SIEMENS

SIMATIC NET

Industrial Remote Communication
Remote Networks
User-specific firewall

Getting Started

07/2020

C79000-G8976-C539-03

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: C79000-G8976-C539-03
℗ 06/2020 Subject to change

Preface

Purpose

Access via the user-specific firewall is configured based on an example.

IP settings for the examples

Note

The IP settings used in the examples were freely chosen.

In a real network, you would need to adapt these IP settings to avoid possible address conflicts.

General naming conventions

The designation . . .	stands for . . .
SCT	Security Configuration Tool
SINEC PNI	Primary Network Initialization
Device	M87x M81x M826 S615
M87x	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4
M81x	SCALANCE M812-1 SCALANCE M816-1
M826	SCALANCE M826-2
M804PB	SCALANCE M804PB
S615	SCALANCE S615
M-800	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4 SCALANCE M812-1 SCALANCE M816-1 SCALANCE M826-2 SCALANCE M804PB

Further documentation

- Operating instructions

  These documents contain information on installing and connecting the products and on approvals for the products. The configuration and the integration of the devices in a network are not described in these instructions.

  – SCALANCE M874, M876

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

  – SCALANCE M812, M816

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

  – SCALANCE M804PB:

    Entry ID: 109759601 (https://support.industry.siemens.com/cs/ww/en/view/109759601)

  – SCALANCE M826:

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

  – SCALANCE S615:

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

- "Web based Management" configuration manual

  This document is intended to provide you with the information you require to commission and configure devices using the Web Based Management.

  – SCALANCE M-800:

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

  – SCALANCE S615:

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

- Configuration manual Command Line Interface

  This document contains the CLI commands supported by the devices.

  – SCALANCE M-800

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

  – SCALANCE S615

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

- Industrial Ethernet Security – Basics and Application

  This document contains information about working with the SCT (Security Configuration Tool).

  Entry ID: 56577508 (https://support.industry.siemens.com/cs/ww/de/view/56577508/en)
- SIMATIC NET Industrial Ethernet Network manual

  This document contains information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network.

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

SIMATIC NET manuals

You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:

- using the search function:

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

  Enter the entry ID of the relevant manual or the article number of the device as the search term.
- In the navigation panel on the left hand side in the area "Industrial Communication":

  Link to the area "Industrial Communication"
  (https://support.industry.siemens.com/cs/ww/en/ps/15247/man)

  Go to the required product group and make the following settings:
  "Entry list" tab, Entry type "manual"

Training, Service & Support

You will find information on Training, Service & Support in the multi--language document "DC_support_99.pdf" on the data medium supplied with the documentation.

SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary on the Internet at the following address:

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

Security information

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

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

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

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

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

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

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

Table of contents

Access via user-specific firewall 1

1.1 Introduction

In this example configuration, a service technician is to access the Web server of the CPU, but not the WBM of the SCALANCE S615, via the control center. The station or the CPU can be reached via the SCALANCE S615.

Access for the service technician is controlled by the following objects:

- User
- Pulley
- Remote access

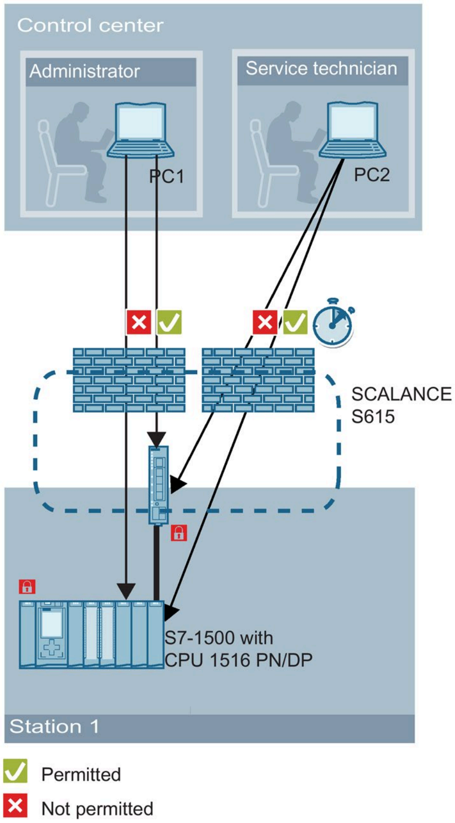
  Three settings are available for the remote access: only, none, additional.
- Rule set

For this example, the "Maintenance" user with the "User" role and "only" remote access is created for the service technician. This means that the service technician can only access the WBM page of the user-specific firewall.

With the "None", only access to the WBM of the SCALANCE S615 would be possible and with the "additional" setting, access to both would be possible.

The firewall is enabled on the SCALANCE S615 by default. The user-specific rule set "Station_1" is created so that the "Maintenance" user can access the Web server of the CPU. Firewall rules that are required for remote access can be summarized with a rule set.

In this case, a firewall rule is created for access via HTTPS and assigned to the rule set. In addition, access is limited to one hour.



The "Maintenance" user needs to log in with his or her user data via the user-specific firewall. When login is successful, the current rule set and the remaining time are displayed.

Now the user can log in to the Web server of the CPU with his or her user data. The prerequisite is that a corresponding user is created in the user management of the CPU.

During the access time, the WBM page "User Specific Firewall Information" cannot be closed. If needed, the user can extend the access time via the "Reset Timeout" button.

There are three options to log off the "Maintenance" user:

- The permitted access time of one hour has expired.
- The user logs off.
- The device administrator deactivates the active user using the "Force Deactivate" button.

