20er Studenten-Lizenz**
  Bestellnr.: 6ES7822-1AC05-4YA5

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

Bitte beachten Sie, dass diese Trainer Pakete ggf. durch Nachfolge-Pakete ersetzt werden. Eine Übersicht über die aktuell verfügbaren SCE Pakete finden Sie unter: siemens.de/sce/tp

Fortbildungen

Für regionale Siemens SCE Fortbildungen kontaktieren Sie Ihren regionalen SCE Kontaktpartner:
siemens.de/sce/contact

Weitere Informationen rund um SCE

siemens.de/sce

Verwendungshinweis

Die SCE Lern-/Lehrunterlage für die durchgängige Automatisierungslösung Totally Integrated Automation (TIA) wurde für das Programm “Siemens Automation Cooperates with Education (SCE)“ speziell zu Ausbildungszwecken für öffentliche Bildungs- und F&E-Einrichtungen erstellt. Siemens übernimmt bezüglich des Inhalts keine Gewähr.

Diese Unterlage darf nur für die Erstausbildung an Siemens Produkten/Systemen verwendet werden.
D. h. Sie kann ganz oder teilweise kopiert und an die Auszubildenden/Studierenden zur Nutzung im Rahmen deren Ausbildung/Studiums ausgehändigt werden. Die Weitergabe sowie Vervielfältigung dieser Unterlage und Mitteilung Ihres Inhalts ist innerhalb öffentlicher Aus- und Weiterbildungsstätten für Zwecke der Ausbildung oder im Rahmen des Studiums gestattet.

Ausnahmen bedürfen der schriftlichen Genehmigung durch Siemensmailto:. Alle Anfragen hierzu an scesupportfinder.i-ia@siemens.com.

Zuwiderhandlungen verpflichten zu Schadensersatz. Alle Rechte auch der Übersetzung sind vorbehalten, insbesondere für den Fall der Patentierung oder GM-Eintragung.

Der Einsatz für Industriekunden-Kurse ist explizit nicht erlaubt. Einer kommerziellen Nutzung der Unterlagen stimmen wir nicht zu.

Wir danken der TU Dresden, der Fa. Michael Dziallas Engineering und allen weiteren Beteiligten für die Unterstützung bei der Erstellung dieser SCE Lern-/Lehrunterlage.

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

Inhaltsverzeichnis

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

Industrial Security mit S7-1500 und SCALANCE S615

1 Zielstellung

In diesem Kapitel lernen Sie Industrial Ethernet Security SCALANCE S615 zu konfigurieren und eine S7-1500 Steuerung sicher mit anderen Netzen zu verbinden.

Es können die unter Kapitel 3 aufgeführten SIMATIC S7-Steuerungen eingesetzt werden.

2 Voraussetzung

Dieses Kapitel baut auf das Kapitel OPC UA mit SIMATIC S7-1500 als OPC-Server auf. Zur Durchführung dieses Kapitels können Sie z. B. auf das folgende Projekt zurückgreifen: „SCE_DE_092-300_OPC_UA_S7-1500_R1807.zap15“.

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

3 Benötigte Hardware und Software

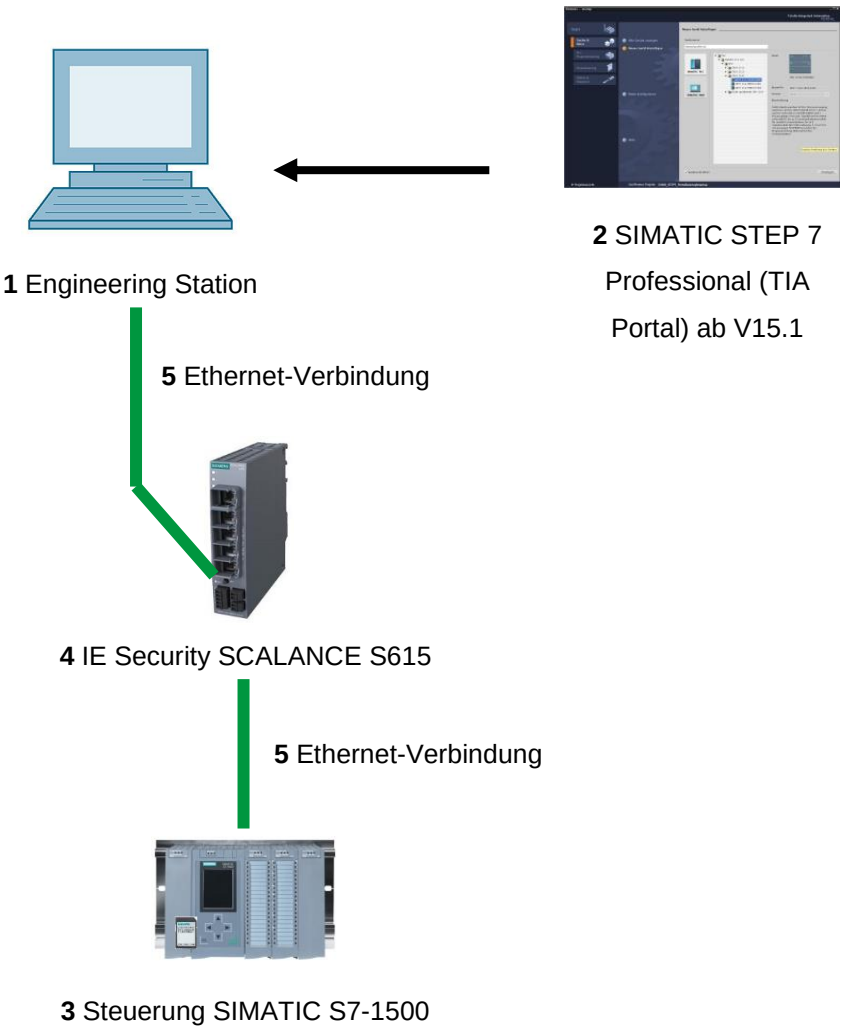
1 Engineering Station: Voraussetzungen sind Hardware und Betriebssystem (weitere Informationen siehe Readme/Liesmich auf den TIA Portal Installations-DVDs)

2 Software SIMATIC STEP 7 Professional im TIA Portal – ab V15.1

3 Steuerung SIMATIC S7-1500, z. B. CPU 1516F-3 PN/DP – ab Firmware V2.1 mit Memory Card

4 Industrial Ethernet Security SCALANCE S615

5 Ethernet-Verbindung zwischen Engineering Station und SCALANCE S615 und zwischen Steuerung und SCALANCE S615



Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

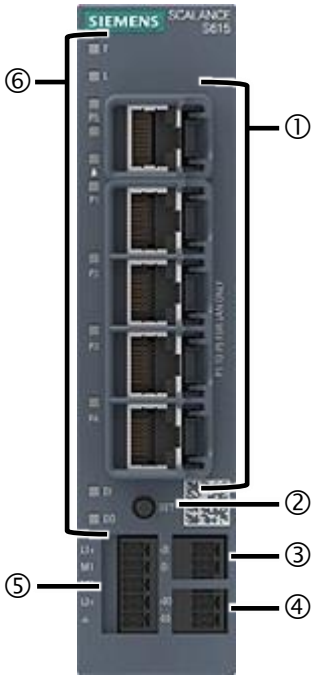
4 Theorie

4.1 Aufbau und Bedienung des SCALANCE S615

Im folgenden Abschnitt finden Sie eine kurze Beschreibung des SCALANCE S615. Weiterführende Details und Informationen finden Sie in den Handbüchern, die unter support.automation.siemens.com heruntergeladen werden können.

4.1.1 Industrial Ethernet Security S615

Der SCALANCE S615 ist ein industrieller Ethernet Router und Firewall für die Prozessautomatisierung.

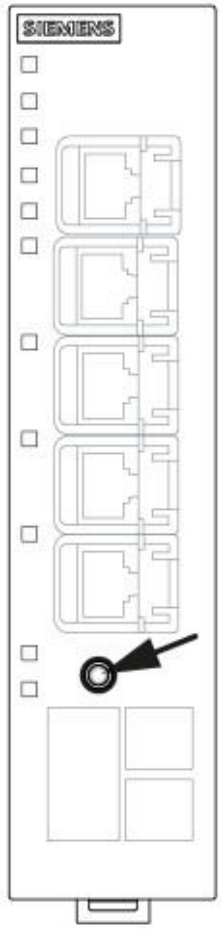


(1) Netzwerk Ports
(2) SET-Taster
(3) Digitaler Eingang
(4) Digitaler Ausgang
(5) Netzeingang für die Spannungsversorgung
(6) LED-Anzeige

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

4.1.2 Taster SET

Der SET-Taster ist bei einem SCALANCE S615 auf der Gehäusevorderseite angebracht.



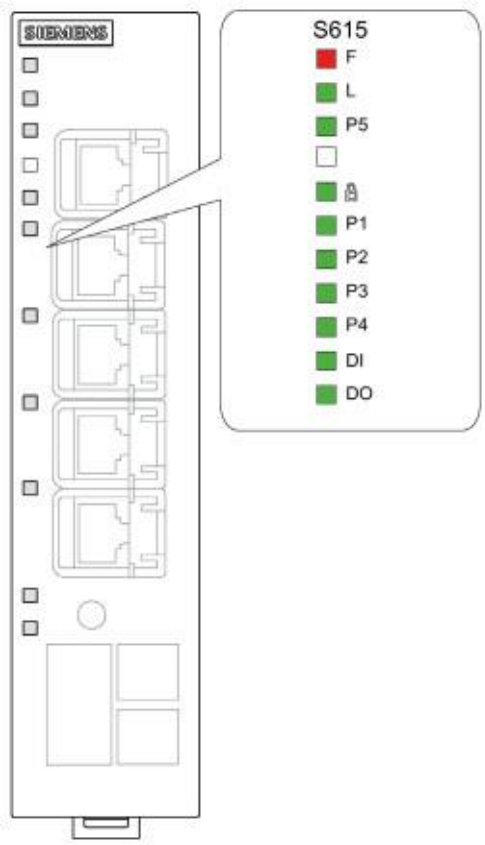
Der SET-Taster hat mehrere Funktionen. Bei kurzem Tasten unter 3 Sekunden führt das Gerät einen Neustart durch. Durch langes Drücken über 10 Sekunden setzt sich das Gerät auf die Werkseinstellungen zurück.

Der Taster kann auch genutzt werden, um das Gerät in den Bootloader zu bringen. Im Falle einer defekten Firmware kann mit Hilfe des Bootloaders eine neue Firmware aufgespielt werden. Genauere Informationen zu dem Thema finden Sie im Handbuch.

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

4.1.3 LED Meldeleuchten

Auf dem SCALANCE S615 befinden sich verschiedene LEDs, die einen Überblick über den Zustand des Systems bieten.



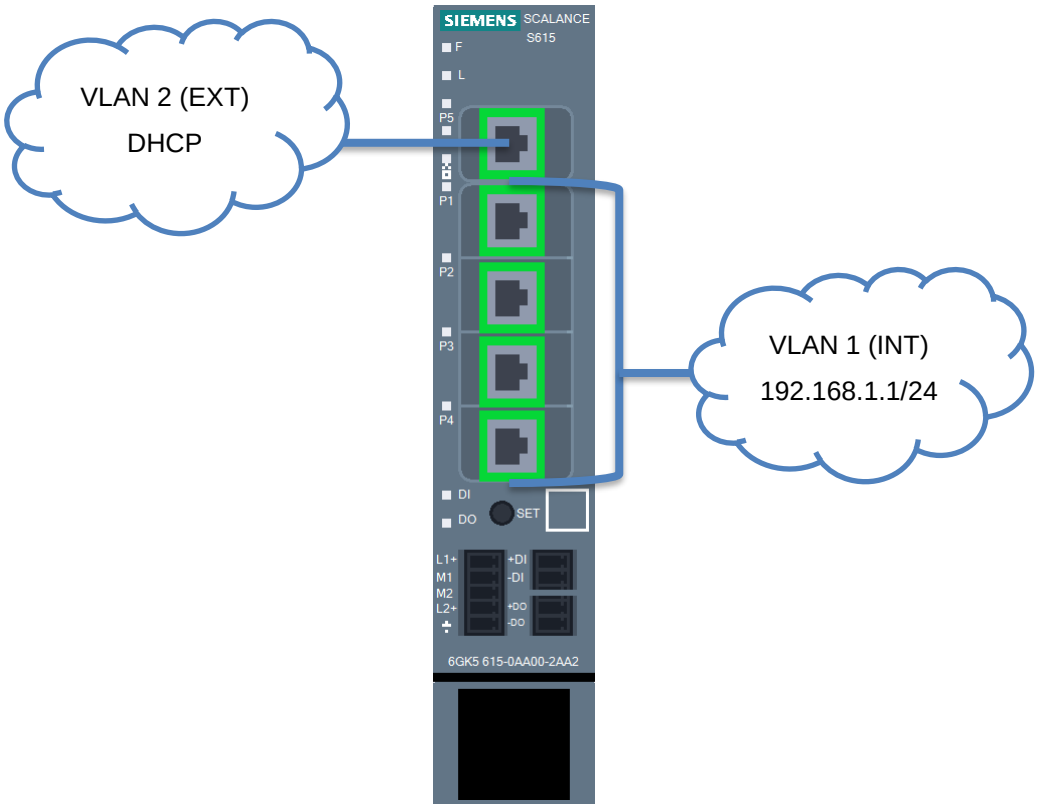
F	LED zur Anzeige des Fehlerstatus
L	LED zur Anzeige der Spannungsversorgung
🔒	LED zur Anzeige der VPN-Verbindungen
DI	LED zur Anzeige des digitalen Eingangs
DO	LED zur Anzeige des digitalen Ausgangs
P	LEDs zur Anzeige des Portstatus

Eine genaue Beschreibung zu jeder LED können Sie dem Handbuch des Geräts entnehmen.

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

4.1.4 Netzwerk Ports

Der SCALANCE S615 verfügt über fünf Netzwerk Ports. Davon sind die ersten vier werksseitig als VLAN 1 (INT) und der fünfte als VLAN 2 (EXT) konfiguriert.



Diese Verschaltung kann beliebig verändert werden. Standardmäßig ist das VLAN 2 als unsicheres externes Netz konfiguriert und das VLAN 1 als zu schützendes internes Netz.

Das VLAN 1 ist in den Werkseinstellungen mit der IP 192.168.1.1/24 konfiguriert. Das Gerät im VLAN 2 besitzt hingegen keine feste IP-Adresse, sondern mit Hilfe von DHCP kann eine dynamische IP-Adresse einstellt werden.

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

4.2 VLAN: Virtuelle Netzwerke

Geräte wie z. B. Switche verfügen meist über mehrere Netzwerk Ports, die alle zum Netzwerk gehören. Ein Teilnehmer an Port A kann also ungehindert mit einem Teilnehmer an Port B kommunizieren. Um einzelne Teilnehmer voneinander zu trennen, müssten entsprechend pro Netzwerk eigene physikalische Geräte eingesetzt werden.

Mit Hilfe von Virtual Local Area Networks (VLANs) kann ein physikalisches Netzwerkgerät in virtuelle Netzwerke unterteilt werden. Jeder Port wird dabei einem VLAN fest zugewiesen. Ein Teilnehmer an einem Port im VLAN 1 kann jetzt nur noch mit Teilnehmern im VLAN 1 kommunizieren. Dabei wird jedes VLAN mit einer eindeutigen ID im Gerät konfiguriert. Diese ID ist in der Regel 12 Bit lang und wird dezimal dargestellt.

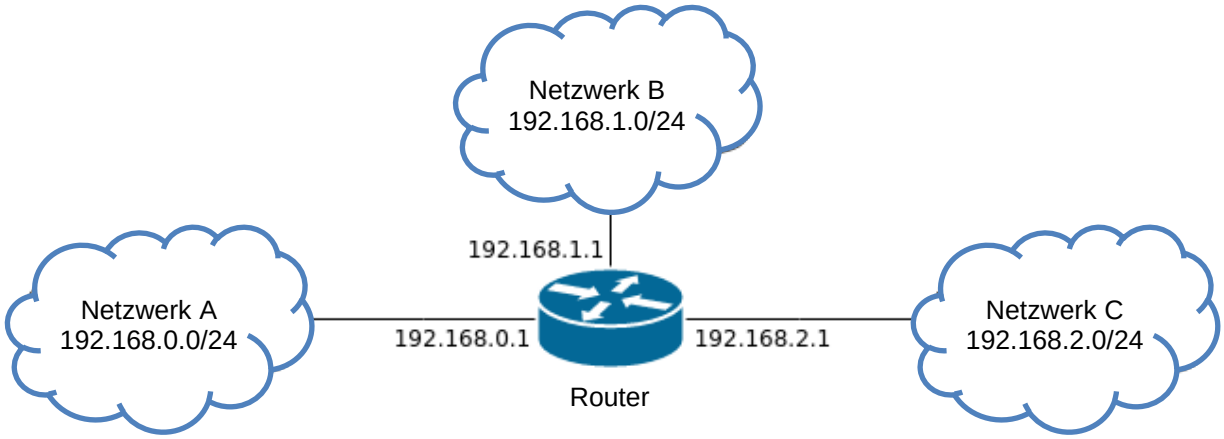
Es besteht die Option einem Port auch mehrere VLANs zuzuweisen. Pakete, die einen solchen Port verlassen, werden mit einem Tag versehen, welcher die ID des VLANs enthält. Eingehende Pakete werden auf einen vorhandenen Tag untersucht und das Paket dem VLAN mit der im Tag enthaltenen ID zugewiesen. Die Gegenstelle an einem solchen Port muss natürlich auch entsprechend konfiguriert sein, um die Tags korrekt auszuwerten.

So kann dieselbe physikalische Netzwerkstruktur kostengünstig genutzt werden, um einzelne Teilnehmergruppen voneinander zu separieren.

Der SCALANCE S615 ist werksseitig in zwei separate Netzwerke unterteilt. Ein sicheres Netzwerk mit der VLAN ID 1 und ein unsicheres mit der VLAN ID 2 (siehe Abschnitt 4.1.4).

4.3 Router

Im Gegensatz zu einem Switch ist ein Router in der Lage verschiedene Netze miteinander zu koppeln. Dazu besitzt er eine physikalische Verbindung und eine passende IP-Adresse zu jedem Netz. Dadurch ist er für andere Teilnehmer im Netz erreichbar und kann Pakete zwischen den angeschlossenen Netzen vermitteln.



Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

4.4 Firewall

Eine Firewall kann, Pakete, welche sie passieren, filtern. Dafür kann das Gerät unterschiedliche Kriterien nutzen, z. B. Quell- und Zieladressen oder TCP-Ports. Leistungsstärkere Geräte sind auch in der Lage, komplexere Dinge zu verstehen, z. B. welche Daten der Benutzer gerade an eine Webseite sendet.

Der SCALANCE S615 ist Router und Firewall zugleich und kann Pakete überprüfen, die durch ihn von einem VLAN in ein anderes geroutet werden (Layer 3). D. h. er kann keine Pakete kontrollieren, die innerhalb eines VLAN durch ihn weitergeleitet werden (Layer 2).

Die Firewall im S615 kann Informationen bis zum Layer 4 verarbeiten. Das beinhaltet IP-Adressen und das genutzte Protokoll z. B. TCP oder UDP und die dabei genutzten Ports.

Das Filtern selbst geschieht mit Hilfe eines Regelwerks, das in Form einer Tabelle vorliegt. Jede Zeile entspricht dabei einer Regel.

Quell-IP	Ziel-IP	Protokoll	Quell-Port	Ziel-Port	Aktion
192.168.1.24/32	192.168.2.5/32	any			Accept
192.168.1.0/24	0.0.0.0/0	tcp	*	443	Accept
0.0.0.0/0	0.0.0.0/0	any			Drop

Dieses Regelwerk wird von oben nach unten abgearbeitet und die erste passende Regel wird genutzt. Im obigen Beispiel wäre der Teilnehmer mit der IP 192.168.1.24 in der Lage, jegliche Art von Kommunikation mit dem Teilnehmer 192.168.2.5 aufzubauen.

Teilnehmer aus dem Netz 192.168.1.x können jede andere Adresse über TCP und Port 443 (HTTPS) kontaktieren. Die letzte Regel sorgt dafür, dass alle anderen Pakete verworfen werden.

In der Regel bietet es sich an eine von drei Aktionen auszuführen.

– Pakete können akzeptiert (Accept) und damit weitergeleitet werden.

– Es besteht ebenfalls die Möglichkeit sie zu verwerfen bzw. wegzuwerfen (Drop). Der Absender wird dabei über den Verbleib des Pakets nicht informiert.

– Zuletzt bietet sich die Option an, die Pakete zurückzuweisen (Reject). Hierbei bekommt der Absender eine passende Rückmeldung, dass seine Pakete abgelehnt wurden.

In den meisten Fällen werden Accept und Drop genutzt und Reject nur für spezielle Fälle verwendet.

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

4.4.1 Implizite Regel

Was passiert mit Paketen, die auf keine konfigurierte Regel passen? Die Antwort ist abhängig vom Hersteller des Filters. Die meisten Hersteller haben am Ende des Regelwerks eine implizite Regel, die entweder alles zulässt oder alles fallen lässt. Meist kann dieses Verhalten angepasst werden.

Im Falle des SCALANCE S615 verwirft (Drop) die implizite Regel alle Pakete.

4.4.2 Stateful Inspection

Die meisten Firewalls filtern nicht einfach nur einkommende Pakete, sondern merken sich auch, welcher Computer welche Verbindung aufgebaut hat. Ein Computer der z. B. eine Webseite aufruft, bekommt vom Server Antwortpakete. Damit diese Antwortpakete nicht auch in den Filterregeln definiert werden müssen, überprüfen moderne Firewalls Pakete nur während des Verbindungsaufbaus.

