SIEMENS

Learn-/Training Document

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

TIA Portal Module 142-200
Industrial Security with SIMATIC S7-1500
and SCALANCE S615

siemens.com/sce

SIEMENS

Global Industry
Partner of
WorldSkills
International

worldskills

Matching SCE Trainer Packages for this Learn-/Training Document

Industrial Communication SIMATIC NET

- **IE SCALANCE S615 with SINEMA RC Basic software**
  Order no.: 6GK1950-0BB13
- **IE SCALANCE S615 LAN Router**
  Order no.: 6GK1950-0BB23

SIMATIC Controllers

- **SIMATIC CPU 1516F PN/DP Safety**
  Order no.: 6ES7516-3FN00-4AB2
- **SIMATIC ET 200SP Open Controller CPU 1515SP PC F and HMI RT SW**
  Order no.: 6ES7677-2SB42-4AB1
- **SIMATIC ET 200SP Distributed Controller CPU 1512SP F-1 PN Safety**
  Order no.: 6ES7512-1SK00-4AB2
- **SIMATIC S7 CPU 1516-3 PN/DP**
  Order no.: 6ES7516-3AN00-4AB3
- **SIMATIC CPU 1512C PN with software and PM 1507**
  Order no.: 6ES7512-1CK00-4AB1
- **SIMATIC CPU 1512C PN with Software, PM 1507 and CP 1542-5 (PROFIBUS)**
  Order no.: 6ES7512-1CK00-4AB2
- **SIMATIC CPU 1512C PN with Software**
  Order no.: 6ES7512-1CK00-4AB6
- **SIMATIC CPU 1512C PN with software and CP 1542-5 (PROFIBUS)**
  Order no.: 6ES7512-1CK00-4AB7

SIMATIC STEP 7 Software for Training

- **SIMATIC STEP 7 Professional V15.1 - Single License**
  Order no.: 6ES7822-1AA05-4YA5
- **SIMATIC STEP 7 Professional V15.1 - 6+20 User Classroom License**
  Order no.: 6ES7822-1BA05-4YA5
- **SIMATIC STEP 7 Professional V15.1 - 6+20 User Upgrade License**
  Order no.: 6ES7822-1AA05-4YE5
- **SIMATIC STEP 7 Professional V15.1 - Student License for 20 Users**
  Order no.: 6ES7822-1AC05-4YA5

Note that these trainer packages are replaced with successor packages when necessary. An overview of the currently available SCE packages is available at: siemens.com/sce/tp

Continued training

For regional Siemens SCE continued training, get in touch with your regional SCE contact siemens.com/sce/contact

Additional information regarding SCE

siemens.com/sce

Information regarding use

The SCE Learn-/Training Document for the integrated automation solution Totally Integrated Automation (TIA) was prepared for the program "Siemens Automation Cooperates with Education (SCE)" specifically for training purposes for public educational facilities and R&D institutions. Siemens does not guarantee the contents.

This document is to be used only for initial training on Siemens products/systems. This means it can be copied in whole or in part and given to trainees/students for use within the scope of their training/course of study. Disseminating or duplicating this document and sharing its content is permitted within public training and advanced training facilities for training purposes or as part of a course of study.

Exceptions require written consent from the Siemens. Send all related requests to scesupportfinder.i-ia@siemens.com.

Offenders will be held liable. All rights including translation are reserved, particularly if a patent is granted or a utility model or design is registered.

Use for industrial customer courses is explicitly not permitted. We do not consent to commercial use of the Learn-/Training Document.

We wish to thank the TU Dresden and the Michael Dziallas Engineering Corporation and all other involved persons for their support during the preparation of this Learn-/Training Document.

Table of contents

Industrial security with S7-1500 and SCALANCE S615

1 Goal

In this chapter you will learn to configure Industrial Ethernet Security SCALANCE S615 and to connect an S7-1500 controller to other networks securely.

The SIMATIC S7 controllers listed in chapter 3 can be used.

2 Requirement

This chapter builds on the chapter OPC UA with SIMATIC S7-1500 as OPC server. To perform the work in this chapter, you can use the following project, for example: "SCE_EN_092-300_OPC_UA_S7-1500_R1807.zap15".

3 Required hardware and software

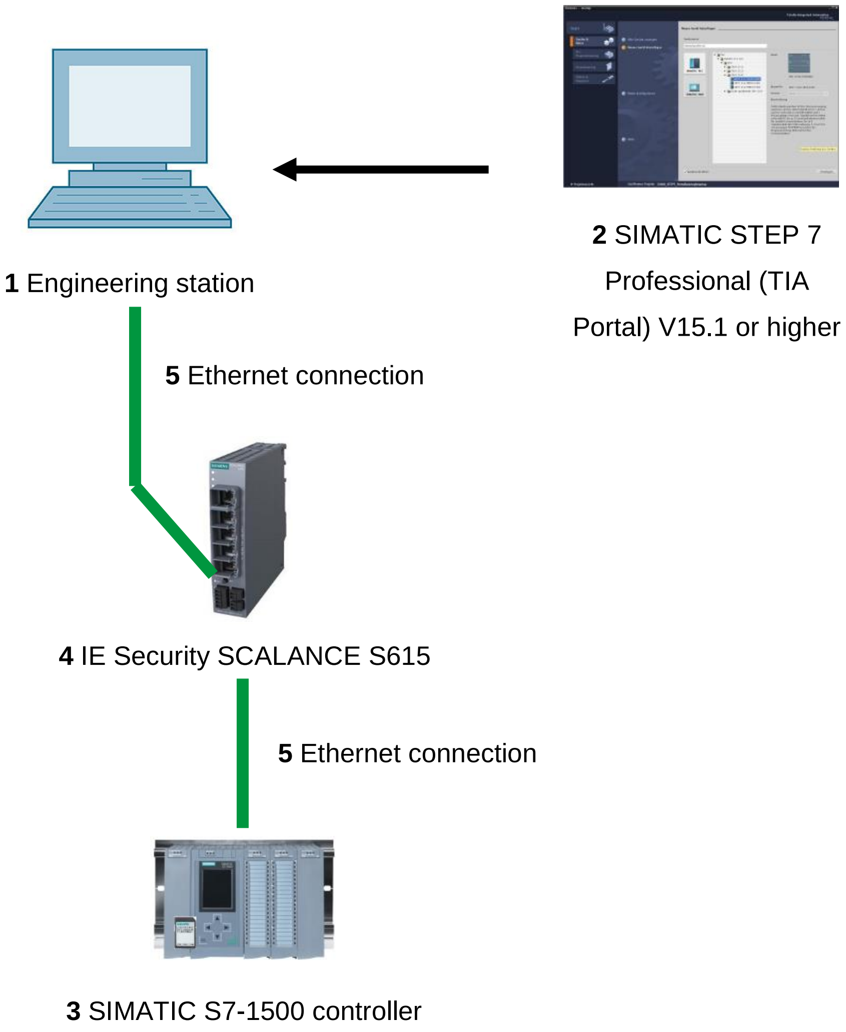
1 Engineering station: Requirements include hardware and operating system (for additional information, see Readme on the TIA Portal Installation DVDs)

2 SIMATIC STEP 7 Professional software in TIA Portal – V15.1 or higher

3 SIMATIC S7-1500 controller, e.g. CPU 1516F-3 PN/DP – Firmware V2.1 or higher with memory card

4 Industrial Ethernet Security SCALANCE S615

5 Ethernet-connection between engineering station and SCALANCE S615 and between control and SCALANCE S615


1 Engineering station
2 SIMATIC STEP 7 Professional (TIA Portal) V15.1 or higher
5 Ethernet connection
4 IE Security SCALANCE S615
5 Ethernet connection
3 SIMATIC S7-1500 controller

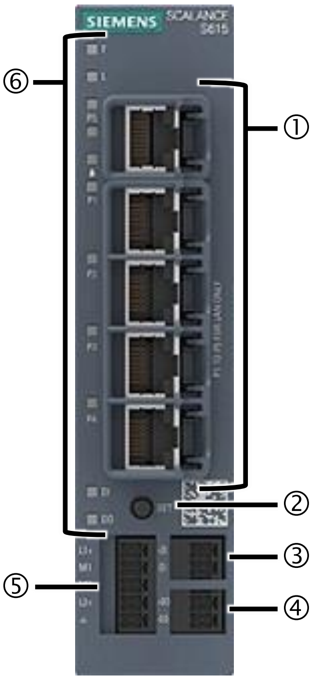
4 Theory

4.1 Structure and operation of SCALANCE S615

The following section provides a short description of the SCALANCE S615. Additional details and information can be found in the manuals, which can be downloaded from support.automation.siemens.com.

4.1.1 Industrial Ethernet Security S615

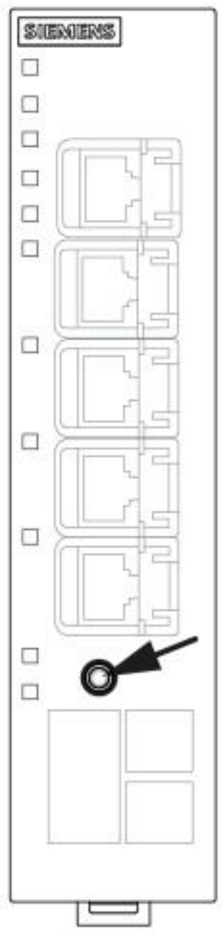
The SCALANCE S615 is an industrial Ethernet router and firewall for process automation.



(1) Network ports
(2) SET button
(3) Digital input
(4) Digital output
(5) Supply input for the power supply
(6) LED display

4.1.2 SET button

The SET button on a SCALANCE S615 is located on the front of the housing.

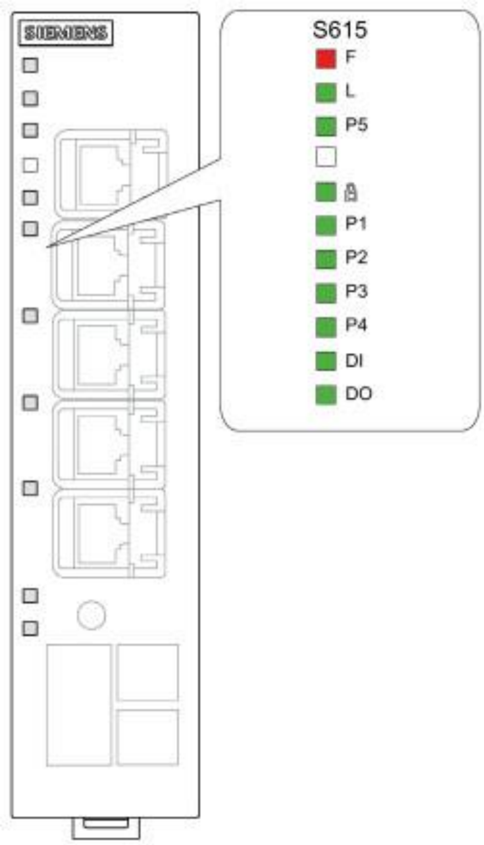


The SET button has several functions. If the button is pressed briefly for less than 3 seconds, the device performs a restart. When pressed for longer than 10 seconds, the device is reset to the factory settings.

The button can also be used to bring the device into the boot loader. In case of a defective firmware, a new firmware can be installed using the boot loader. More detailed information on this topic can be found in the manual.

4.1.3 LED indicator lights

SCALANCE S615 is equipped with various LEDs that provide an overview of the system status.

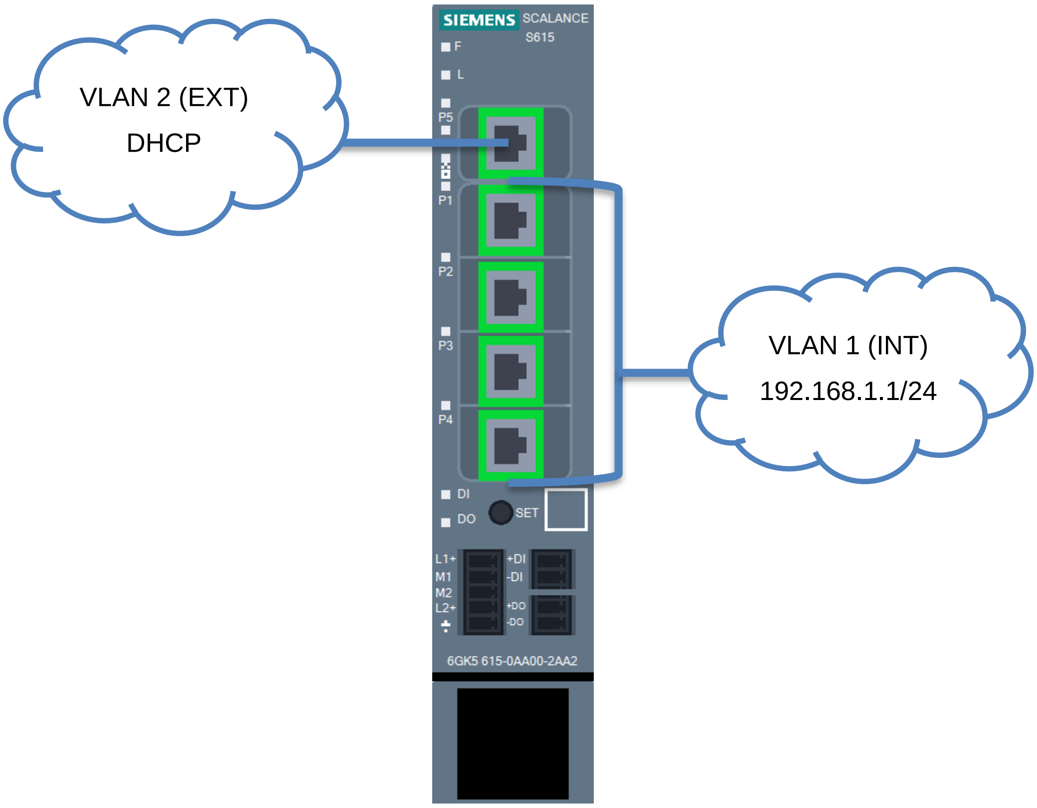


F	LED to display the error status
L	LED to display the power supply
🔒	LED to display the VPN connections
DI	LED to display the digital input
DO	LED to display the digital output
P	LEDs to display the port status

A detailed description of each LED can be found in the manual of the device.

4.1.4 Network ports

SCALANCE S615 has five network ports. The first four ports are factory configured as VLAN 1 (INT) and the fifth as VLAN 2 (EXT).



This interconnection can be changed as desired. By default, VLAN 2 is configured as an insecure external network and VLAN 1 as a protective internal network.

VLAN 1 is configured in the factory settings with IP 192.168.1.1/24. However, the device in the VLAN 2 does not have a fixed IP address, instead a dynamic IP address can be set using DHCP.

4.2 VLAN: Virtual networks

Devices, such as switches, usually have multiple network ports, all of which belong to the network. A device at port A can therefore communicate unhindered with a device at port B. To separate the individual devices from each other, dedicated physical devices would have to be used accordingly per network.

Virtual Local Area Networks (VLANs) can be used to divide a physical network device into virtual networks. Each port is permanently assigned to a VLAN. A device on a port in VLAN 1 can now only communicate with devices in VLAN 1. Each VLAN is configured with a unique ID in the device. This ID is generally 12 bits long and is displayed in decimal form.

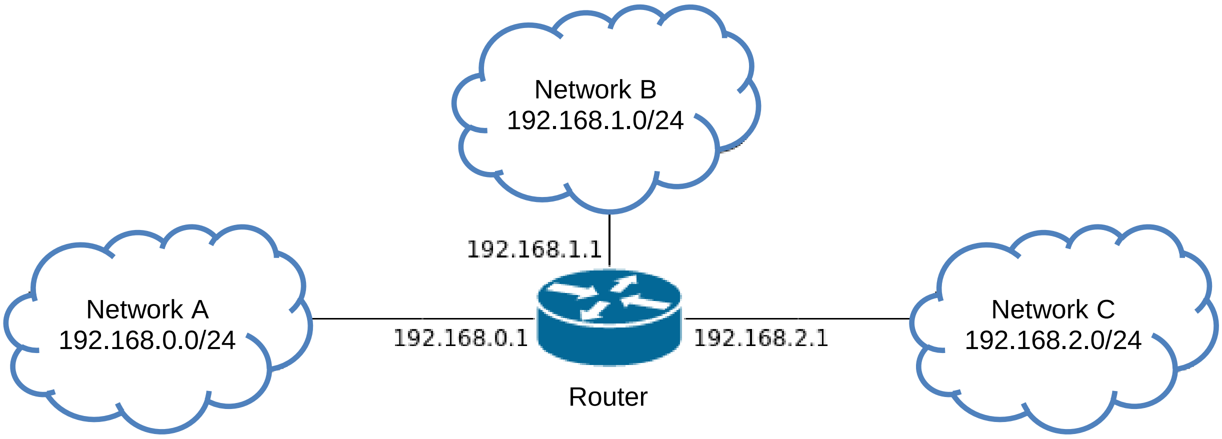
You have the option of assigning several VLANs to one port. Packets leaving such a port will be provided with a tag containing the ID of the VLAN. Incoming packets are checked for an existing tag and the packet is assigned to the VLAN with the ID contained in the tag. To evaluate the tags correctly, the partner on such a port must of course be configured accordingly.

The same physical network structure can therefore be used cost-effectively to separate individual device groups from each other.

SCALANCE S615 is divided into two separate networks at the factory. A secure network with VLAN ID 1 and an insecure network with VLAN ID 2 (see section 4.1.4).

4.3 Router

In contrast to a switch, a router can connect different networks with each other. It has a physical connection and a suitable IP address for each network. This makes it accessible to other devices in the network and allows it to exchange packets between the connected networks.



4.4 Firewall

A firewall can filter packets that pass through it. The device can use different criteria for this purpose, such as source and target addresses or TCP ports. More powerful devices are also able to understand more complex things, such as what data the user is currently sending to a website.

SCALANCE S615 is both a router and firewall and can check packets that are routed through it from one VLAN to another (layer 3). This means it is not able to control packets that are forwarded through it within a VLAN (layer 2).

The firewall in the S615 can process information up to layer 4. This includes IP addresses and the protocol used, e.g. TCP or UDP, and the ports used.

The filtering itself is done based on a rule set that exists in the form of a table. Each line hereby corresponds to one rule.

Source IP	Destination IP	Protocol	Source port	Destination port	Action
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

This rule set is processed from top to bottom and the first matching rule is used. In the above example, the node with the IP 192.168.1.24 would be able to establish any type of communication with node 192.168.2.5.

Nodes from network 192.168.1.x would be able to contact any other address via TCP and port 443 (HTTPS). The last rule ensures that all other packets are dropped.

It is generally possible to execute one of three actions.

– Packets can be accepted and forwarded.

– It is also possible to reject or drop them. In this case, the sender is not informed about the whereabouts of the packet.

– Finally, it is possible to reject the packets. In this case, the sender receives corresponding feedback that its packets were rejected.

Accept and Drop are used in most cases, and Reject is only used for special cases.

4.4.1 Implicit rule

What happens to packets that match none of the configured rules? The answer depends on the manufacturer of the filter. Most manufacturers have an implicit rule at the end of the rule set that either allows everything or drops everything. This behavior can usually be adjusted.

In the case of SCALANCE S615, the implicit rule drops all packets.

4.4.2 Stateful inspection

Most firewalls do not just filter incoming packets, they also remember which computer has established which connection. For example, a computer that calls a website gets response packets from the server. Modern firewalls check packets only during connection setup, so that these response packets do not also have to be defined in the filter rules.

If node 192.168.1.5 tries to reach an encrypted web page on node 192.168.3.25 via port 443, this connection setup is checked against the rule set. If the rule set accepts this connection, the firewall remembers the validity of this connection in a special session table. Any subsequent packet belonging to this connection, whether from the client or web server, on any source or destination port, is now accepted by the firewall.

Using this method, the administrator only must generate the rule set required for the connection setup.

4.5 CIDR notation

To ensure the most efficient use of existing IP addresses, these are nowadays classified with the subnet mask and not by the IP address.

The subnet mask is often represented as a suffix added at the end the actual address. This representation is also called CIDR (Classless Inter-Domain Routing) notation.

→ Example: 192.168.0.1/24

The suffix /24 indicates the number of bits set in the subnet mask. In the example, the first 24 bits of the subnet mask would be set.

→ Binary: 11111111.11111111.11111111.00000000

→ Decimal: 255.255.255.0

In the firewall rules this notation is used to define ranges for the source and destination addresses. The suffix specifies the bit up to which the address on the packet must match the address in the rule.

Address in the rule set	Description
192.168.1.1/32	All bits must match. Only the address 192.168.1.1 conforms to the rule
192.168.1.0/24	The first 3 octets must match. All addresses that begin with 192.168.1.x conform to the rule.
0.0.0.0/0	No bit must match. All addresses conform to the rule
192.168.1.0/25	The first 3 octets and the highest bit of the 4th octet must match. Here only the addresses 192.168.1.0 to 192.168.1.127 conform to the rule

Appropriate tools can be helpful for more complex ranges, such as the last example. A simple Internet search for "subnet computers" or "CIDR computers" should produce enough online tools.

A helpful intuitive tool can be found for example here:
heise.de/netze/tools/netzwerkrechner/

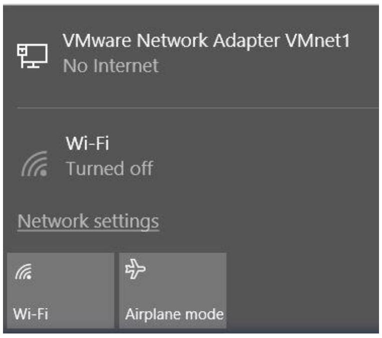
4.6 Setting the IP address on the programming device

To program SIMATIC S7-1500 from the PC, the programming device or a laptop, you need a TCP/IP connection or, optionally, a PROFIBUS connection.

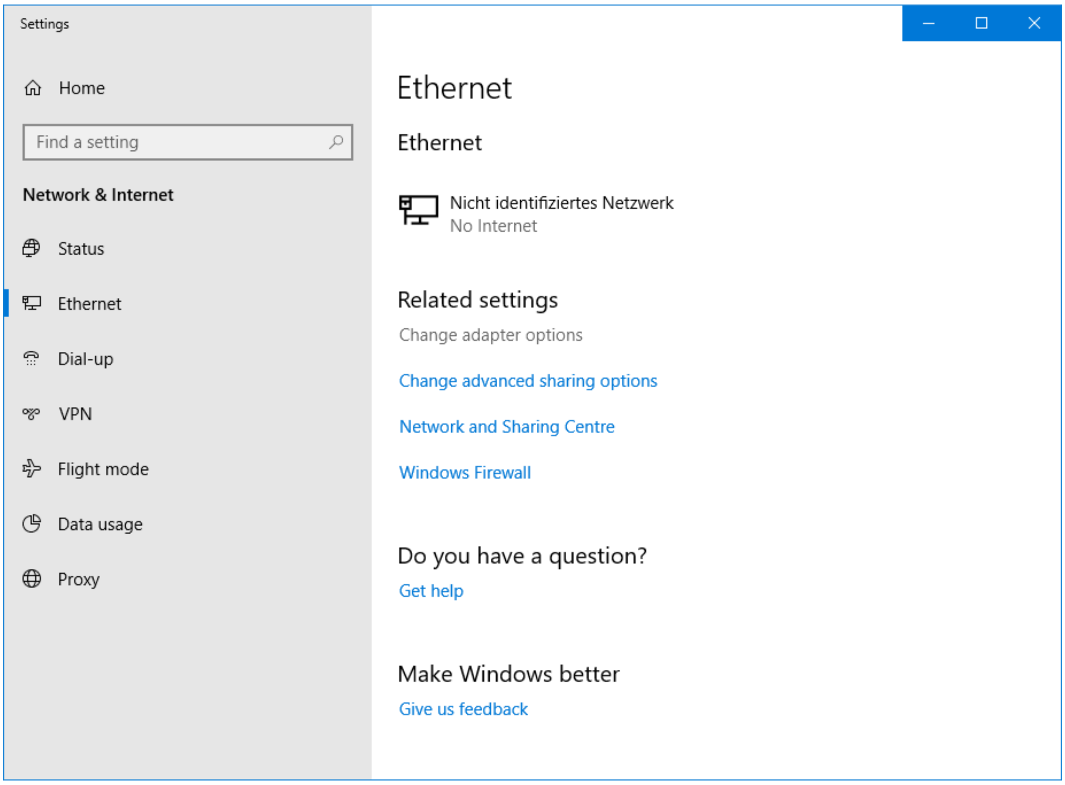
For the PC and SIMATIC S7-1500 to communicate with each other via TCP/IP, it is important that the IP addresses of both devices match.

The procedure for setting the IP address of a computer with Windows 10 operating system is presented in the following.

→ Locate the network icon in the taskbar at the bottom and click → "Network settings".



→ In the network settings window that opens, click → "Ethernet" and then → "Change adapter options".