Settings used

For the configuration example, the devices are given the following IP address settings:

Device	VLAN	IP address
PC 1	Control center: VLAN2	192.168.50.10 255.255.255.0 Gateway: 192.168.50.1 (IP address of the SCALANCE S615)
PC 2	Control center: VLAN2	192.168.50.20 255.255.255.0 Gateway: 192.168.50.1 (IP address of the SCALANCE S615)
SCALANCE S615	Control center: VLAN2 (P5)	192.168.50.1 255.255.255.0
	Station 1: VLAN1 (P1 - P4)	192.168.16.42 255.255.255.0
S7-1500 with CPU 1516 PN/DP	Station 1: VLAN1	192.168.16.43 55.255.255.0

You use PC1 to configure the SCALANCE S615 via Web Based Management. To do so, you must assign the IP address to the PC network adapter. In the extended TCP/IP settings of the network adapter configuration you have the option of adding additional IP addresses.

Note

You can also use SCALANCE M-800 devices. The configuration described below relates to the SCALANCE S615.

Note

The IP settings used in the configuration example were freely chosen.

In a real network, you would need to adapt these IP settings to avoid possible address conflicts.

Requirement

- The SCALANCE S615 can be reached via PC2 and you are logged in to the WBM as "admin".
- Firmware version 6.2

Steps in configuration

The following steps are required for the configuration:

1. Creating a user (Page 13)
2. Creating a user-defined rule set (Page 14)
3. Configuring the rule set (Page 15)
4. Logging on via user-specific firewall (Page 29)

1.2 Configuring access with the WBM

1.2.1 Creating a user

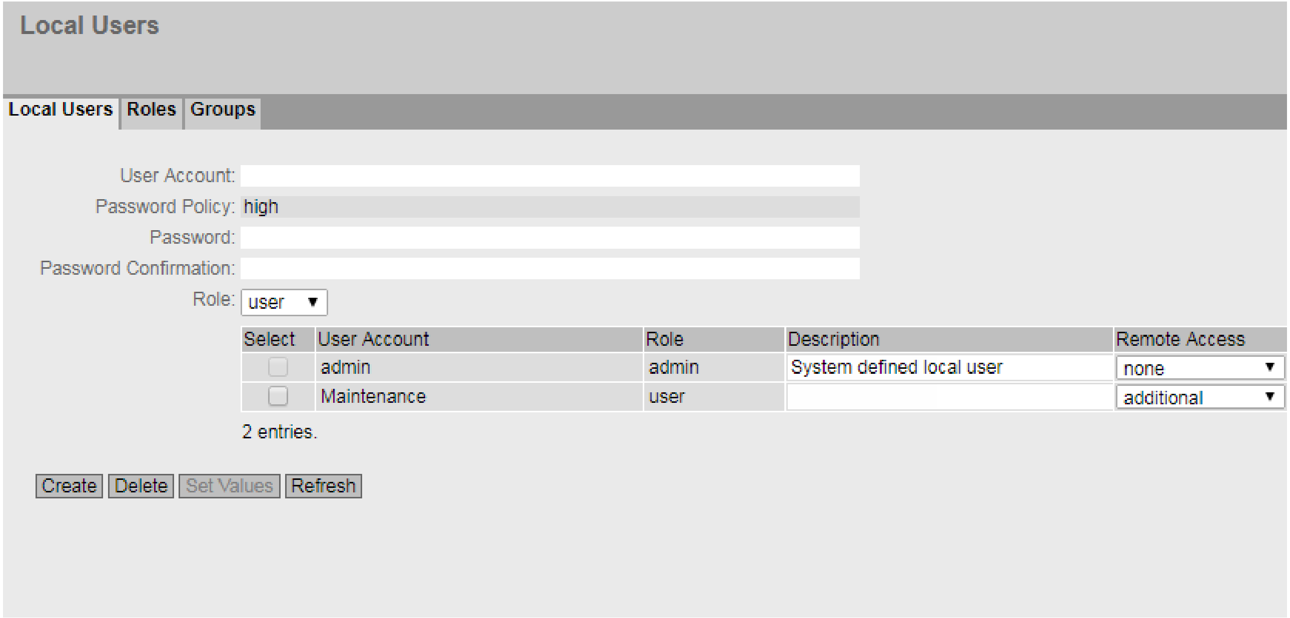
Procedure

1. Click on "Security > Users" in the navigation area and on the "Local users" tab in the content area.
2. Enter "Maintenance" for "User Account".
3. Define a password for the user. The password must be at least 8 characters long and contain at least 1 uppercase letter, 1 special character and 1 number.
4. Repeat the password.
5. For "Role", select the entry "user".
6. Click the "Create" button.

   A new entry is created in the table.
7. For "Remote access", select the entry "only". Click the "Set Values" button.

Result

The "Maintenance" user has been created.



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 ▾
□	Maintenance	user		additional ▾

2 entries.

1.2.2 Creating a user-specific rule set

Creating a rule set

1. Click on "Security > Firewall" in the navigation area and on the "User Specific" tab in the content area.
2. Enter "Station_1" for the name and click "Create".