Versucht der Teilnehmer 192.168.1.5 eine verschlüsselte Webseite auf dem Teilnehmer 192.168.3.25 über Port 443 zu erreichen, so wird dieser Verbindungsaufbau anhand des Regelwerks überprüft. Akzeptiert das Regelwerk diese Verbindung so merkt sich die Firewall, in einer speziellen Sitzungstabelle, die Gültigkeit dieser Verbindung. Jedes nachfolgende Paket, welches zu dieser Verbindung gehört, egal ob vom Client oder Webserver, egal auf welchem Quell- oder Zielport, wird jetzt durch die Firewall akzeptiert.

Durch diese Technik muss der Administrator nur das für den Verbindungsaufbau nötige Regelwerk erstellen.

4.5 CIDR Notation

Um eine möglichst effiziente Nutzung der vorhanden IP-Adressen zu gewährleisten, werden diese heutzutage mit der Subnetzmaske klassifiziert und nicht durch die IP-Adresse selbst.

Die Subnetzmaske wird häufig in Form eines Suffixes an der eigentlichen Adresse dargestellt. Diese Darstellung wird auch als CIDR (Classless Inter-Domain Routing) Notation bezeichnet.

→ Beispiel: 192.168.0.1/24

Das Suffix /24 gibt die Anzahl der gesetzten Bits in der Subnetzmaske an. Im Beispiel wären also die ersten 24 Bit der Subnetzmaske gesetzt.

→ Binär: 11111111.11111111.11111111.00000000

→ Dezimal: 255.255.255.0

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

Im Regelwerk der Firewall wird diese Notation genutzt, um bei den Quell- und Zieladressen Bereiche zu definieren. Das Suffix gibt hier also an, bis zu welchem Bit die Adresse am Paket mit der Adresse in der Regel übereinstimmen muss.

Adresse im Regelwerk	Beschreibung
192.168.1.1/32	Alle Bits müssen übereinstimmen. Nur die Adresse 192.168.1.1 deckt sich mit der Regel
192.168.1.0/24	Die ersten 3 Oktette müssen übereinstimmen. Alle Adressen, die mit 192.168.1.x beginnen decken sich mit der Regel.
0.0.0.0/0	Kein Bit muss übereinstimmen. Alle Adressen decken sich mit der Regel
192.168.1.0/25	Die ersten 3 Oktette und das höchste Bit des 4 Oktettes müssen übereinstimmen. Hier decken sich nur noch die Adresse 192.168.1.0 bis 192.168.1.127 mit der Regel

Für komplexere Bereiche wie im letzten Beispiel können entsprechende Tools hilfreich sein. Eine einfache Internetsuche nach „Subnetz Rechner“ oder „CIDR Rechner“ sollte genügend Online Tools hervorbringen.

Ein hilfreiches intuitives Tool finden Sie zum Beispiel hier:
heise.de/netze/tools/netzwerkrechner/

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

4.6 IP-Adresse einstellen am Programmiergerät

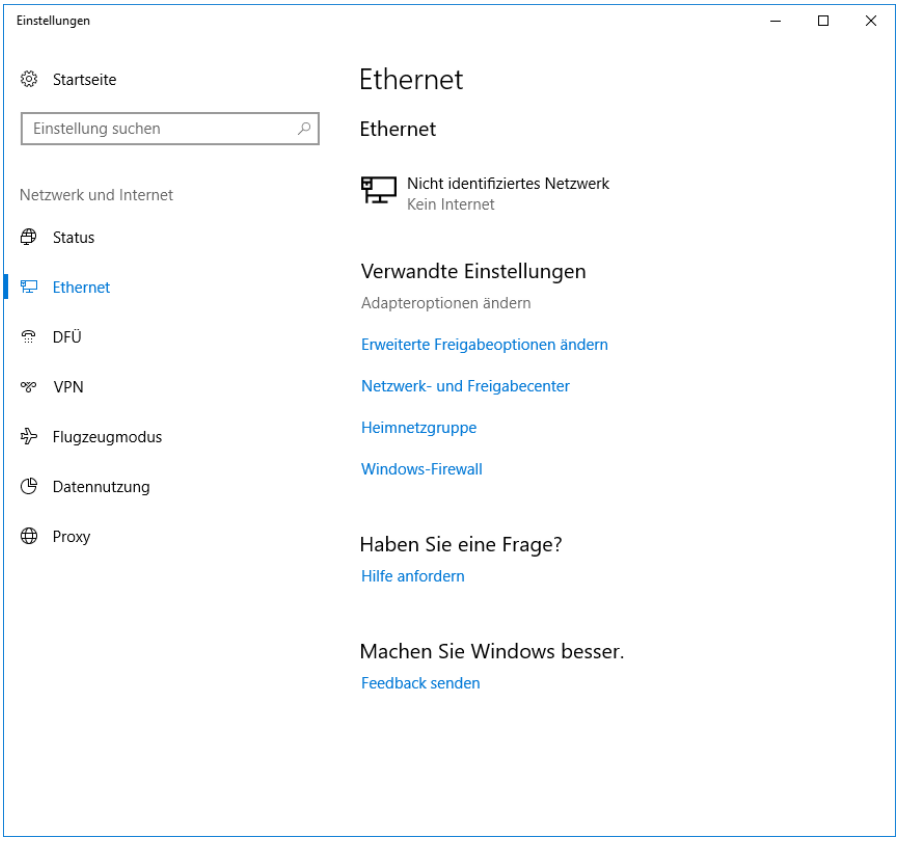
Um vom PC, dem PG oder einem Laptop aus SIMATIC S7-1500 programmieren zu können, wird eine TCP/IP-Verbindung oder optional eine PROFIBUS-Verbindung benötigt.

Damit PC und SIMATIC S7-1500 über TCP/IP miteinander kommunizieren können, ist es wichtig, dass die IP-Adressen der beiden Geräte zusammenpassen.

Zuerst wird hier gezeigt, wie die IP-Adresse eines Rechners mit dem Betriebssystem Windows 10 eingestellt werden kann.

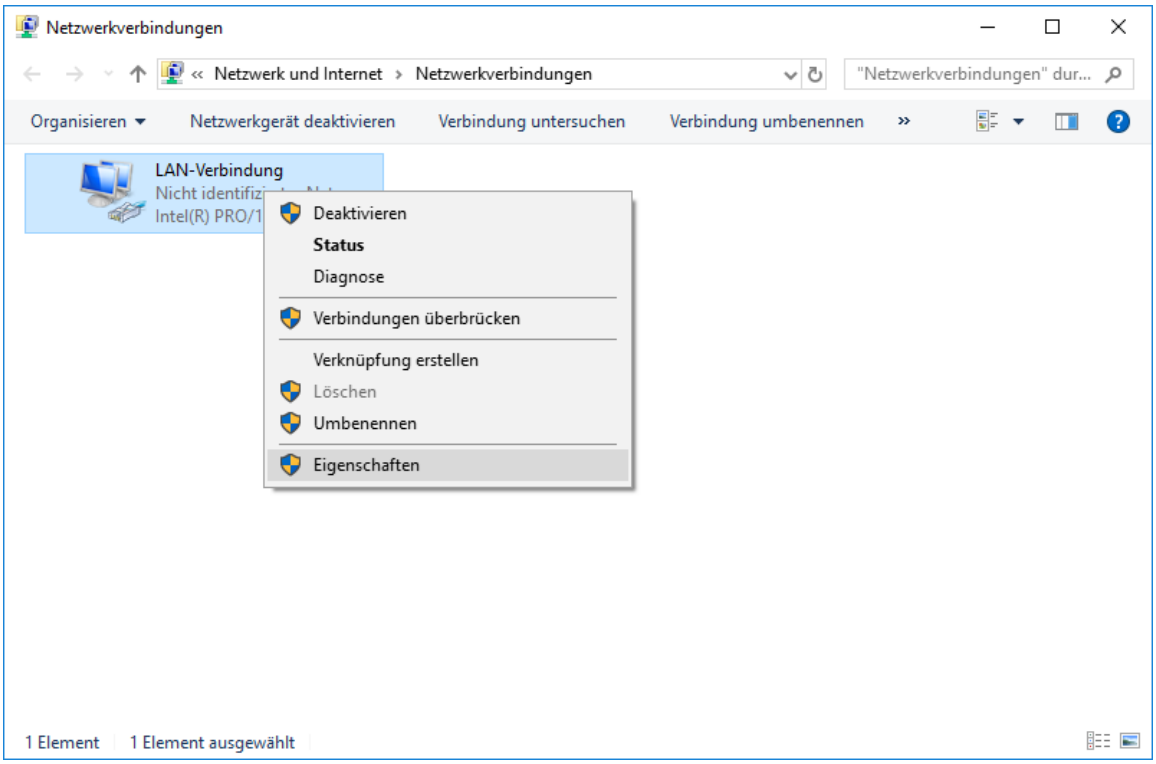
→ Lokalisieren Sie das Netzwerksymbol unten in der Taskleiste  und klicken Sie anschließend auf → „Netzwerkeinstellungen“.

→ Im geöffneten Fenster der Netzwerkeinstellungen klicken Sie auf → „Ethernet“ und anschließend auf → „Adapteroptionen ändern“.

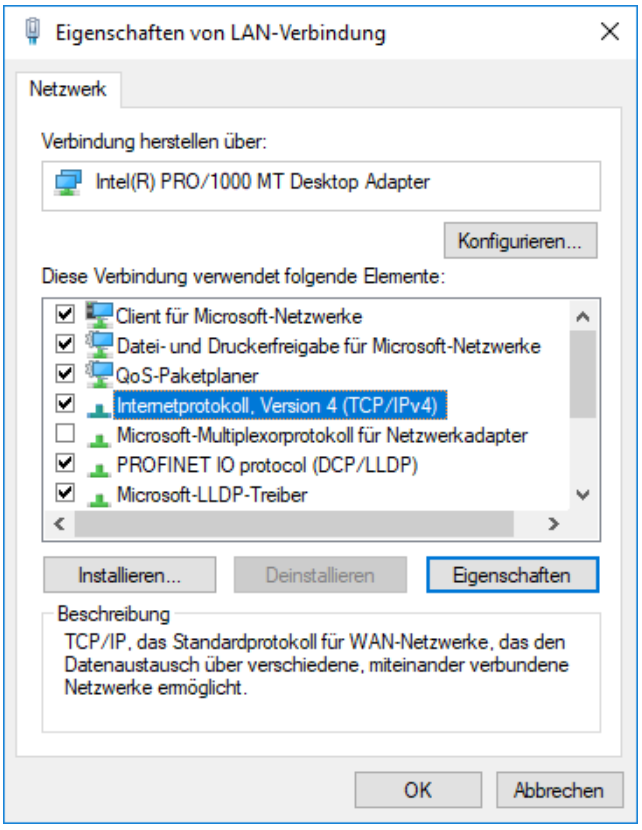


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Wählen Sie die gewünschte → „LAN-Verbindung“ aus, mit der Sie sich mit der Steuerung verbinden möchten und klicken auf → „Eigenschaften“.

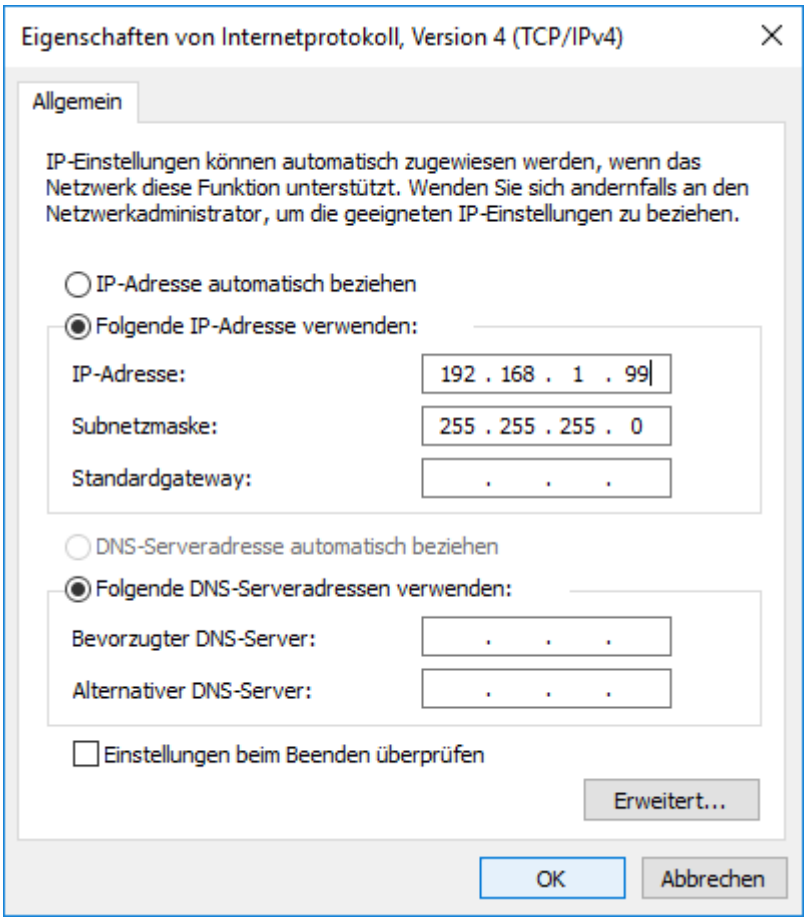


→ Wählen Sie anschließend zum → „Internetprotokoll Version 4 (TCP/IP)“ die → „Eigenschaften“.



Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Jetzt können Sie z. B. die IP-Adresse: 192.168.1.99 mit der Subnetzmaske 255.255.255.0 verwenden und die Einstellungen übernehmen. (→ „OK“)



Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

5 Aufgabenstellung

In diesem Kapitel soll die Hardware und das Programm aus Kapitel „SCE_DE_092-300_OPC_UA_S7-1500“, um den SCALANCE S615 erweitert werden.

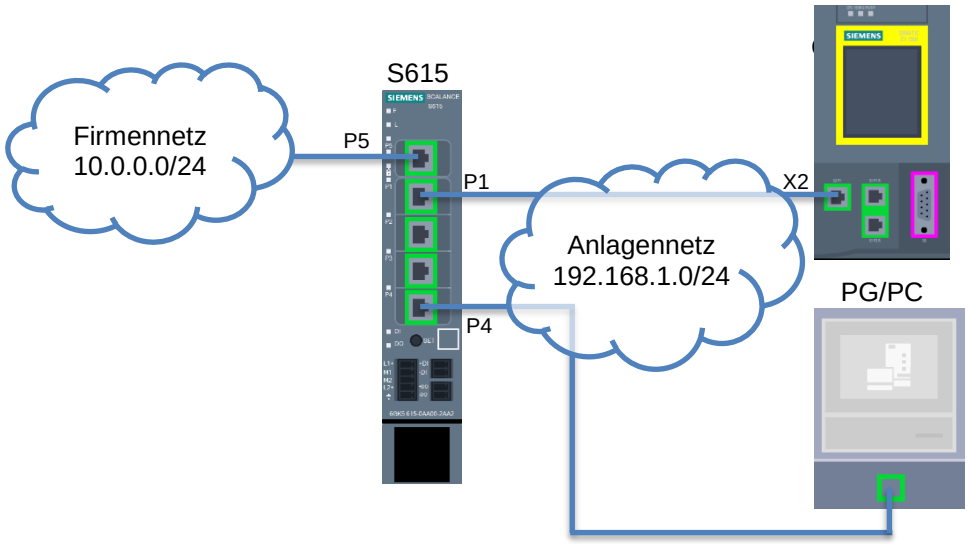
Mit Hilfe des SCALANCE S615 soll ein gesicherter Zugriff auf die Steuerung aus dem Firmennetzwerk ermöglicht werden. Der Webserver auf der CPU soll dabei zu Diagnosezwecken frei zugänglich sein, während der Zugang zur Programmierung mittels des TIA Portals nur authentifizierten Benutzern erlaubt sein soll.

6 Planung

Als Erstes muss der SCALANCE S615 mit einer neuen IP-Adresse konfiguriert und die Grundkonfiguration vorgenommen werden.

Anschließend kann in der CPU 1516F der S615 als Router eingetragen und die Konfiguration auf die CPU übertragen werden.

Nach erfolgreicher Grundkonfiguration beider Geräte kann die physikalische Vernetzung der Komponenten wie folgt aufgebaut werden.



Als Letztes werden die Zugriffsregeln im SCALANCE S615 angelegt und getestet.

WICHTIG:

Da sich das Programmiergerät während der Inbetriebnahme in verschiedenen Subnetzen befinden wird, dürfen Sie auf keinen Fall eine projektspezifische IP-Adresse durch das TIA Portal anlegen lassen. Konfigurieren Sie stattdessen die korrekten IP-Einstellungen statisch in das Programmiergerät. Später wird der S615 die korrekten IP-Adressen dynamisch vergeben.

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

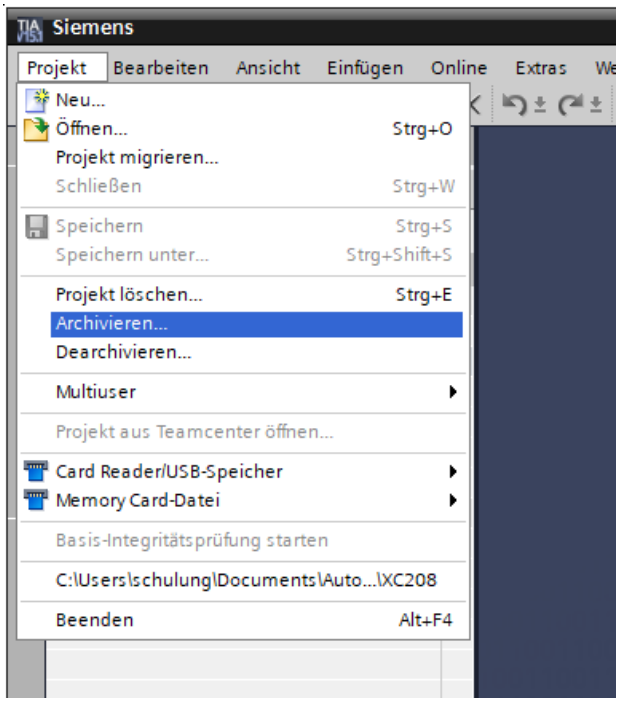
7 Strukturierte Schritt-für-Schritt-Anleitung

Im Folgenden finden Sie eine Anleitung wie Sie die Planung umsetzen können. Sollten Sie schon bereits entsprechende Vorkenntnisse haben, so reichen Ihnen die nummerierten Schritte zur Bearbeitung aus. Ansonsten folgen Sie einfach den folgenden bebilderten Schritten der Anleitung.

7.1 Dearchivieren eines vorhandenen Projekts

→ Bevor Sie das Projekt „SCE_DE_092-300 OPC UA S7-1500_R1807.zap15“ aus dem Kapitel „SCE_DE_092-300 OPC UA S7-1500“ erweitern können, müssen Sie dieses dearchivieren.

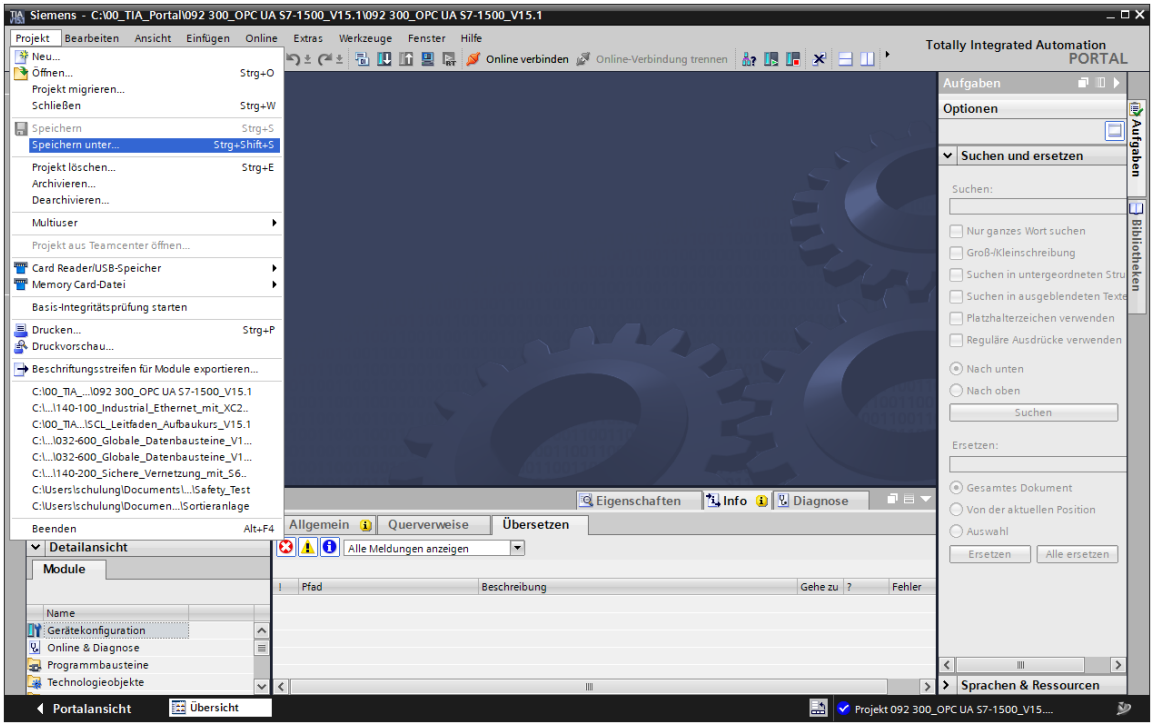
→ Zum Dearchivieren eines vorhandenen Projekts müssen Sie aus der Projektansicht heraus unter → Projekt → Dearchivieren das jeweilige Archiv aussuchen. Bestätigen Sie Ihre Auswahl anschließend mit Öffnen. (→ Projekt → Dearchivieren → Auswahl eines .zap-Archivs … → Öffnen)



→ Wählen Sie als Nächstes das Zielverzeichnis, in welches das dearchivierte Projekt gespeichert werden soll. Bestätigen Sie Ihre Auswahl mit „OK“. (→ Zielverzeichnis … → Ordner auswählen)

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Das dearchivierte und geöffnete Projekt speichern Sie unter dem Namen 142-200_Industrial_Security_mit_S615. (→ Projekt → Speichern unter … → 142-200_Industrial_Security_mit_S615 → Speichern)



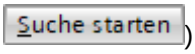
7.2 Einstellen der IP-Adresse des SCALANCE S615

→ Verbinden Sie das Programmiergerät mit dem Port 4 des SCALANCE S615.