Ethernet

Ethernet

Nicht identifiziertes Netzwerk
No Internet

Related settings

Change adapter options

Change advanced sharing options

Network and Sharing Centre

Windows Firewall

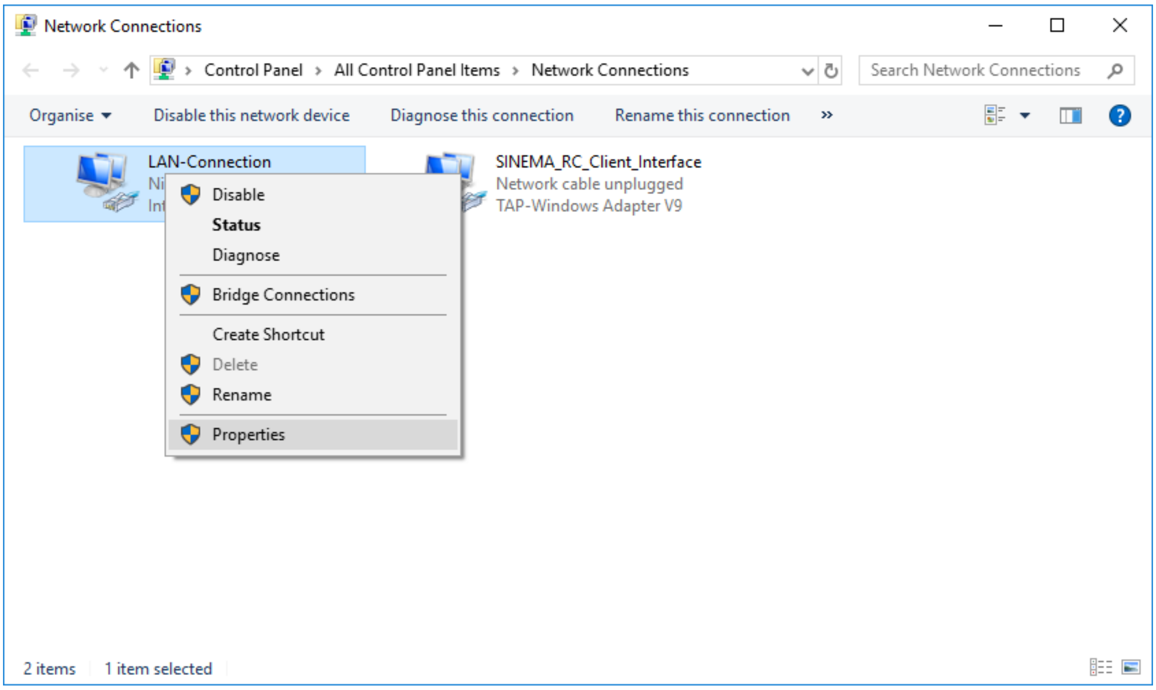
Do you have a question?

Get help

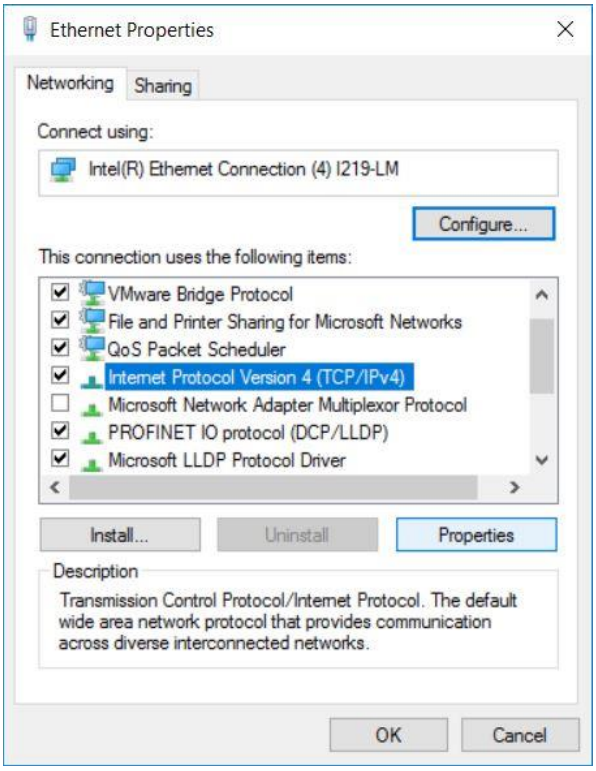
Make Windows better

Give us feedback

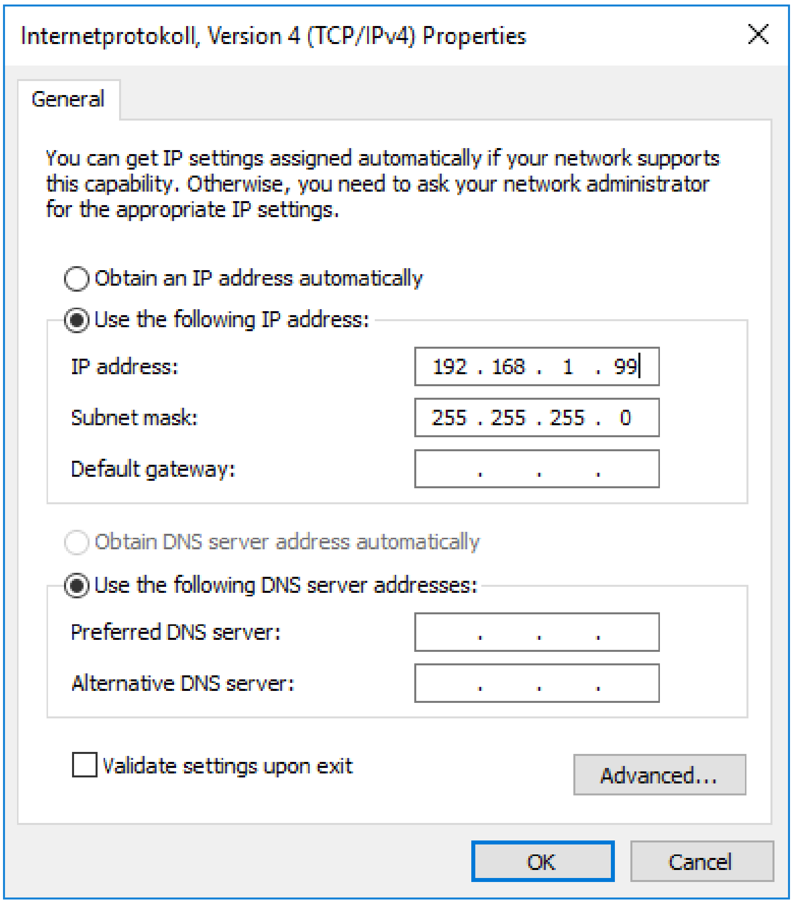
→ Select the desired → "LAN connection" that you want to use to connect to the controller and click → "Properties".



→ Next, select the → "Properties" for → "Internet Protocol Version 4 (TCP/IP)".


Ethernet Properties
Networking
Sharing
Connect using:
Intel(R) Ethernet Connection (4) I219-LM
Configure...
This connection uses the following items:
☑ VMware Bridge Protocol
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Protocol
☑ PROFINET IO protocol (DCP/LLDP)
☑ Microsoft LLDP Protocol Driver
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel

→ You can now use, for example, the following IP address: 192.168.1.99 with the subnet mask 255.255.255.0 and apply the settings (→ "OK")



Internetprotokoll, Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 99

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternative DNS server: . . .

□ Validate settings upon exit

5 Task

In this section, the hardware and the program from chapter "SCE_EN_092-300_OPC_UA_S7-1500" shall be extended by the SCALANCE S615.

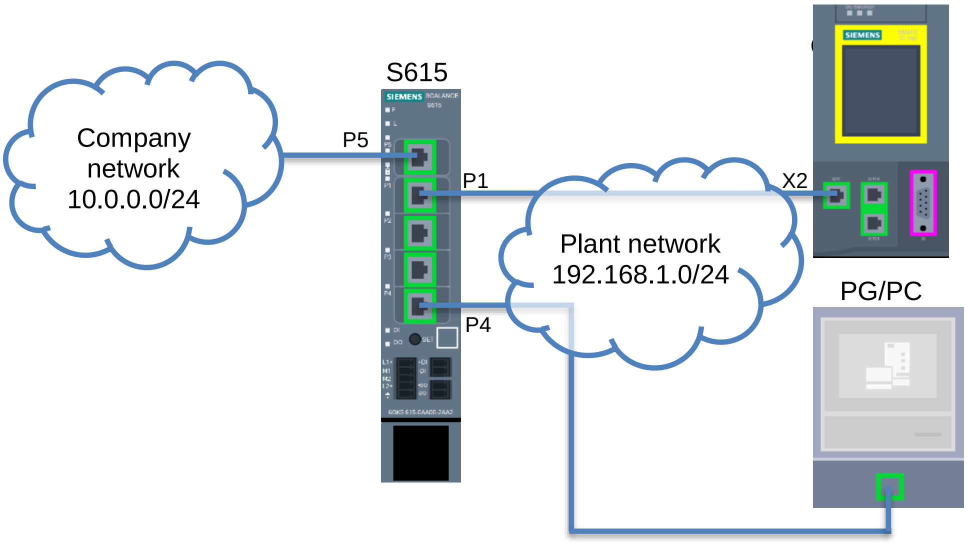
Using SCALANCE S615, a secured access to the controller from the company network is to be enabled. The web server on the CPU is to be freely accessible for diagnostic purposes, while only authenticated users are to be allowed access to the programming via the TIA Portal.

6 Planning

First, the SCALANCE S615 must be configured with a new IP address and the basic configuration carried out.

The S615 can then be entered in the CPU 1516F as a router, and the configuration can be transferred to the CPU.

After successful basic configuration of both devices, the physical networking of the components can be set up as follows.



Finally, the access rules will be created and tested in SCALANCE S615.

IMPORTANT:

Because the programming device is located in different subnets during commissioning, you must never allow the TIA Portal to generate a project-specific IP address. Instead, configure the correct IP settings statically in the programming device. Later, the S615 is assigned the correct IP addresses dynamically.

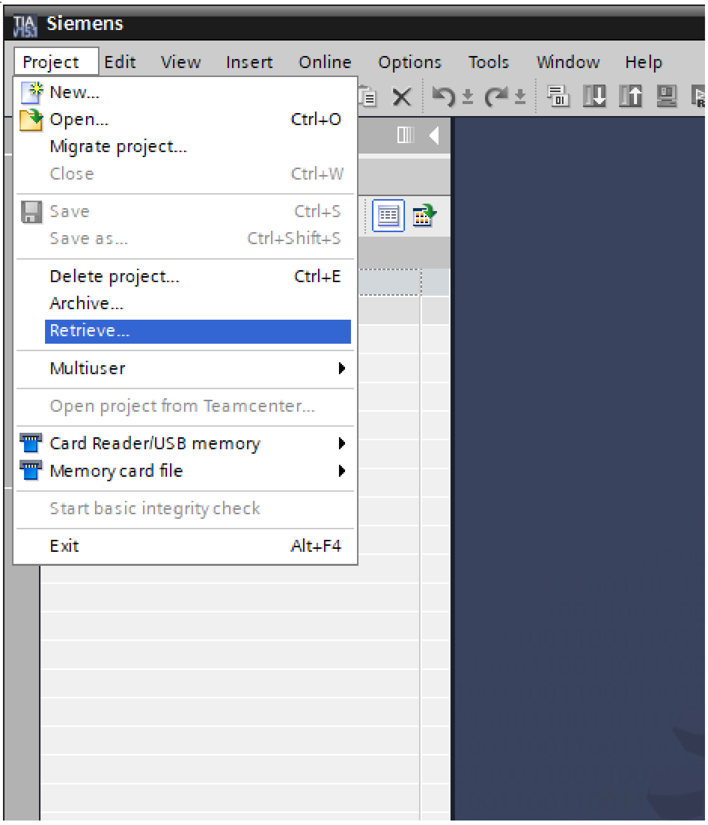
7 Structured step-by-step instructions

You can find instructions on how to carry out planning below. If you already have a good understanding of everything, it is enough to focus on the numbered steps. Otherwise, simply follow the steps of the instructions illustrated below.

7.1 Retrieving an existing project

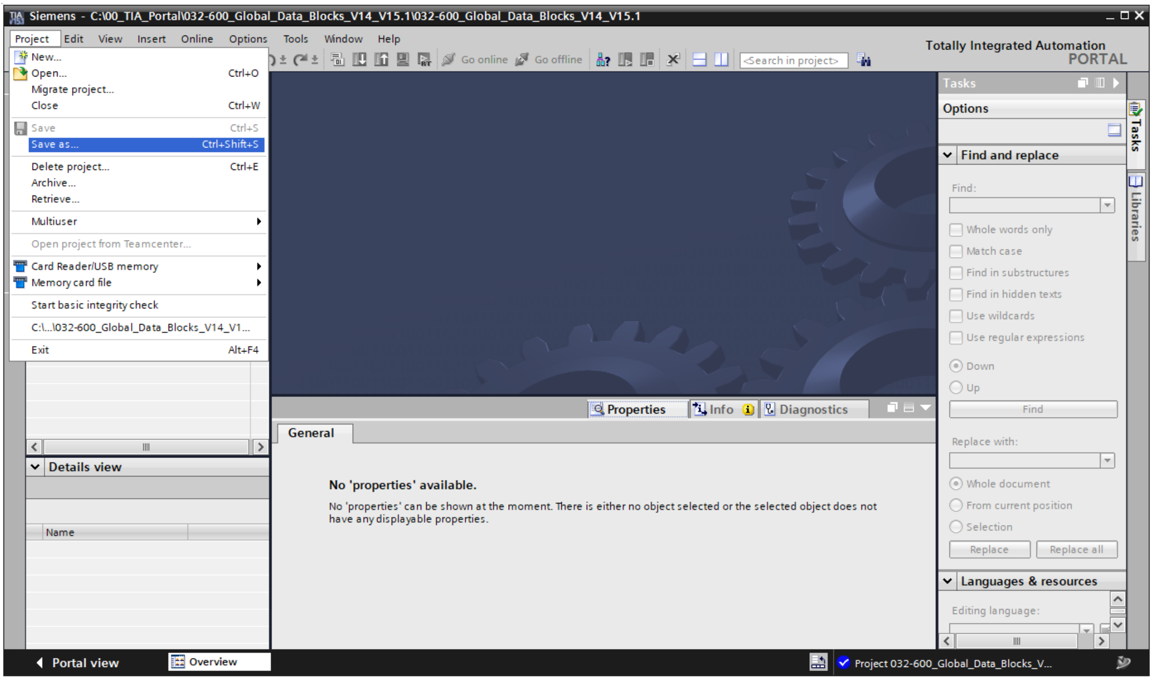
→ Before you can extend the project "SCE_EN_092-300 OPC UA S7-1500_R1807.zap15" from chapter "SCE_EN_092-300 OPC UA S7-1500", you have to retrieve it from the archive.

→ To retrieve an existing project that has been archived, you must select the relevant archive from the project view under → Project → Retrieve. Confirm your selection with "Open". (→ Project → Retrieve → Select a .zap archive … → Open)



→ As the next step, select the target directory where the retrieved project it to be stored. Confirm your selection with "OK". (→ Destination directory … → Select folder)

→ Save the retrieved and opened project under the name 142-200_Industrial_Security_with_S615. (→ Project → Save as … → 142-200_Industrial_Security_with_S615 → Save)



Siemens - C:\00_TIA_Portal\032-600_Global_Data_Blocks_V14_V15.1\032-600_Global_Data_Blocks_V14_V15.1

No 'properties' available.

No 'properties' can be shown at the moment. There is either no object selected or the selected object does not have any displayable properties.

7.2 Setting the IP address of the SCALANCE S615

→ Connect the programming device to port 4 of the SCALANCE S615.

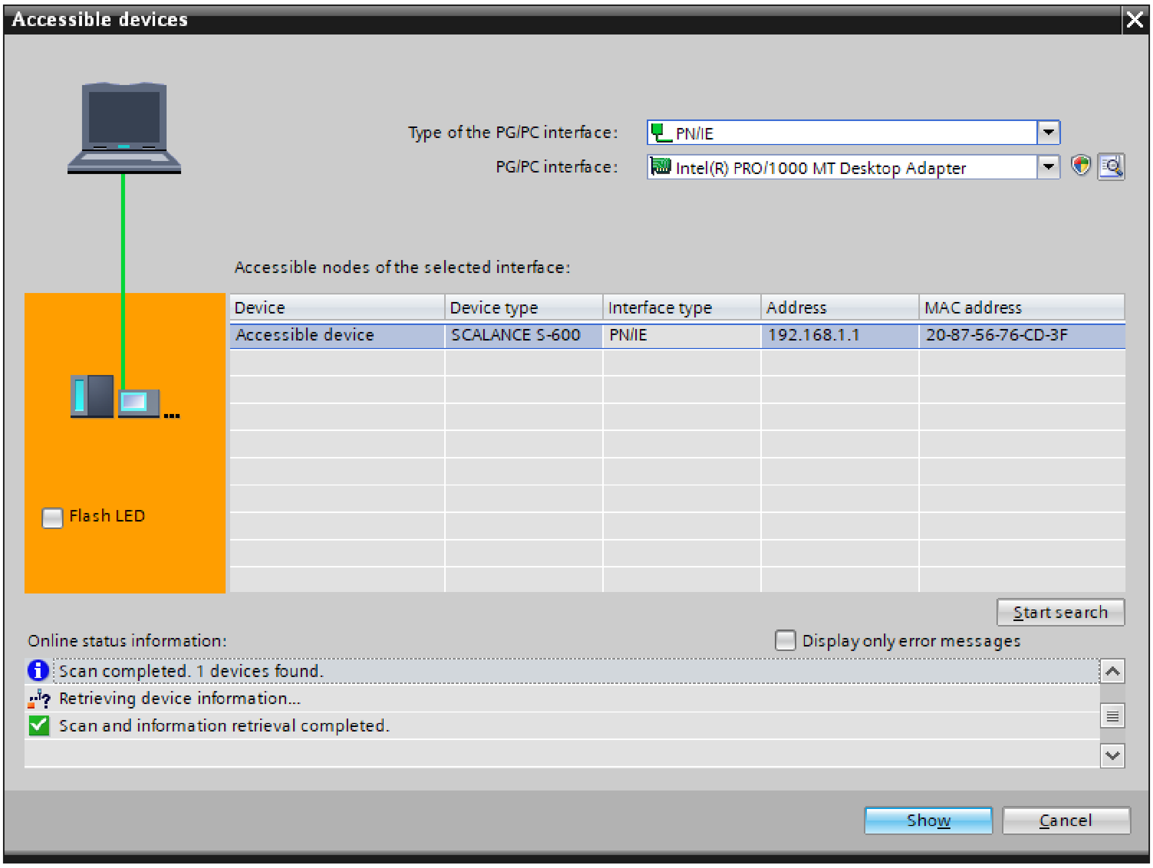
→ Disconnect all other connections to the SCALANCE S615

→ Make sure that your programming device is in subnet 192.168.1.0/24. Follow the instructions in section 4.6.

→ Open the search for Accessible devices. (→)

→ Select your PN/IE interface and start the search. (→ Start search)

→ Select the SCALANCE S-600 and click on "Show". (→ Show)



Accessible devices

Type of the PG/PC interface: PN/IE

PG/PC interface: Intel(R) PRO/1000 MT Desktop Adapter

Accessible nodes of the selected interface:

Device	Device type	Interface type	Address	MAC address
Accessible device	SCALANCE S-600	PN/IE	192.168.1.1	20-87-56-76-CD-3F

□ Flash LED

Online status information:

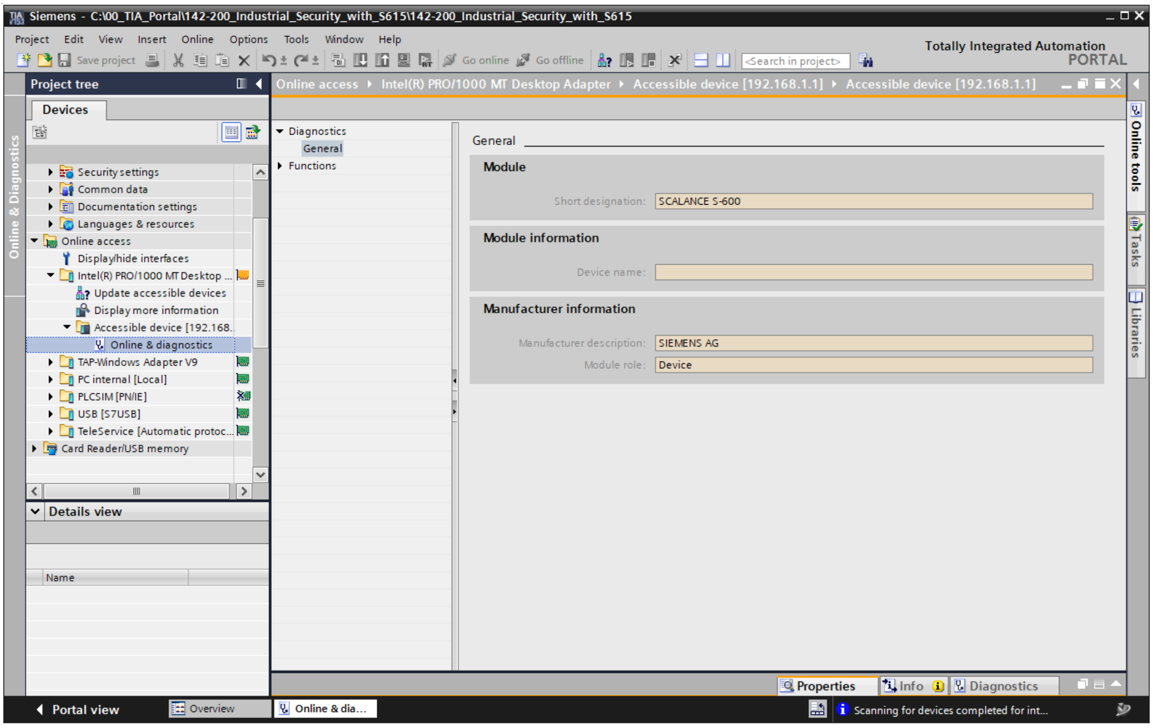
□ Display only error messages

Scan completed. 1 devices found.

Retrieving device information...

Scan and information retrieval completed.

→ Under "Online access", open the "Online & diagnostics" item of the displayed device.


Siemens - C:\00_TIA_Portal\142-200_Industrial_Security_with_S615\142-200_Industrial_Security_with_S615
Project Edit View Insert Online Options Tools Window Help
Save project
Go online
Go offline
<Search in project>
Totally Integrated Automation
PORTAL
Project tree
Devices
Security settings
Common data
Documentation settings
Languages & resources
Online access
Display/hide interfaces
Intel(R) PRO/1000 MT Desktop ...
Update accessible devices
Display more information
Accessible device [192.168...
Online & diagnostics
TAP-Windows Adapter V9
PC internal [Local]
PLCSIM [PN/IE]
USB [S7USB]
TeleService [Automatic protoc...
Card Reader/USB memory
Details view
Name
Online & Diagnostics
Online access ▸ Intel(R) PRO/1000 MT Desktop Adapter ▸ Accessible device [192.168.1.1] ▸ Accessible device [192.168.1.1]
Diagnostics
General
Functions
Online tools
Tasks
Libraries
Properties
Info
Diagnostics
Portal view
Overview
Online & dia...
Scanning for devices completed for int...