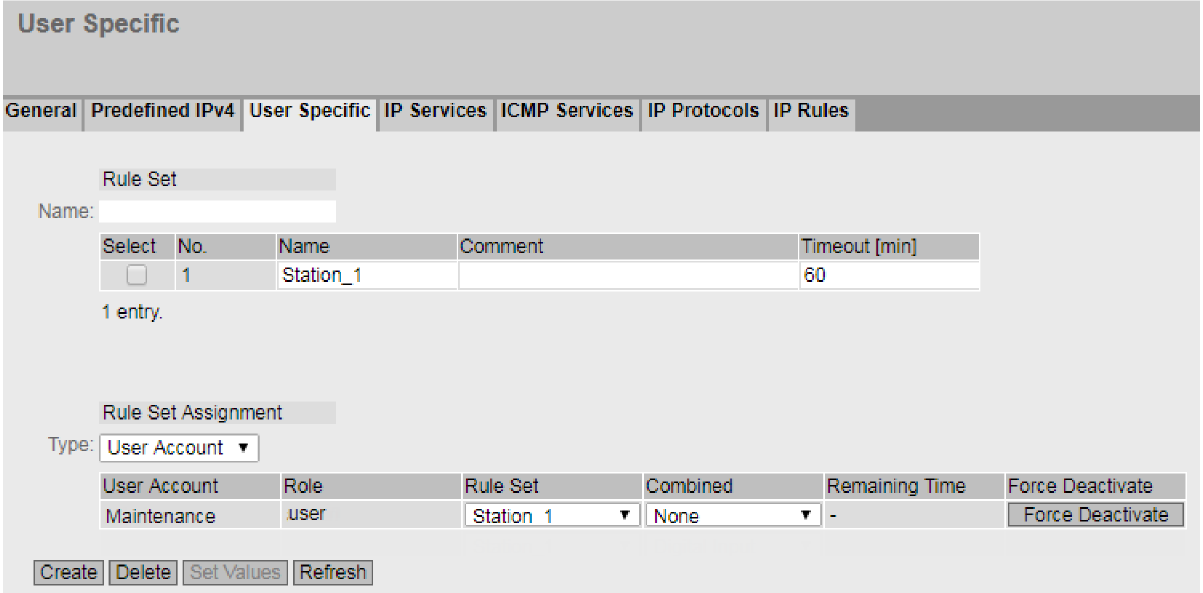
   A new entry is created in the table.
3. To limit access to one hour, enter "60" for "Timeout [Min.]".
4. Click the "Set Values" button.

Assigning a rule set to a user

1. Select the "User account" for "Type". Only users with remote access "only" or "additional" can be selected.
2. Select "Station_1" for "Rule set".
3. Click the "Set Values" button.

Result

The rule set "Station_1" has been created and assigned to the "Maintenance" user.



Rule Set

Name:

Select	No.	Name	Comment	Timeout [min]
□	1	Station_1		60

1 entry.

Rule Set Assignment

Type: User Account ▼

User Account	Role	Rule Set	Combined	Remaining Time	Force Deactivate
Maintenance	user	Station_1 ▼	None ▼	-	Force Deactivate

1.2.3 Creating an IP rule and assigning the rule set

In this example, the service technician should only receive access to the Web server of the CPU. The HTTPS service (TCP port 443) is required for access.

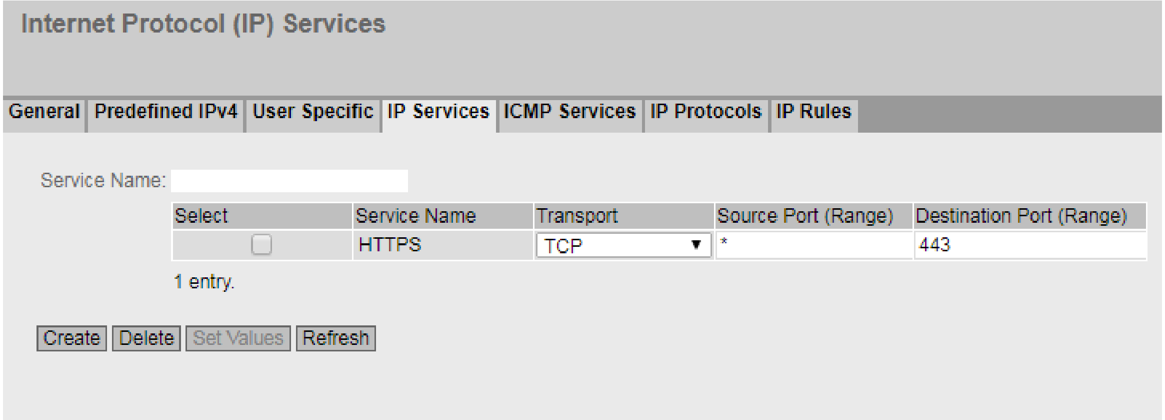
Create HTTPS service

1. Click on "Security > Firewall" in the navigation area and on the "IP Services" tab in the content area.
2. Enter "HTTPS" for "Service Name" and click on the "Create" button. A new entry is created in the table.
3. Configure HTTPS with the following settings:

Transport	TCP
Destination Port (Range)	443 (default port)

4. Click the "Set Values" button.

Result



Internet Protocol (IP) Services

Service Name:

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

1 entry.

Creating a firewall rule and assigning it to a rule set

Create firewall rule

1. Click on "Security" > "Firewall" in the navigation area and on the "IP Rules" tab in the content area.
2. Click "Create". A new entry is created in the table.
3. Configure the firewall rule for HTTPS.

   Access is enabled for all users using the "Station_1" rule set:

Action	Accept
From	vlan2 (EXT)
To	vlan1 (INT)
Source (Range)	DYNAMIC If the rule set is activated by a user, the placeholder DYNAMIC is replaced by the IP address of the end device used.
Destination (Range)	Web server of the CPU 192.168.16.43
Service	HTTPS

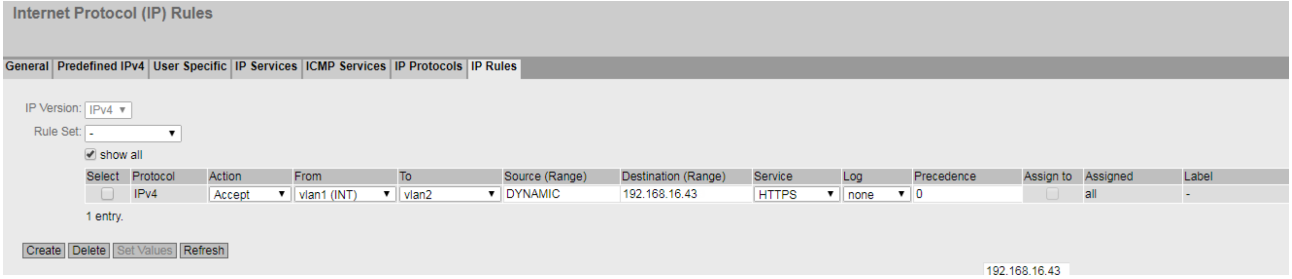
4. Click on "Set Values".