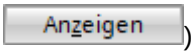
→ Trennen Sie alle anderen Verbindungen zum SCALANCE S615

→ Stellen Sie sicher, dass Ihr Programmiergerät sich im Subnetz 192.168.1.0/24 befindet. Folgen Sie den Anweisungen in Abschnitt 4.6.

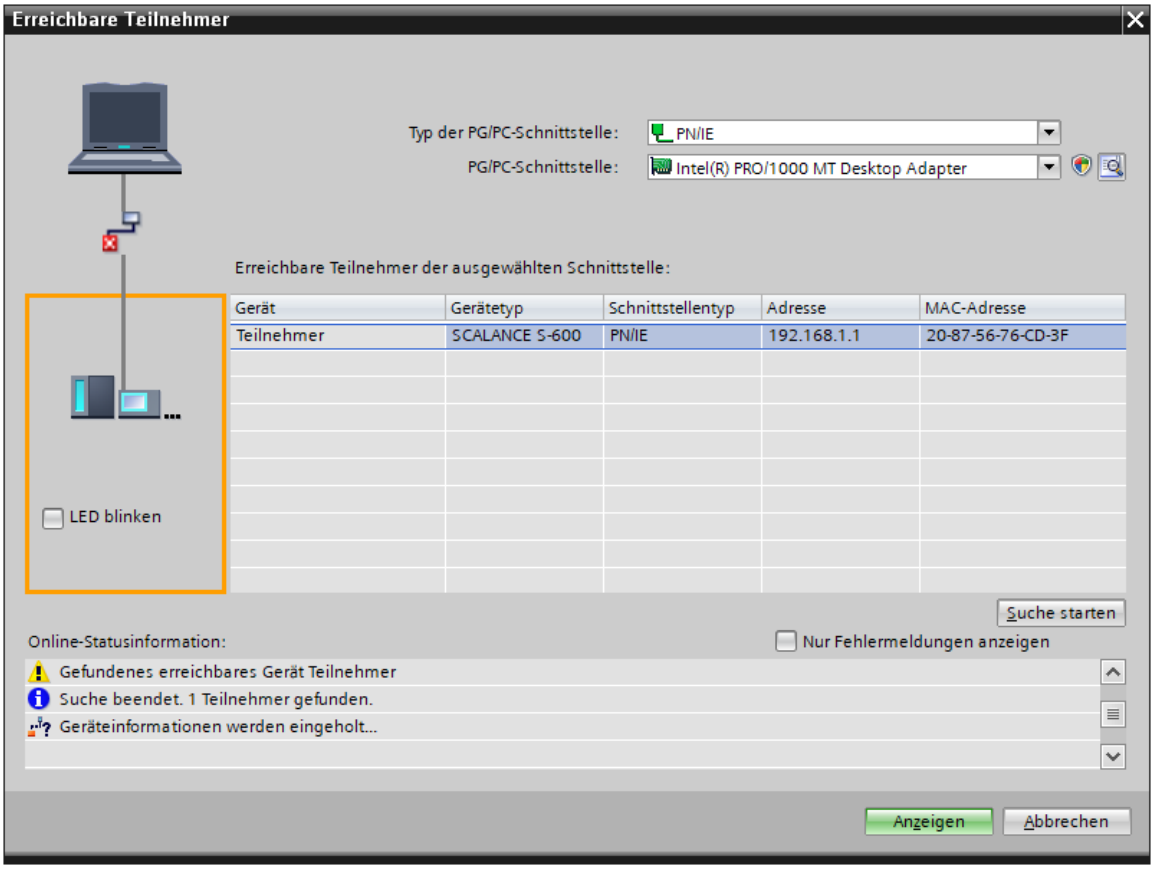
→ Öffnen Sie die Suche nach Erreichbaren Teilnehmern. (→ )

→ Wählen Sie Ihre PN/IE Schnittstelle aus und starten Sie die Suche. (→ 

)

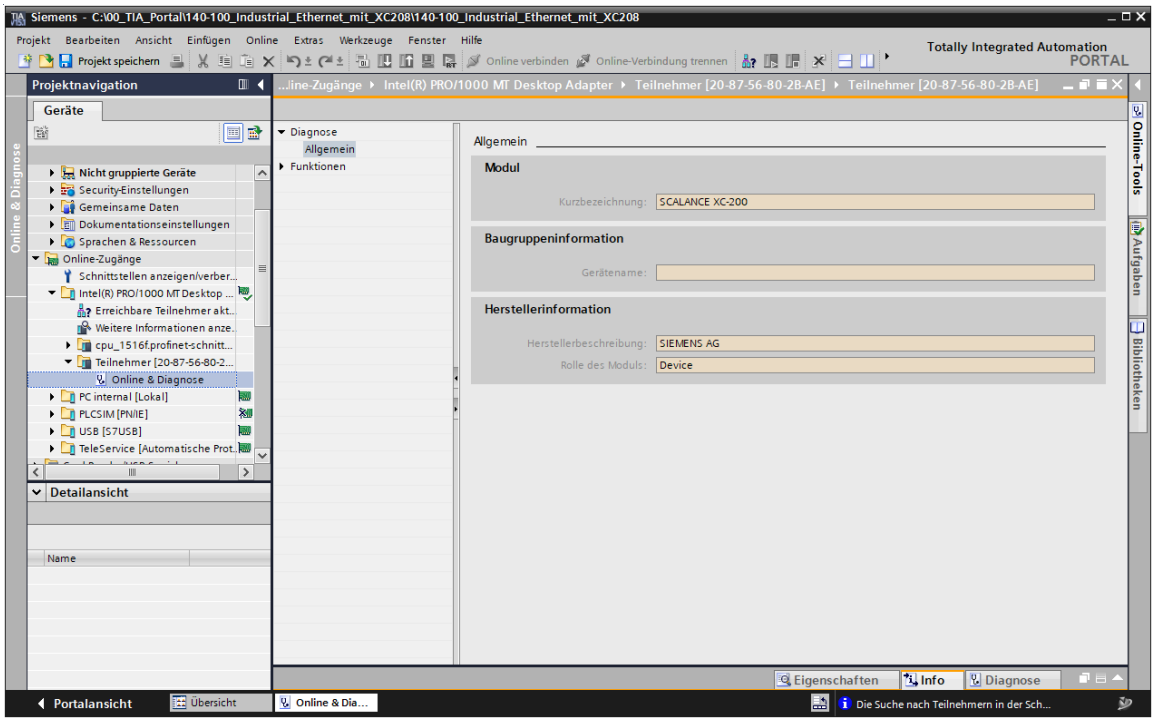
→ Wählen Sie den SCALANCE S-600 aus und klicken Sie auf „Anzeigen“. (→ 

)

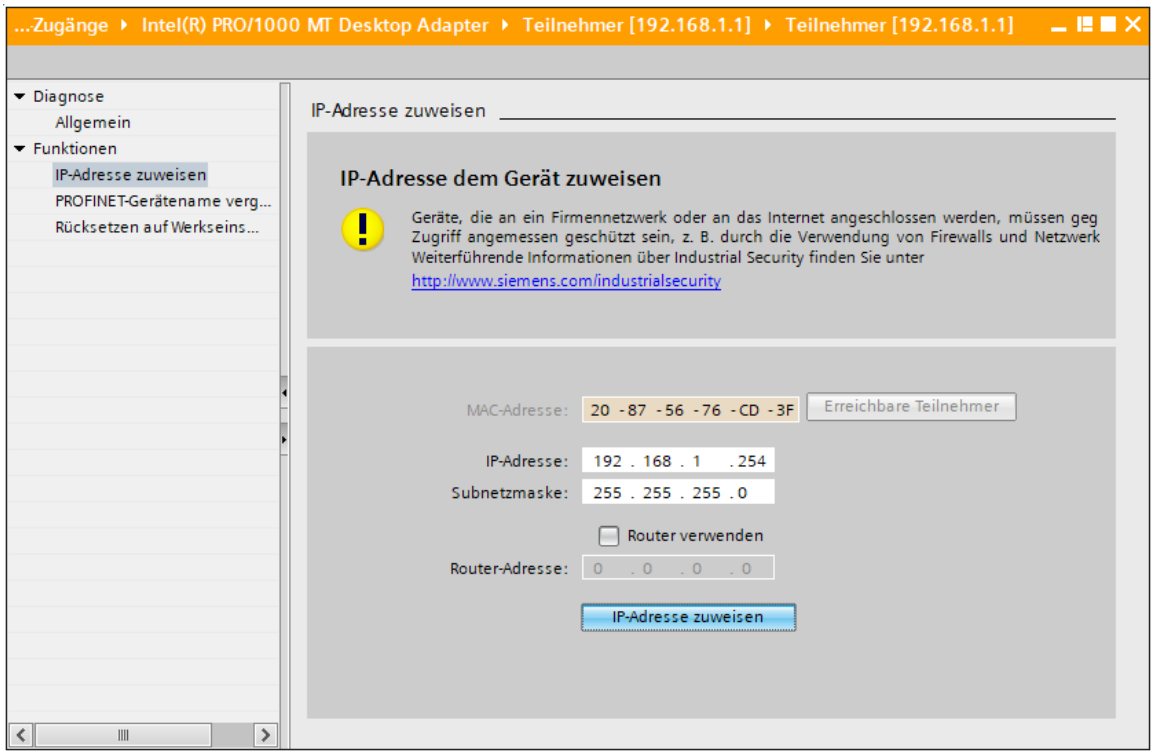


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Öffnen Sie unter „Online-Zugänge“ den Punkt „Online&Diagnose“ des angezeigten Teilnehmers.



→ Stellen Sie die IP-Adresse auf 192.168.1.254/24. (→ Funktionen → IP-Adresse zuweisen → IP-Adresse: 192.168.1.254 → Subnetzmaske: 255.255.255.0 → IP-Adresse zuweisen)

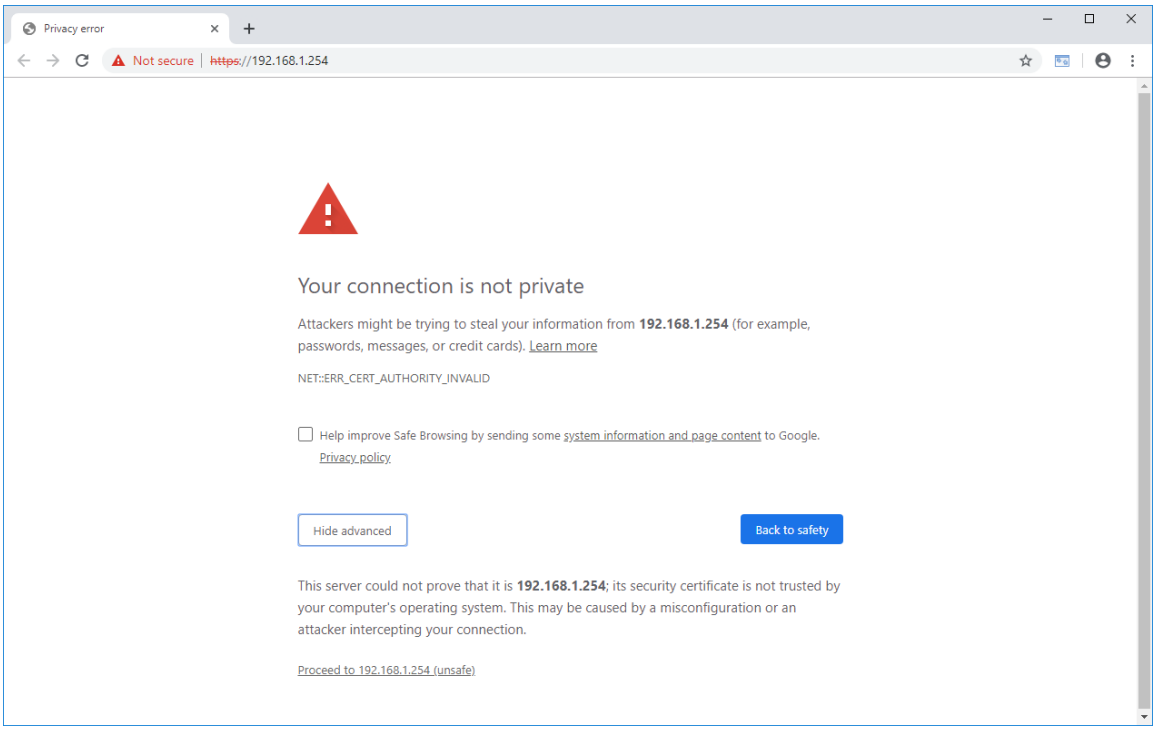


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

7.3 Grundkonfiguration des SCALANCE S615

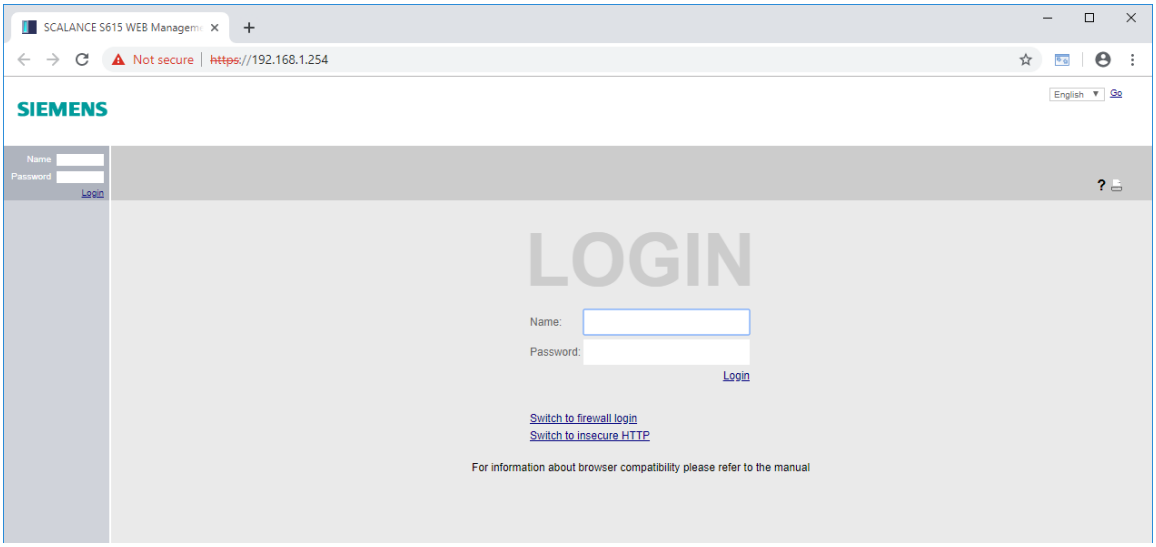
→ Öffnen Sie im Browser die Weboberfläche des SCALANCE S615. (→ https://192.168.1.254)

→ Die Weboberfläche des SCALANCE S615 ist mit einem selbstsignierten Zertifikat geschützt. Bestätigen Sie die Ausnahme, um fortzufahren.



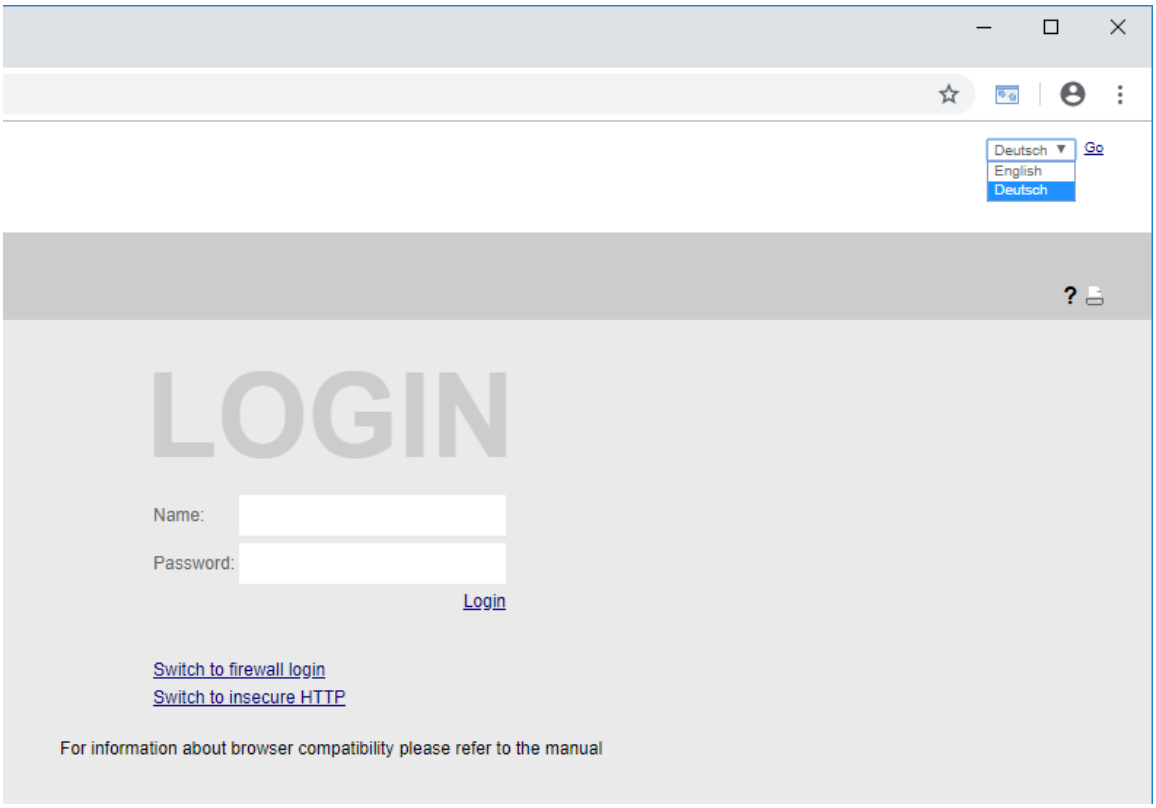
Hinweis:

– *Je nach Browser sieht das Bestätigen des Zertifikats etwas anders aus.*

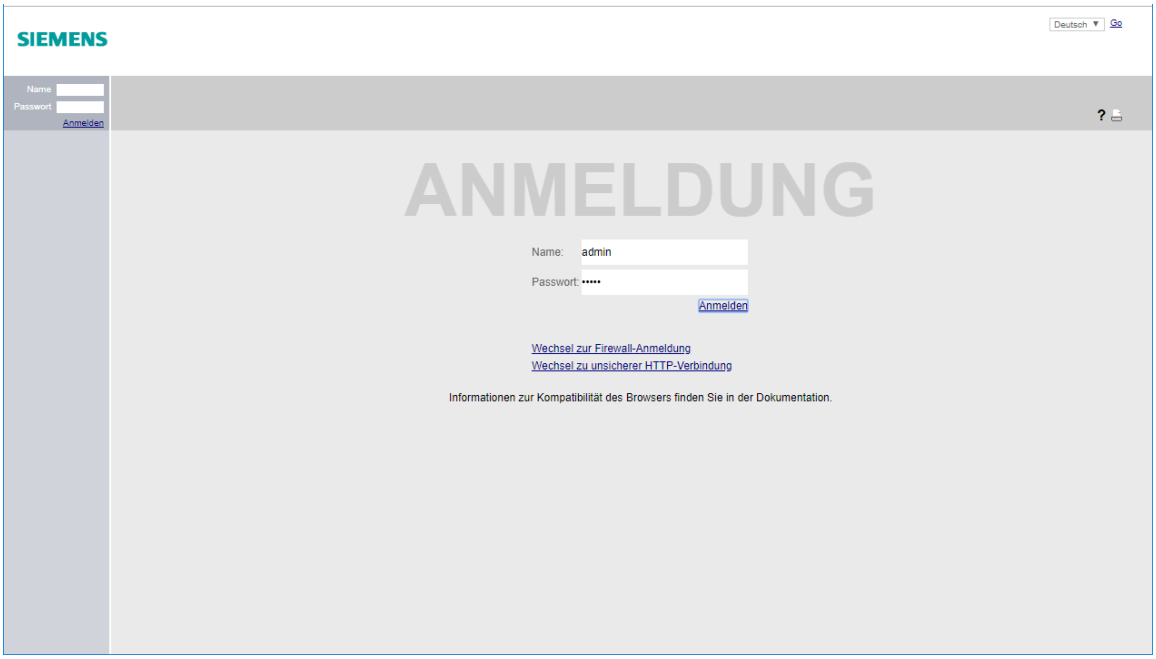


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Wechseln Sie als Erstes die Sprache der Oberfläche auf Deutsch. (→ Deutsch → Go)

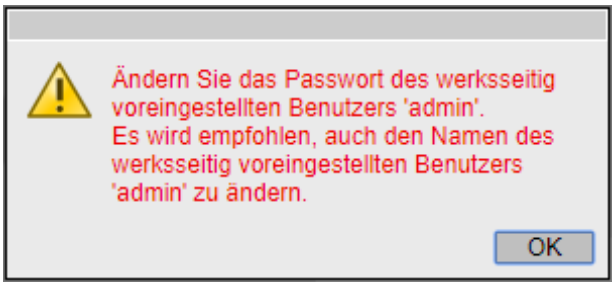


→ Als Nächstes können Sie sich mit dem Benutzer „admin“ und dem Passwort „admin“ einloggen. (→ Name: admin → Password: admin → Login)



Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Der Standardzugang muss vor dem ersten Login geändert werden. (→ OK)



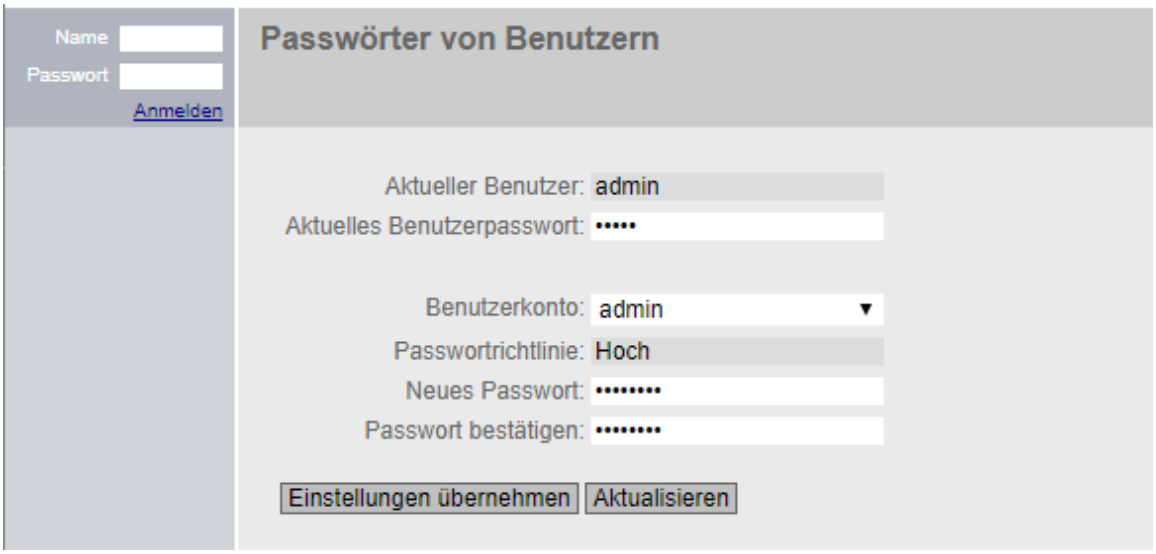
→ Geben Sie zuerst das alte Passwort ein „admin“ und anschließend zweimal ein neues Passwort.