General

Module

Short designation: SCALANCE S-600

Module information

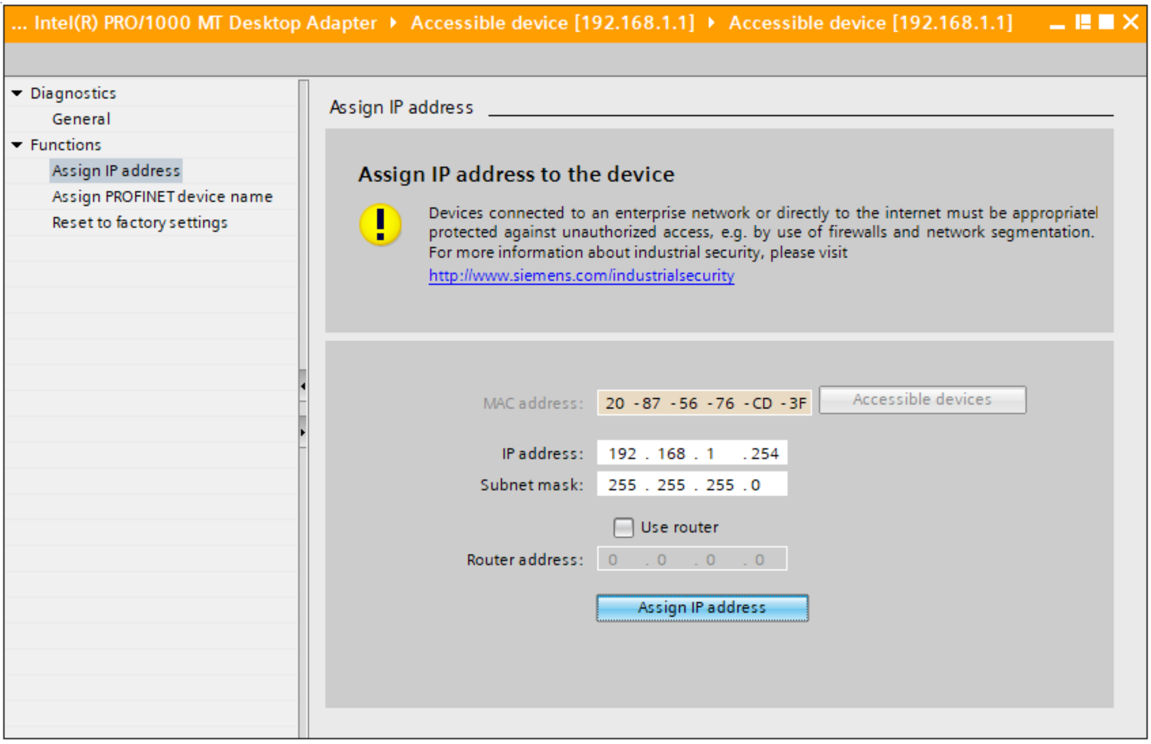
Device name:

Manufacturer information

Manufacturer description: SIEMENS AG

Module role: Device

→ Set the IP address to 192.168.1.254/24. (→ Functions → Assign IP address → IP address: 192.168.1.254 → Subnet mask: 255.255.255.0 → Assign IP address)


... Intel(R) PRO/1000 MT Desktop Adapter ▸ Accessible device [192.168.1.1] ▸ Accessible device [192.168.1.1]
Diagnostics
General
Functions
Assign IP address
Assign PROFINET device name
Reset to factory settings
Accessible devices
Assign IP address

Assign IP address

Assign IP address to the device

Devices connected to an enterprise network or directly to the internet must be appropriately protected against unauthorized access, e.g. by use of firewalls and network segmentation. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity

MAC address: 20 -87 -56 -76 -CD -3F

IP address: 192 . 168 . 1 . 254

Subnet mask: 255 . 255 . 255 . 0

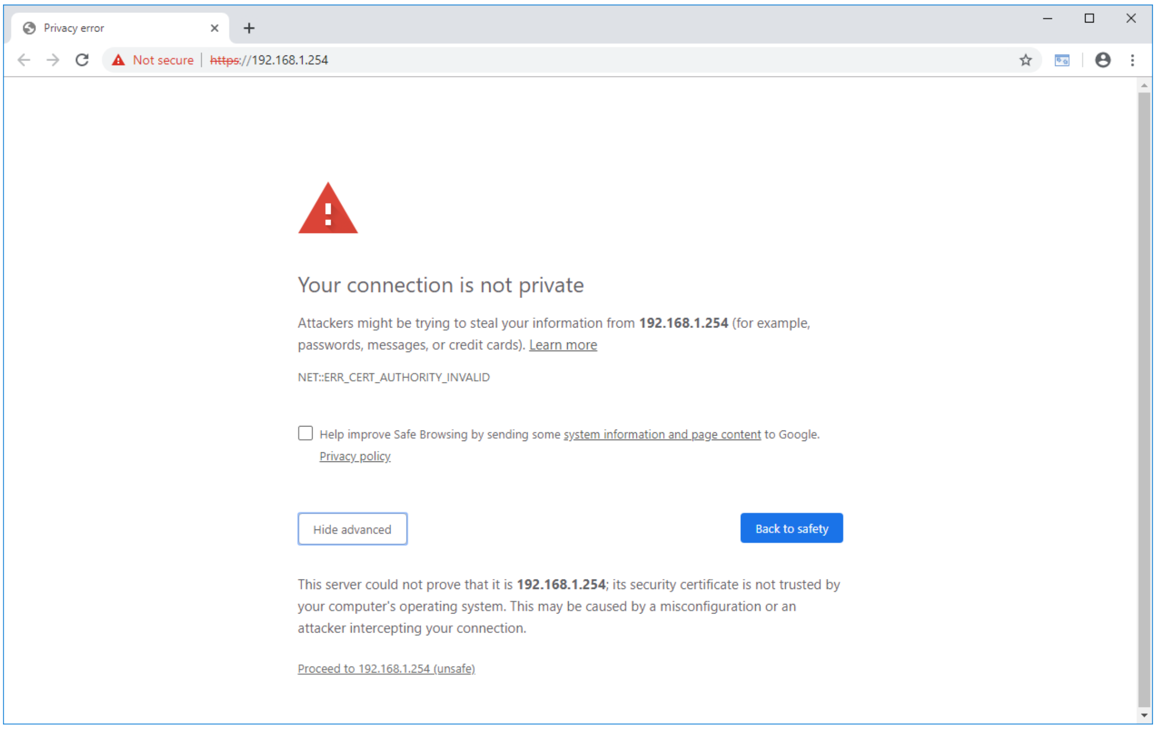
□ Use router

Router address: 0 . 0 . 0 . 0

7.3 Basic configuration of the SCALANCE S615

→ In the browser, open the SCALANCE S615 web interface (→ https://192.168.1.254).

→ The web interface of the SCALANCE S615 is protected with a self-signed certificate. To continue, confirm the exception.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

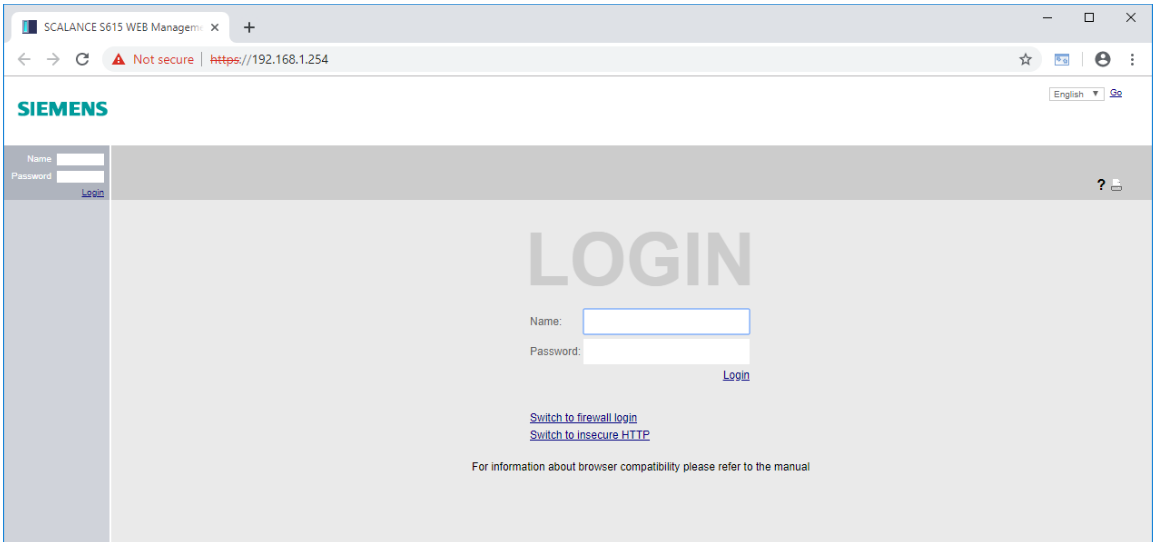
□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.1.254 (unsafe)

Note:

– *Depending on the browser, the confirmation of the certificate looks somewhat different.*

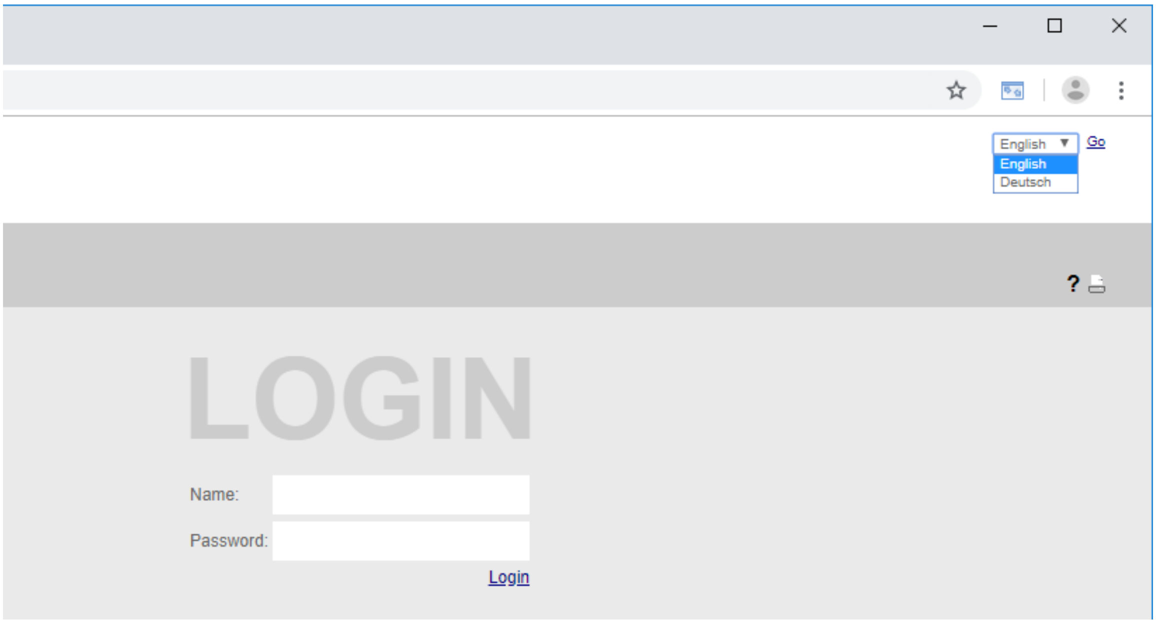

SCALANCE S615 WEB Managem
Not secure | ~~https~~://192.168.1.254
English
Go
SIEMENS
Name
Password
Login
?
LOGIN

Name:

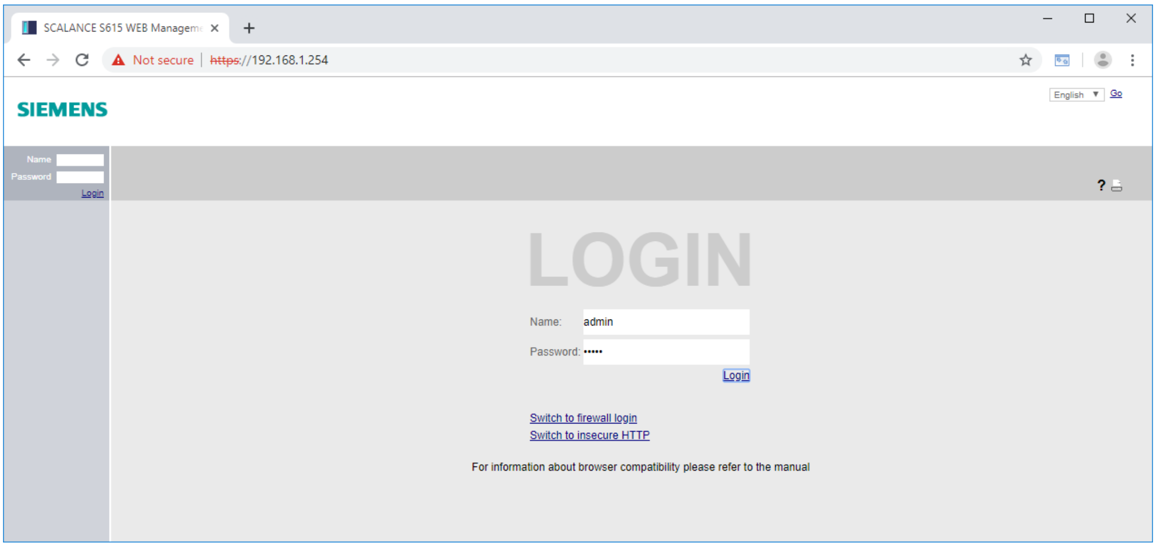
Password:

For information about browser compatibility please refer to the manual

→ First change the language of the user interface to English. (→ English → Go)



→ Next you can log in with the user "admin" and the password "admin". (→ Name: admin → Password: admin → Login)

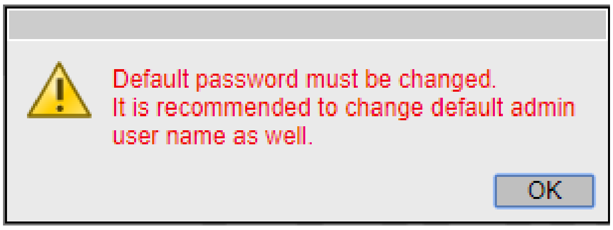


Name: admin

Password: •••••

For information about browser compatibility please refer to the manual

→ The default access must be changed before the first login. (→ OK)



Default password must be changed.
It is recommended to change default admin user name as well.

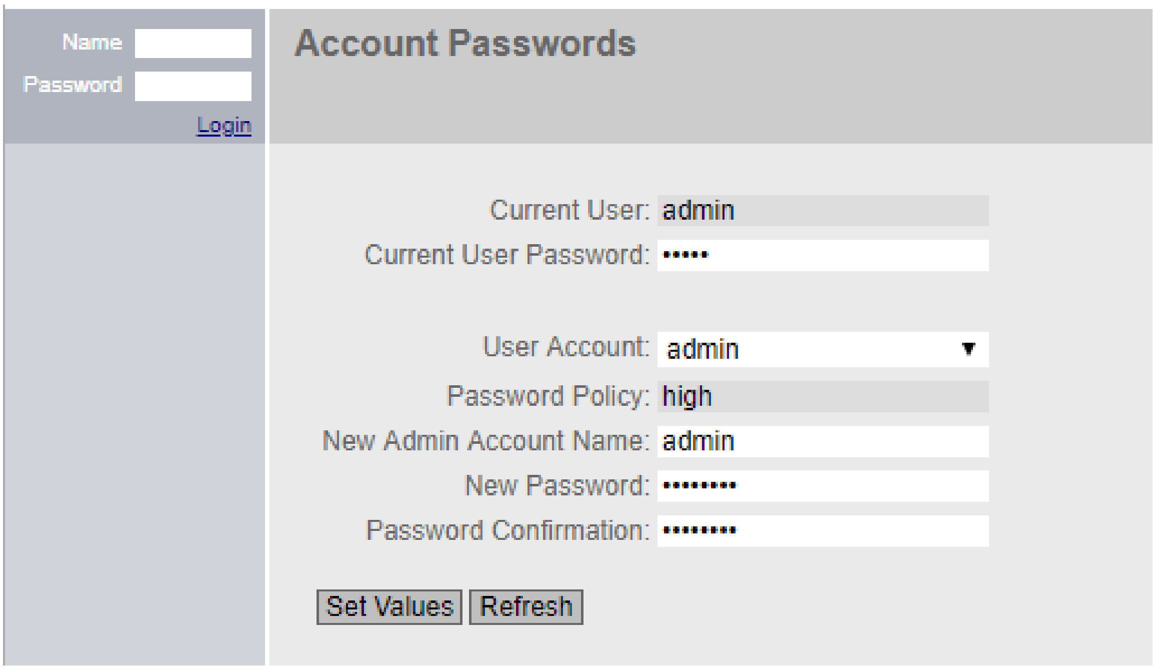
→ First enter the old password "admin" and then a new password twice.

→ Current user password: admin

→ New password: ***

→ Confirm password: ***

→ Apply settings



Account Passwords

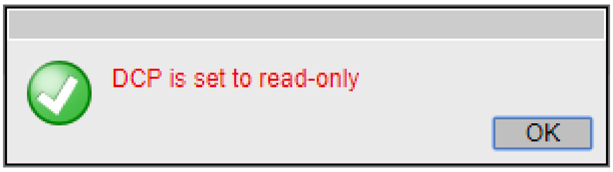
Current User: admin
Current User Password: •••••

User Account: admin
Password Policy: high
New Admin Account Name: admin
New Password: ••••••••
Password Confirmation: ••••••••

Note:

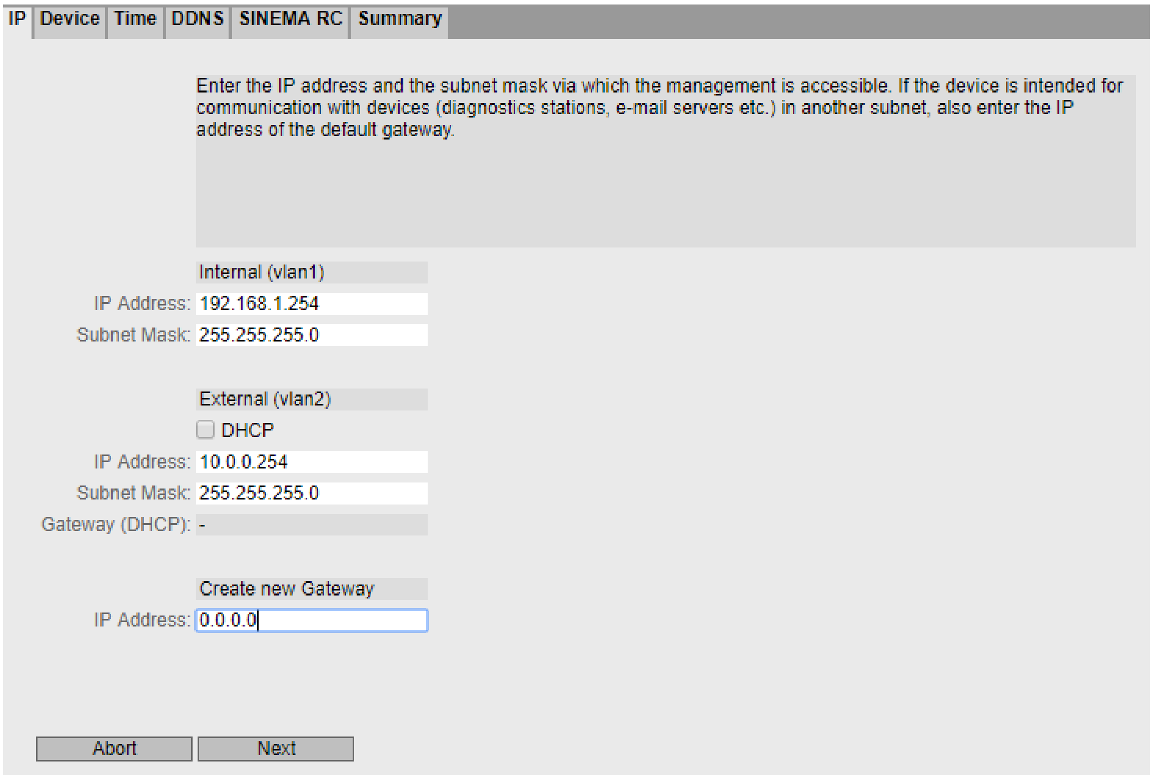
– *The new password needs at least eight characters, a number, an uppercase character and a special character!*

→ Once the access data and login has been successfully changed, DCP access to the device is permitted only in read-only mode. (→ OK)



DCP is set to read-only

→ In the following configuration wizard, set VLAN 2 to the static address 10.0.0.254/24 and click "Next". (External (vlan2) → DHCP → IP Address: 10.0.0.254 → ☐ Subnet Mask: 255.255.255.0 → Next)



Enter the IP address and the subnet mask via which the management is accessible. If the device is intended for communication with devices (diagnostics stations, e-mail servers etc.) in another subnet, also enter the IP address of the default gateway.

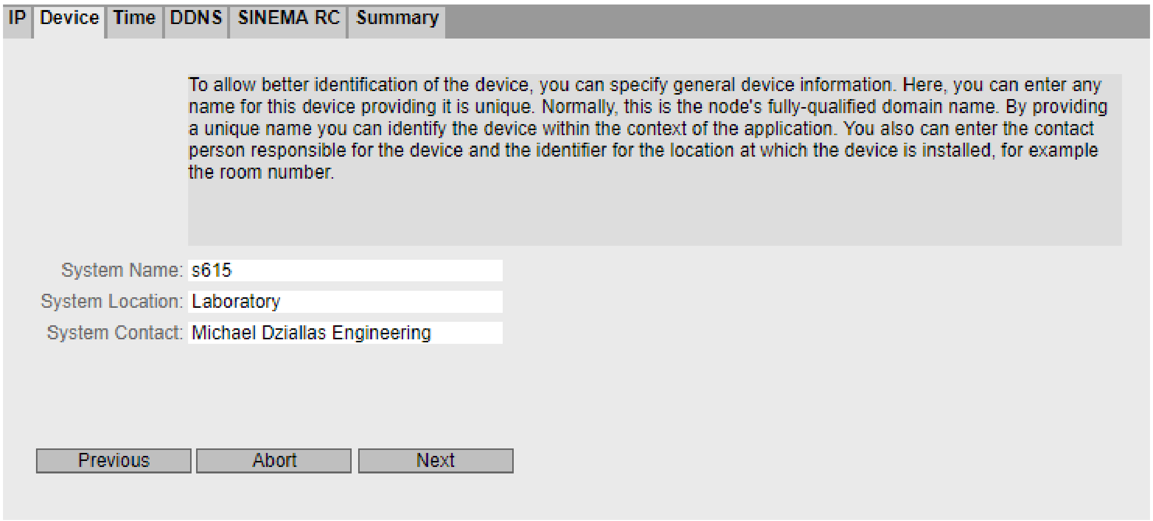
Internal (vlan1)
IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0

External (vlan2)
☐ DHCP
IP Address: 10.0.0.254
Subnet Mask: 255.255.255.0
Gateway (DHCP): -

Create new Gateway
IP Address: 0.0.0.0

→ Fill in the identification data as required and click "Next".

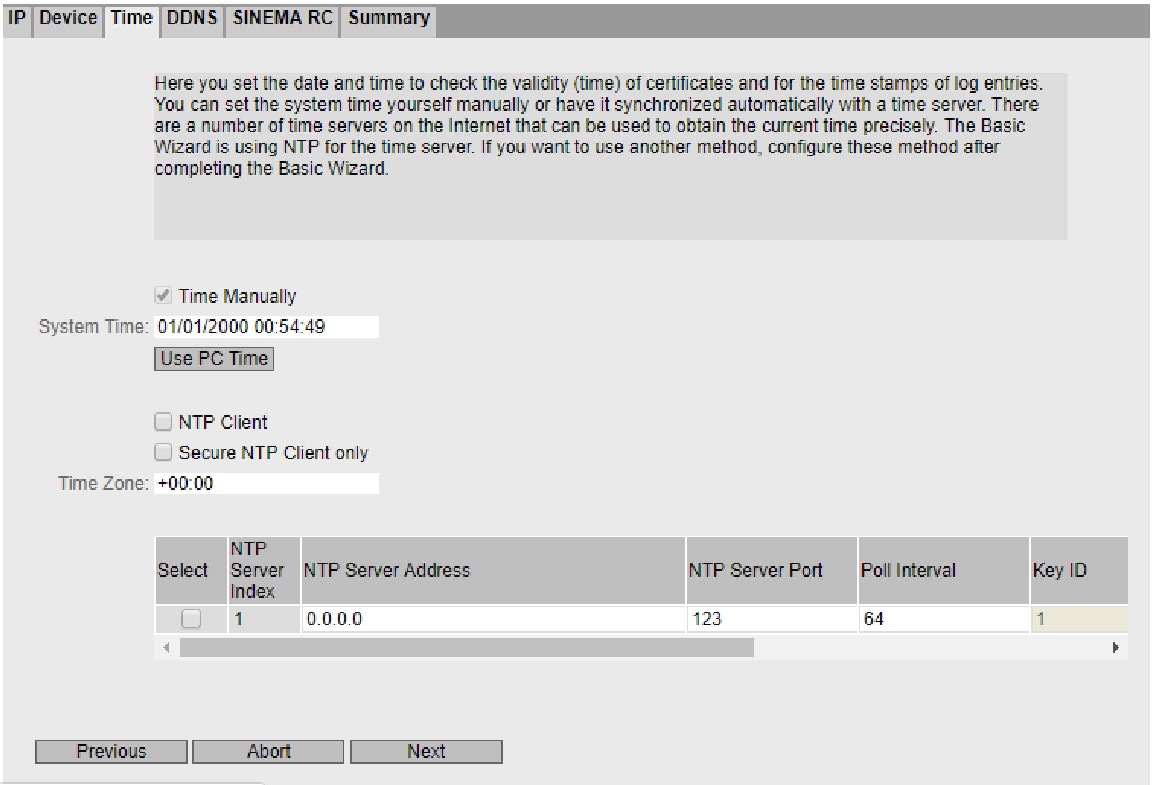
(→ System Name: … → System Location: … → System Contact: … → Next)



To allow better identification of the device, you can specify general device information. Here, you can enter any name for this device providing it is unique. Normally, this is the node's fully-qualified domain name. By providing a unique name you can identify the device within the context of the application. You also can enter the contact person responsible for the device and the identifier for the location at which the device is installed, for example the room number.