Assigning to a rule set

1. Select the rule set "Station_1" and enable the "Show all" setting.
2. Enable the "Assign" setting.
3. Click on "Set Values".

Result

Overview of the configuration



Internet Protocol (IP) Rules

IP Version: IPv4 ▾

Rule Set: - ▾

☑ show all

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service	Log	Precedence	Assign to	Assigned	Label
□	IPv4	Accept ▾	vlan1 (INT) ▾	vlan2 ▾	DYNAMIC	192.168.16.43	HTTPS ▾	none ▾	0	□	all	-

1 entry.

1.3 Configuring access with TIA

1.3.1 Creating a user

Requirement

- PC/PG with TIA Portal V16
- A new project has been created in the TIA Portal and the network view is open.

  The information system of the TIA Portal contains all background information, step-by-step instructions and examples you need for working with the TIA Portal.

Integrating SCALANCE S615

1. In the hardware catalog, click on the input box of the search function.
2. Enter the article number (6GK5 615-0AA00-2AA2) as a search term or the name of the S615.
3. Click the "Start search" button.
4. Drag-and-drop the SCALANCE S615 to the network view.

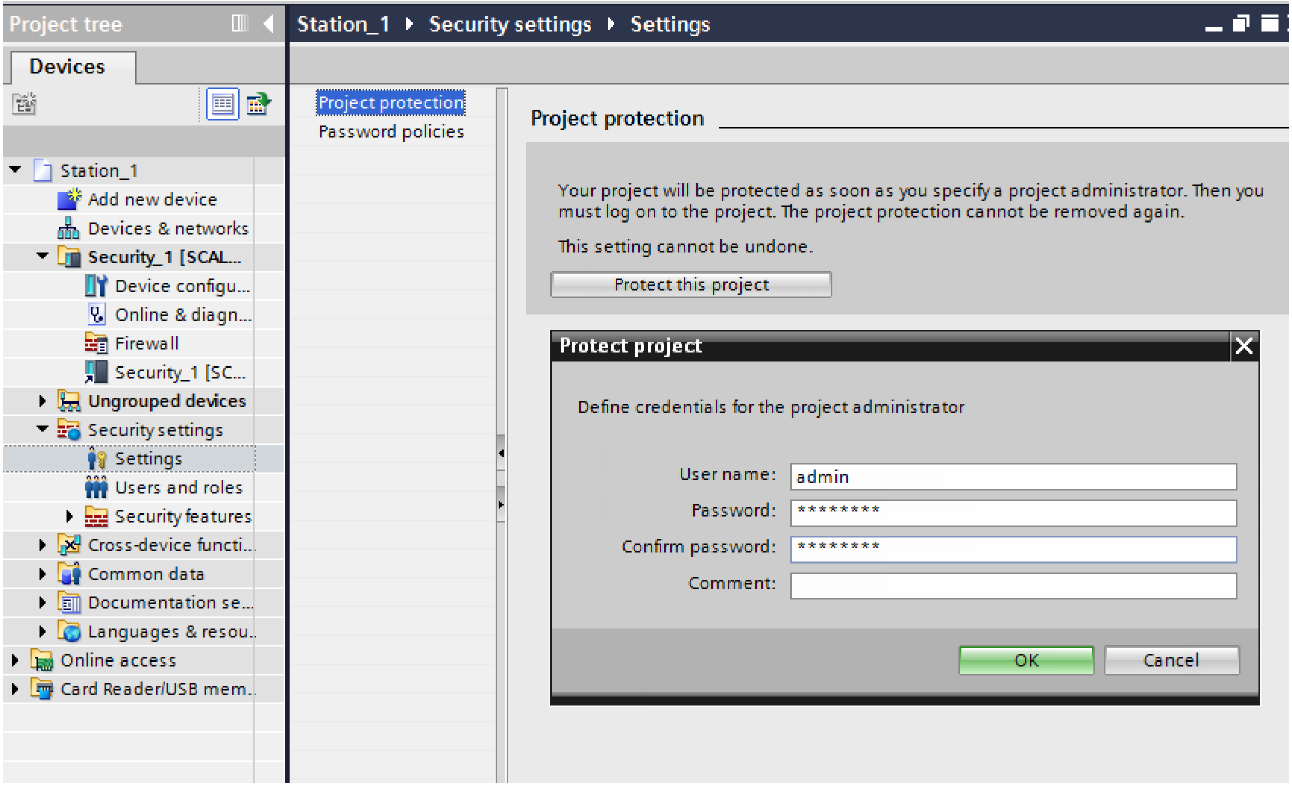
Procedure

Configuring project administrator

In the user administration, you can protect the TIA Portal project from unauthorized access. A project administrator is automatically created when you activate the user administration. The user administrator creates the additional user "Maintenance".

1. Open the "Security settings" folder in the project tree. Double-click on the "Settings" entry.
2. The editor for user administration opens and the area for project protection is displayed.