→ Aktuelles Benutzerpasswort: admin

→ Neues Passwort: ***

→ Passwort bestätigen: ***

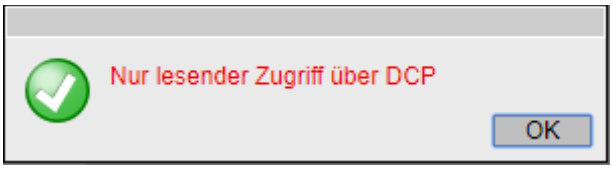
→ Einstellungen übernehmen



Hinweis:

– *Das neue Passwort benötigt mindestens acht Zeichen, eine Zahl, ein groß geschriebenes Zeichen und ein Sonderzeichen!*

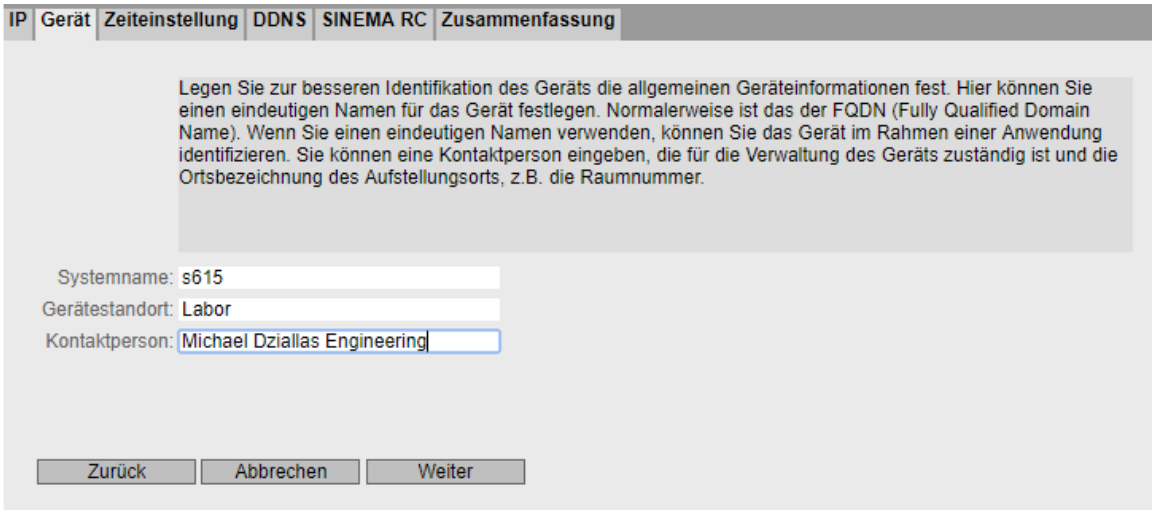
→ Nach erfolgreicher Änderung der Zugangsdaten und Anmeldung wird der DCP-Zugriff auf das Gerät nur noch lesend zugelassen. (→ OK)



Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

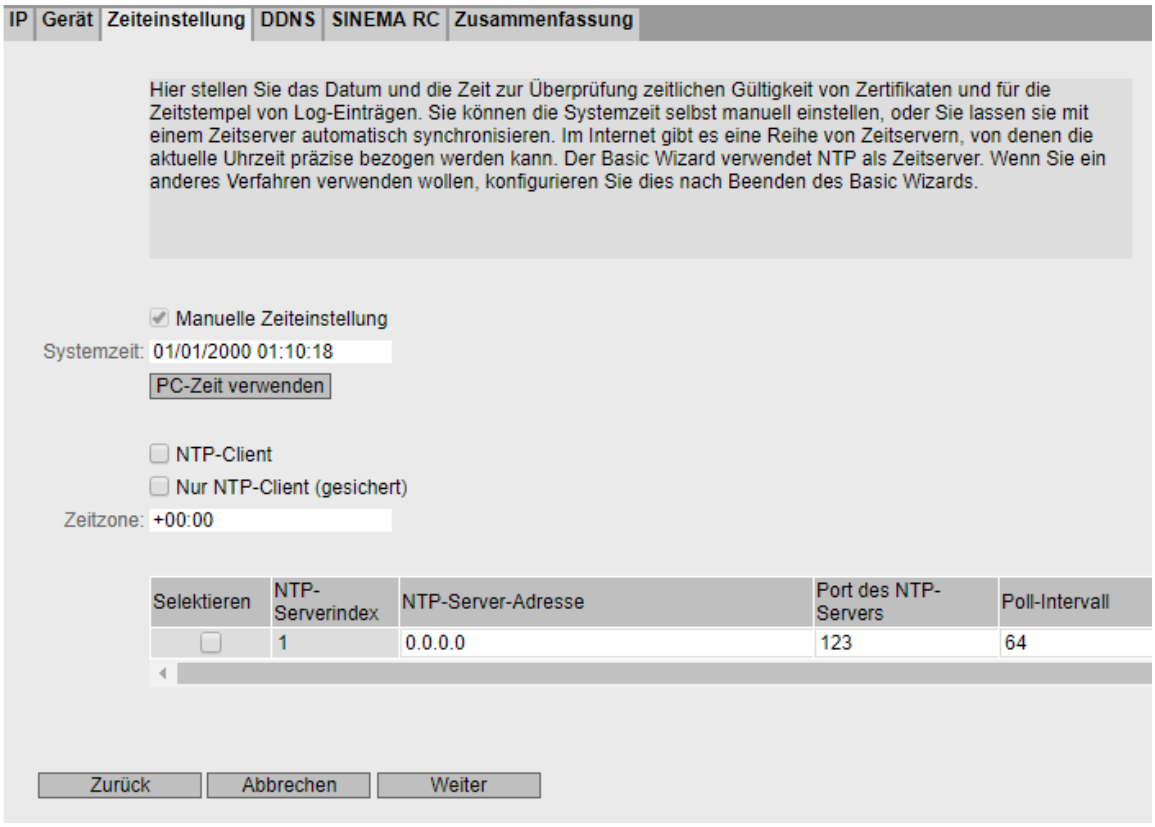
→ Stellen Sie im folgenden Konfigurationsassistenten das VLAN 2 auf die statische Adresse 10.0.0.254/24 und klicken Sie auf „Weiter“. (Extern (vlan2) → DHCP → IP-Adresse: 10.0.0.254 → ☐ Subnetzmaske: 255.255.255.0 → Weiter)

→ Füllen Sie die Identifikationsdaten nach Belieben aus und klicken Sie „Weiter“. (→ Systemname: … → Gerätestandort: … → Kontaktperson: … → Weiter)

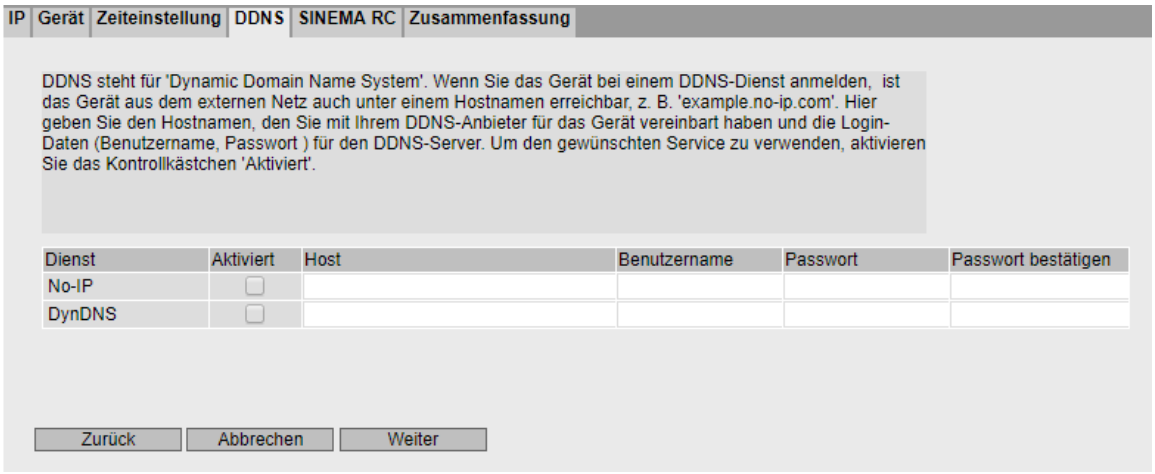


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Übernehmen Sie die Zeit vom PC und klicken Sie „Weiter“. (→ PC-Zeit verwenden → Weiter)

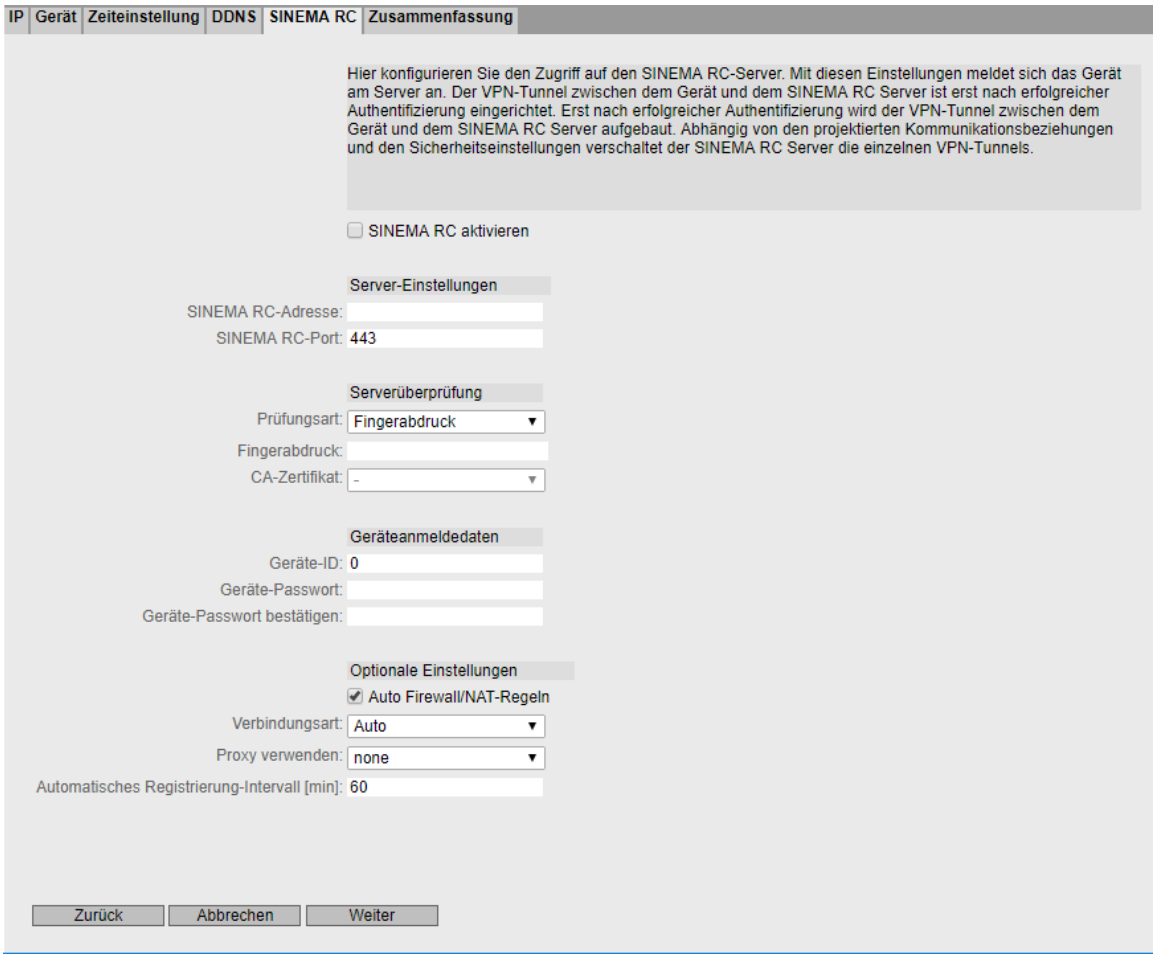


→ Überspringen Sie die dynamischen DNS Einstellungen mit „Weiter“. (→ Weiter)



Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Überspringen Sie die SINEMA RC Einstellungen mit „Weiter“. (→ Weiter)

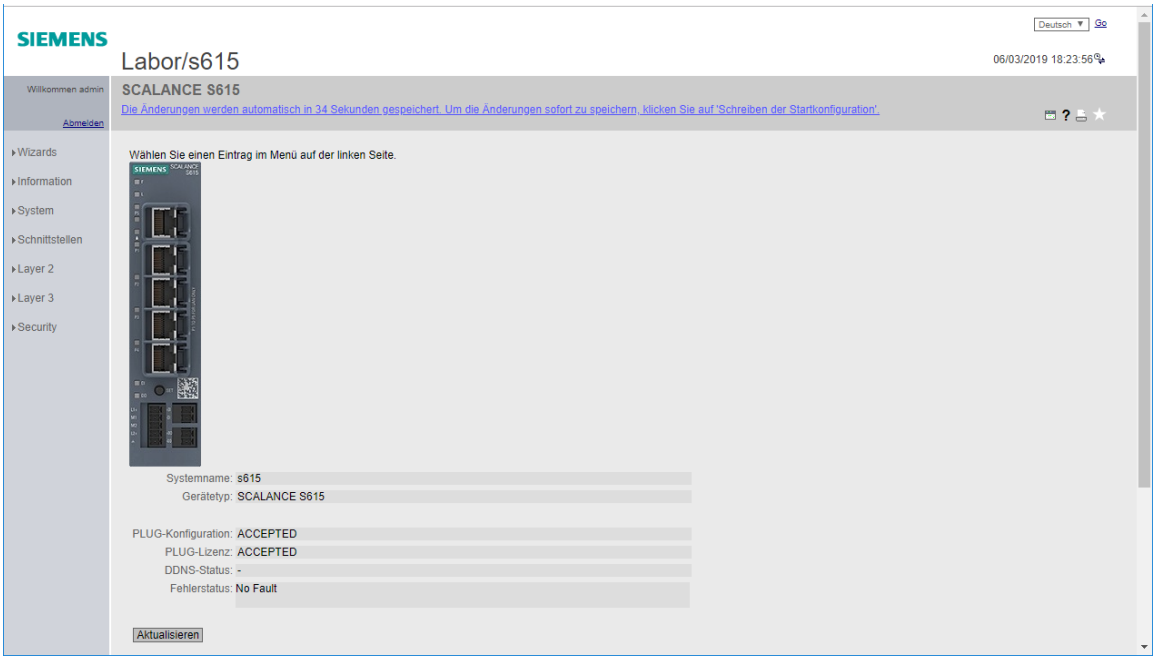


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Überprüfen Sie erneut alle Einstellungen in der Zusammenfassung und Bestätigen Sie die Konfiguration. (→ Einstellungen übernehmen)

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Nach Übernahme der Einstellungen landen Sie in der endgültigen Weboberfläche des SCALANCE S615.

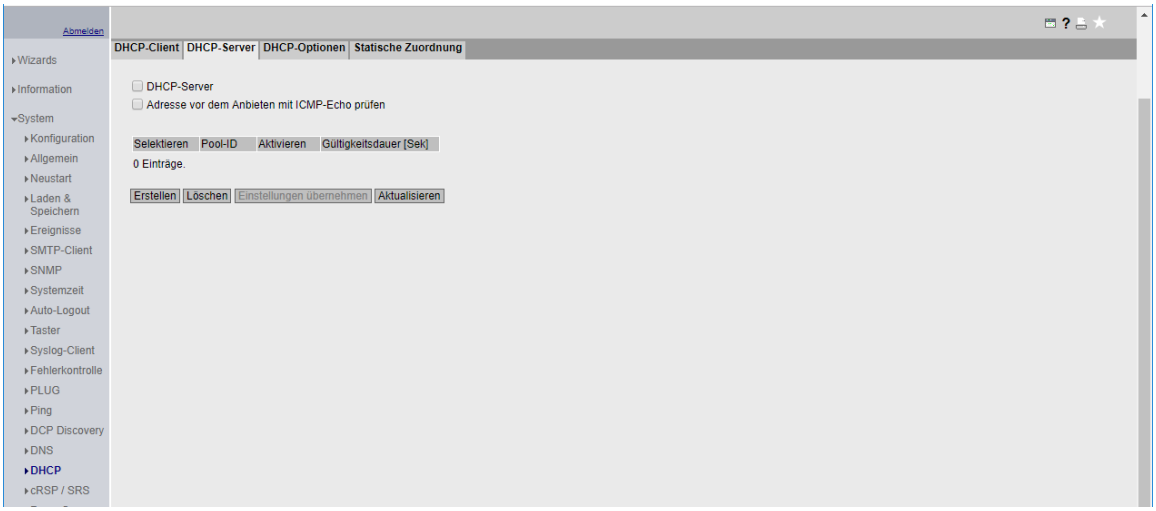


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

7.4 Konfiguration des DHCP-Servers

Um die Verbindung mit dem Anlagennetz so einfach wie möglich für den Service-Techniker und auch später bei den Tests zu gestalten, wird der SCALANCE S615 sowohl im gesicherten als auch im ungesicherten Bereich dynamische Adressen vergeben.