System Name: s615
System Location: Laboratory
System Contact: Michael Dziallas Engineering

→ Accept the PC time and click "Next". (→ Use PC Time → Next)



Here you set the date and time to check the validity (time) of certificates and for the time stamps of log entries. You can set the system time yourself manually or have it synchronized automatically with a time server. There are a number of time servers on the Internet that can be used to obtain the current time precisely. The Basic Wizard is using NTP for the time server. If you want to use another method, configure these method after completing the Basic Wizard.

☑ Time Manually

System Time: 01/01/2000 00:54:49

Use PC Time

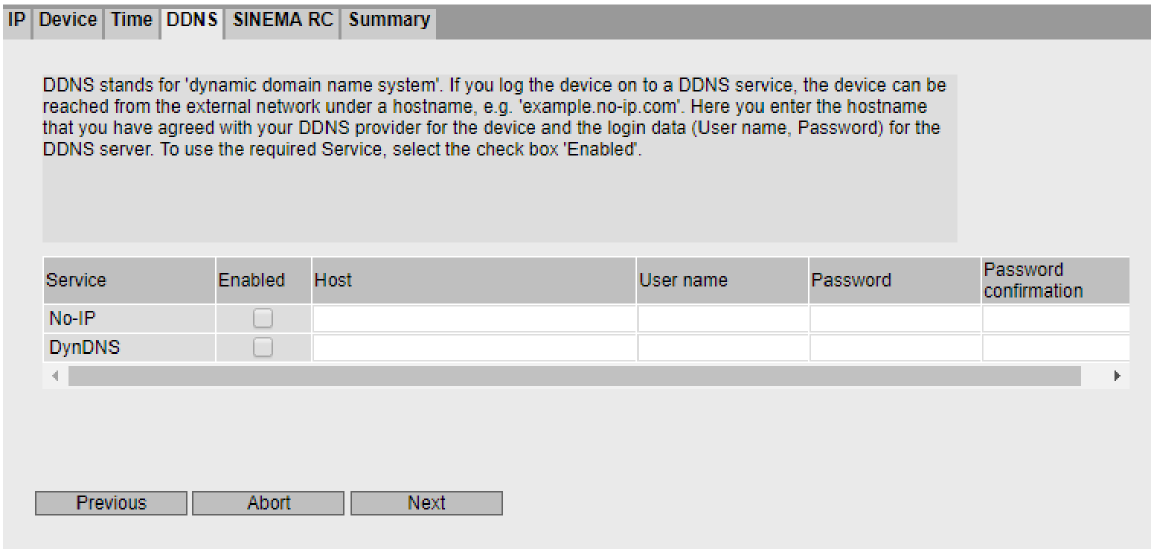
□ NTP Client

□ Secure NTP Client only

Time Zone: +00:00

Select	NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval	Key ID
□	1	0.0.0.0	123	64	1

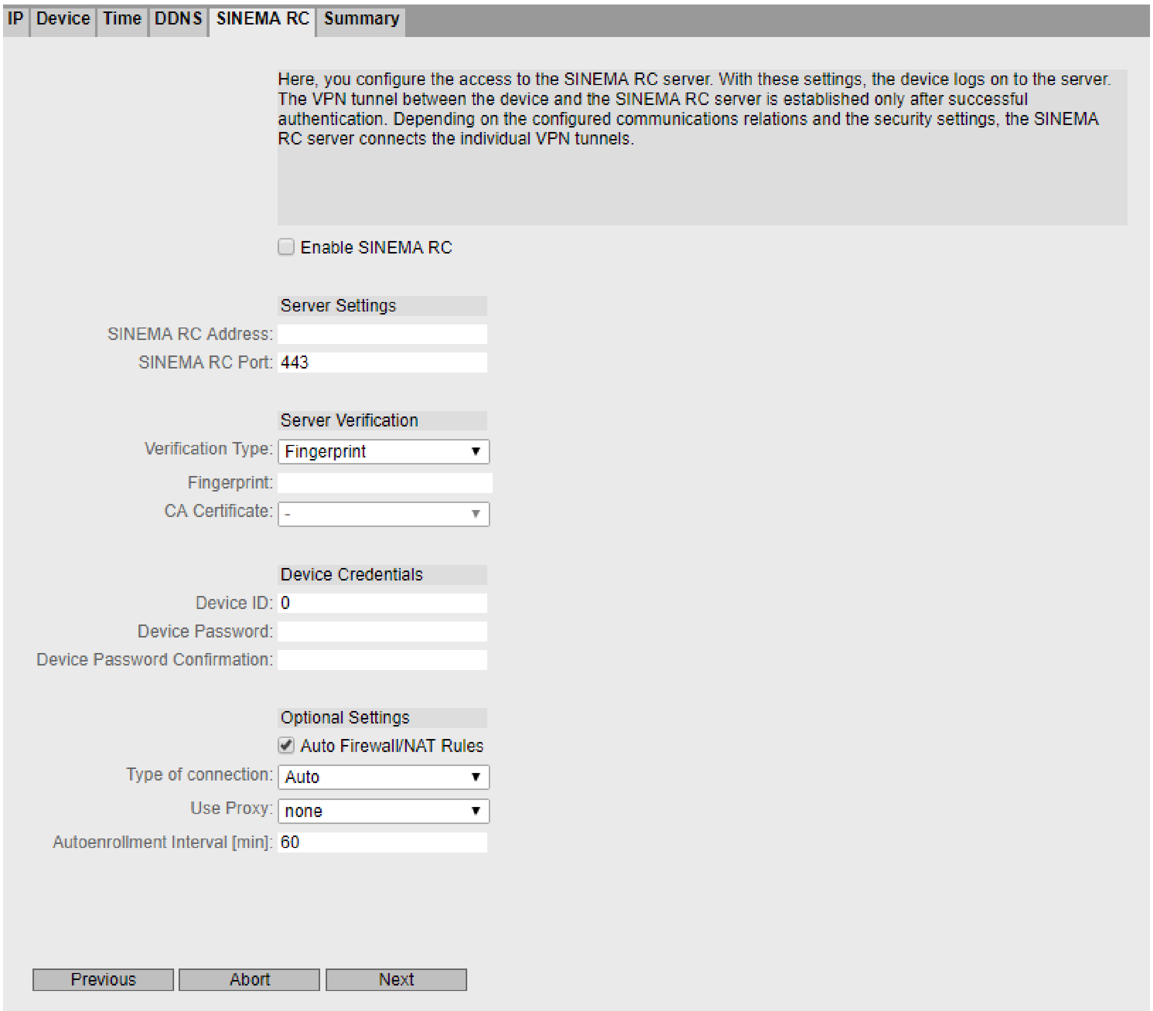
→ Skip the dynamic DNS settings with "Next". (→ Next)



DDNS stands for 'dynamic domain name system'. If you log the device on to a DDNS service, the device can be reached from the external network under a hostname, e.g. 'example.no-ip.com'. Here you enter the hostname that you have agreed with your DDNS provider for the device and the login data (User name, Password) for the DDNS server. To use the required Service, select the check box 'Enabled'.

Service	Enabled	Host	User name	Password	Password confirmation
No-IP	□				
DynDNS	□				

→ Skip the SINEMA RC settings with "Next". (→ Next)



Here, you configure the access to the SINEMA RC server. With these settings, the device logs on to the server. The VPN tunnel between the device and the SINEMA RC server is established only after successful authentication. Depending on the configured communications relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.

□ Enable SINEMA RC

Server Settings

SINEMA RC Address:

SINEMA RC Port: 443

Server Verification

Verification Type: Fingerprint

Fingerprint:

CA Certificate: -

Device Credentials

Device ID: 0

Device Password:

Device Password Confirmation:

Optional Settings

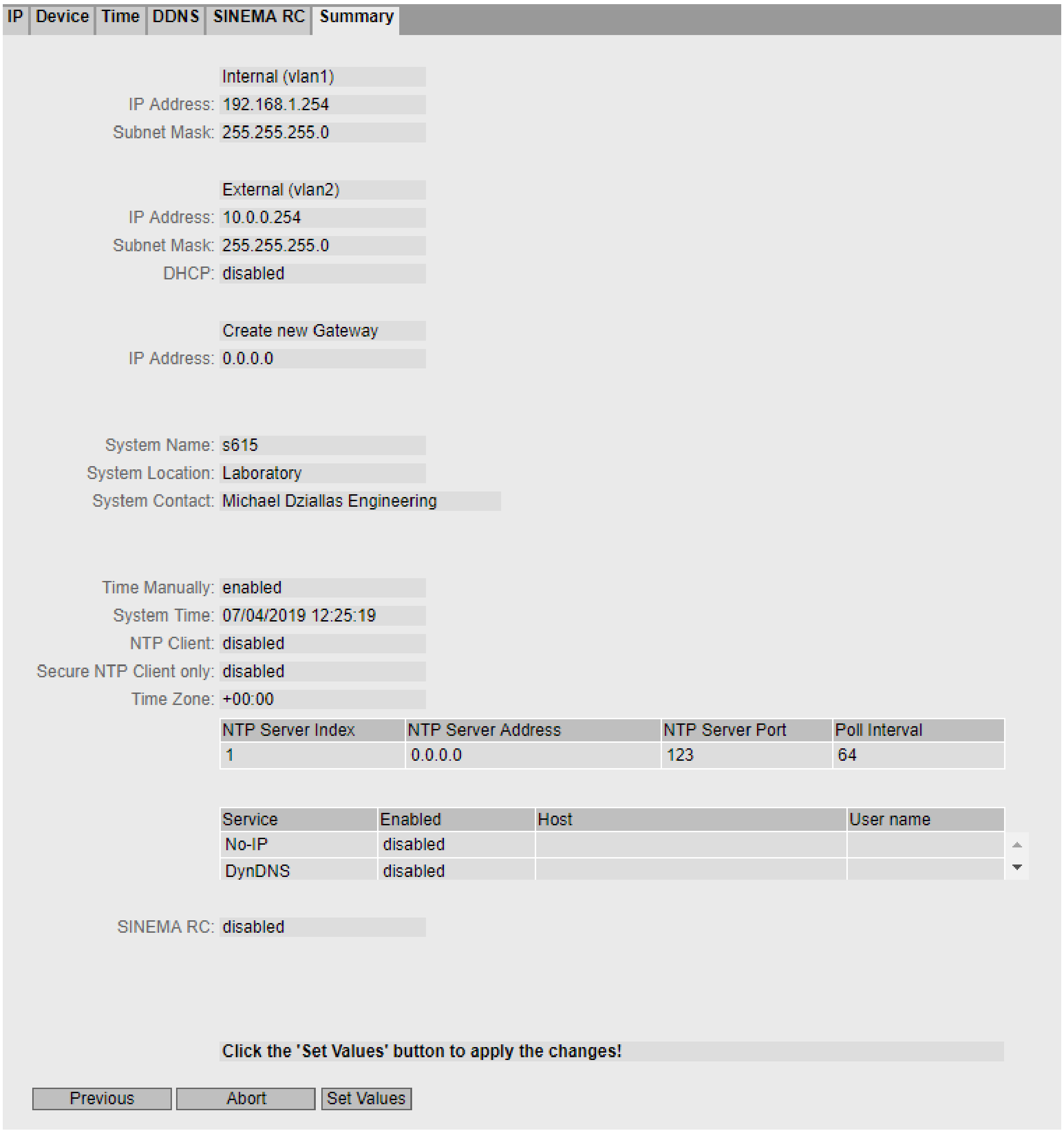
☑ Auto Firewall/NAT Rules

Type of connection: Auto

Use Proxy: none

Autoenrollment Interval [min]: 60

→ Check all settings again in the summary and confirm the configuration. (→ Set Values)



	Internal (vlan1)
IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
	External (vlan2)
IP Address:	10.0.0.254
Subnet Mask:	255.255.255.0
DHCP:	disabled
	Create new Gateway
IP Address:	0.0.0.0
System Name:	s615
System Location:	Laboratory
System Contact:	Michael Dziallas Engineering
Time Manually:	enabled
System Time:	07/04/2019 12:25:19
NTP Client:	disabled
Secure NTP Client only:	disabled
Time Zone:	+00:00

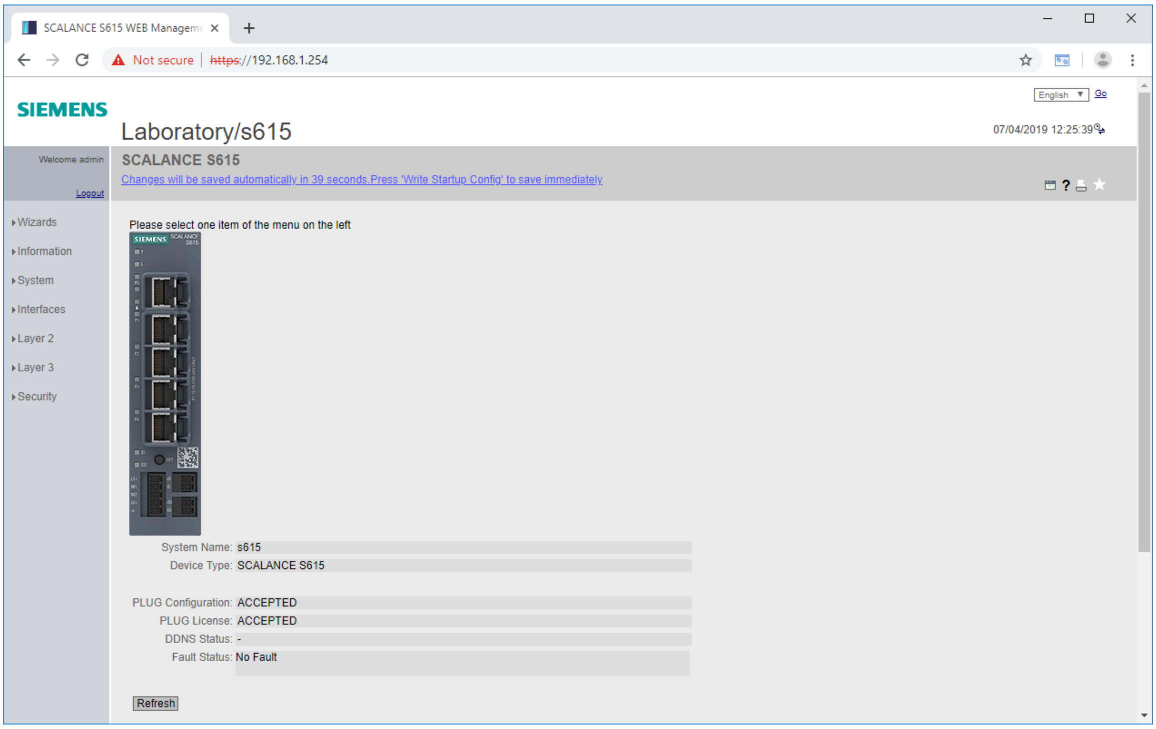
NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval
1	0.0.0.0	123	64

Service	Enabled	Host	User name
No-IP	disabled		
DynDNS	disabled		

SINEMA RC: disabled

Click the 'Set Values' button to apply the changes!

→ After accepting the settings, you will be taken to the final web interface of the SCALANCE S615.



Laboratory/s615

07/04/2019 12:25:39

SCALANCE S615

Changes will be saved automatically in 39 seconds.Press 'Write Startup Config' to save immediately

Please select one item of the menu on the left

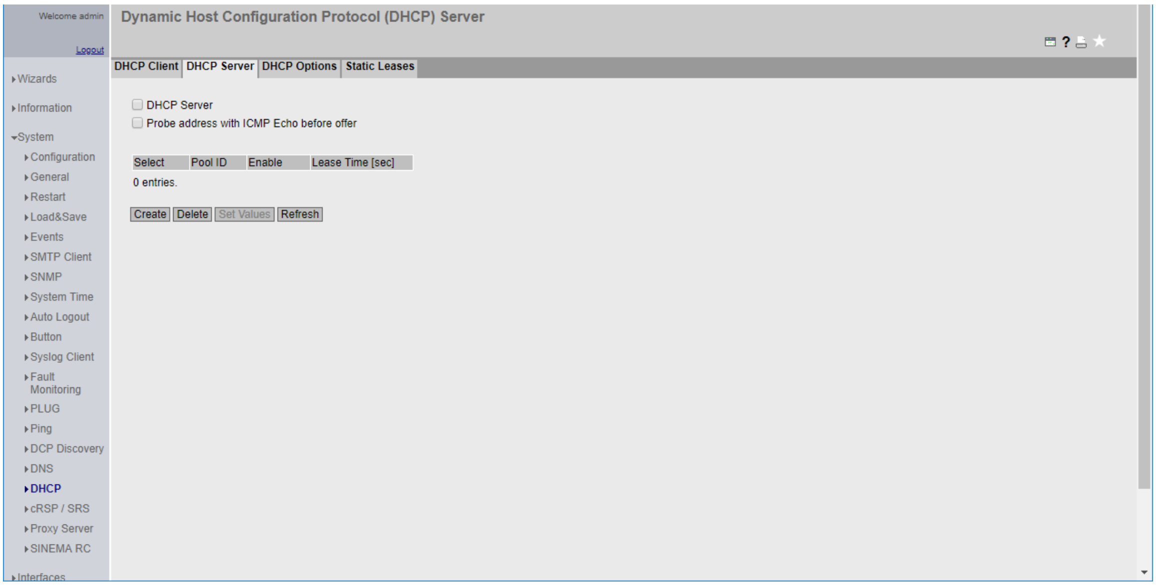
System Name: s615
Device Type: SCALANCE S615

PLUG Configuration: ACCEPTED
PLUG License: ACCEPTED
DDNS Status: -
Fault Status: No Fault

7.4 Configuration of the DHCP server

To make the connection to the plant network as easy as possible for the service technician and later during the tests, the SCALANCE S615 is assigned dynamic addresses both in the secured and in the unsecured range.

→ In the menu system, go to the DHCP server settings. (→ System → DHCP → DHCP Server)



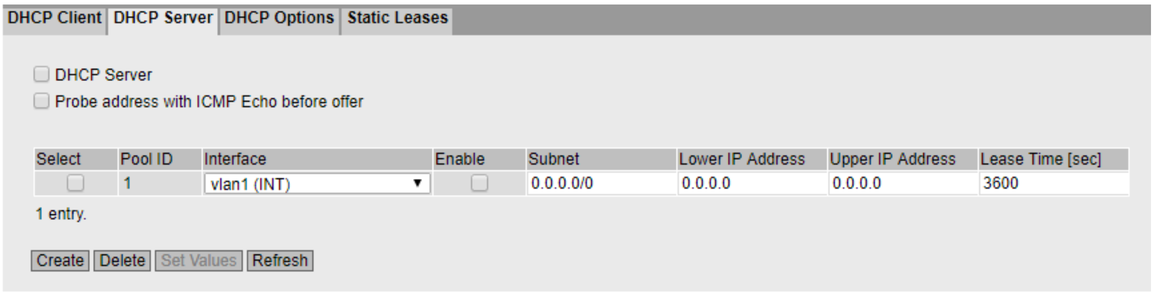
Dynamic Host Configuration Protocol (DHCP) Server

□ DHCP Server
□ Probe address with ICMP Echo before offer

Select	Pool ID	Enable	Lease Time [sec]

0 entries.

→ First generate a new pool of IP addresses. (→ Create)



□ DHCP Server
□ Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
□	1	vlan1 (INT)	□	0.0.0.0/0	0.0.0.0	0.0.0.0	3600

1 entry.

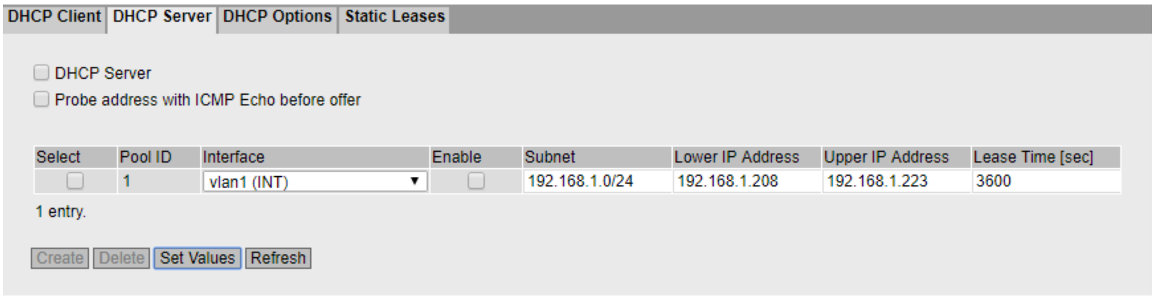
→ Select vlan1 for the interface. (→ Interface: vlan1 (INT))

→ Set the correct subnet. (→ Subnet: 192.168.1.0/24)

→ Set the first IP address. (→ Lower IP Address: 192.168.1.208)

→ Set the last IP address. (→ Upper IP Address: 192.168.108.223)

→ Apply the settings. (→ Set Values)

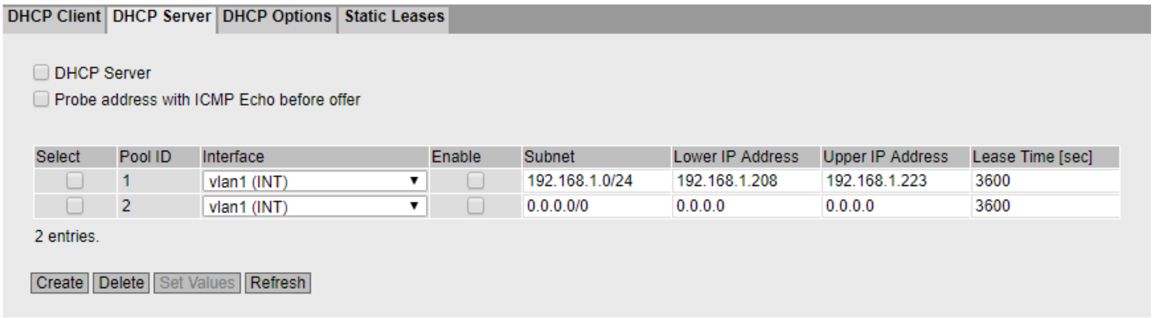


□ DHCP Server
□ Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
□	1	vlan1 (INT) ▾	□	192.168.1.0/24	192.168.1.208	192.168.1.223	3600

1 entry.

→ Generate another pool of IP addresses (→ Generate)



□ DHCP Server
□ Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
□	1	vlan1 (INT) ▾	□	192.168.1.0/24	192.168.1.208	192.168.1.223	3600
□	2	vlan1 (INT) ▾	□	0.0.0.0/0	0.0.0.0	0.0.0.0	3600

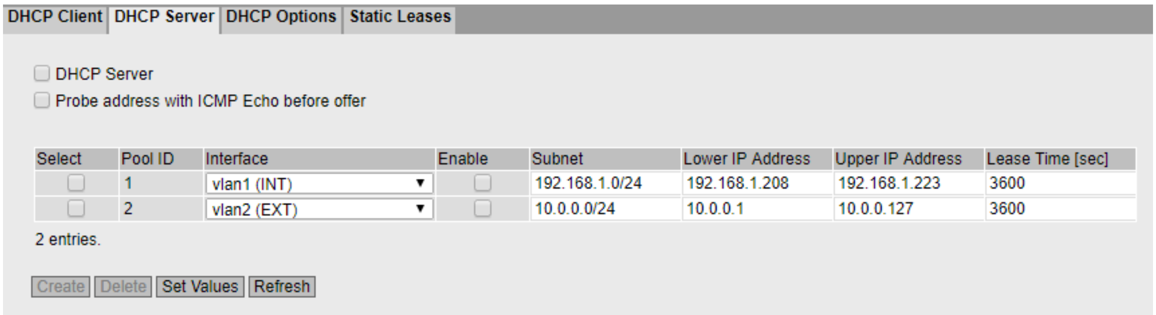
2 entries.