3. Click the "Protect this project" button.



Project protection

Your project will be protected as soon as you specify a project administrator. Then you must log on to the project. The project protection cannot be removed again.

This setting cannot be undone.

Protect project

Define credentials for the project administrator

User name: admin

Password: ********

Confirm password: ********

Comment:

Specify the credentials for the project administrator.

4. Double-click on the "Users and roles" entry.
5. Open the "Users" tab.
6. Select the project administrator and activate the "NET Administrator" role in the "Assigned roles" area.

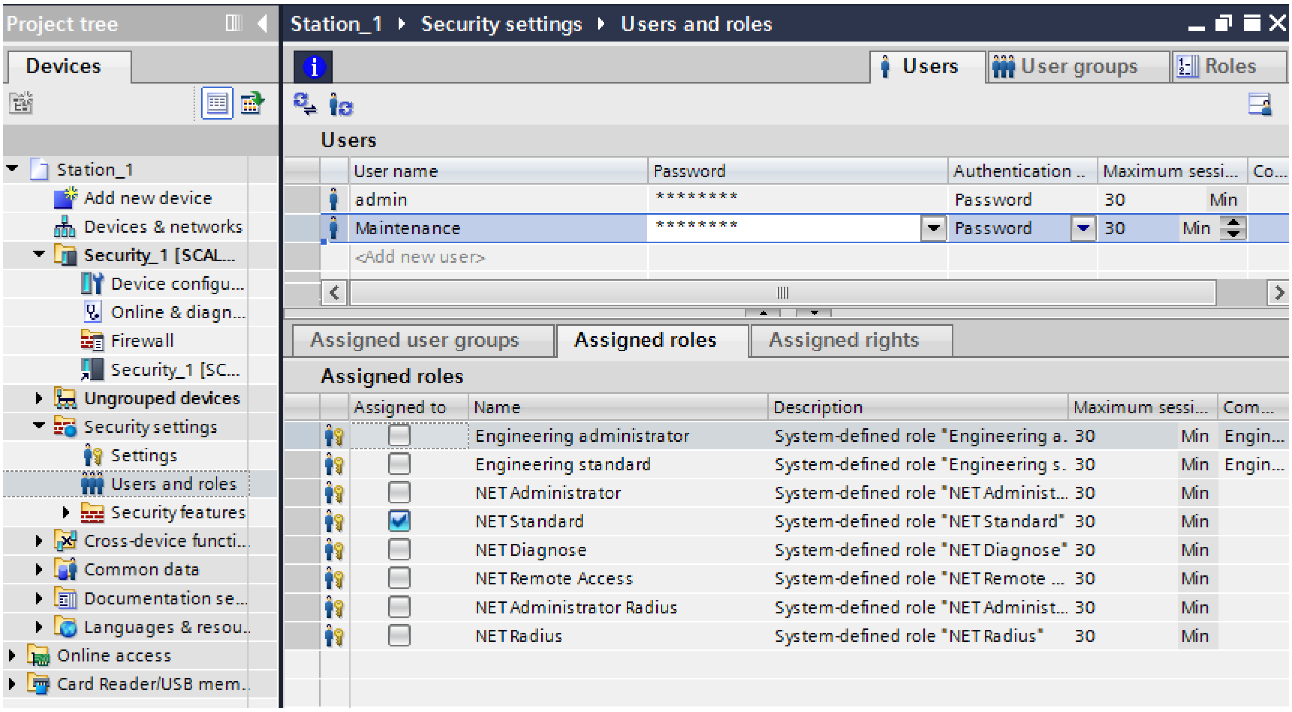
   To configure, diagnose and load the S615, the project administrator must also have the role "NET Administrator".

Creating the "Maintenance" user

1. Click "Add new user".

   A submenu opens in which you can select the user type.
2. Click "Add new project user".

3. Enter the user name "Maintenance" and specify a password.
4. Select the user "Maintenance" and activate the "NET Standard" role in the "Assigned roles" area.



Users

User name	Password	Authentication ..	Maximum sessi...		Co...
admin	********	Password	30	Min	
Maintenance	********	Password	30	Min	
<Add new user>					

Assigned roles

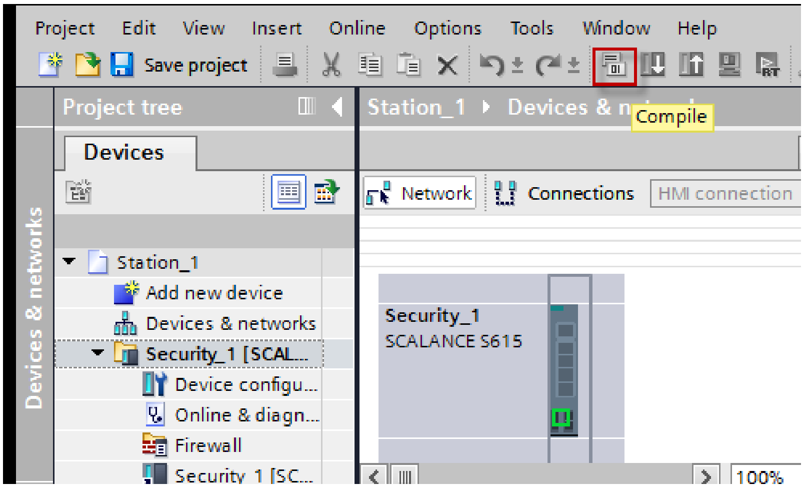
Assigned to	Name	Description	Maximum sessi...		Com...
☐	Engineering administrator	System-defined role "Engineering a.	30	Min	Engin...
☐	Engineering standard	System-defined role "Engineering s.	30	Min	Engin...
☐	NET Administrator	System-defined role "NET Administ...	30	Min	
☑	NET Standard	System-defined role "NET Standard"	30	Min	
☐	NET Diagnose	System-defined role "NET Diagnose"	30	Min	
☐	NET Remote Access	System-defined role "NET Remote ...	30	Min	
☐	NET Administrator Radius	System-defined role "NET Administ...	30	Min	
☐	NET Radius	System-defined role "NET Radius"	30	Min	

Result

The project administrator is configured and the user "Maintenance" has been created.