→ Wechseln Sie im Menü System auf die DHCP-Server Einstellungen. (→ System → DHCP → DHCP-Server)



→ Erstellen Sie zunächst einen neuen Pool an IP-Adressen. (→ Erstellen)

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

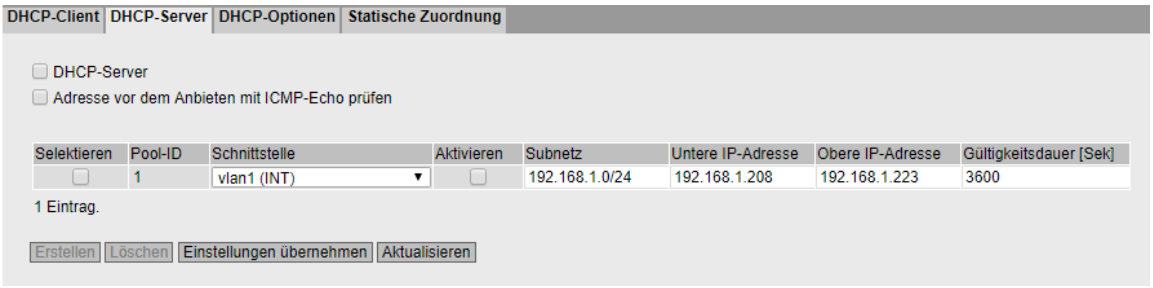
→ Wählen Sie für die Schnittstelle vlan1 aus. (→ Schnittstelle: vlan1 (INT))

→ Stellen Sie das korrekte Subnetz ein. (→ Subnetz: 192.168.1.0/24)

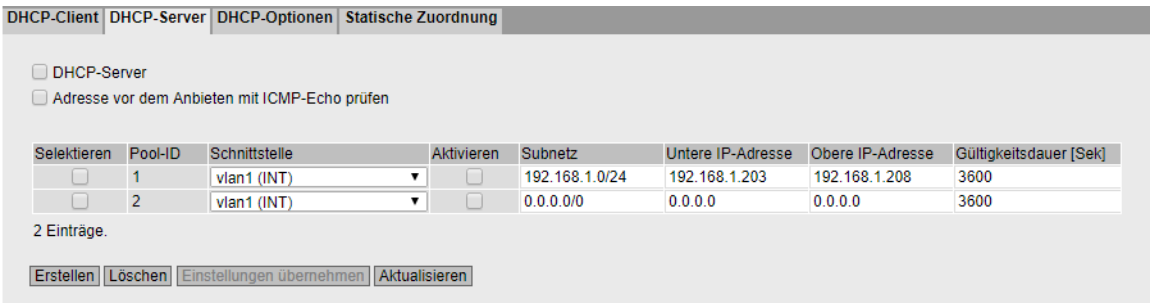
→ Setzen Sie die erste IP-Adresse. (→ Untere IP-Adresse: 192.168.1.208)

→ Setzen Sie die letzte IP-Adresse. (→ Obere IP-Adresse: 192.168.108.223)

→ Übernehmen Sie die Einstellungen. (→ Einstellungen übernehmen)



→ Erstellen Sie einen weiteren Pool an IP-Adressen (→ Erstellen)

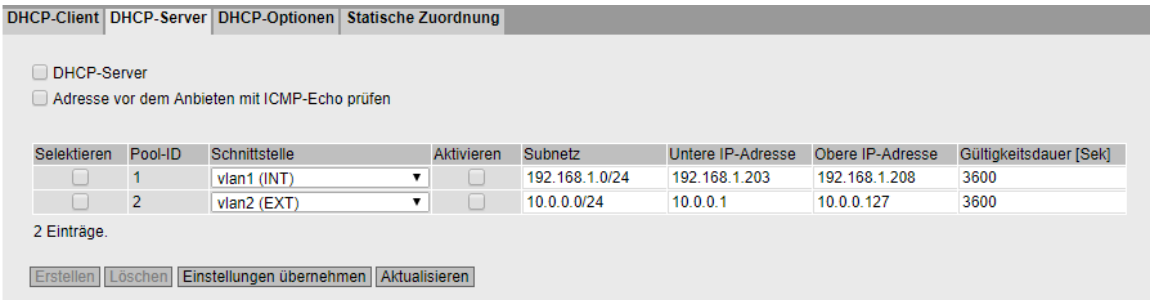


→ Wählen Sie für die Schnittstelle vlan2 aus. (→ Schnittstelle: vlan2 (EXT))

→ Stellen Sie das korrekte Subnetz ein. (→ Subnetz: 10.0.0.0/24)

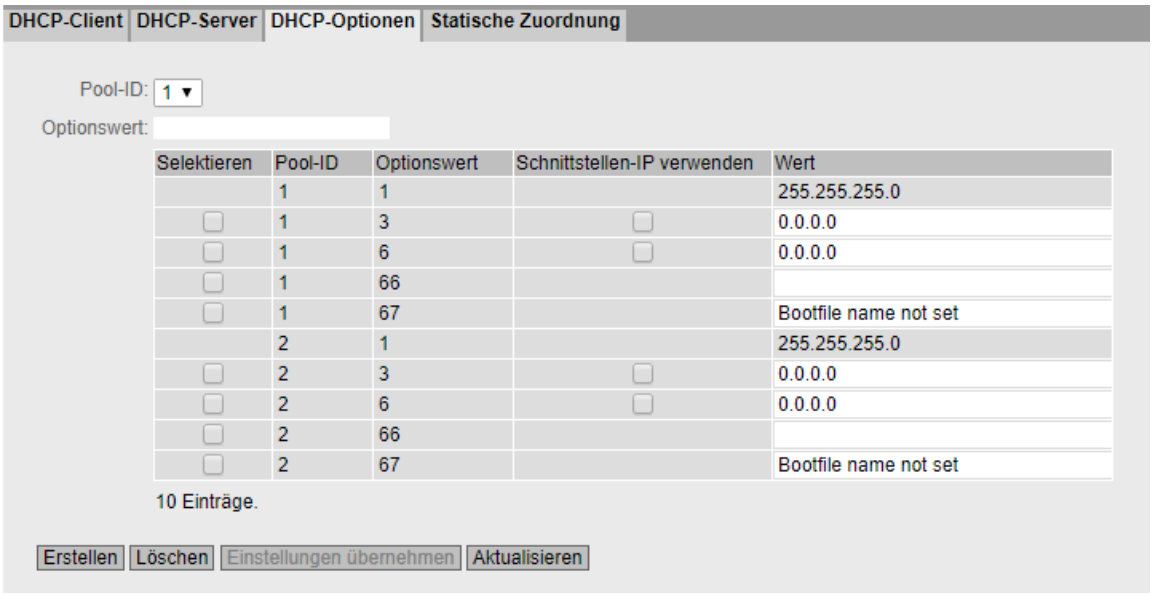
→ Setzen Sie die erste IP-Adresse. (→ Untere IP-Adresse: 10.0.0.1)

→ Setzen Sie die letzte IP-Adresse. (→ Obere IP-Adresse: 10.0.0.127)



Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Wechseln Sie in den Reiter DHCP-Optionen (→ DHCP-Optionen)



→ Verwenden Sie in beiden Pools, bei der Option 3 die Schnittstellen-IP und übernehmen Sie die Einstellungen.

(→ Pool-ID: 1 → Optionswert: 3 → ☑ Schnittstellen-IP verwenden)

(→ Pool-ID: 2 → Optionswert: 3 → ☑ Schnittstellen-IP verwenden)

(→ Einstellungen übernehmen)

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Wechseln Sie zurück auf den DHCP-Server. (→ DHCP-Server)

→ Aktivieren Sie den DHCP-Server. (→ ☑ DHCP-Server)

→ Aktivieren Sie die beiden Pools. (→ ☑ Aktivieren)

→ Übernehmen Sie die Einstellungen (→ Einstellungen übernehmen)

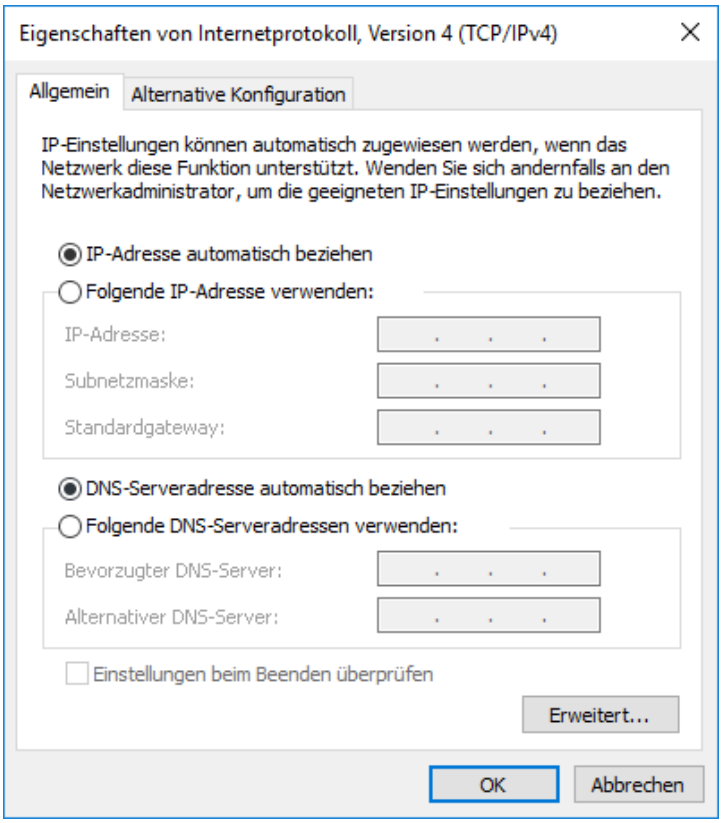
Hinweis:

– *Der S615 wird darauffolgend auf den Ports 1 bis 4 Adressen aus dem Subnetz 192.168.1.0/24 verteilen und auf dem Port 5 aus dem Netz 10.0.0.0/24. Dabei wird er jeweils seine eigene IP als Gateway mitliefern.*

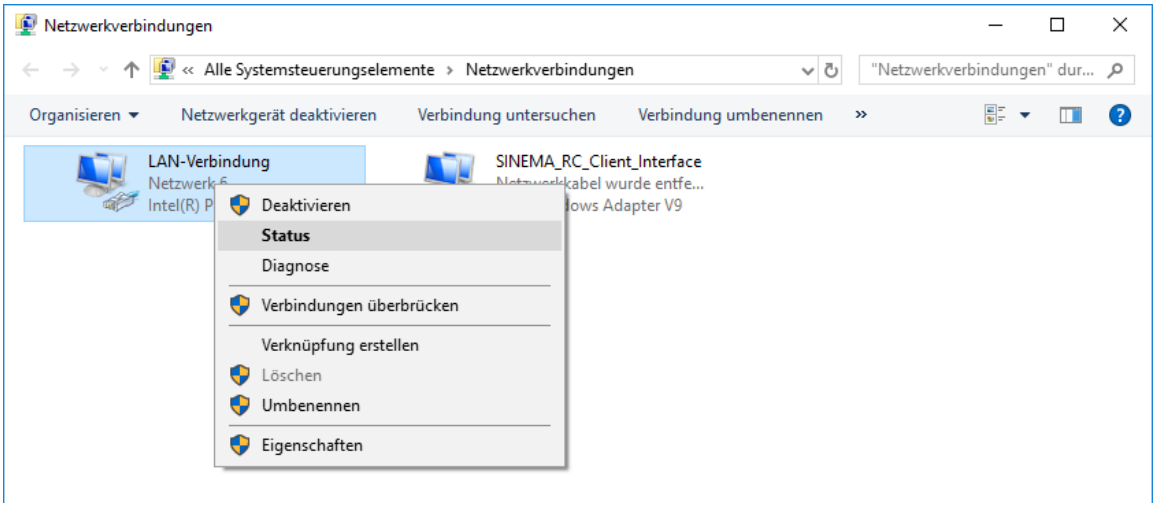
Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Für die Einstellungen am Programmiergerät folgen Sie den Anweisungen im Abschnitt 4.6 bis zu den Einstellungen des Internetprotokolls, Version 4 (TCP/IP).

→ Beziehen Sie die IP-Adresse automatisch anstelle der statischen Konfiguration. (→ IP-Adresse automatisch beziehen → DNS-Serveradresse automatisch beziehen)

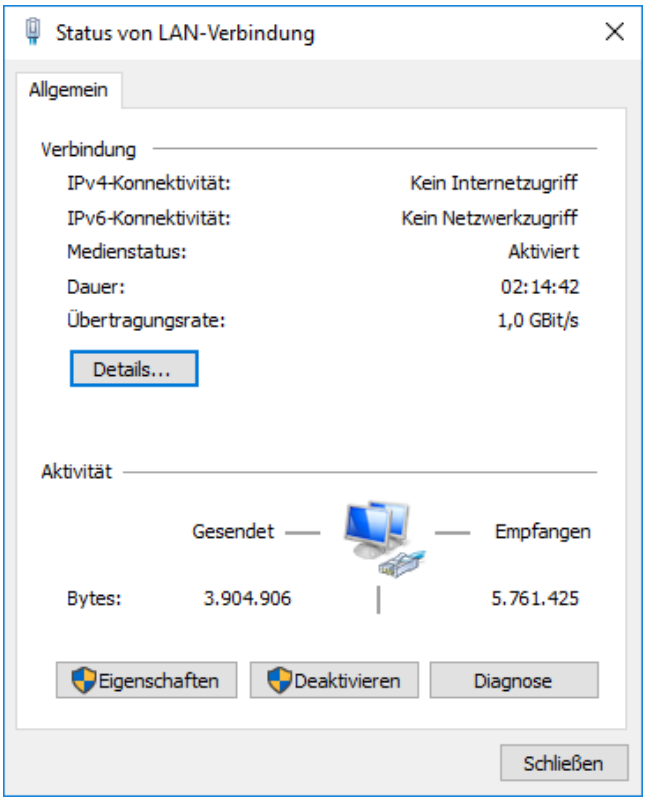


→ Bestätigen Sie die Änderungen und öffnen Sie in den Netzwerkverbindungen den Status der Verbindung. (→ LAN-Verbindung → Status)

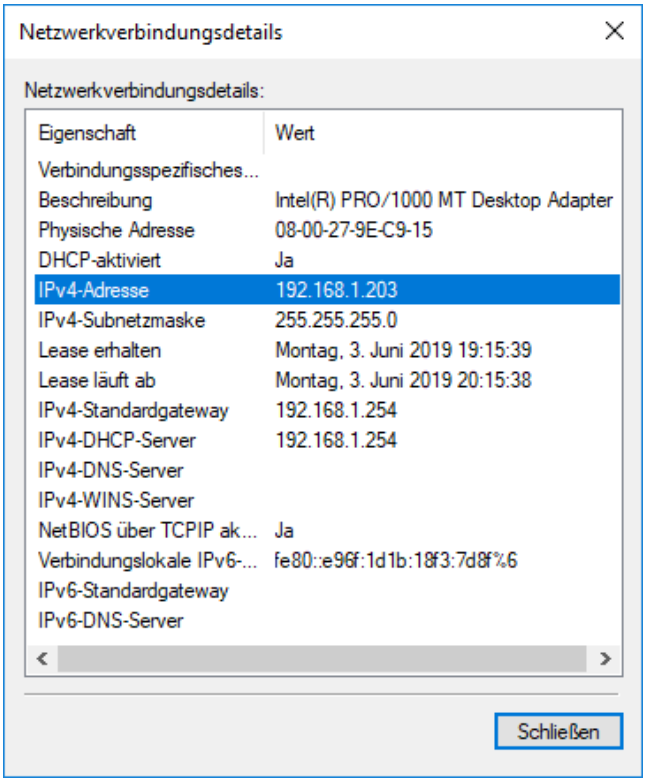


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Klicken Sie auf Details. (→ Details)



→ Stellen Sie sicher, dass das Programmiergerät eine passende IP-Adresse und ein Gateway zugewiesen bekommen hat.

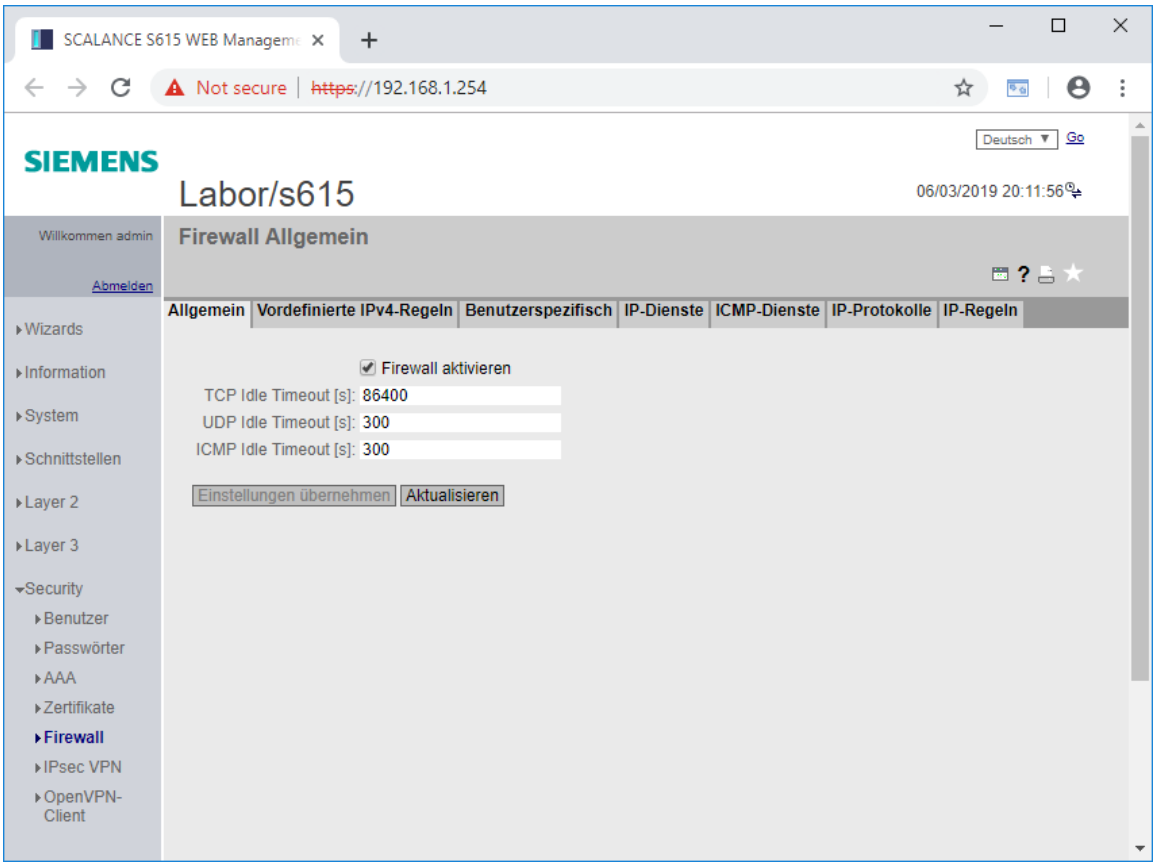


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

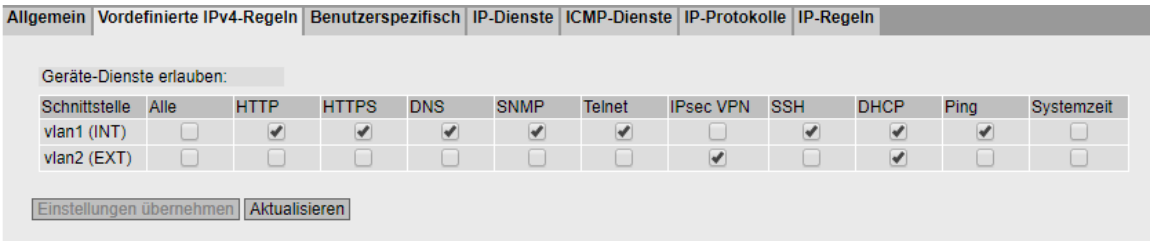
7.5 Einrichten der Firewall

In der Werkskonfiguration lässt der SCALANCE S615 keine Verbindungen zwischen den beiden VLANs zu. Geräte an den Ports 1 bis 4 können also nicht mit Geräten am Port 5 kommunizieren und umgekehrt. Damit also Geräte z.B. aus dem Firmennetz auf den OPC UA Server der CPU zugreifen können muss diese Verbindung freigegeben werden."

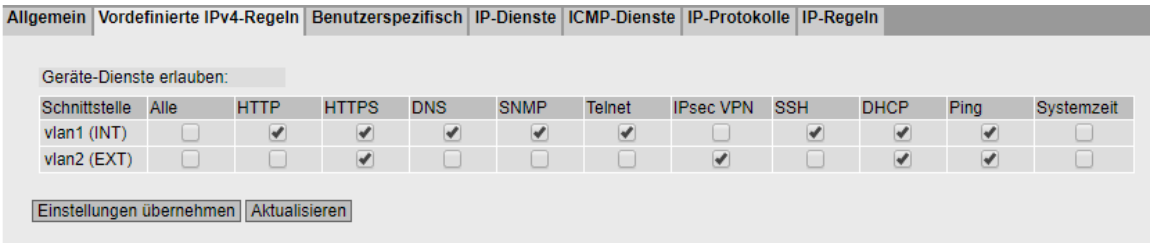
→ Öffnen Sie die Firewall Einstellungen im Menü Security. (→ Security → Firewall)



→ Wechseln Sie auf den Reiter Vordefinierte IPv4-Regeln. (→ Vordefinierte IPv4-Regeln)



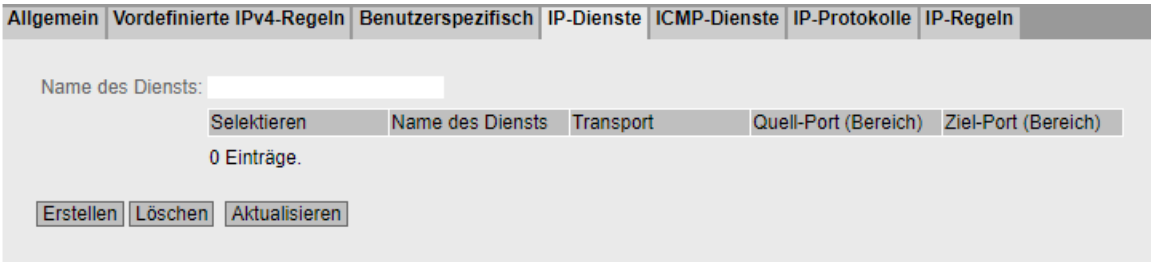
→ Erlauben Sie von extern den Zugriff via HTTPS und Ping auf den S615 und übernehmen Sie die Einstellungen. (→ vlan2 (EXT) → ☑ HTTPS → ☑ Ping)



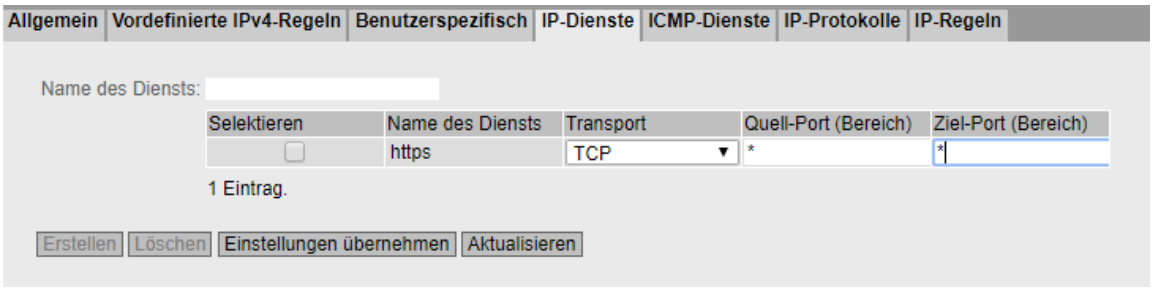
Hinweis:

– *Der Haken bei HTTPS erlaubt von außen den Zugriff auf die Konfigurationsoberfläche und sollte nicht unüberlegt eingeschaltet werden. Wir benötigen diesen Zugriff jedoch später für die Authentifizierung am S615. Da das außen angeschlossene Firmennetz kein öffentliches Netzwerk ist, ist das Risiko hier relativ gering. Ein am Internet angeschlossener SCALANCE S615 sollte von extern nur IPsec VPN, Ping und je nach Konfiguration DHCP erlauben.*