→ Select vlan2 for the interface. (→ Interface: vlan2 (EXT))

→ Set the correct subnet. (→ Subnet: 10.0.0.0/24)

→ Set the first IP address. (→ Lower IP Address: 10.0.0.1)

→ Set the last IP address. (→ Upper IP Address: 10.0.0.127)

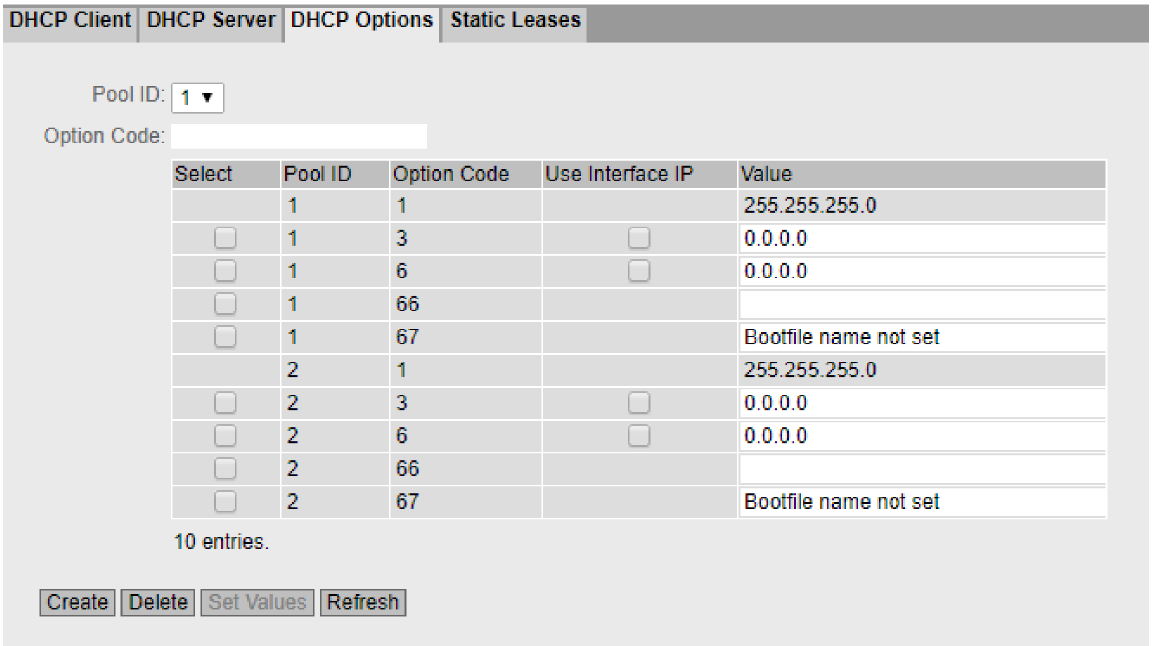


□ DHCP Server
□ Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
□	1	vlan1 (INT) ▾	□	192.168.1.0/24	192.168.1.208	192.168.1.223	3600
□	2	vlan2 (EXT) ▾	□	10.0.0.0/24	10.0.0.1	10.0.0.127	3600

2 entries.

→ Go to the DHCP Options tab (→ DHCP Options)



Pool ID: 1 ▾

Option Code:

Select	Pool ID	Option Code	Use Interface IP	Value
	1	1		255.255.255.0
☐	1	3	☐	0.0.0.0
☐	1	6	☐	0.0.0.0
☐	1	66		
☐	1	67		Bootfile name not set
	2	1		255.255.255.0
☐	2	3	☐	0.0.0.0
☐	2	6	☐	0.0.0.0
☐	2	66		
☐	2	67		Bootfile name not set

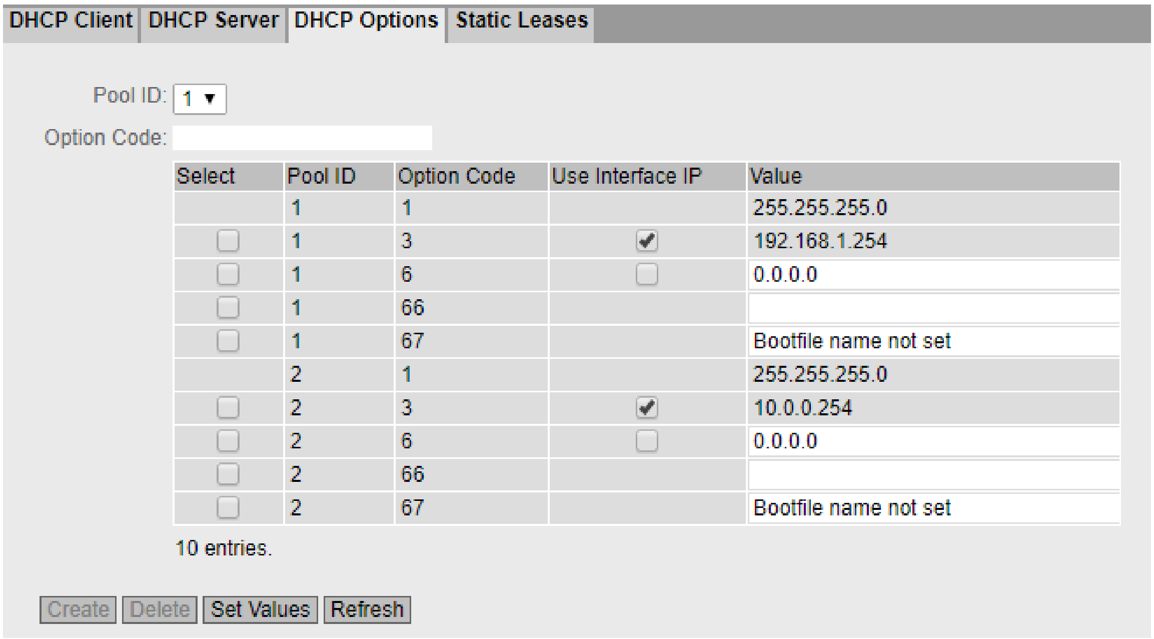
10 entries.

→ In both pools, use the interface IP for option 3 and accept the settings.

(→ Pool ID: 1 → Option Code: 3 → ☑Use Interface IP)

(→ Pool ID: 2 → Option value: 3 → ☑Use Interface IP)

(→ Set Values)



Pool ID: 1 ▾

Option Code:

Select	Pool ID	Option Code	Use Interface IP	Value
	1	1		255.255.255.0
☐	1	3	☑	192.168.1.254
☐	1	6	☐	0.0.0.0
☐	1	66		
☐	1	67		Bootfile name not set
	2	1		255.255.255.0
☐	2	3	☑	10.0.0.254
☐	2	6	☐	0.0.0.0
☐	2	66		
☐	2	67		Bootfile name not set

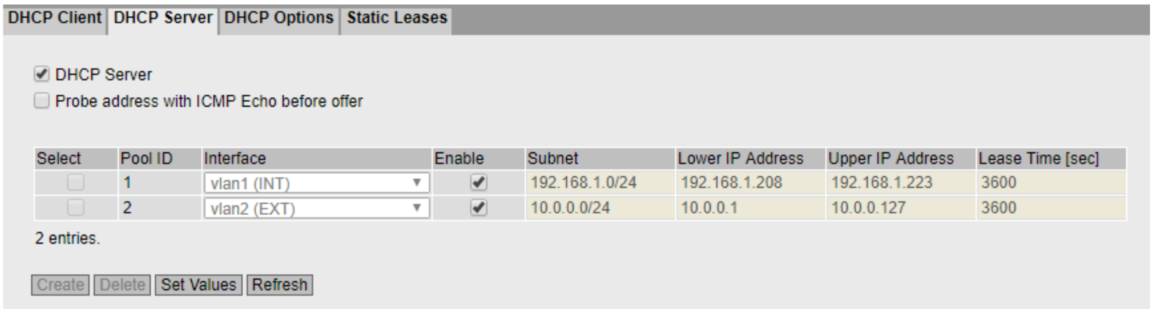
10 entries.

→ Go back to the DHCP server. (→ DHCP Server)

→ Select the DHCP server. (→ ☑ DHCP Server)

→ Select the two pools. (→ ☑ Select)

→ Apply the settings (→ Set Values)



☑ DHCP Server

□ Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
□	1	vlan1 (INT)	☑	192.168.1.0/24	192.168.1.208	192.168.1.223	3600
□	2	vlan2 (EXT)	☑	10.0.0.0/24	10.0.0.1	10.0.0.127	3600

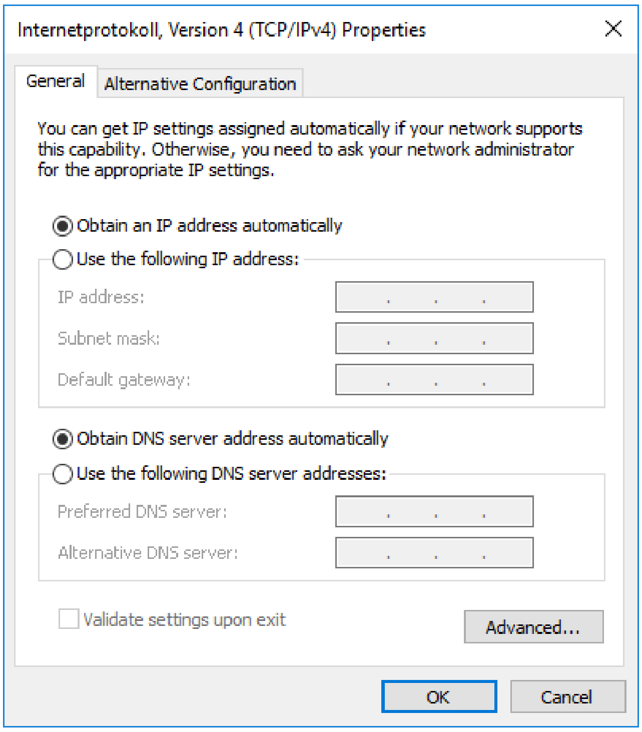
2 entries.

Note:

– *S615 will then distribute addresses from subnet 192.168.1.0/24 to ports 1 to 4 and from network 10.0.0.0/24 to port 5. In each case it supplies its own IP as gateway.*

→ For the settings on the programming device, follow the instructions in section 4.6 up to the settings of the Internet protocol, version 4 (TCP/IP).

→ Obtain the IP address automatically instead of the static configuration. (→ Obtain an IP address automatically → Obtain DNS server address automatically)



Internetprotokoll, Version 4 (TCP/IPv4) Properties

General | Alternative Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

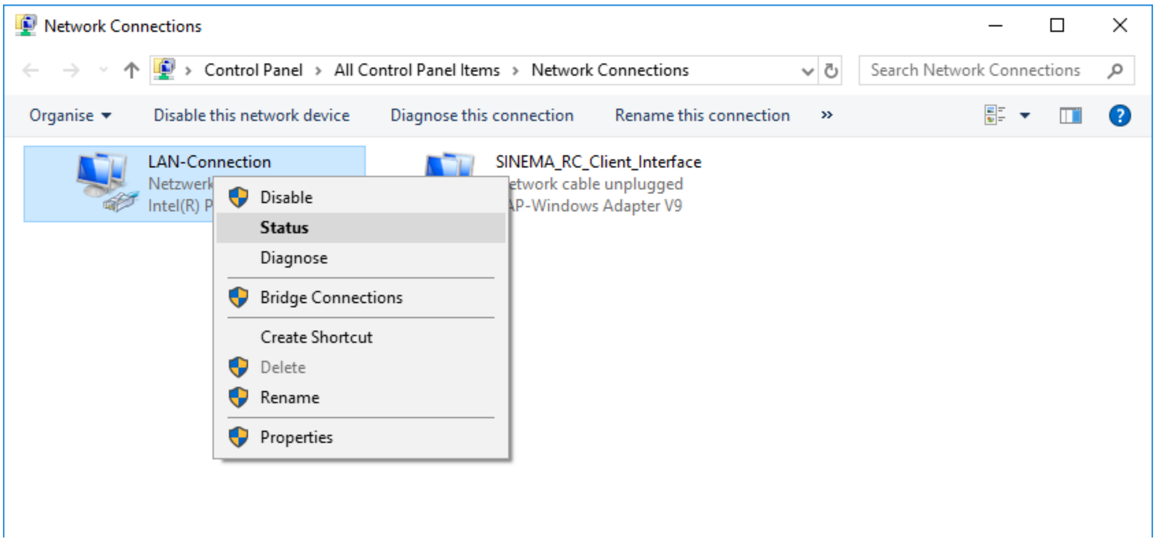
○ Use the following DNS server addresses:

Preferred DNS server: . . .

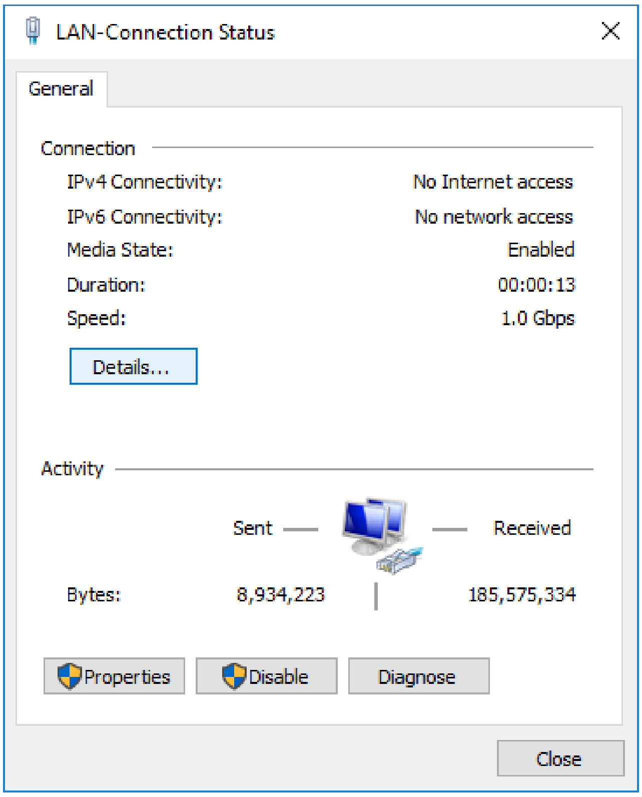
Alternative DNS server: . . .

□ Validate settings upon exit

→ Confirm the changes and open the status of the connection in the network connections. (→ LAN connection → Status)



→ Click Details. (→ Details)



LAN-Connection Status

General

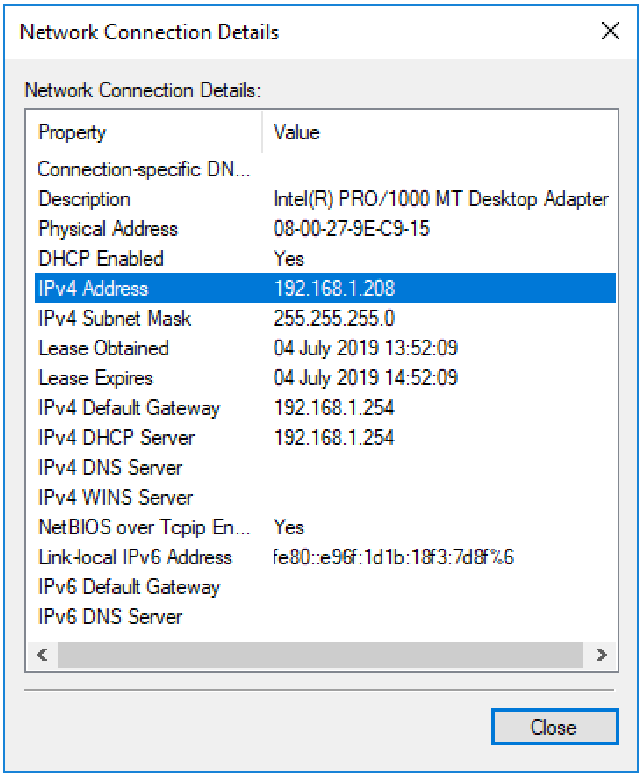
Connection

IPv4 Connectivity:	No Internet access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	00:00:13
Speed:	1.0 Gbps

Activity

	Sent	Received
Bytes:	8,934,223	185,575,334

→ Make sure that the programming device has been assigned a suitable IP address and a gateway.



Network Connection Details

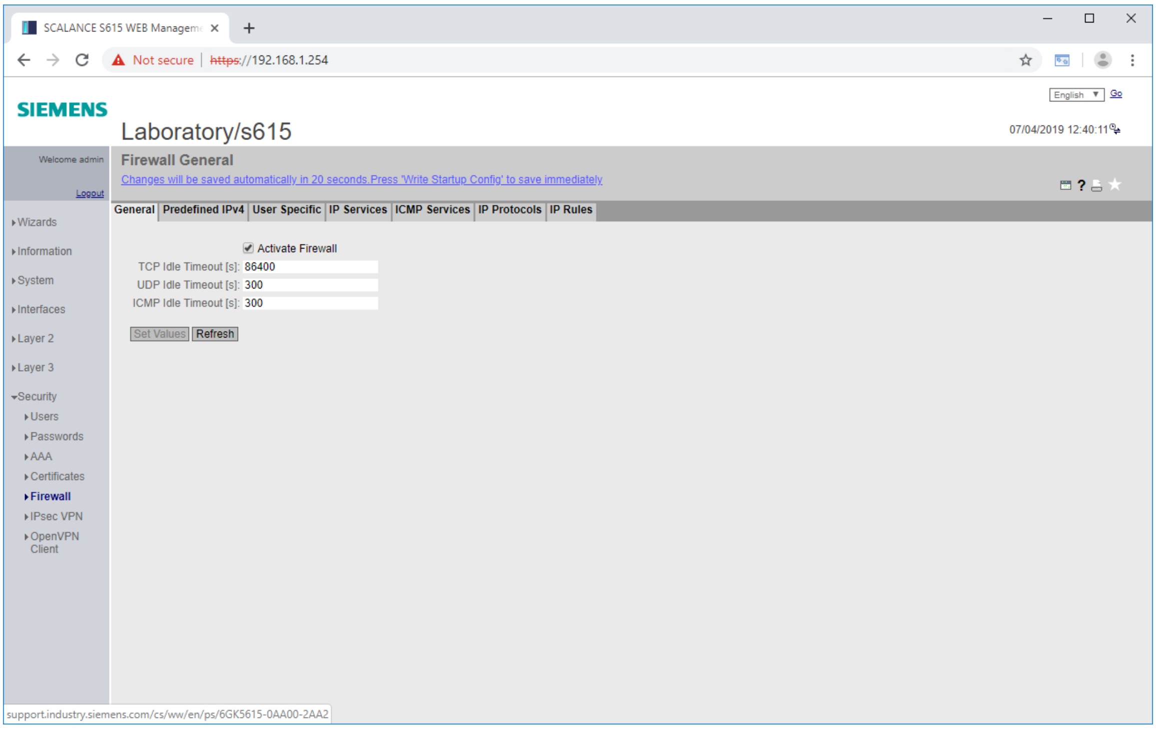
Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) PRO/1000 MT Desktop Adapter
Physical Address	08-00-27-9E-C9-15
DHCP Enabled	Yes
IPv4 Address	192.168.1.208
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	04 July 2019 13:52:09
Lease Expires	04 July 2019 14:52:09
IPv4 Default Gateway	192.168.1.254
IPv4 DHCP Server	192.168.1.254
IPv4 DNS Server	
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::e96f:1d1b:18f3:7d8f%6
IPv6 Default Gateway	
IPv6 DNS Server	

7.5 Setting up the firewall

In the factory configuration, SCALANCE S615 does not allow connections between the two VLANs. Devices on ports 1 to 4 cannot communicate with devices on port 5 and vice versa. This connection must be released so that, for example, devices from the company network can access the OPC UA server of the CPU.

→ Open the firewall settings in the Security menu. (→ Security → Firewall)



Laboratory/s615

07/04/2019 12:40:11

Firewall General

Changes will be saved automatically in 20 seconds.Press 'Write Startup Config' to save immediately

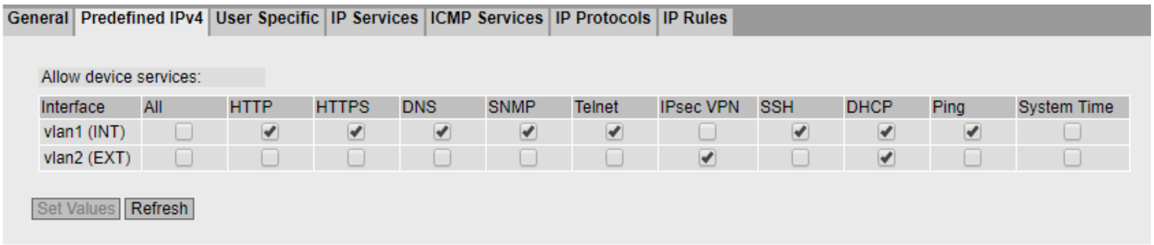
☑ Activate Firewall

TCP Idle Timeout [s]: 86400

UDP Idle Timeout [s]: 300

ICMP Idle Timeout [s]: 300

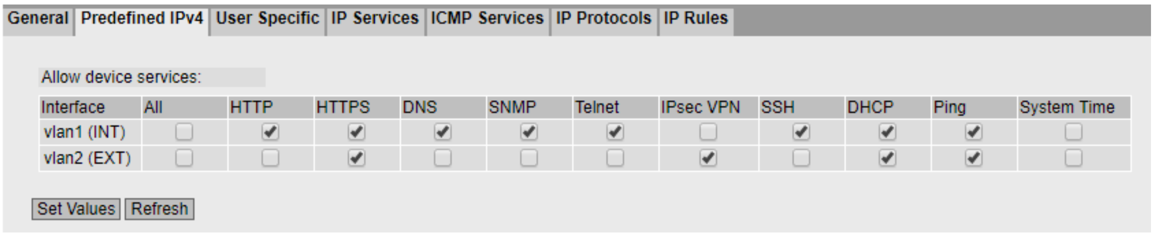
→ Go to the Predefined IPv4 Rules tab. (→ Predefined IPv4 rules)



Allow device services:

Interface	All	HTTP	HTTPS	DNS	SNMP	Telnet	IPsec VPN	SSH	DHCP	Ping	System Time
vlan1 (INT)	☐	☑	☑	☑	☑	☑	☐	☑	☑	☑	☐
vlan2 (EXT)	☐	☐	☐	☐	☐	☐	☑	☐	☑	☐	☐

→ Allow external access via HTTPS and Ping to the S615 and accept the settings. (→ vlan2 (EXT) → ☑ HTTPS → ☑ Ping)



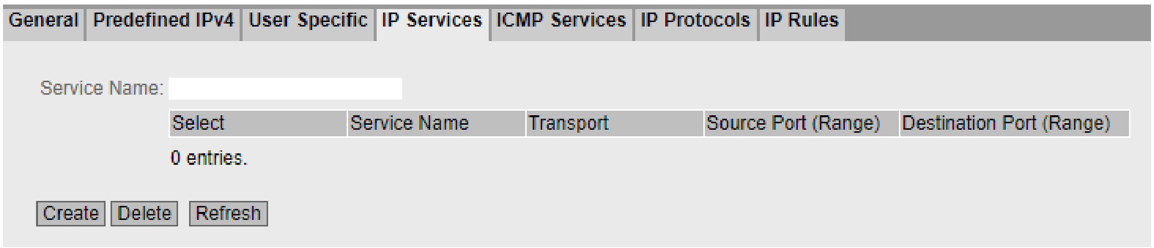
Allow device services:

Interface	All	HTTP	HTTPS	DNS	SNMP	Telnet	IPsec VPN	SSH	DHCP	Ping	System Time
vlan1 (INT)	☐	☑	☑	☑	☑	☑	☐	☑	☑	☑	☐
vlan2 (EXT)	☐	☐	☑	☐	☐	☐	☑	☐	☑	☑	☐

Note:

– *Selecting the check box for HTTPS allows external access to the configuration interface and should not be done without due consideration. However, we need this access later for authentication on the S615. Because the externally connected company network is not a public network, the risk here is relatively low. A SCALANCE S615 connected to the Internet should only allow external IPsec VPN, ping and, depending on the configuration, DHCP.*

→ Go to the IP Services tab. (→ IP Services)

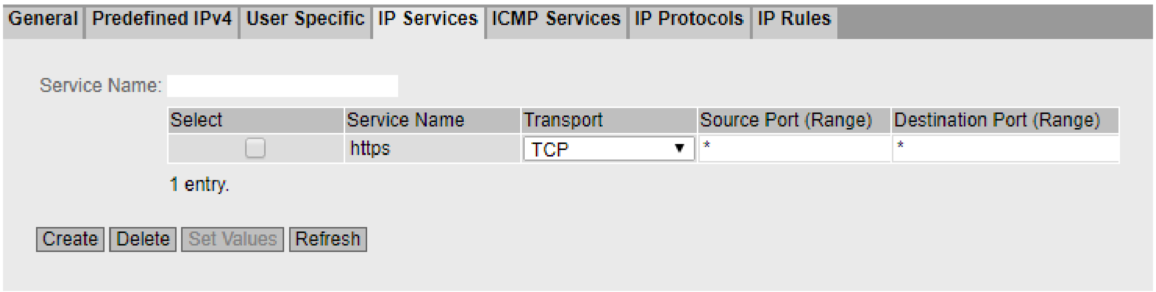


Service Name:

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)

0 entries.