The project must be compiled so that the "Maintenance" user can be selected in the user-defined IP rules.

To compile the project data, select the SCALANCE S615 in the project tree and click on "Compile" in the toolbar.



1.3.2 Configuring an IP address

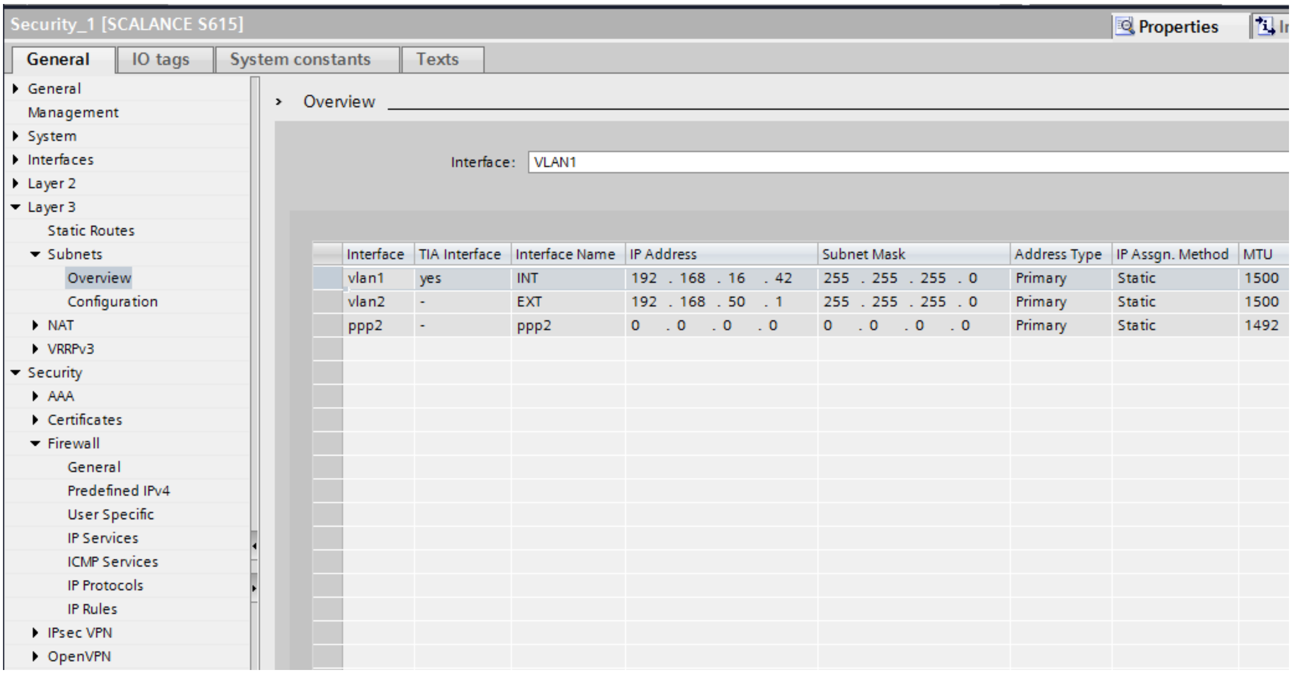
Procedure

1. Open the device folder of the SCALANCE S615 in the project tree.

   Double-click on the "Device configuration" entry.
2. In the "Properties" Inspector window, select the lower-level tab "General".
3. In the Inspector window, configure the IP addresses in "Layer 3 > Subnets > Configuration".
4. For VLAN1, enter the IP address of the internal network (Port 1 to Port 4), see "Settings used (Page 9)" table.
5. Change the interface to vlan2.
6. Deactivate DHCP.
7. For VLAN2, enter the IP address of the internal network (Port 5), see "Settings used (Page 9)" table.

Result

The IP addresses are specified.



Interface: VLAN1

Interface	TIA Interface	Interface Name	IP Address	Subnet Mask	Address Type	IP Assgn. Method	MTU
vlan1	yes	INT	192 . 168 . 16 . 42	255 . 255 . 255 . 0	Primary	Static	1500
vlan2	-	EXT	192 . 168 . 50 . 1	255 . 255 . 255 . 0	Primary	Static	1500
ppp2	-	ppp2	0 . 0 . 0 . 0	0 . 0 . 0 . 0	Primary	Static	1492

1.3.3 Creating a user-specific rule set

Creating a rule set

1. In the Inspector window, click on "Security > Firewall > User Specific".
2. Enter the name "Station_1".
3. Click in the table. Select the entry "New entry" in the shortcut menu.