→ Wechseln Sie in den Reiter IP-Dienste. (→ IP-Dienste)

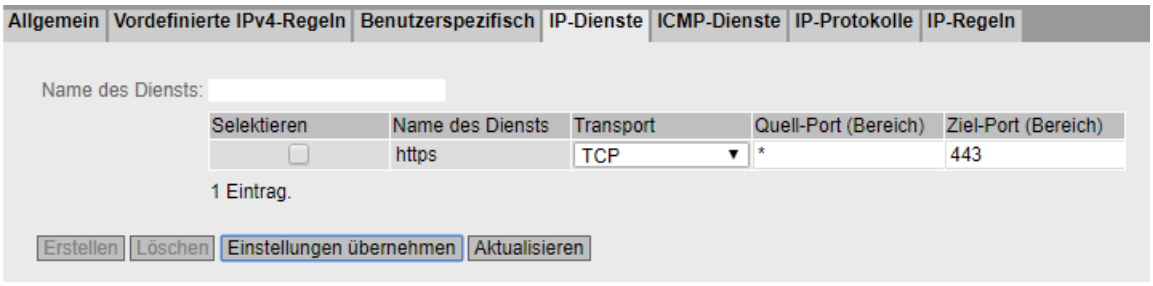


→ Erstellen Sie einen neuen Dienst für den Webserver der CPU. (→ Name des Diensts: https → Erstellen)

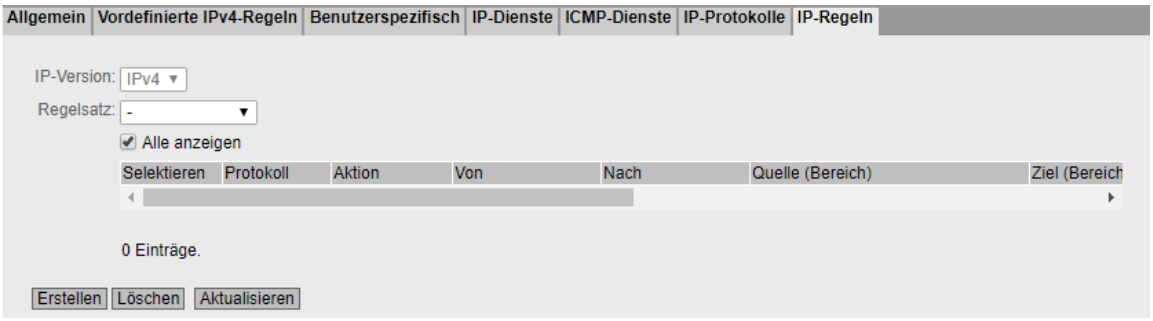


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

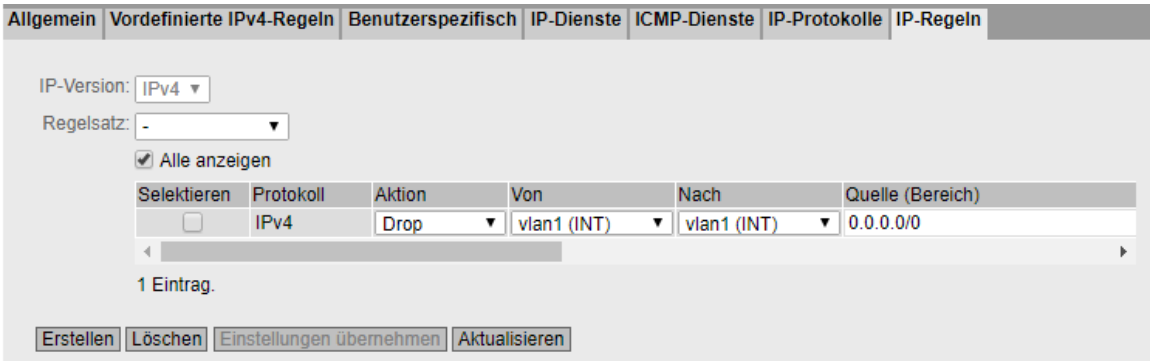
→ Geben Sie den HTTPS Port als Ziel-Port an und übernehmen Sie die Einstellungen. (→ Ziel-Port: 443 → Einstellungen übernehmen)



→ Wechseln Sie auf den Reiter IP-Regeln. (→ IP-Regeln)



→ Erstellen Sie eine neue Regel. (→ Erstellen)



Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Stellen Sie die Aktion auf Accept. (→ Aktion: Accept)

→ Wählen Sie als Quell-Interface vlan2 aus. (→ Von: vlan2 (EXT))

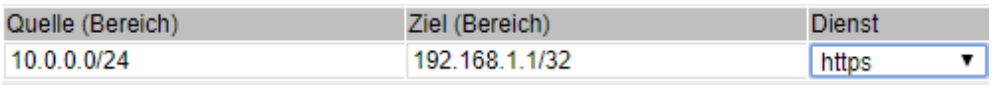
→ Wählen Sie als Ziel-Interface vlan1 aus. (→ Nach: vlan1 (INT))

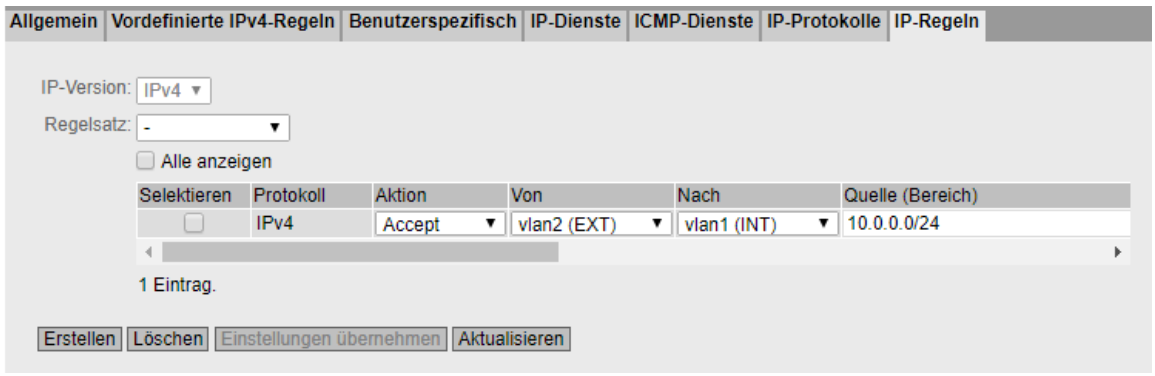
→ Geben Sie als Quellnetz das Firmensubnetz 10.0.0.0/24 an. (→ Quelle: 10.0.0.0/24)

→ Geben Sie Ziel die X2 IP der S7-1500 an. (→ Ziel: 192.168.1.1/32)

→ Wählen Sie als Dienst den soeben erstellten HTTPS Dienst aus. (→ Dienst: https)

→ Übernehmen Sie die Einstellungen. (→ Einstellungen übernehmen)



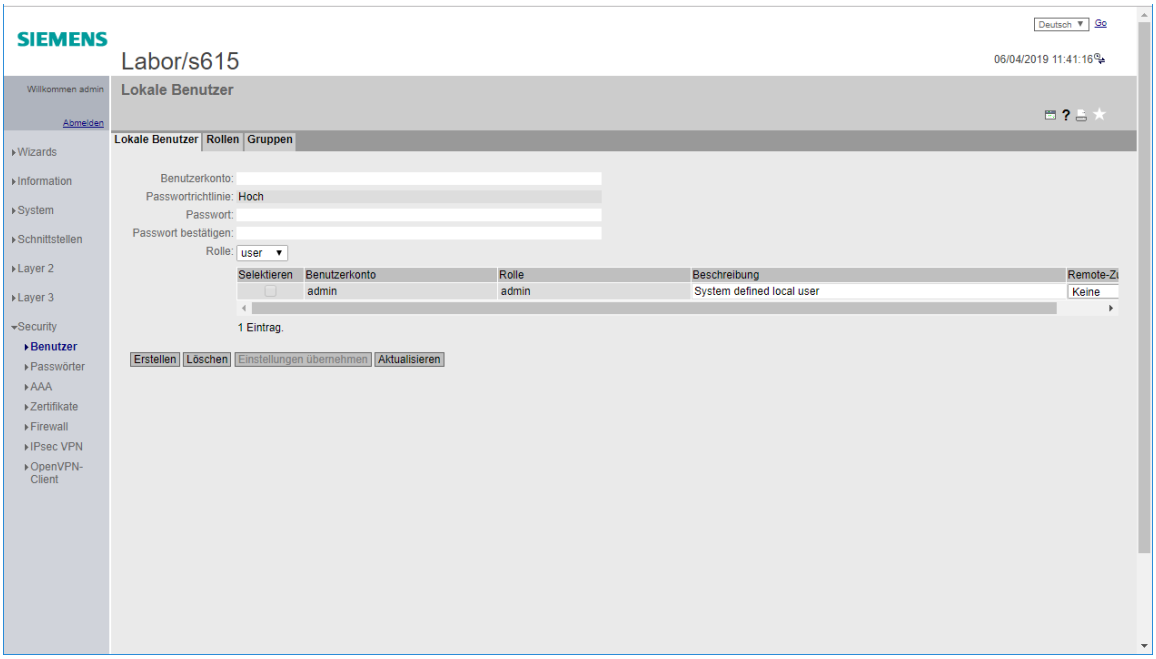


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

7.6 Einrichten des Service Benutzers

Nachdem der Zugriff auf den Webserver von außen eingerichtet worden ist, werden im nächsten Schritt spezifische Regeln angelegt, welche durch die Anmeldung am System mittels eines Benutzers, freigeschaltet werden.

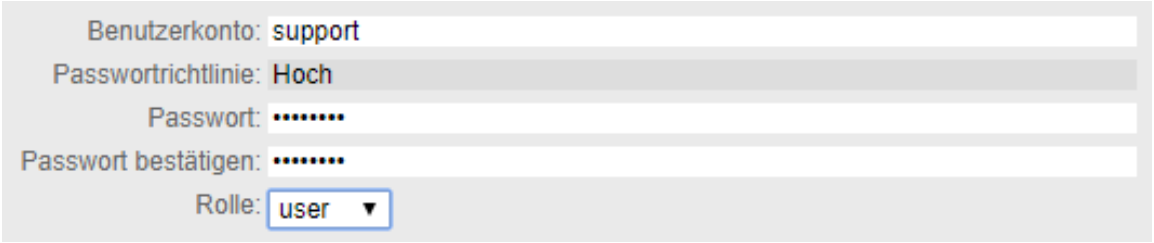
→ Öffnen Sie die Lokale Benutzerverwaltung. (→ Security → Benutzer → Lokale Benutzer)



→ Geben Sie einen neuen Benutzernamen an. (→ Benutzerkonto: Support)

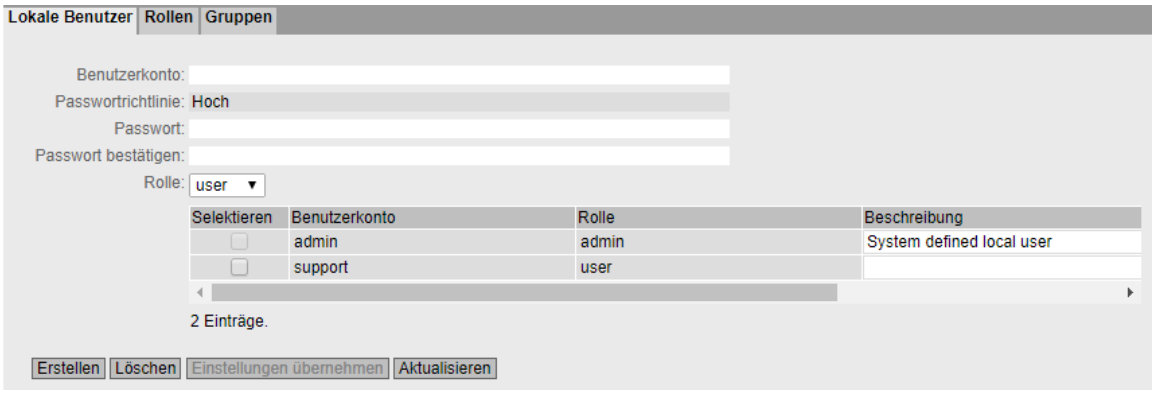
→ Geben Sie ein Passwort an. (→ Passwort: *** → Passwort bestätigen: ***)

→ Wählen Sie als Rolle „user“ aus. (→ Rolle: user)



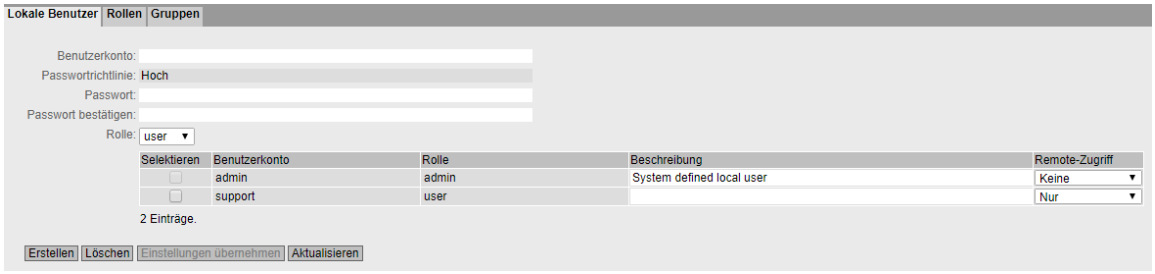
Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Klicken Sie auf Erstellen. (→ Erstellen)



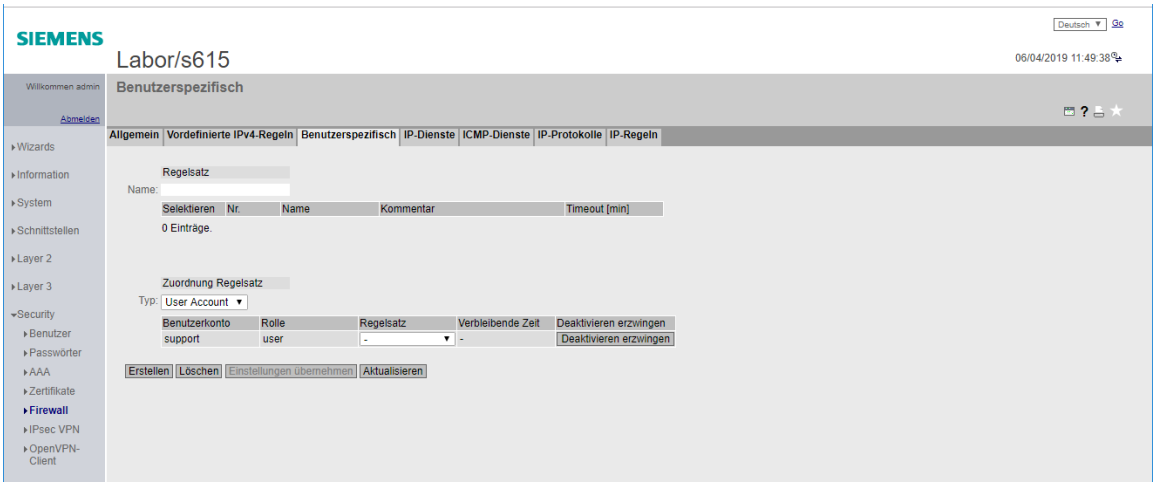
→ Wählen Sie als Remote-Zugriff „nur“ aus. (→ support → Remote-Zugriff: nur)

→ Übernehmen Sie die Einstellungen. (→ Einstellungen übernehmen)



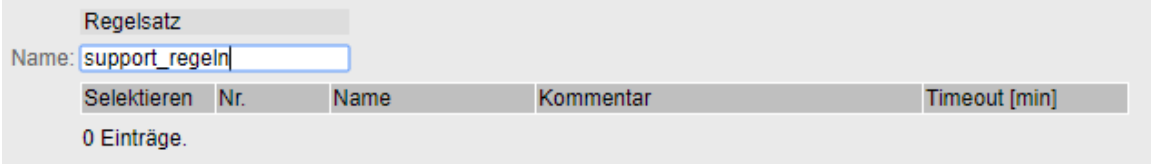
→ Wechseln Sie unter Firewall in den Reiter Benutzerspezifisch.

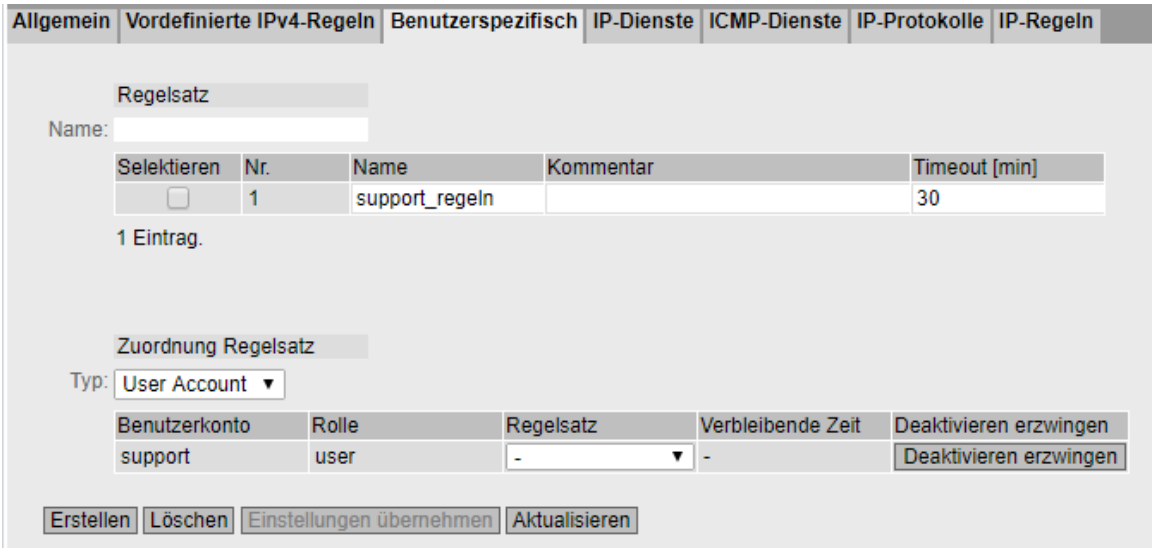
(→ Security → Firewall → Benutzerspezifisch)



Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Fügen Sie einen neuen Regelsatz „support_regeln“ hinzu. (→ Regelsatz → Name: support_regeln → Erstellen)





→ Ordnen Sie dem Benutzer „support“ den Regelsatz „support_regeln“ zu. (→ Zuordnung Regelsatz → support → Regelsatz: support_regeln)

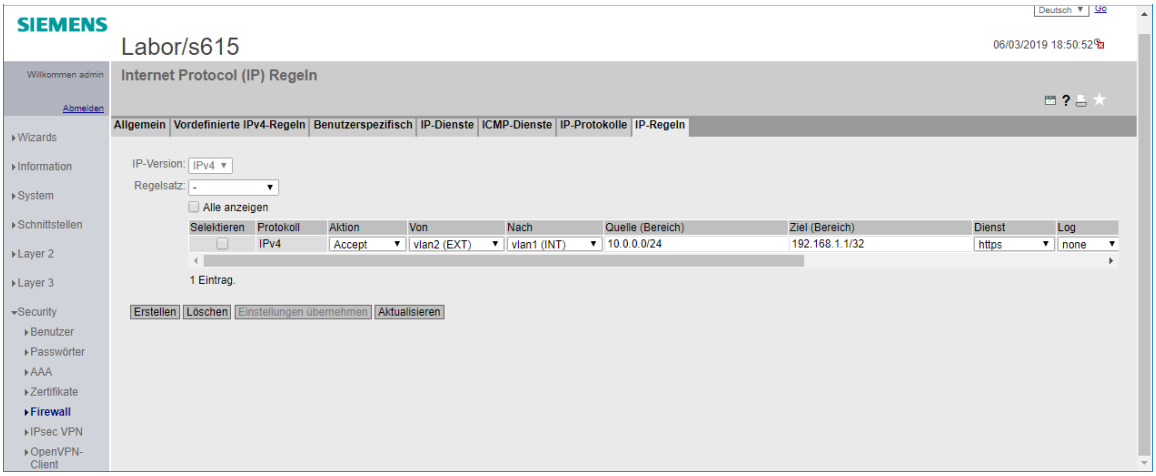
→ Übernehmen Sie die neuen Einstellungen. (→ Einstellungen übernehmen)

Hinweis:

– *Hierdurch wird auf dem Computer des Benutzers „support“, nach erfolgreicher Anmeldung am System, das zusätzliche Regelwerk „support_regeln“ angewendet.*

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Wechseln Sie in den Reiter IP-Regeln. (→ Security → Firewall → IP-Regeln)



→ Erstellen Sie eine neue Regel. (→ Erstellen)

→ Stellen Sie die Aktion auf Accept. (→ Aktion: Accept)

→ Wählen Sie als Quell-Interface vlan2 aus. (→ Von: vlan2 (EXT))

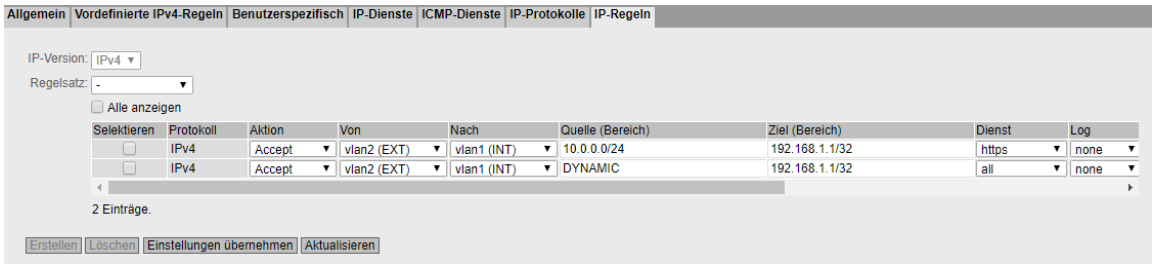
→ Wählen Sie als Ziel-Interface vlan1 aus. (→ Nach: vlan1 (INT))