→ Create a new service for the web server of the CPU. (→ Service Name: https → Create)

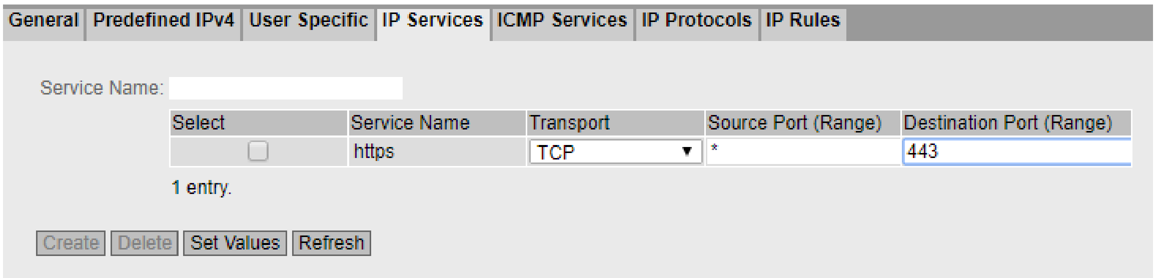


Service Name:

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)
☐	https	TCP ▼	*	*

1 entry.

→ Enter the HTTPS port as the destination port and apply the settings. (→ Destination Port: 443 → Set Values)

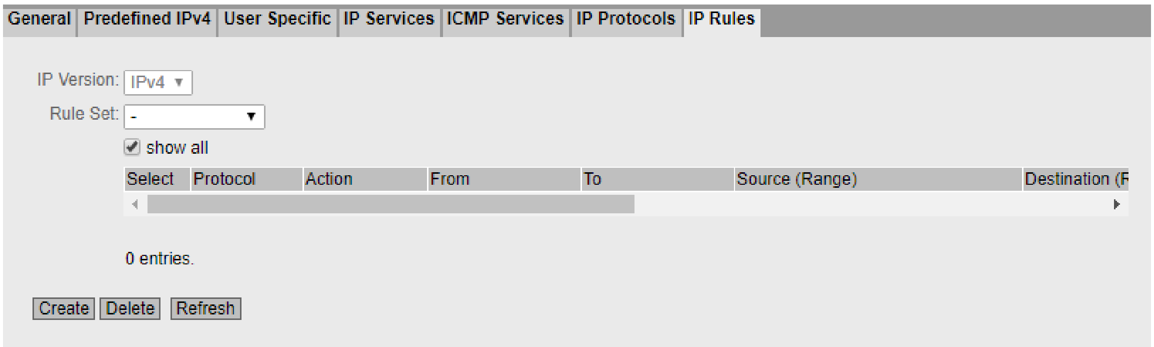


Service Name:

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)
□	https	TCP	*	443

1 entry.

→ Go to the IP Rules tab. (→ IP Rules)



IP Version: IPv4

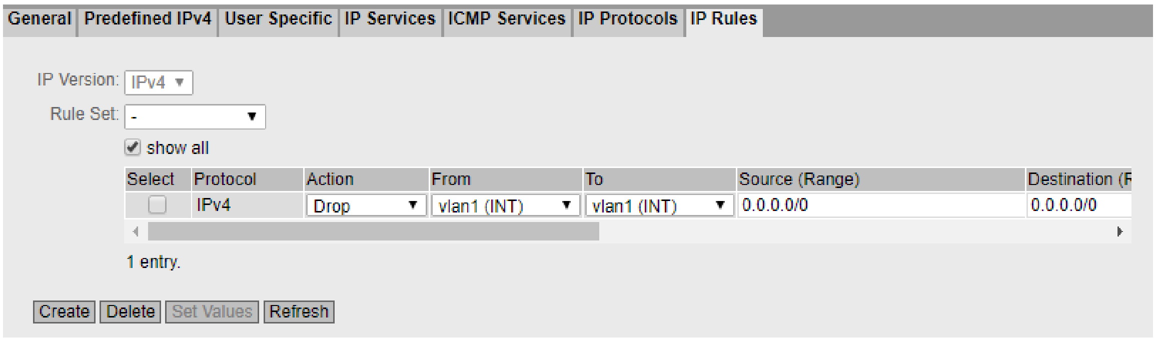
Rule Set: -

☑ show all

Select	Protocol	Action	From	To	Source (Range)	Destination (F

0 entries.

→ Create a new rule. (→ Create)



IP Version: IPv4

Rule Set: -

☑ show all

Select	Protocol	Action	From	To	Source (Range)	Destination (F
□	IPv4	Drop	vlan1 (INT)	vlan1 (INT)	0.0.0.0/0	0.0.0.0/0

1 entry.

→ Set the action to Accept. (→ Action: Accept)

→ Select vlan2 as the source interface. (→ From: vlan2 (EXT))

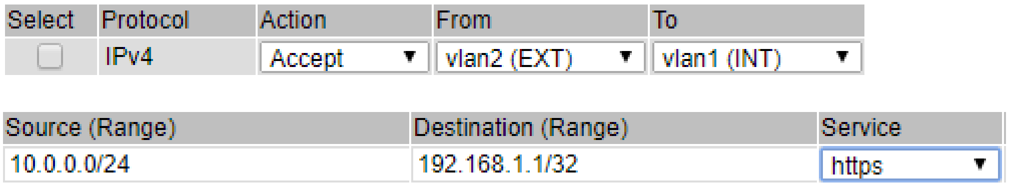
→ Select vlan1 as the destination interface. (→ To: vlan1 (INT))

→ Enter the company subnet 10.0.0.0/24 as the source network. (→ Source: 10.0.0.0/24)

→ Specify the X2 IP of the S7-1500 as the destination. (→ Destination: 192.168.1.1/32)

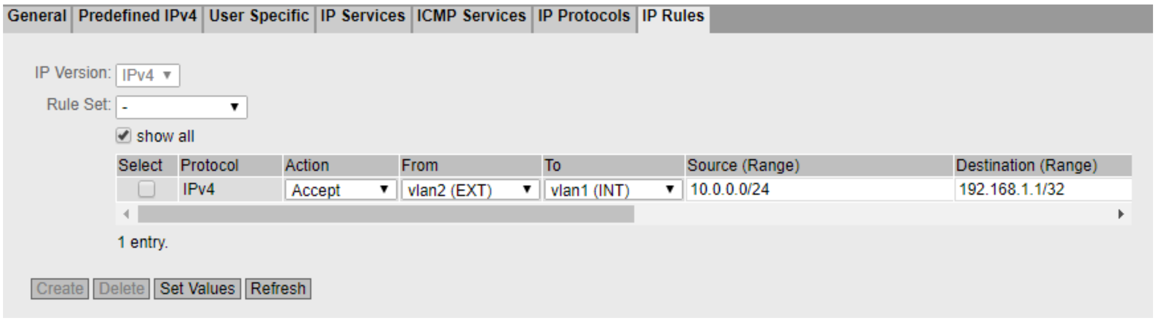
→ As service, select the HTTPS service you just created. (→ Service: https)

→ Apply the settings. (→ Set Values)



Select	Protocol	Action	From	To
□	IPv4	Accept ▼	vlan2 (EXT) ▼	vlan1 (INT) ▼

Source (Range)	Destination (Range)	Service
10.0.0.0/24	192.168.1.1/32	https ▼



IP Version: IPv4 ▼

Rule Set: - ▼

☑ show all

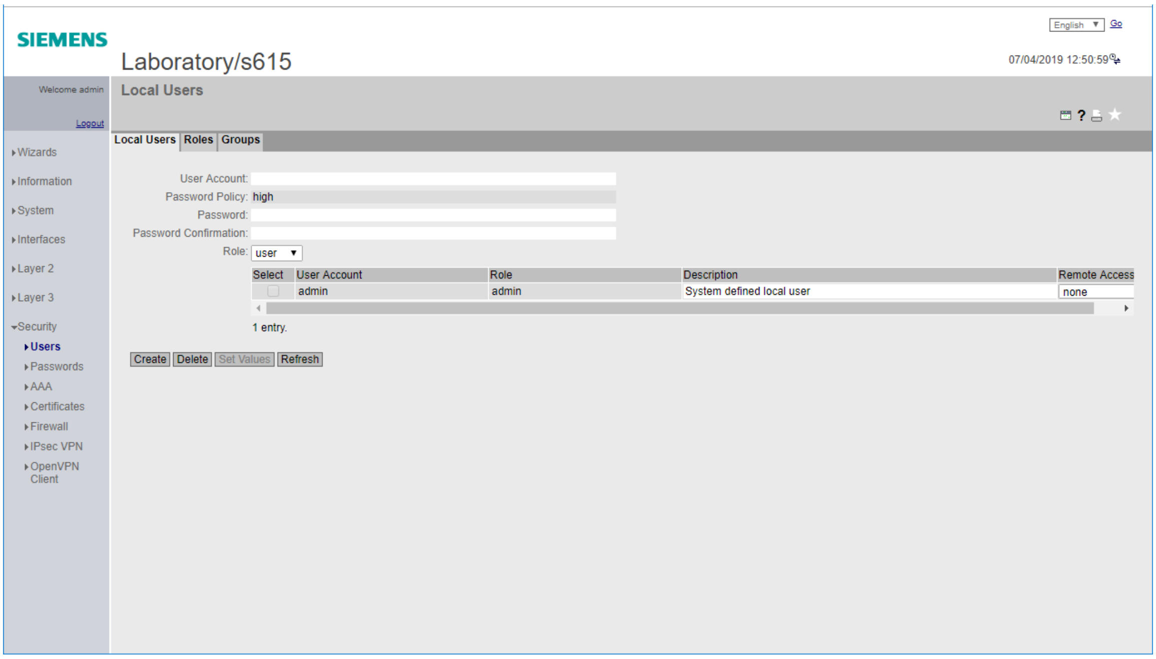
Select	Protocol	Action	From	To	Source (Range)	Destination (Range)
□	IPv4	Accept ▼	vlan2 (EXT) ▼	vlan1 (INT) ▼	10.0.0.0/24	192.168.1.1/32

1 entry.

7.6 Setting up the service user

After external access to the web server has been set up, specific rules are created in the next step, which are activated by logging on to the system with a user.

→ Open the local user administration. (→ Security → Users → Local Users)



User Account:
Password Policy: high
Password:
Password Confirmation:
Role: user

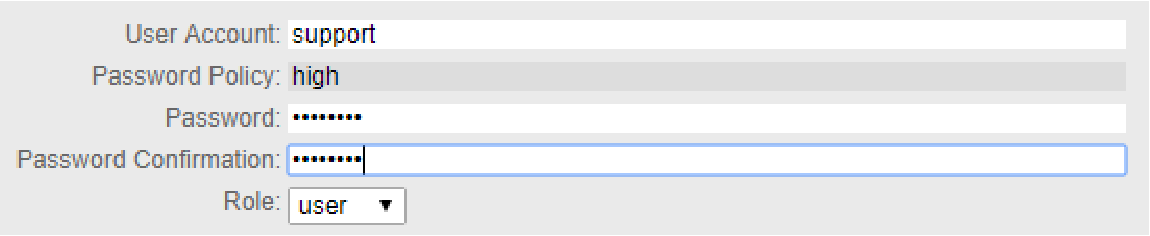
Select	User Account	Role	Description	Remote Access
☐	admin	admin	System defined local user	none

1 entry.

→ Specify a new username. (→ User account: support)

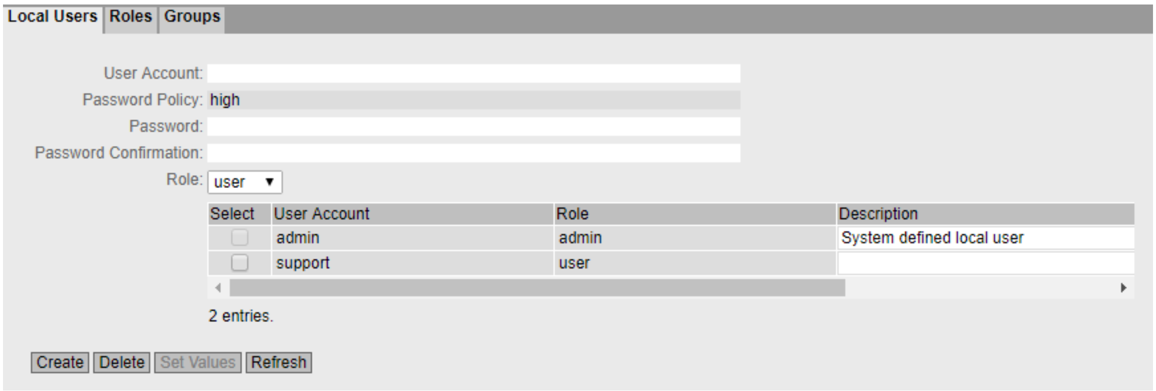
→ Enter a password. (→ Password: *** → Confirm password: ***)

→ Select "user" as role. (→ Role: user)



User Account: support
Password Policy: high
Password: ••••••••
Password Confirmation: ••••••••
Role: user

→ Click Create. (→ Create)



User Account:

Password Policy: high

Password:

Password Confirmation:

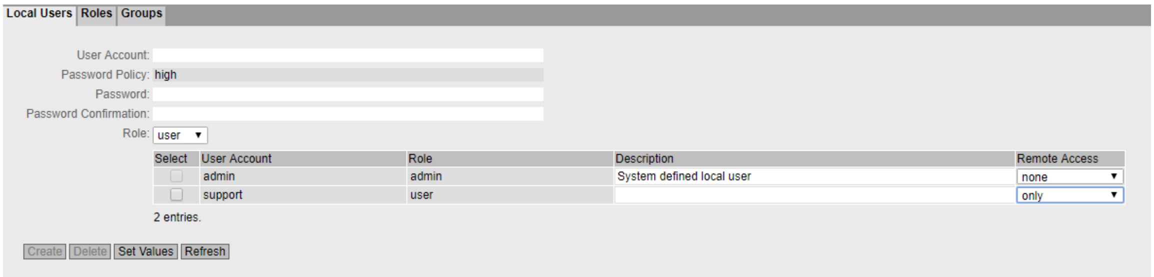
Role: user

Select	User Account	Role	Description
□	admin	admin	System defined local user
□	support	user	

2 entries.

→ Select "only" as remote access (→ support → Remote access: only)

→ Apply the settings. (→ Set Values)



User Account:

Password Policy: high

Password:

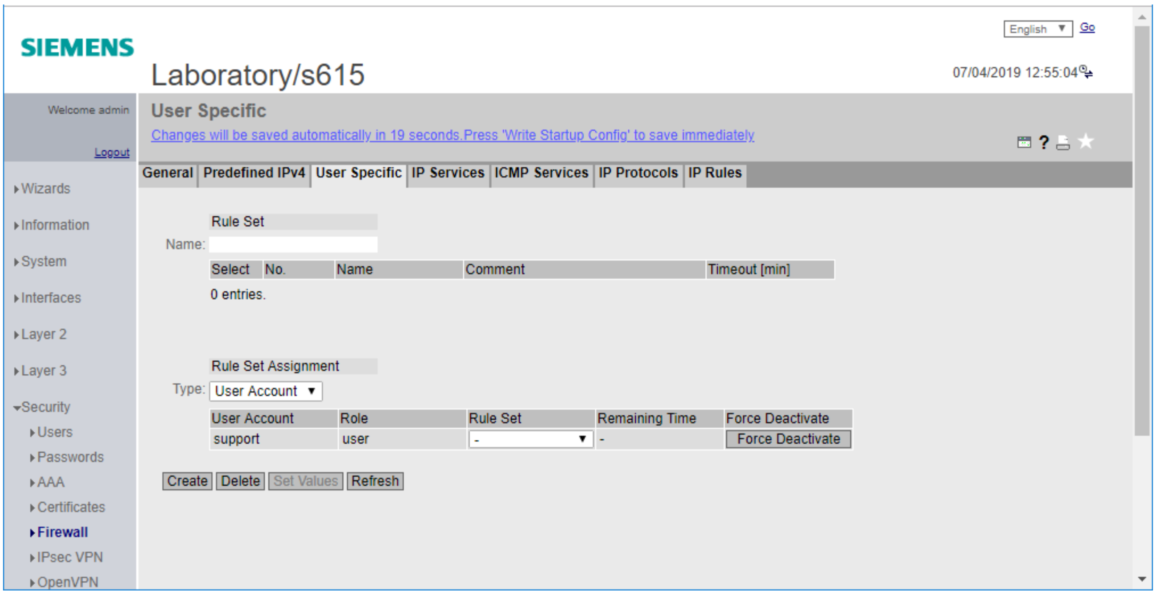
Password Confirmation:

Role: user

Select	User Account	Role	Description	Remote Access
□	admin	admin	System defined local user	none
□	support	user		only

2 entries.

→ Under firewall, switch to the User Specific tab. (→ Security → Firewall → User Specific)



Laboratory/s615

07/04/2019 12:55:04

User Specific

Changes will be saved automatically in 19 seconds.Press 'Write Startup Config' to save immediately

Rule Set

Name:

Select	No.	Name	Comment	Timeout [min]

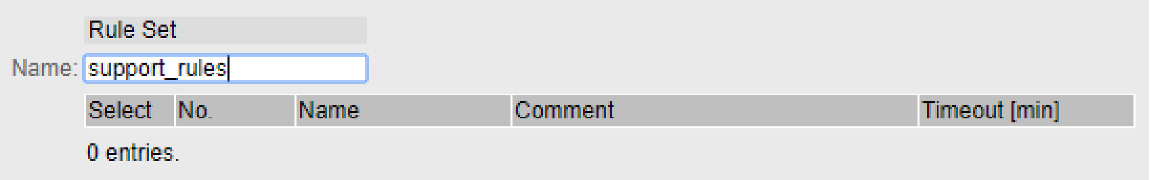
0 entries.

Rule Set Assignment

Type: User Account

User Account	Role	Rule Set	Remaining Time	Force Deactivate
support	user	-	-	Force Deactivate

→ Add a new rule set "support_rules". (→ Rule Set → Name: support_rules → Create)

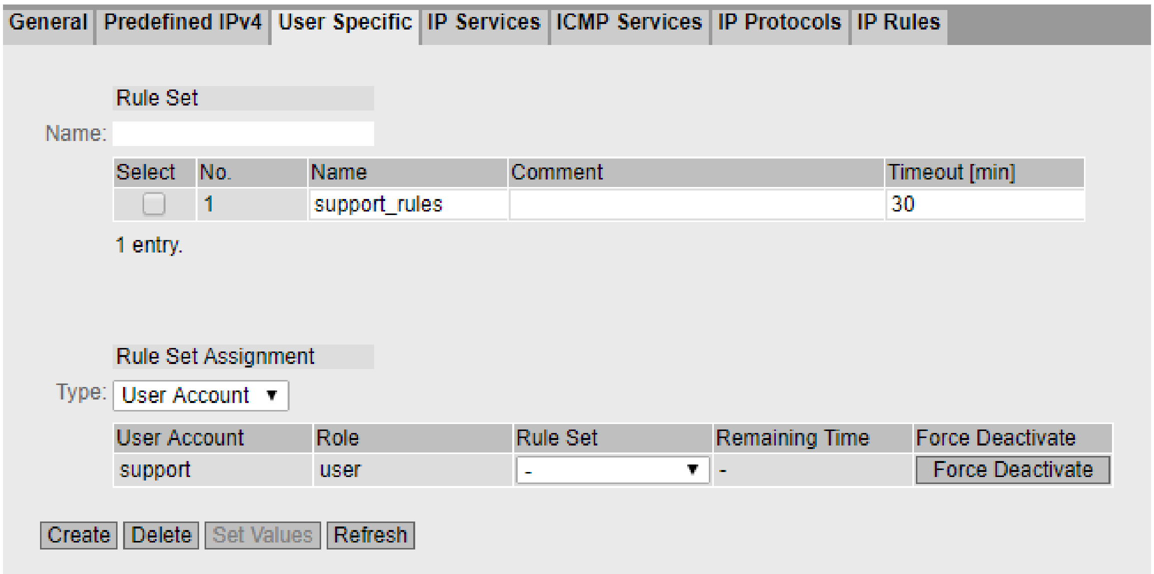


Rule Set

Name: support_rules

Select	No.	Name	Comment	Timeout [min]

0 entries.



Rule Set

Name:

Select	No.	Name	Comment	Timeout [min]
□	1	support_rules		30

1 entry.

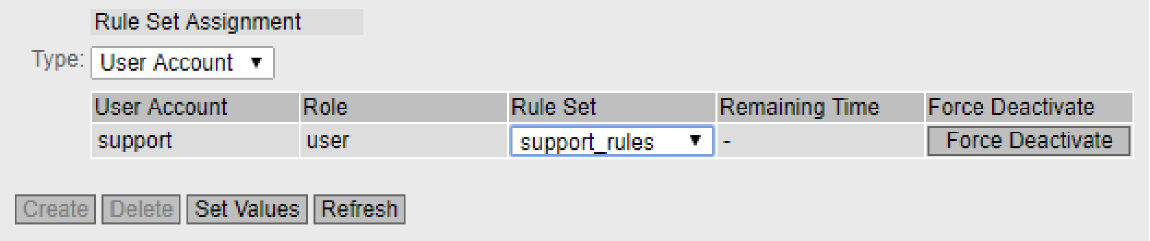
Rule Set Assignment

Type: User Account ▼

User Account	Role	Rule Set	Remaining Time	Force Deactivate
support	user	- ▼	-	Force Deactivate

→ Assign the rule set "support_rules" to the user "support". (→ Rule Set Assignment → support → Rule Set: support_rules)

→ Apply the new settings. (→ Set Values)



Rule Set Assignment

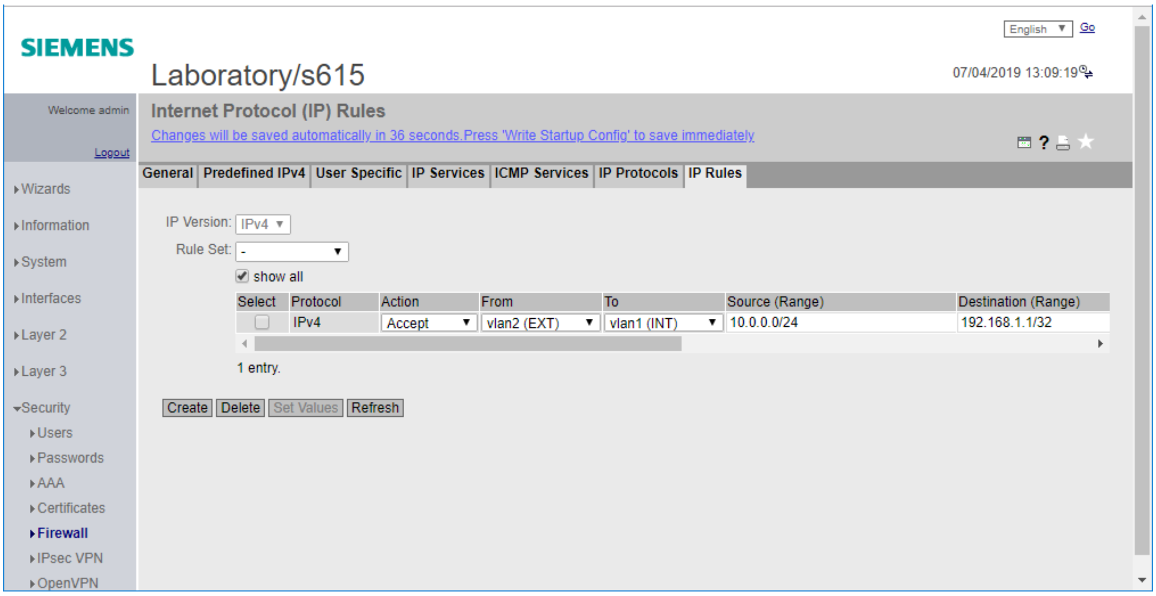
Type: User Account ▼

User Account	Role	Rule Set	Remaining Time	Force Deactivate
support	user	support_rules ▼	-	Force Deactivate

Note:

– *This will apply the additional rule set "support_rules" to the computer of the user "support" after successful login to the system.*

→ Go to the IP Rules tab. (→ Security → Firewall → IP Rules)



Internet Protocol (IP) Rules

Changes will be saved automatically in 36 seconds.Press 'Write Startup Config' to save immediately

IP Version: IPv4

Rule Set: -

☑ show all

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)
□	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.0/24	192.168.1.1/32

1 entry.