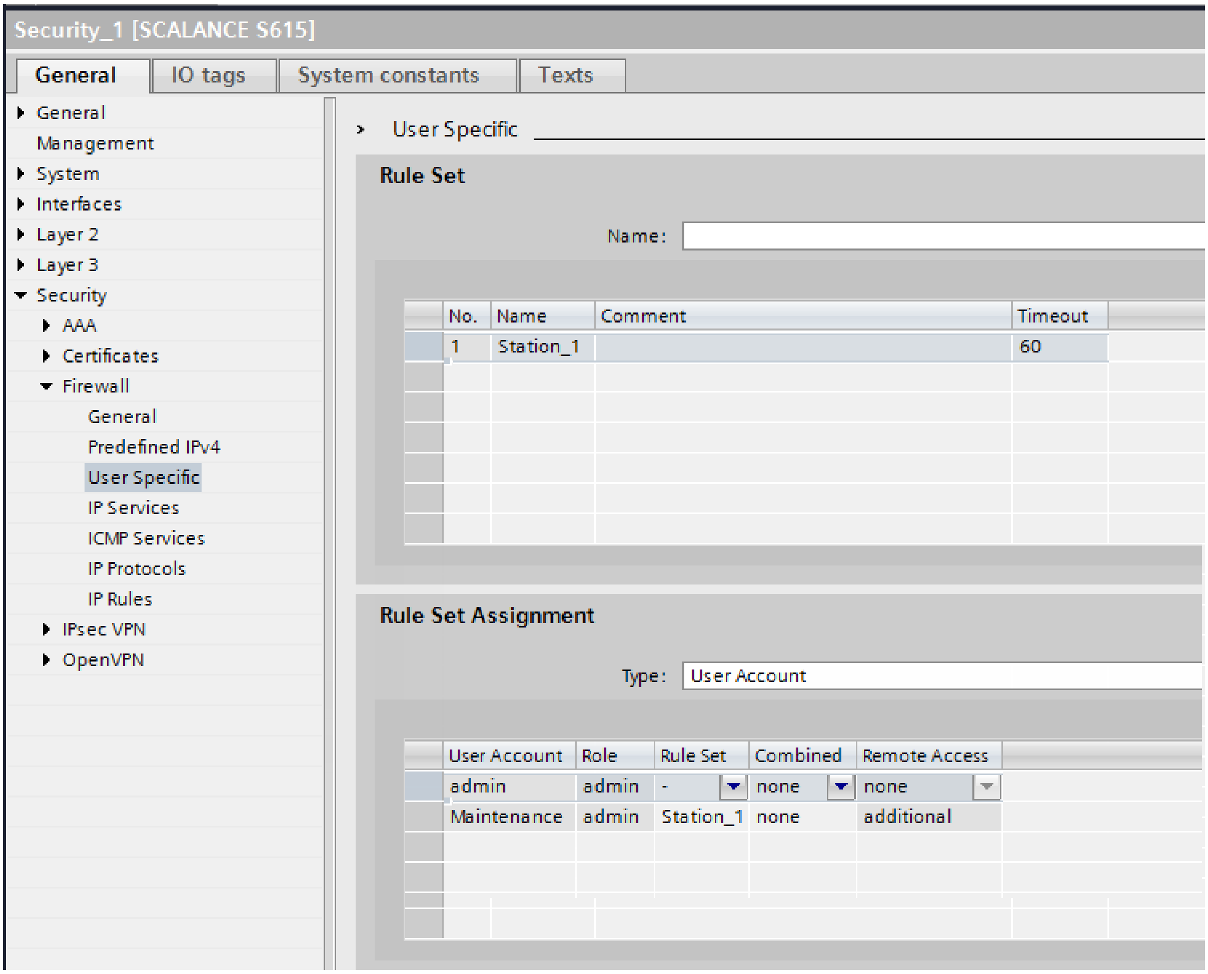
   A new entry is created in the table.
4. To limit access to one hour, enter "60" for "Timeout [Min.]".

Assigning a rule set to a user

1. Scroll to the group "Rule Set Assignment".
2. Select the "User account" for "Type".
3. Assign the Rule Set "Station_1" to the "Maintenance" user.
4. Compile the project.

Result

The rule set "Station_1" has been created and assigned to the "Maintenance" user. After the compilation, "additional" is automatically set for "Remote Access".



Rule Set

Name:

No.	Name	Comment	Timeout
1	Station_1		60

Rule Set Assignment

Type: User Account

User Account	Role	Rule Set	Combined	Remote Access
admin	admin	-	none	none
Maintenance	admin	Station_1	none	additional

1.3.4 Creating an IP rule and assigning the rule set

In this example, the service technician should only receive access to the Web server of the CPU. The HTTPS service (TCP port 443) is required for access.