→ Geben Sie als Quellnetz „DYNAMIC“ an. (→ Quelle: DYNAMIC)

→ Geben Sie als Ziel die X2 IP der S7-1500 an. (→ Ziel: 192.168.1.1/32)

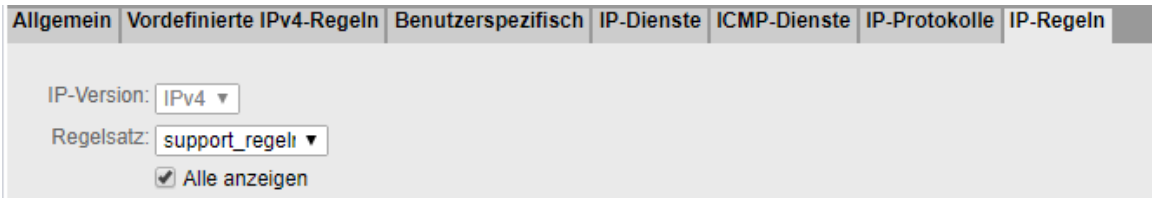
→ Wählen Sie als Dienst „all“ aus. (→ Dienst: all)

→ Übernehmen Sie die Einstellungen. (→ Einstellungen übernehmen)

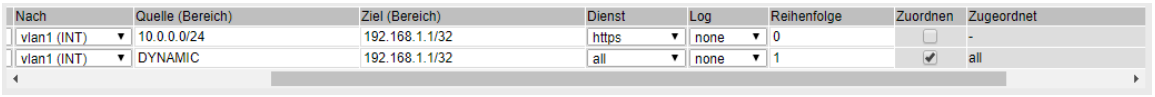


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

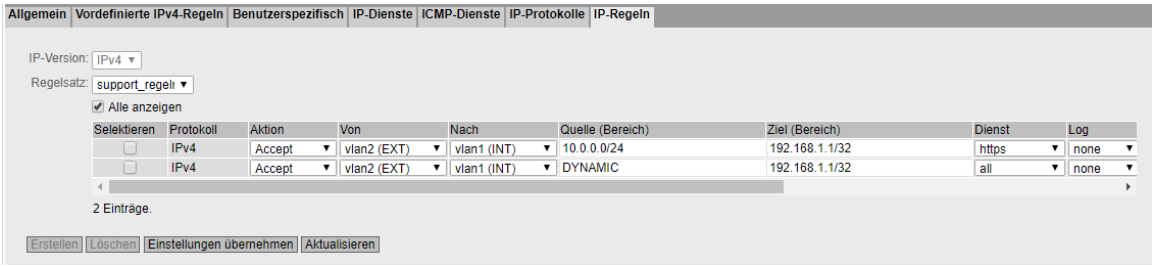
→ Wählen Sie als Nächstes unter Regelsatz „support_regeln“ aus. (→ Regelsatz: support_regeln → Alle anzeigen)



→ Markieren Sie bei der soeben angelegten Regel die Option Zuordnen. (→ Zuordnen)



→ Übernehmen Sie die Einstellungen. (→ Einstellungen übernehmen)



Hinweis:

– *Der Platzhalter DYNAMIC wird bei der Anmeldung mit der IP des angemeldeten Benutzers ersetzt. Durch die Zuordnung der Regel an das Regelwerk „support_regeln“ ist diese erst aktiv, nachdem der entsprechende Benutzer sich angemeldet hat.*

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

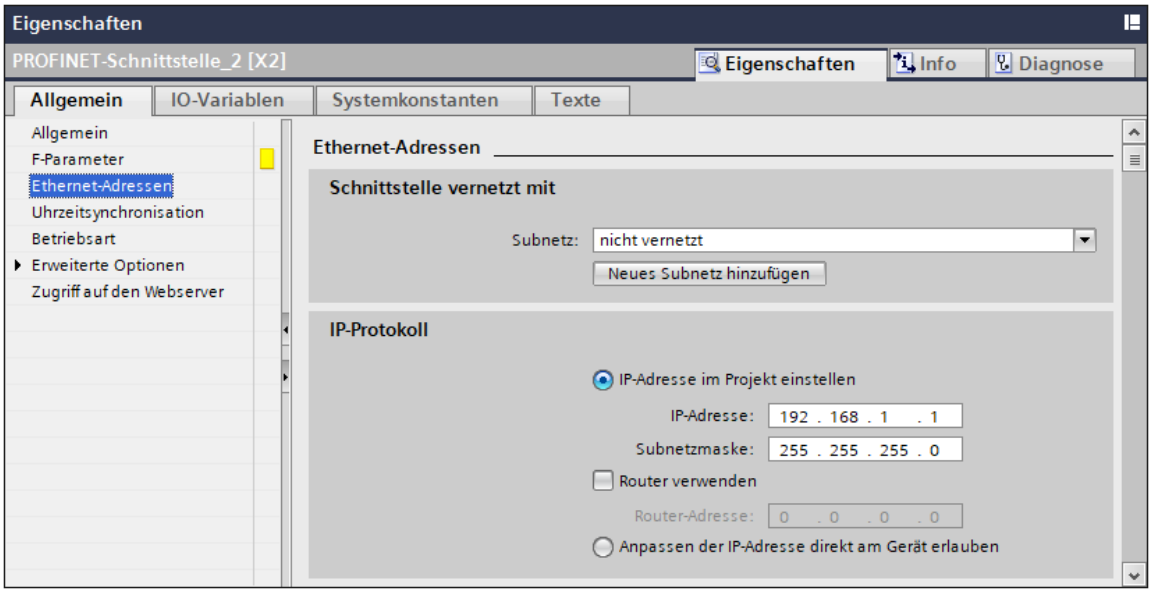
7.7 Konfiguration der CPU 1516F

Daraufhin muss in der CPU 1516F die Netzwerkkonfiguration angepasst und übertragen werden.

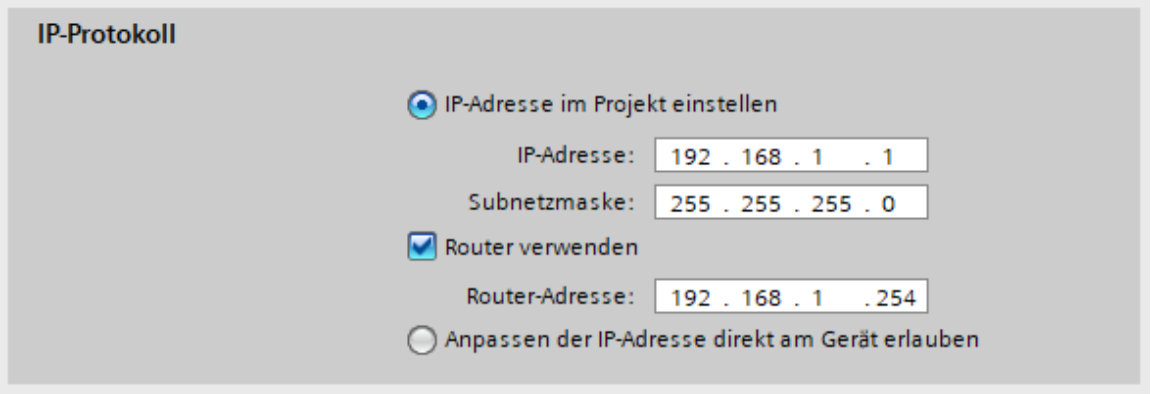
→ Verbinden Sie die Schnittstelle X2 der CPU 1516F-3 PN/DP mit dem Port 1 des SCALANCE S615.

→ Öffnen Sie im TIA Portal die Eigenschaften der X2-Schnittstelle der CPU_1516F. (→ CPU_1516F → X2 → Eigenschaften)

→ Wechseln Sie in die IP-Konfiguration. (→ Ethernet-Adressen → IP-Protokoll)

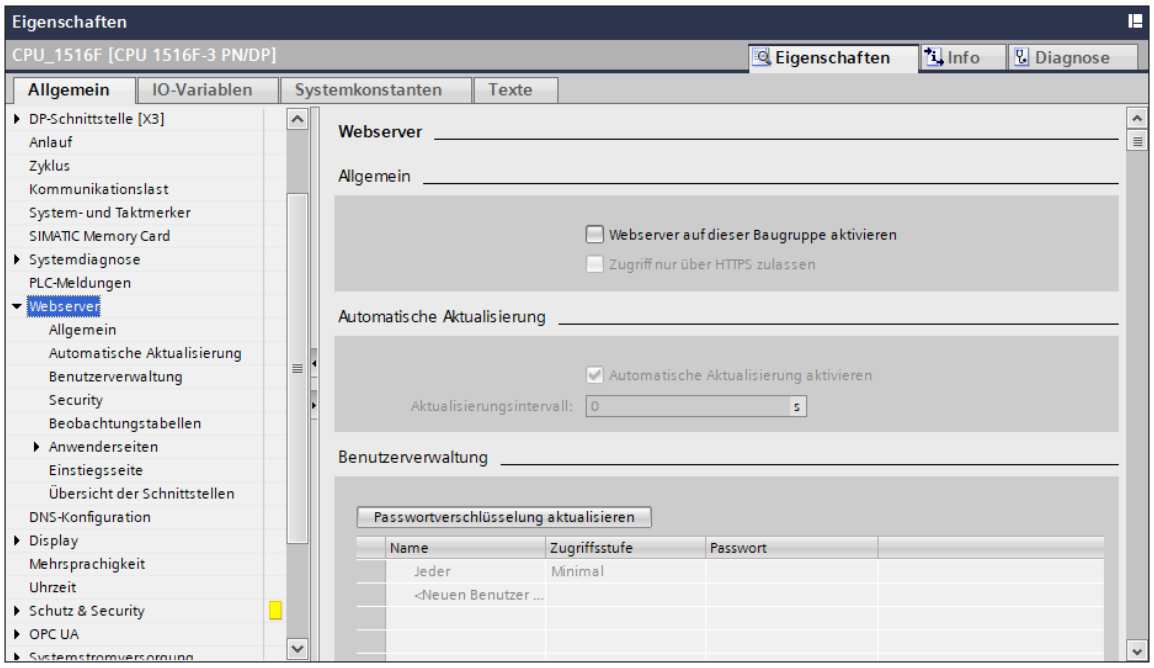


→ Stellen Sie die IP-Adresse des S615 als Router ein. (→ ☑Router verwenden → Router-Adresse: 192.168.1.254)



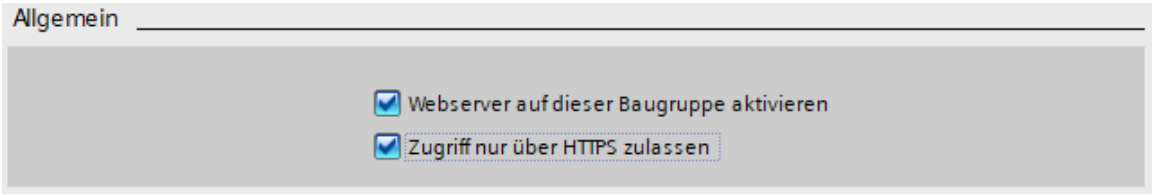
Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Öffnen Sie die Eigenschaften des Webservers der CPU 1516F-3 PN/DP. (→ CPU_1516F → Eigenschaften → Webserver)

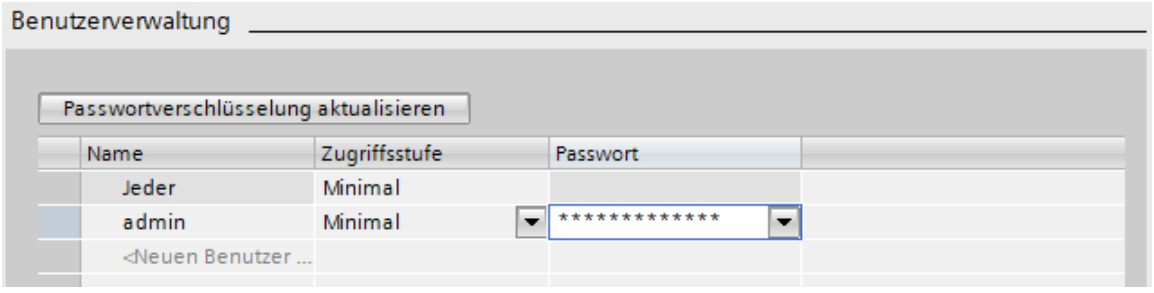


→ Aktivieren Sie den Webserver. (→ Allgemein → ☑ Webserver auf dieser Baugruppe aktivieren)

→ Schränken Sie den Zugriff auf HTTPS ein. (→ Allgemein → ☑ Zugriff nur über HTTPS zulassen)

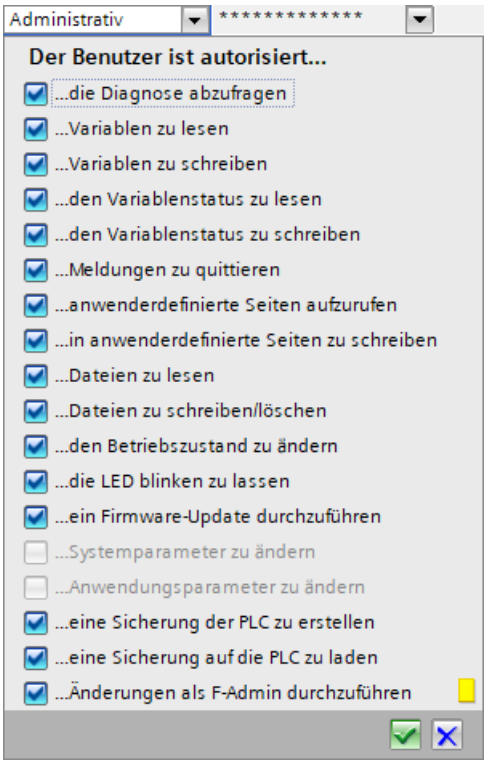


→ Legen Sie einen neuen Benutzer an. (→ Benutzerverwaltung → Name: admin → Passwort: ***)

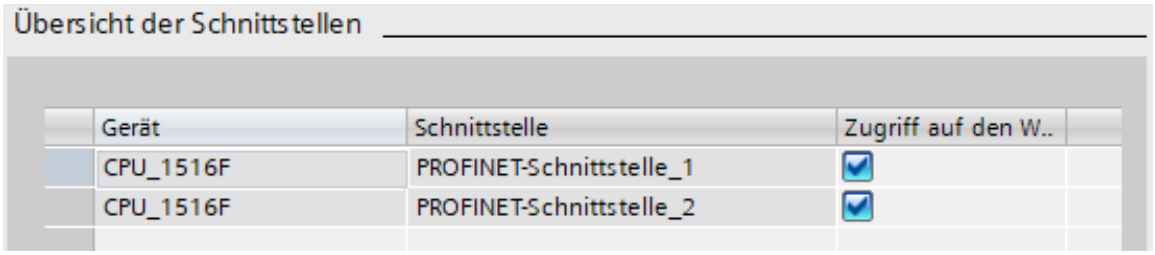


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Setzen Sie hier die Zugriffsstufe des neuen Benutzers auf Administrativ. (→ Benutzerverwaltung → admin → Zugriffsstufe → Administrativ)

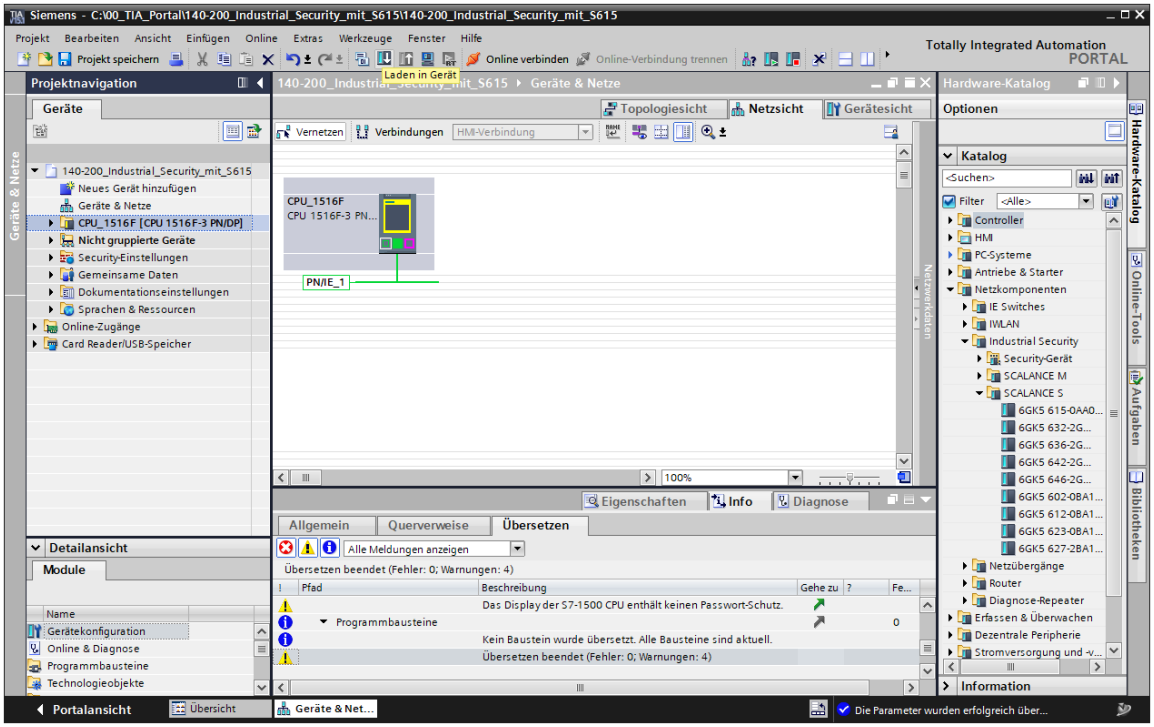


→ Aktivieren Sie nun den Webserver auf der Schnittstelle X2. (→ Übersicht der Schnittstellen → PROFINET-Schnittstelle_2)

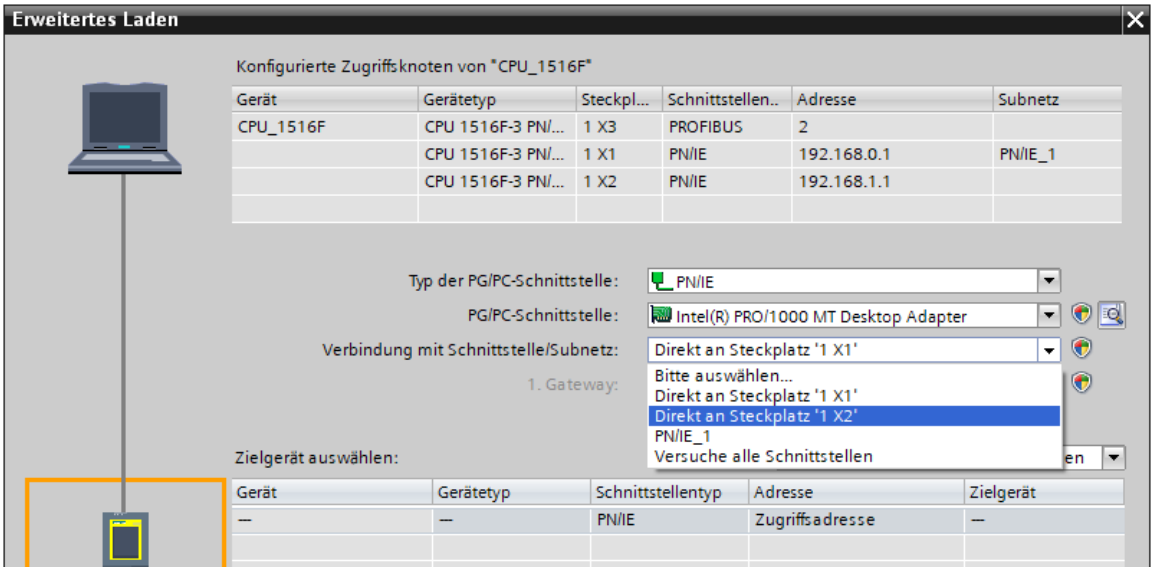


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Laden Sie die Konfiguration in die CPU. (→ CPU_1516F →  → )



→ Achten Sie beim Ladevorgang darauf, dass Sie nun mit der Schnittstelle X2 verbunden sind. (→ Verbindung mit Schnittstelle/Subnetz: Direkt an Steckplatz ‚1 X2')

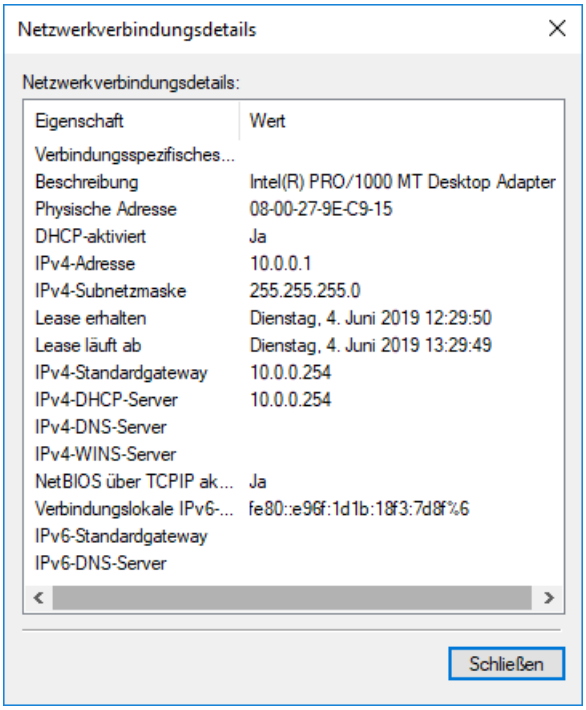


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

7.8 Testen des Regelwerkes

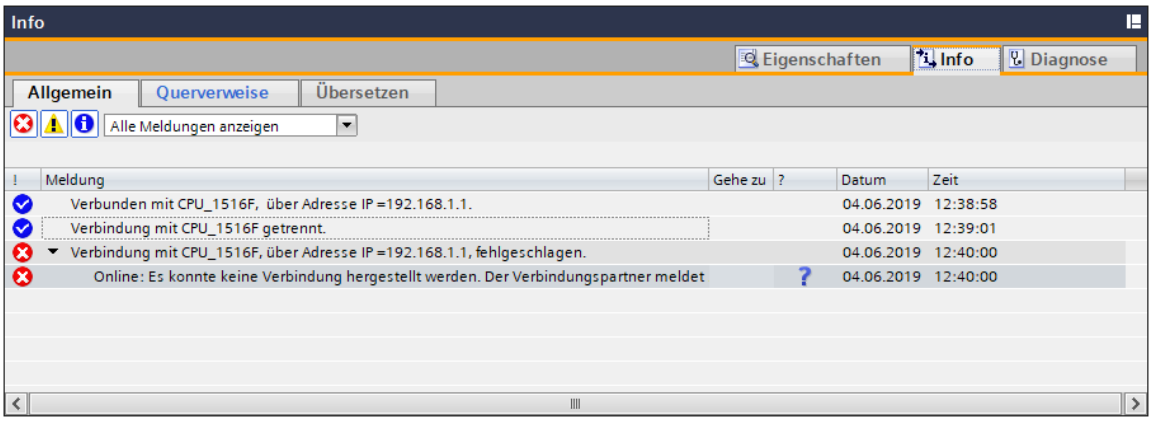
→ Verbinden Sie den Computer mit dem Port 5 auf dem SCALANCE S615.