→ Create a new rule. (→ Create)

→ Set the action to Accept. (→ Action: Accept)

→ Select vlan2 as the source interface. (→ From: vlan2 (EXT))

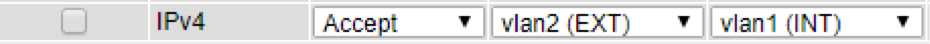
→ Select vlan1 as the destination interface. (→ To: vlan1 (INT))

→ Enter "DYNAMIC" as the source network. (→ Source: DYNAMIC)

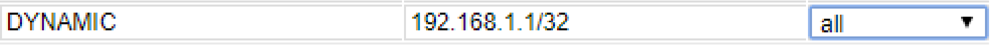
→ Enter the X2 IP of the S7-1500 as the destination. (→ Destination: 192.168.1.1/32)

→ Select "all" as service. (→ Service: all)

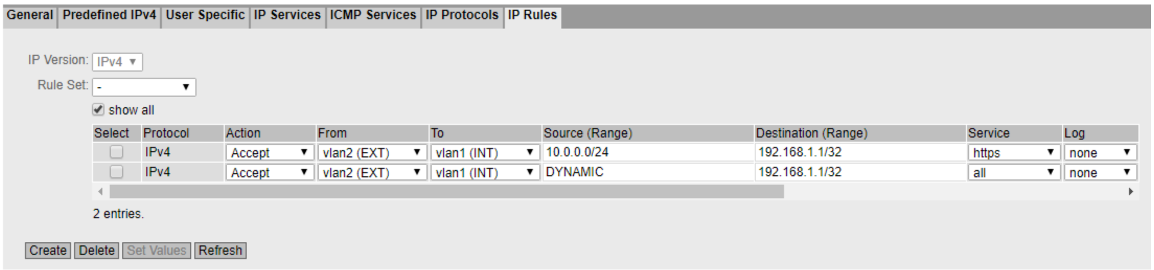
→ Apply the settings. (→ Set Values)



□	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)



DYNAMIC	192.168.1.1/32	all


General | Predefined IPv4 | User Specific | IP Services | ICMP Services | IP Protocols | IP Rules
Create | Delete | Set Values | Refresh

IP Version: IPv4

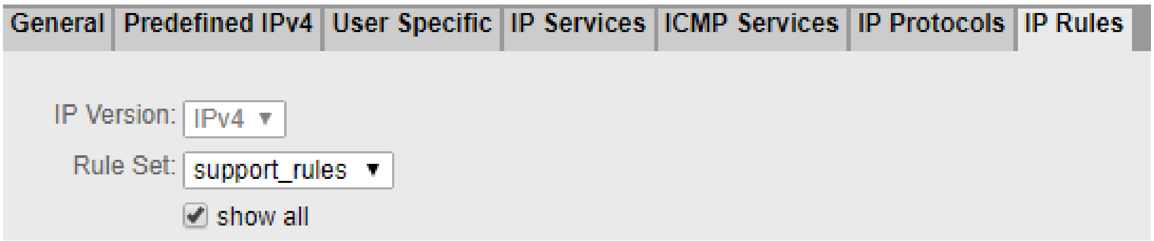
Rule Set: -

☑ show all

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service	Log
□	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	10.0.0.0/24	192.168.1.1/32	https	none
□	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	DYNAMIC	192.168.1.1/32	all	none

2 entries.

→ Next, select "support_rules" under rule set. (→ Rule Set: support_rules → ☑ show all)

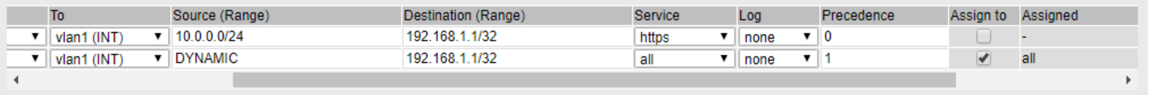


IP Version: IPv4

Rule Set: support_rules

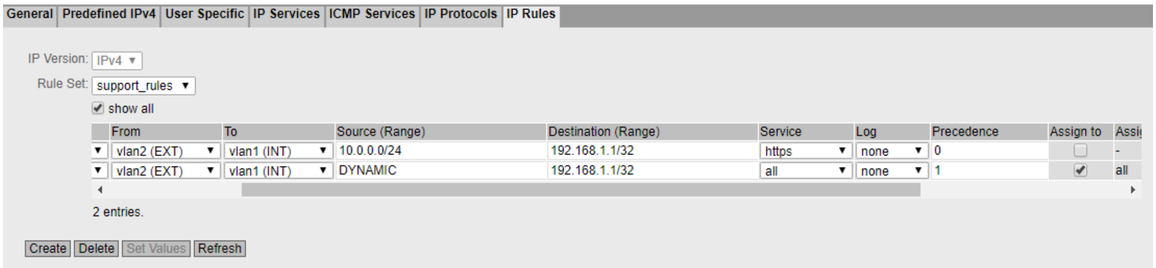
☑ show all

→ Select the "Assign to" check box in the rule you have just created. (→ ☑ Assign to)



	To	Source (Range)	Destination (Range)	Service	Log	Precedence	Assign to	Assigned
▼	vlan1 (INT) ▼	10.0.0.0/24	192.168.1.1/32	https ▼	none ▼	0	□	-
▼	vlan1 (INT) ▼	DYNAMIC	192.168.1.1/32	all ▼	none ▼	1	☑	all

→ Apply the settings. (→ Set Values)



IP Version: IPv4

Rule Set: support_rules

☑ show all

	From	To	Source (Range)	Destination (Range)	Service	Log	Precedence	Assign to	Assi
▼	vlan2 (EXT) ▼	vlan1 (INT) ▼	10.0.0.0/24	192.168.1.1/32	https ▼	none ▼	0	□	-
▼	vlan2 (EXT) ▼	vlan1 (INT) ▼	DYNAMIC	192.168.1.1/32	all ▼	none ▼	1	☑	all

2 entries.

Note:

– *The placeholder DYNAMIC is replaced with the IP of the logged-in user during login. Due to the assignment of the rule to the rule set "support_rules", this rule is only active after the corresponding user has logged in.*

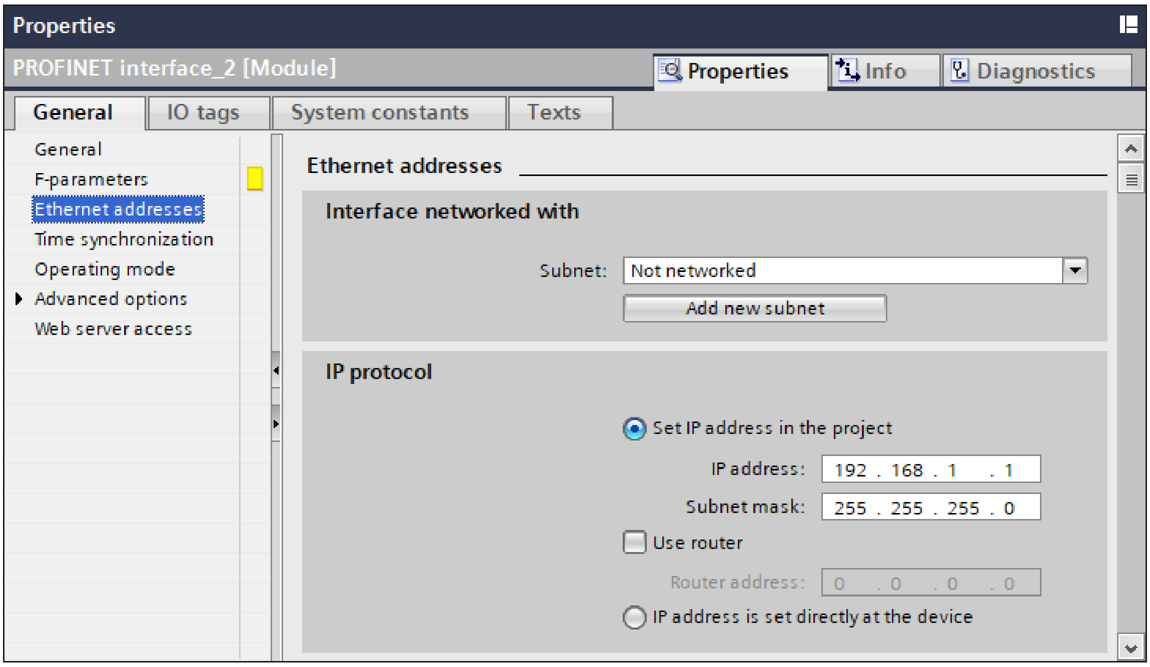
7.7 Configuration of the CPU 1516F

The network configuration must then be adapted and transferred to the CPU 1516F.

→ Connect the X2 interface of the CPU 1516F-3 PN/DP to port 1 of the SCALANCE S615.

→ Open the properties of the X2 interface of the CPU_1516F in the TIA Portal. (→ CPU_1516F → X2 → Properties)

→ Go the IP configuration. (→ Ethernet addresses → IP protocol)



Subnet: Not networked

● Set IP address in the project

IP address: 192 . 168 . 1 . 1

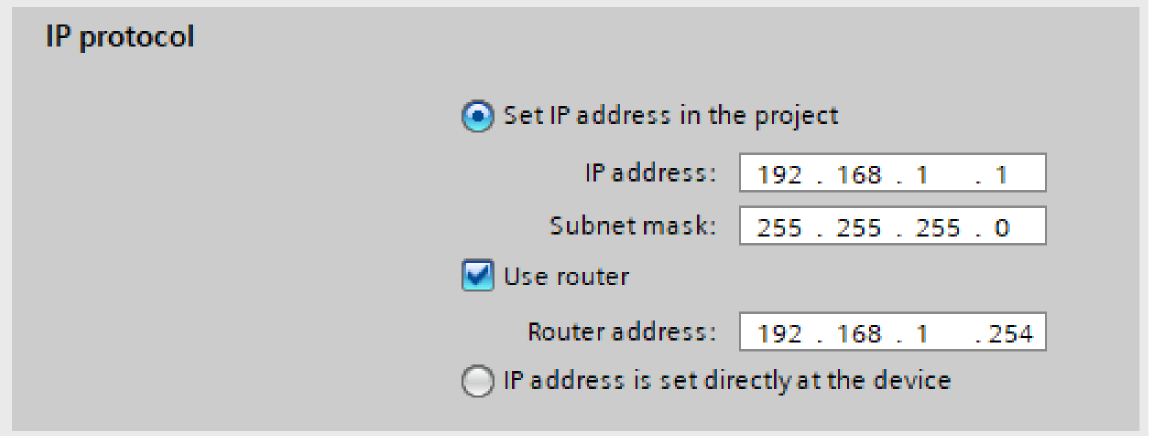
Subnet mask: 255 . 255 . 255 . 0

□ Use router

Router address: 0 . 0 . 0 . 0

○ IP address is set directly at the device

→ Set the IP address of the S615 as router. (→ ☑Use router → Router address: 192.168.1.254)



● Set IP address in the project

IP address: 192 . 168 . 1 . 1

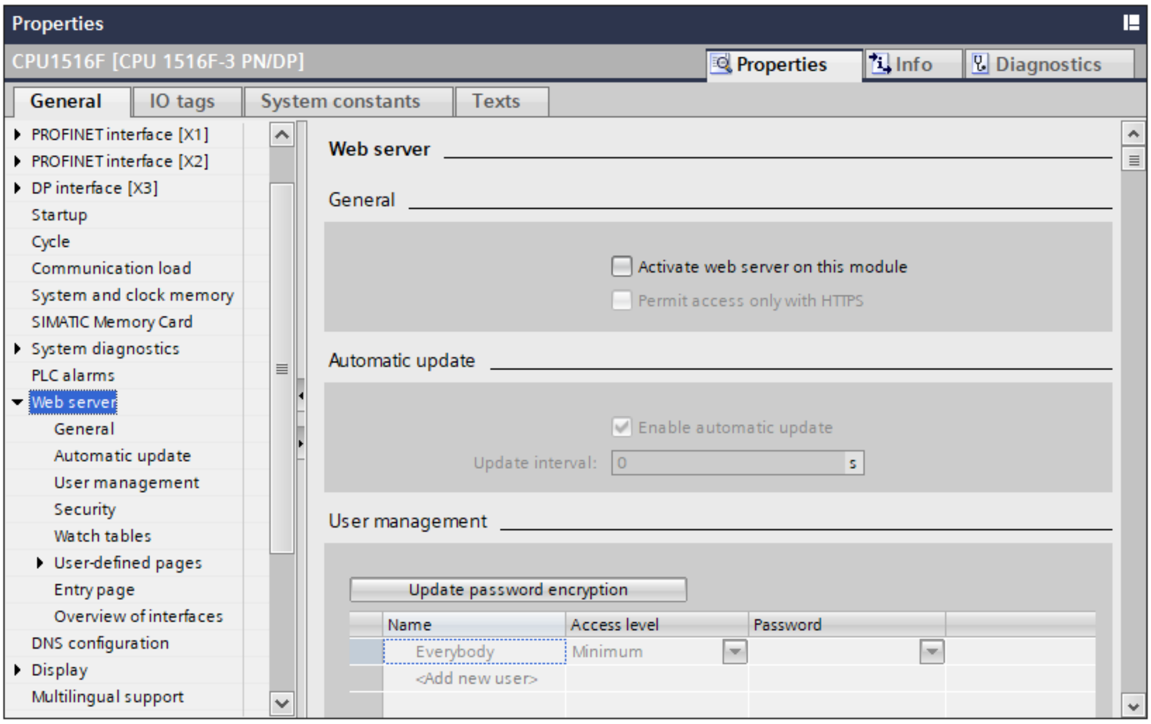
Subnet mask: 255 . 255 . 255 . 0

☑ Use router

Router address: 192 . 168 . 1 . 254

○ IP address is set directly at the device

→ Open the properties of the web server of the CPU 1516F-3 PN/DP. (→ CPU_1516F → Properties → Web server)



Properties

CPU1516F [CPU 1516F-3 PN/DP]

Properties | Info | Diagnostics

General | IO tags | System constants | Texts

- PROFINET interface [X1]
- PROFINET interface [X2]
- DP interface [X3]
- Startup
- Cycle
- Communication load
- System and clock memory
- SIMATIC Memory Card
- System diagnostics
- PLC alarms
- Web server
  - General
  - Automatic update
  - User management
  - Security
  - Watch tables
  - User-defined pages
  - Entry page
  - Overview of interfaces
- DNS configuration
- Display
- Multilingual support

Web server

General

□ Activate web server on this module

□ Permit access only with HTTPS

Automatic update

☑ Enable automatic update

Update interval: 0 s

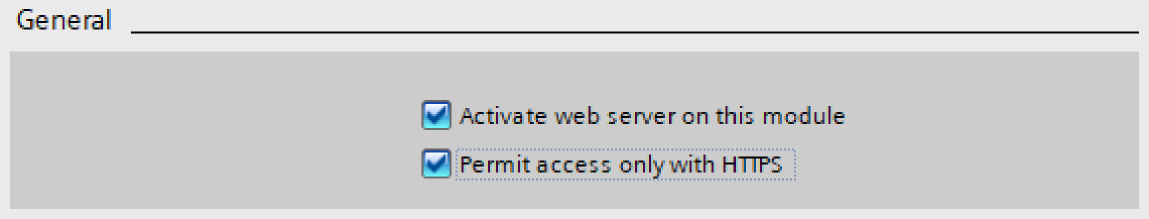
User management

Update password encryption

Name	Access level	Password
Everybody	Minimum	
<Add new user>		

→ Activate the web server. (→ General → ☑ Activate web server on this module)

→ Restrict access to HTTPS. (→ General → ☑ Permit access only with HTTPS)

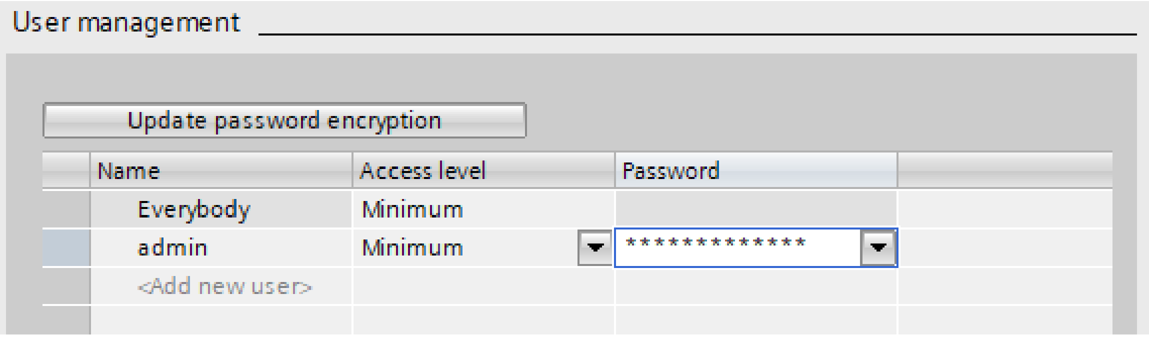


General

☑ Activate web server on this module

☑ Permit access only with HTTPS

→ Create a new user. (→ User management → Name: admin → Password: ***)

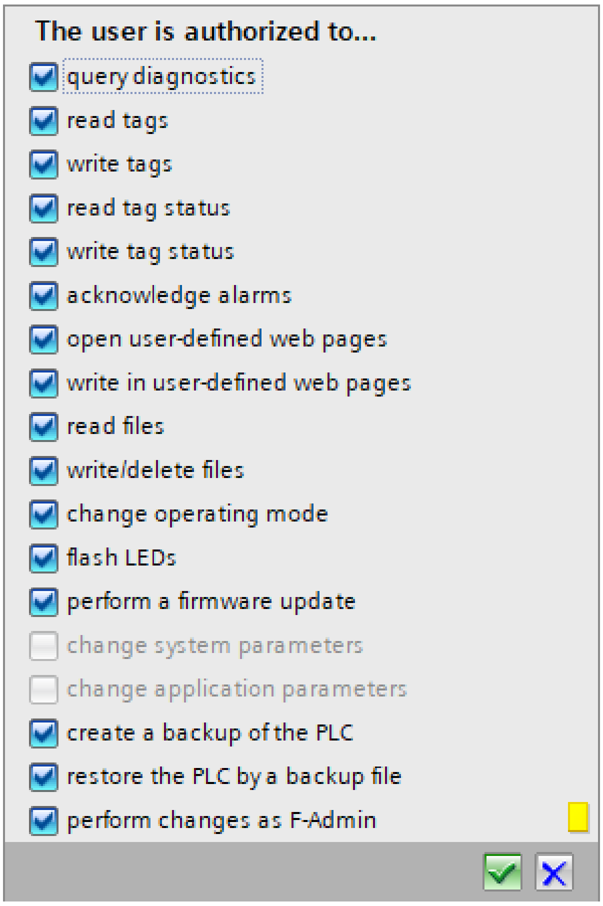


User management

Update password encryption

Name	Access level	Password
Everybody	Minimum	
admin	Minimum	*************
<Add new user>		

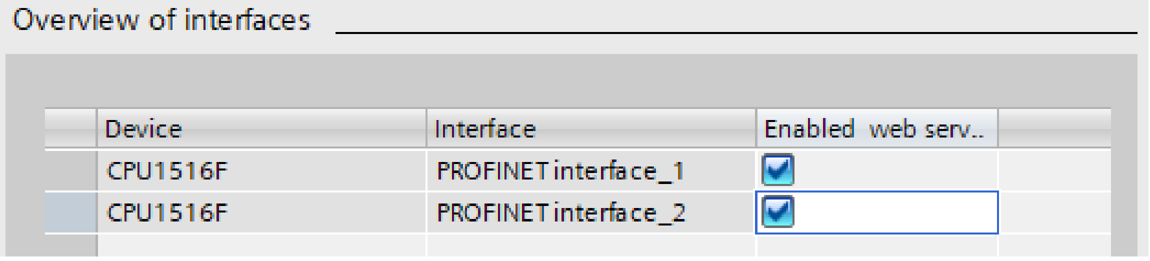
→ Set the access level of the new user to Administrative. (→ User management → admin → Access level → Administrative)



The user is authorized to...

- ☑ query diagnostics
- ☑ read tags
- ☑ write tags
- ☑ read tag status
- ☑ write tag status
- ☑ acknowledge alarms
- ☑ open user-defined web pages
- ☑ write in user-defined web pages
- ☑ read files
- ☑ write/delete files
- ☑ change operating mode
- ☑ flash LEDs
- ☑ perform a firmware update
- □ change system parameters
- □ change application parameters
- ☑ create a backup of the PLC
- ☑ restore the PLC by a backup file
- ☑ perform changes as F-Admin

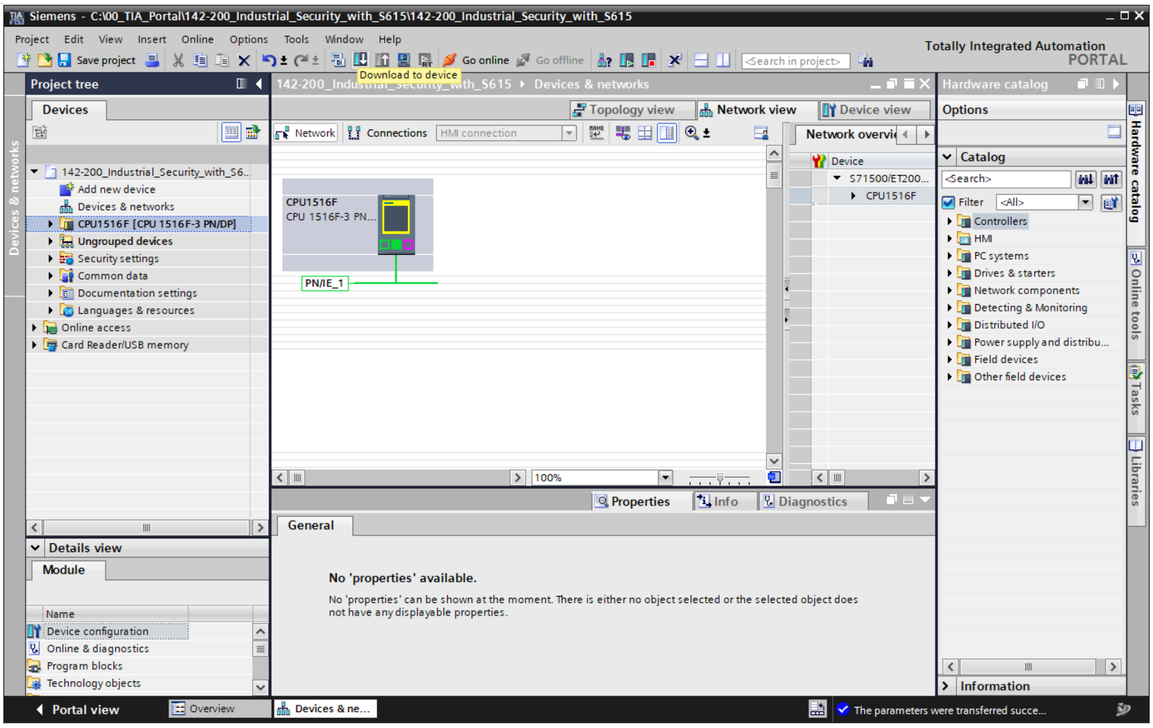
→ Enable the web server on interface X2. (→ Overview of interfaces → PROFINET interface_2)



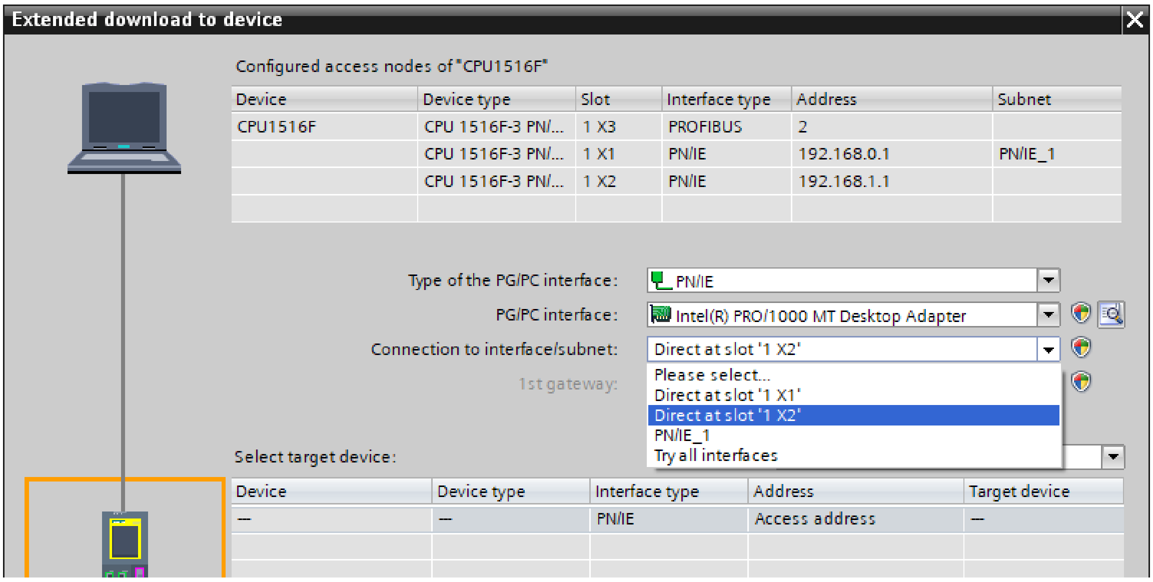
Overview of interfaces

	Device	Interface	Enabled web serv..
	CPU1516F	PROFINET interface_1	☑
	CPU1516F	PROFINET interface_2	☑

→ Download the configuration to the CPU. (→ CPU_1516F → ☐ → ☐)



→ When downloading, make sure that you are now connected to interface X2! (→ Connection to interface/subnet: Direct at slot '1 X2')



Extended download to device

Configured access nodes of "CPU1516F"

Device	Device type	Slot	Interface type	Address	Subnet
CPU1516F	CPU 1516F-3 PN/...	1 X3	PROFIBUS	2	
	CPU 1516F-3 PN/...	1 X1	PN/IE	192.168.0.1	PN/IE_1
	CPU 1516F-3 PN/...	1 X2	PN/IE	192.168.1.1	

Type of the PG/PC interface: PN/IE

PG/PC interface: Intel(R) PRO/1000 MT Desktop Adapter

Connection to interface/subnet: Direct at slot '1 X2'

1st gateway:

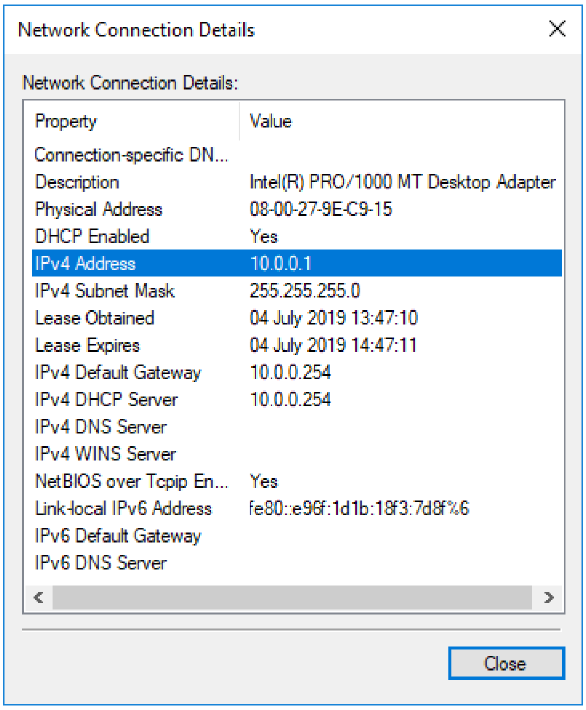
Select target device:

Device	Device type	Interface type	Address	Target device
—	—	PN/IE	Access address	—

7.8 Testing the rule set

→ Connect the computer to port 5 on the SCALANCE S615.