→ Stellen Sie sicher, dass der Computer eine neue Adresse im Subnetz 10.0.0.0/24 vom SCALANCE S615 bekommen hat. (→ LAN-Verbindung → Status)



→ Öffnen Sie mit dem Browser den Webserver der CPU 1516F-3 PN/DP. (→ https://192.168.1.1)

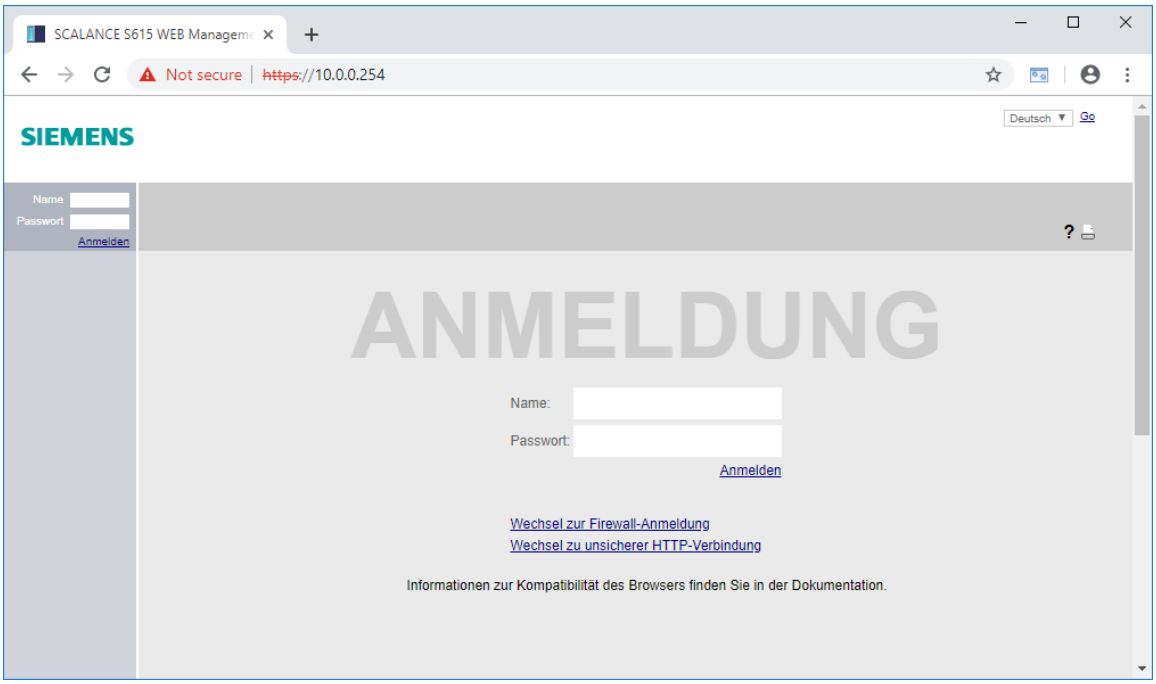
→ Versuchen Sie mit dem TIA Portal eine Online-Verbindung zur CPU 1516F-3 PN/DP aufzubauen. (→ TIA Portal → CPU_1516F → Online verbinden)



Hinweis:

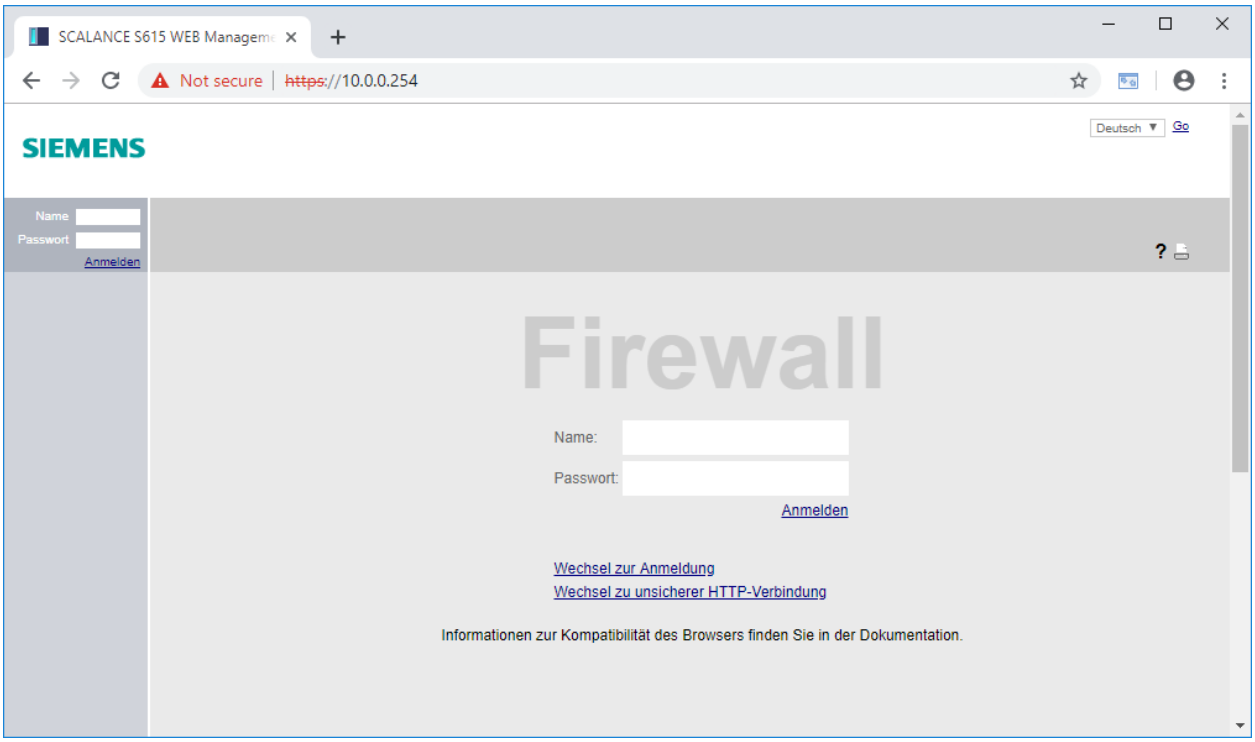
– *Ein Verbindungsaufbau mit der CPU_1516F sollte zu diesem Zeitpunkt nicht möglich sein, da nur Port 443 und 4840 freigeschaltet sind.*

→ Öffnen Sie im Browser die Weboberfläche des SCALANCE S615, da Sie sich diesmal auf der externen Seite des Gerätes befinden, nutzen Sie bitte die externe IP-Adresse des Gerätes. (→ https://10.0.0.254)

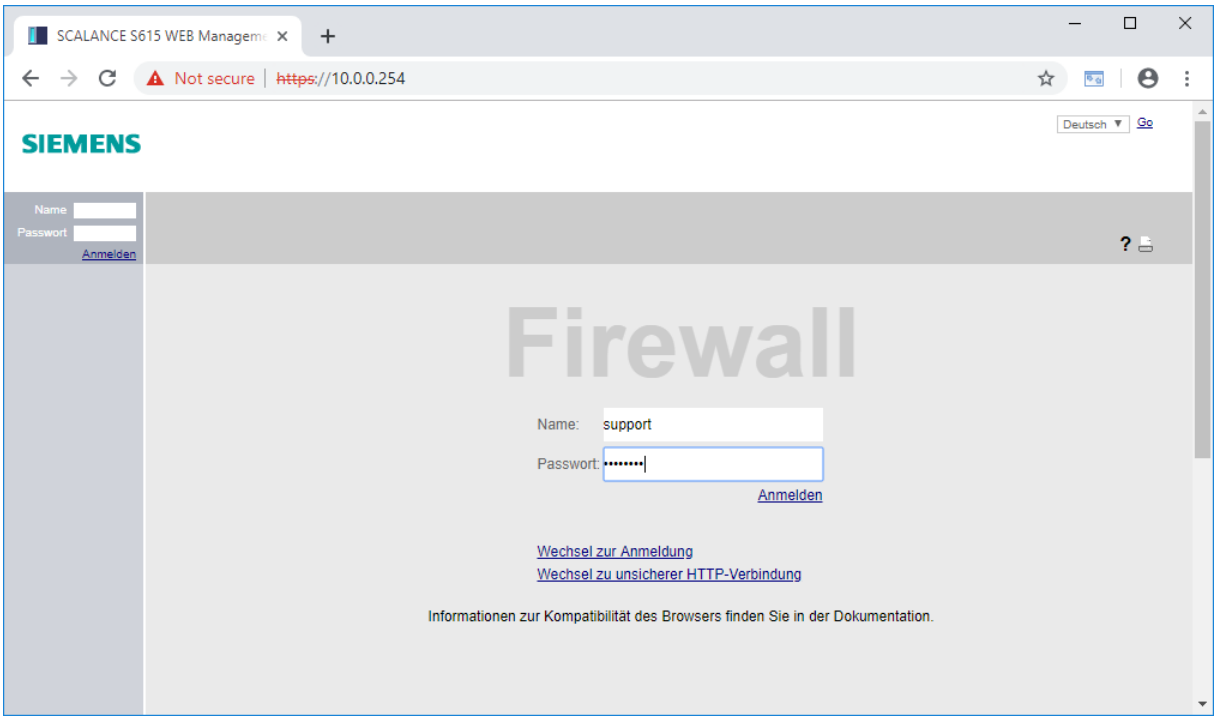


Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Wechseln Sie zur Firewall-Anmeldung. (→ Wechsel zur Firewall-Anmeldung)



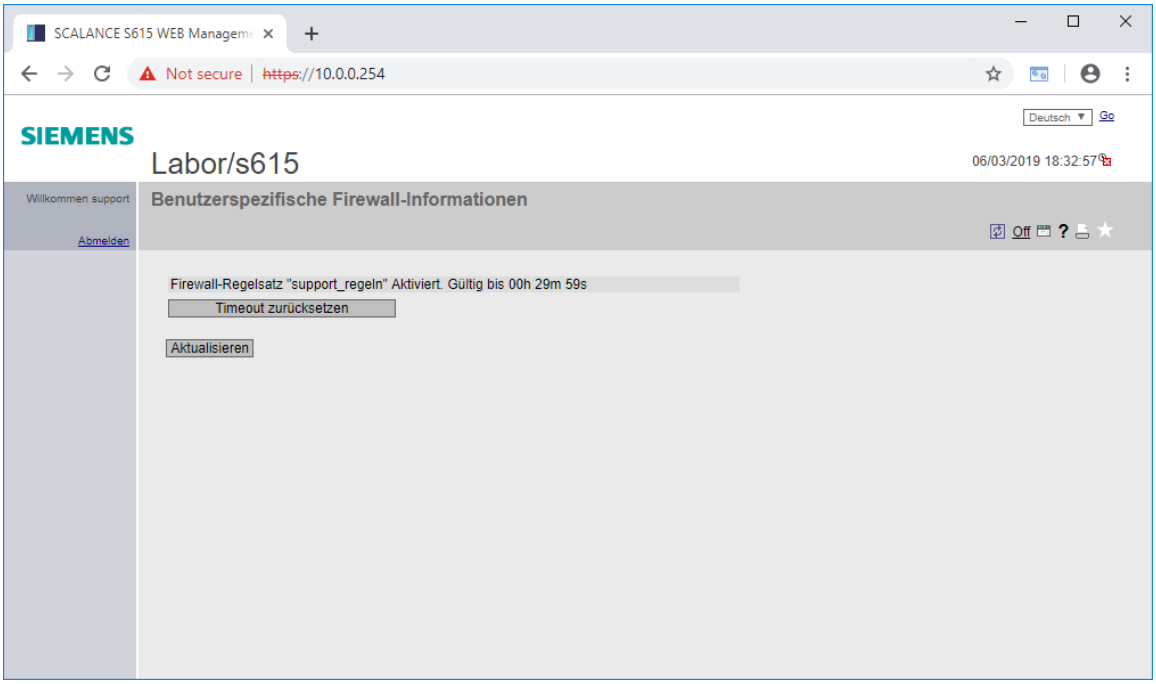
→ Melden Sie sich mit dem Benutzer „support“ an. (→ Name: support → Passwort: ***)



→ Klicken Sie auf Anmelden. (→ Anmelden)

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

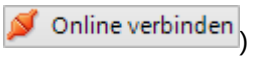
→ Der Firewall-Regelsatz „support_regeln“ sollte daraufhin für 30 Minuten aktiviert worden sein.



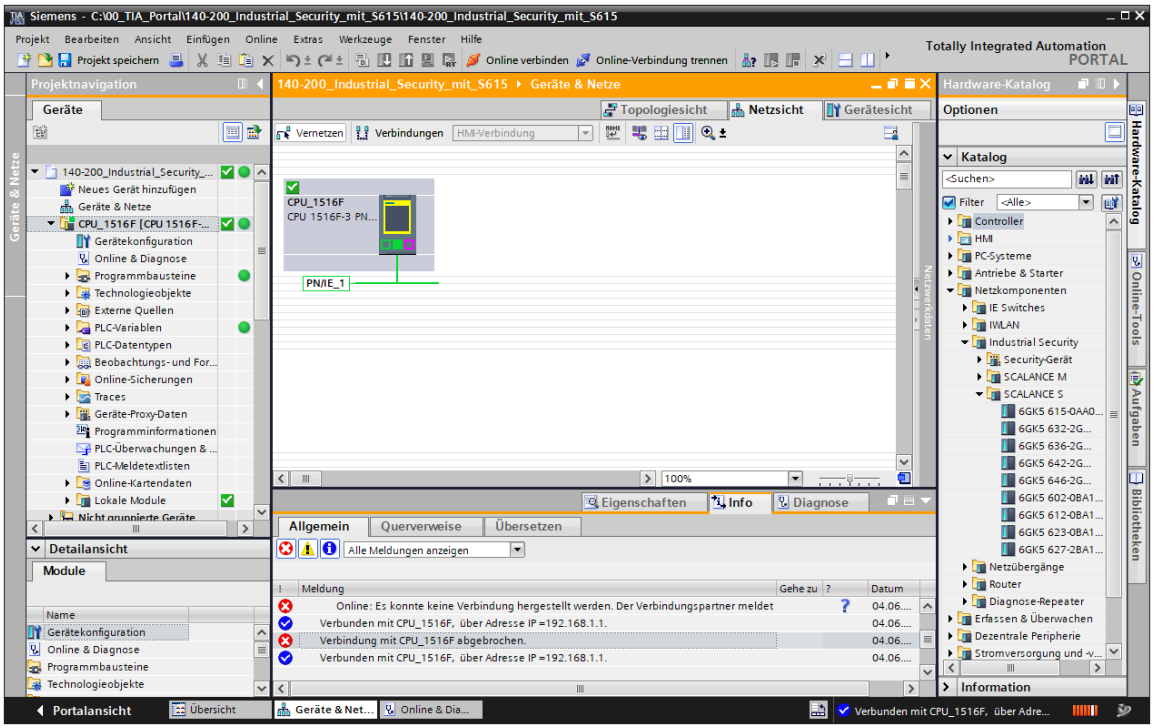
Hinweis:

– *Mit der Schaltfläche „Timeout zurücksetzen“ können Sie die Gültigkeit der Regelsätze wieder auf 30 Minuten zurücksetzen. Mit einem Klick auf Abmelden, werden alle Regelsätze wieder beendet.*

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

→ Versuchen Sie erneut eine Online-Verbindung mit der CPU 1516F-3 PN/DP im TIA Portal herzustellen. (→ TIA Portal → CPU_1516F → 

)



Hinweis:

– *Diesmal sollte der Verbindungsaufbau durch das zusätzliche Regelwerk einwandfrei funktionieren.*

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

7.9 Checkliste – Schritt-für-Schritt-Anleitung

Die nachfolgende Checkliste hilft den Auszubildenden/Studierenden selbstständig zu überprüfen, ob alle Arbeitsschritte der Schritt-für-Schritt-Anleitung sorgfältig abgearbeitet wurden und ermöglicht eigenständig das Modul erfolgreich abzuschließen.

Nr.	Beschreibung	geprüft
1	Projekt erfolgreich dearchiviert	
2	Programmiergerät auf den Port 4 des S615 gesteckt	
3	IP-Adresse erfolgreich gesetzt	
4	Webmanagement angemeldet und Passwort geändert	
5	System mit dem Assistenten korrekt konfiguriert	
6	DHCP-Pool für vlan1 erstellt	
7	DHCP-Pool für vlan2 erstellt	
8	DHCP-Optionen für beide Pools korrekt konfiguriert	
9	DHCP-Server und beide Pools aktiviert	
10	Programmiergerät bezieht IP automatisch	
11	Globale Regel für HTTPS zur CPU hinzugefügt	
12	Support-Benutzer angelegt	
13	Support-Regelwerk angelegt	
14	Webserver auf der CPU_1516F aktiviert	
15	Programmiergerät auf den Port 5 des S615 gesteckt	
16	Programmiergerät bezieht auch hier IP automatisch	
17	Webserver der CPU 1516F erfolgreich aufgerufen	
18	Keine Online-Verbindung zur CPU_1516F mit TIA möglich	
19	Erfolgreich als Support-Benutzer an der Firewall angemeldet	
21	Online-Verbindung zur CPU_1516F mit TIA nun möglich	

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

8 Übung

8.1 Aufgabenstellung – Übung

Durch die Digitalisierung der Fertigungsanlage wird in diesem Schritt auch ein globaler Zugriff auf den OPC UA Server der Steuerung benötigt. Erstellen Sie eine neue Regel, die den Zugriff auf den OPC UA Server der Steuerung aus dem Firmennetz heraus ermöglicht.

Informieren Sie sich vor der Konfiguration welchen Port die OPC UA Verbindung zur CPU benötigt.

8.2 Planung

Planen Sie nun selbstständig die Umsetzung der Aufgabenstellung.

8.3 Checkliste – Übung

Die nachfolgende Checkliste hilft den Auszubildenden/Studierenden selbständig zu überprüfen, ob alle Arbeitsschritte der Übung sorgfältig abgearbeitet wurden und ermöglicht eigenständig das Modul erfolgreich abzuschließen.

Nr.	Beschreibung	geprüft
1	Neue Regel angelegt	
2	OPC UA Verbindung aus dem Firmennetz erfolgreich aufgebaut	
3	Weiterhin keine Online-Verbindung zur CPU ohne Anmeldung möglich	

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

9 Weiterführende Information

Zur Einarbeitung bzw. Vertiefung finden Sie als Orientierungshilfe weiterführende Informationen, wie z. B.: Getting Started, Videos, Tutorials, Apps, Handbücher, Programmierleitfaden und Trial Software/Firmware, unter nachfolgendem Link:

siemens.de/sce/s7-1500

Voransicht “Weiterführende Informationen“ – In Vorbereitung

Frei verwendbar für Bildungs- / F&E-Einrichtungen. © Siemens 2019. Alle Rechte vorbehalten.

Weitere Informationen

Siemens Automation Cooperates with Education
siemens.de/sce

SCE Lern/Lehrunterlagen
siemens.de/sce/module

SCE Trainer Pakete
siemens.de/sce/tp

SCE Kontakt Partner
siemens.de/sce/contact

Digital Enterprise
siemens.de/digital-enterprise

Industrie 4.0
siemens.de/zukunft-der-industrie

Totally Integrated Automation (TIA)
siemens.de/tia

TIA Portal
siemens.de/tia-portal

SIMATIC Controller
siemens.de/controller

SIMATIC Technische Dokumentation
siemens.de/simatic-doku

Industry Online Support
support.industry.siemens.com

Katalog- und Bestellsystem Industry Mall
mall.industry.siemens.com

Siemens
Digital Industries, FA
Postfach 4848
90026 Nürnberg
Deutschland

Änderungen und Irrtümer vorbehalten
© Siemens 2019