→ Make sure the computer has received a new address in subnet 10.0.0.0/24 from SCALANCE S615. (→ LAN connection → Status)

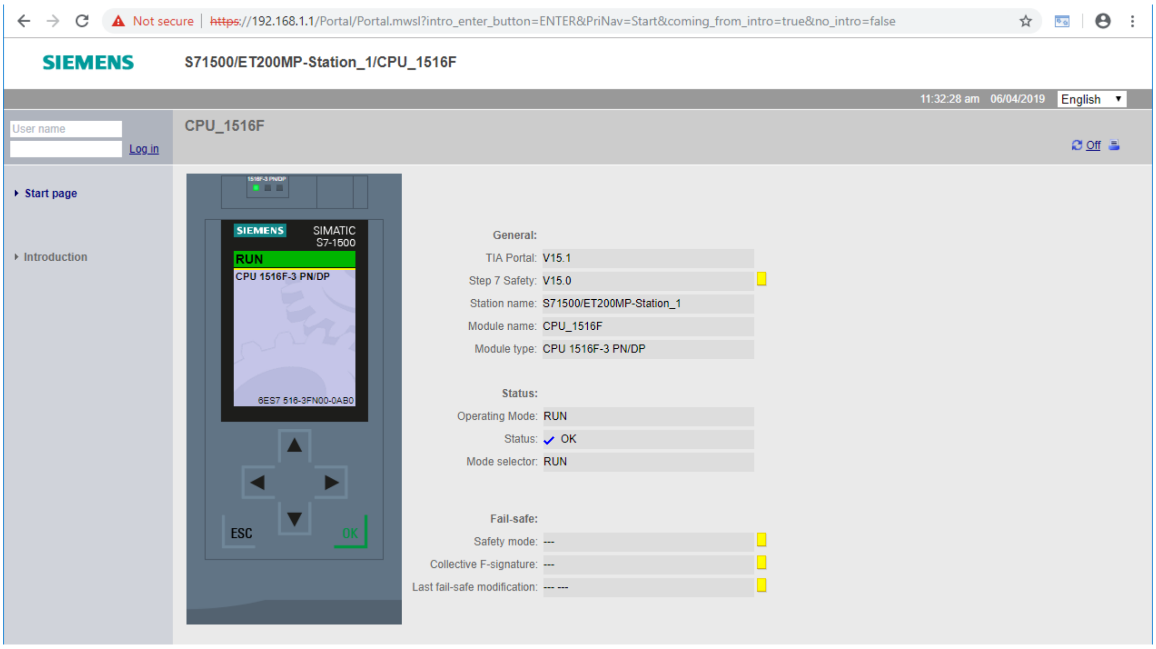


Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) PRO/1000 MT Desktop Adapter
Physical Address	08-00-27-9E-C9-15
DHCP Enabled	Yes
IPv4 Address	10.0.0.1
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	04 July 2019 13:47:10
Lease Expires	04 July 2019 14:47:11
IPv4 Default Gateway	10.0.0.254
IPv4 DHCP Server	10.0.0.254
IPv4 DNS Server	
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::e96f:1d1b:18f3:7d8f%6
IPv6 Default Gateway	
IPv6 DNS Server	

→ Open the web server of the CPU 1516F-3 PN/DP with the browser. (→ https://192.168.1.1)



Not secure | https://192.168.1.1/Portal/Portal.mwsl?intro_enter_button=ENTER&PriNav=Start&coming_from_intro=true&no_intro=false

SIEMENS S71500/ET200MP-Station_1/CPU_1516F

11:32:28 am 06/04/2019 English

CPU_1516F

General:

TIA Portal: V15.1

Step 7 Safety: V15.0

Station name: S71500/ET200MP-Station_1

Module name: CPU_1516F

Module type: CPU 1516F-3 PN/DP

Status:

Operating Mode: RUN

Status: ✓ OK

Mode selector: RUN

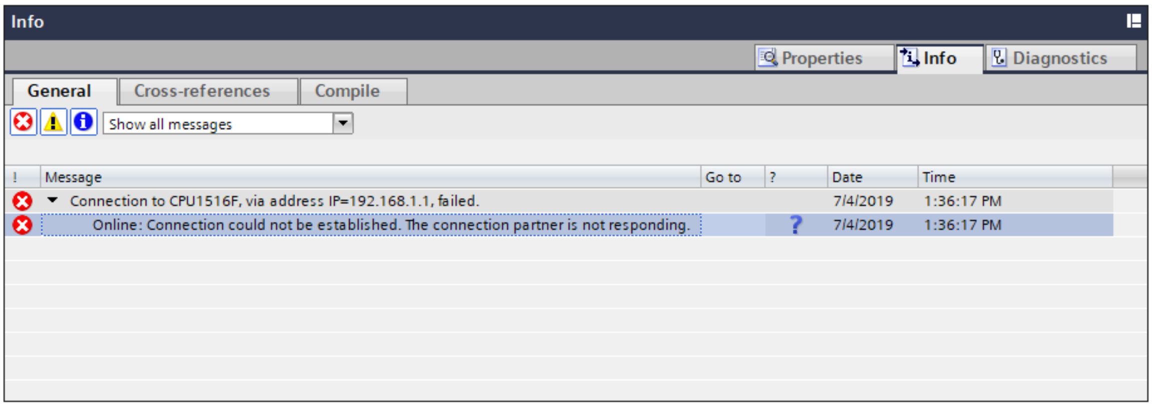
Fail-safe:

Safety mode: ---

Collective F-signature: ---

Last fail-safe modification: --- ---

→ Try to establish an online connection to the CPU 1516F-3 PN/DP with the TIA Portal. (→ TIA Portal → CPU_1516F → Go online)

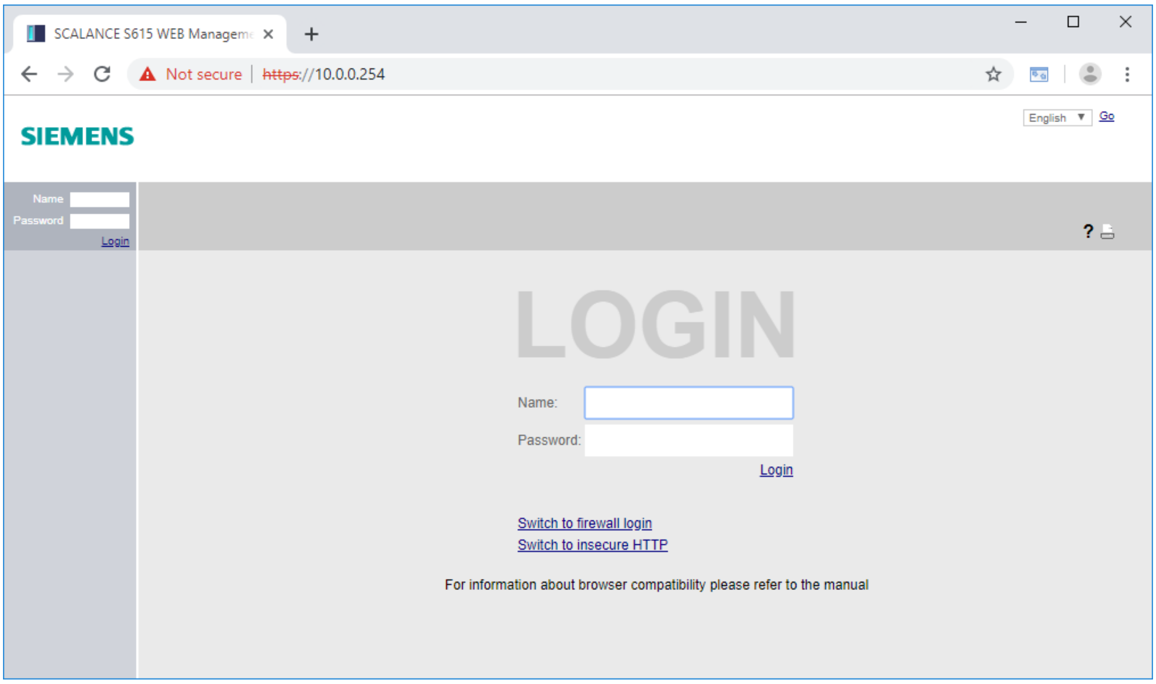


!	Message	Go to	?	Date	Time
⊗	▾ Connection to CPU1516F, via address IP=192.168.1.1, failed.			7/4/2019	1:36:17 PM
⊗	Online: Connection could not be established. The connection partner is not responding.		?	7/4/2019	1:36:17 PM

Note:

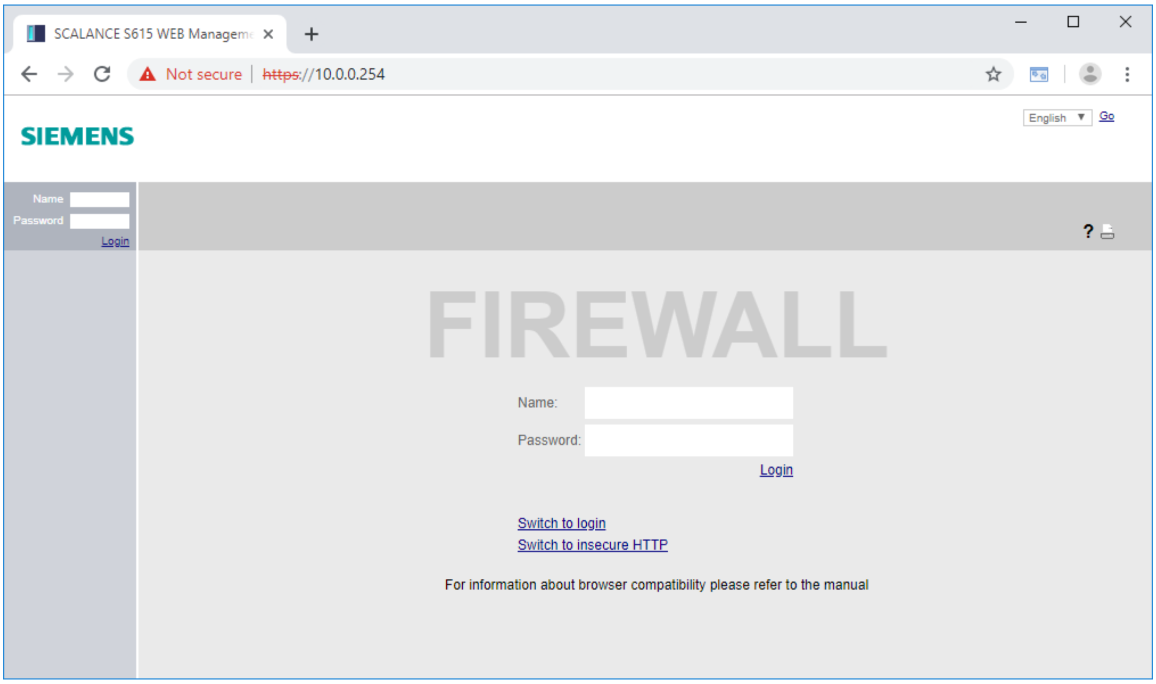
– *A connection setup with the CPU_1516F should not be possible at this time, because only port 443 and 4840 are enabled.*

→ Open the web interface of the SCALANCE S615 in the browser. Because you are on the external side of the device this time, use the external IP address of the device. (→ https://10.0.0.254)



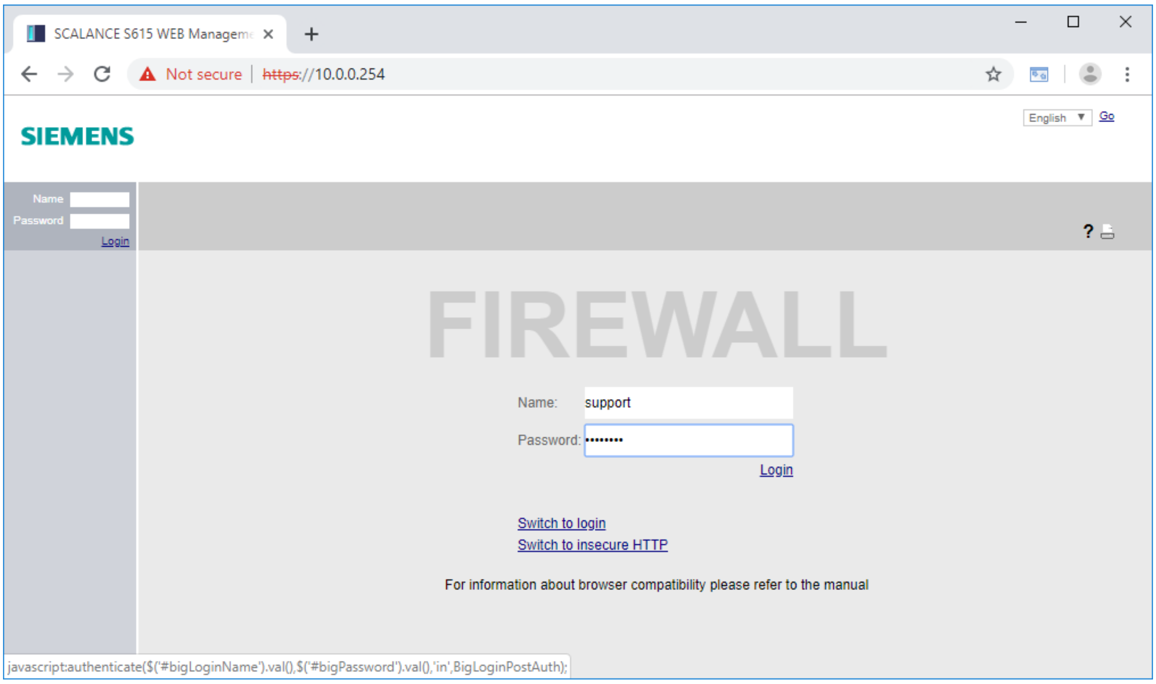
For information about browser compatibility please refer to the manual

→ Go to the firewall login. (→ Switch to firewall login)



For information about browser compatibility please refer to the manual

→ Log in with the user "support". (→ Name: support → Password: ***)



Name: support

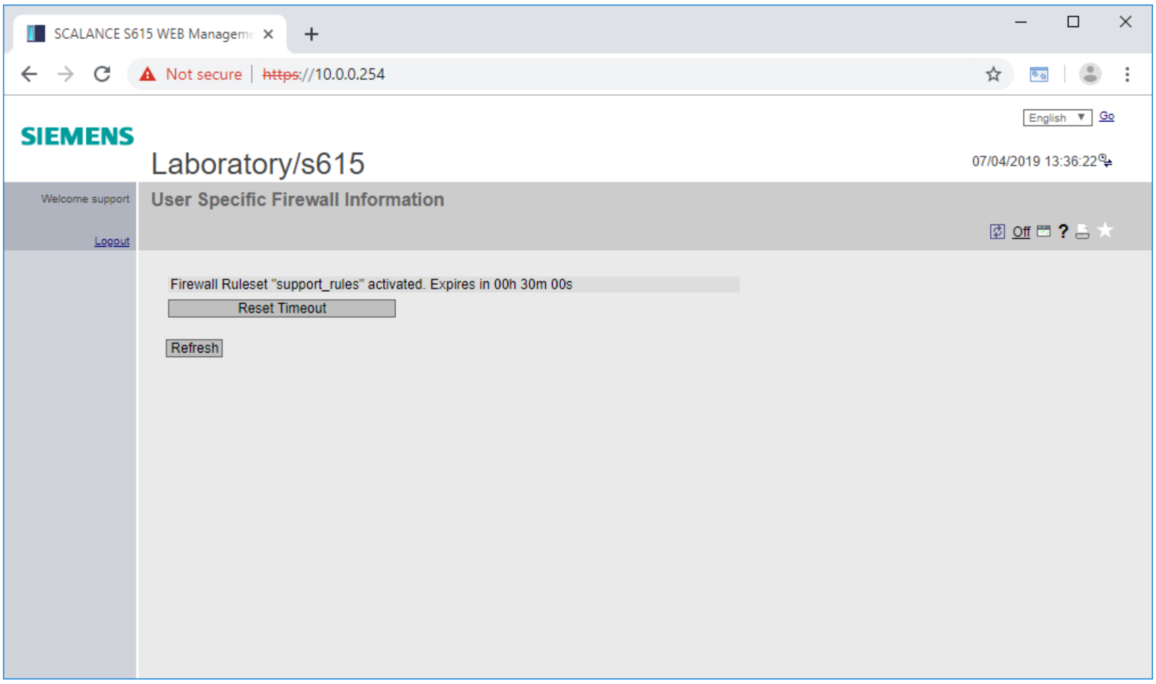
Password: ••••••••

For information about browser compatibility please refer to the manual

javascript:authenticate($('#bigLoginName').val(),$('#bigPassword').val(),'in',BigLoginPostAuth);

→ Click Login. (→ Login)

→ The firewall rule set "support_rules" should then be activated for 30 minutes.

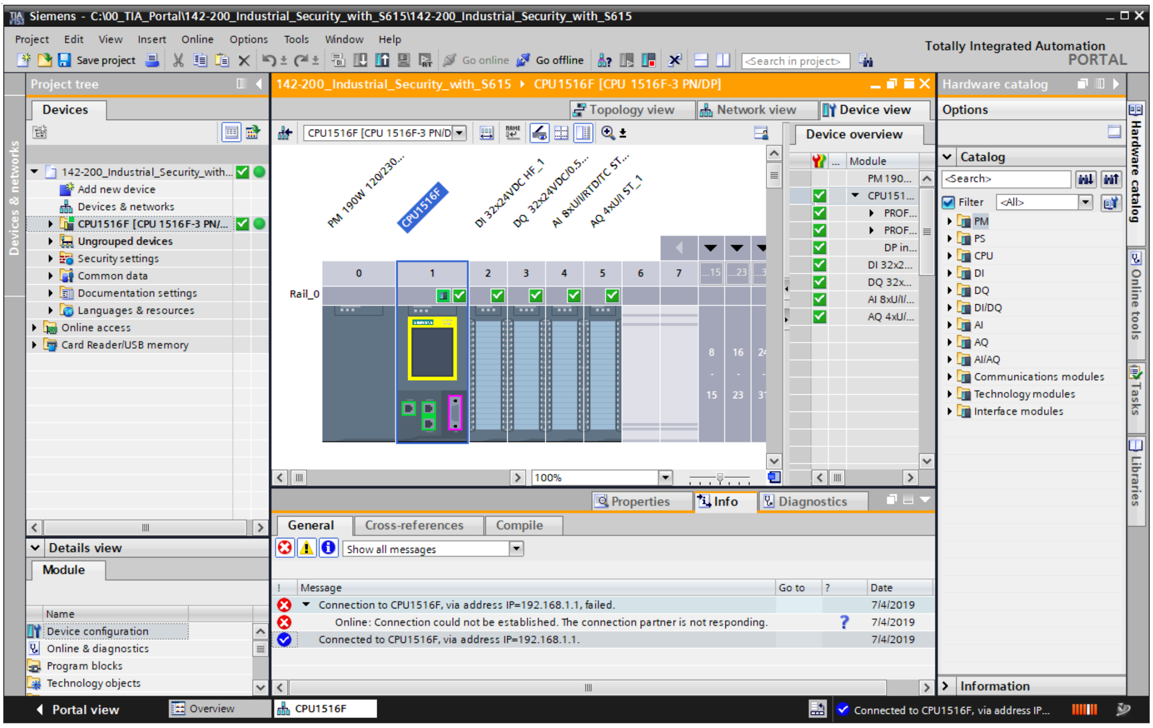


Firewall Ruleset "support_rules" activated. Expires in 00h 30m 00s

Note:

– *With the "Reset Timeout" button, you can reset the validity of the rule sets to 30 minutes. With a click on Logout, all rule sets are terminated again.*

→ Try again to establish an online-connection to the CPU 1516F-3 PN/DP in the TIA Portal. (→ TIA Portal → CPU_1516F → Go online)



!	Message	Go to	?	Date
☒	Connection to CPU1516F, via address IP=192.168.1.1, failed.			7/4/2019
☒	Online: Connection could not be established. The connection partner is not responding.		?	7/4/2019
✓	Connected to CPU1516F, via address IP=192.168.1.1.			7/4/2019

Connected to CPU1516F, via address IP...

Note:

– *This time, the connection setup should work properly through the additional rule set.*

7.9 Checklist – step-by-step instructions

The following checklist helps students/trainees to independently check whether all steps of the step-by-step instructions have been carefully completed and enables them to successfully complete the module on their own.

No.	Description	Checked
1	Project successfully retrieved from archive	
2	Programming device connected to port 4 of the S615	
3	IP address successfully set	
4	Web management login and password changed	
5	System correctly configured with the wizard	
6	DHCP pool created for vlan1	
7	DHCP pool created for vlan2	
8	DHCP options correctly configured for both pools	
9	DHCP server and both pools activated	
10	Programming device obtains IP automatically	
11	Global rule for HTTPS added to CPU	
12	Support user created	
13	Support rule set created	
14	Web server activated on the CPU_1516F	
15	Programming device connected to port 5 of the S615	
16	Programming device automatically obtains IP here too	
17	Web server of the CPU 1516F successfully opened	
18	Online connection to CPU_1516F with TIA not possible	
19	Successfully logged in to the firewall as support user	
21	Online-connection to CPU_1516F with TIA now possible	

8 Exercise

8.1 Task – Exercise

Due to the digitalization of the production plant, a global access to the OPC UA server of controller is also required in this step. Create a new rule that allows access to the OPC UA server of the controller from the company network.

Before the configuration, inform yourself, which port the OPC UA needs to connect to the CPU.

8.2 Planning

Plan the implementation of the task on your own.

8.3 Checklist – Exercise

The following checklist helps students/trainees to independently check whether all steps of the exercise have been carefully completed and enables them to successfully complete the module on their own.

No.	Description	Checked
1	New rule created	
2	OPC UA connection successfully established from the company network	
3	An online connection to the CPU is still not available without login.	

9 Additional information

More information for further practice and consolidation is available as orientation, for example: Getting Started, videos, tutorials, apps, manuals, programming guidelines and trial software / firmware, under the following link:

www.siemens.com/sce/s7-1500

Preview "Additional information" – In preparation

Further Information

Siemens Automation Cooperates with Education
siemens.com/sce

SCE Learn-/Training Documents
siemens.com/sce/documents

SCE Trainer Packages
siemens.com/sce/tp

SCE Contact Partners
siemens.com/sce/contact

Digital Enterprise
siemens.com/digital-enterprise

Industrie 4.0
siemens.com/future-of-manufacturing

Totally Integrated Automation (TIA)
siemens.com/tia

TIA Portal
siemens.com/tia-portal

SIMATIC Controller
siemens.com/controller

SIMATIC Technical Documentation
siemens.com/simatic-docu

Industry Online Support
support.industry.siemens.com

Product catalogue and online ordering system Industry Mall
mall.industry.siemens.com

Siemens
Digital Industries, FA
P.O. Box 4848
90026 Nuremberg
Germany