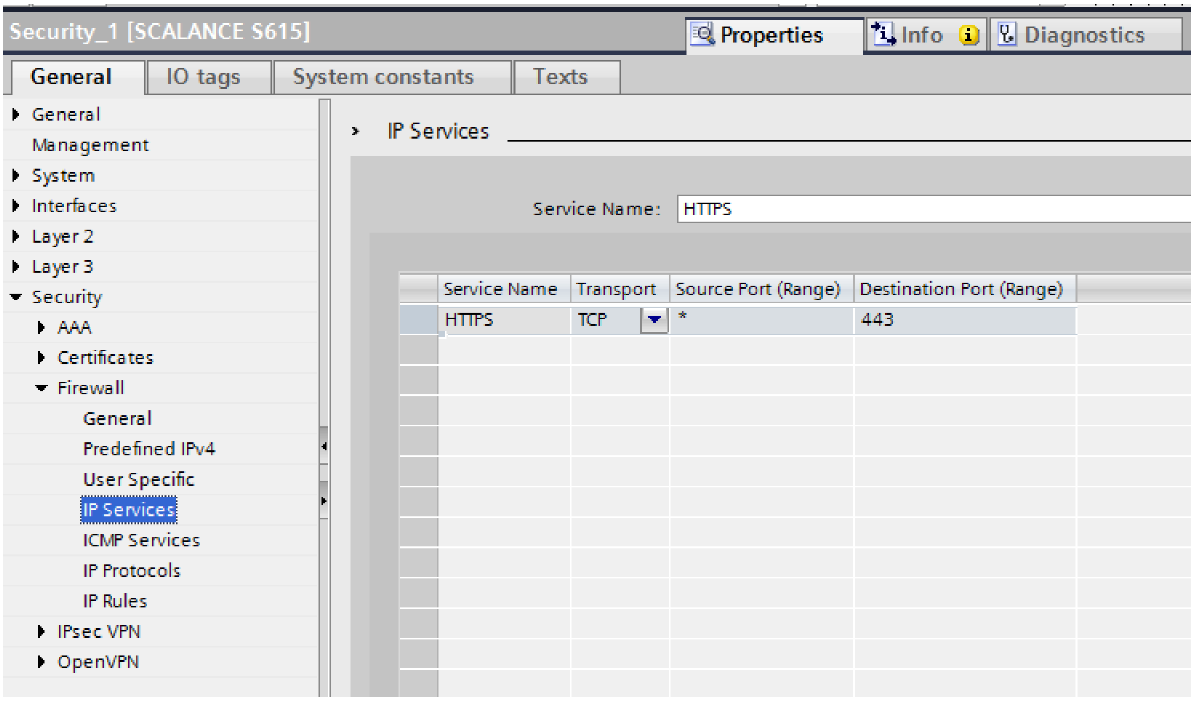
Create HTTPS service

1. In the Inspector window, click on "Security > Firewall > IP Services".
2. Enter "HTTPS" for "Service Name".
3. Click in the table. Select the entry "New entry" in the shortcut menu.

   A new entry is created in the table.
4. Configure HTTPS with the following settings:

Transport	TCP
Destination Port (Range)	443 (default port)

Result



Service Name: HTTPS

Service Name	Transport	Source Port (Range)	Destination Port (Range)
HTTPS	TCP	*	443

Creating a firewall rule and assigning it to a rule set

Create firewall rules

1. In the Inspector window, click on "Security > Firewall > IP Rules".
2. Click in the table. Select the entry "New entry" in the shortcut menu.

   A new entry is created in the table.
3. Configure the firewall rule for HTTPS.

   Access is enabled for all users using the "Station_1" rule set:

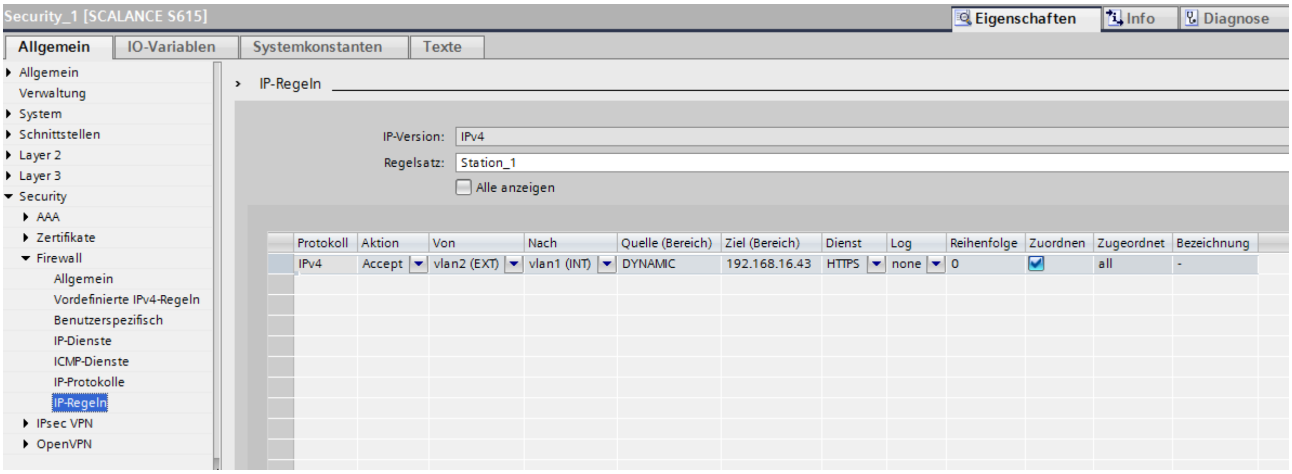
Action	Accept
From	vlan2 (EXT)
To	vlan1 (INT)
Source (Range)	DYNAMIC If the rule set is activated by a user, the placeholder DYNAMIC is replaced by the IP address of the end device used.
Destination (Range)	Web server of the CPU 192.168.16.43
Service	HTTPS

Assigning to a rule set

1. Select the rule set "Station_1" and enable the "Show all" setting.
2. Enable the "Assign" setting.

Result

Overview of the configuration



IP-Version: IPv4

Regelsatz: Station_1

□ Alle anzeigen

Protokoll	Aktion	Von	Nach	Quelle (Bereich)	Ziel (Bereich)	Dienst	Log	Reihenfolge	Zuordnen	Zugeordnet	Bezeichnung
IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	DYNAMIC	192.168.16.43	HTTPS	none	0	☑	all	-

1.3.5 Loading the configuration into the SCALANCE S615

Requirement

- Before you load the configuration into the device, you must save and compile the TIA project. If errors occurred during compiling, remedy them.
- The hardware configuration in the TIA project matches the hardware configuration of the device. If this is not the case, the download will be aborted due to errors.
- The firmware version in the TIA project matches the firmware version of the device.
- The PG/PC is connected to the SCALANCE S615 and reachable.

Note for login to the device

When you connect to the device via HTTPS, for example, with Web Based Management or for loading the configuration from the TIA Portal, you must log in.

When you log in for the first time or following a reset to factory settings, enter the user "admin" preset in the factory and the password "admin".

The password needs to be changed afterward. You can also rename the "admin" user preset in the factory once.

When the device is in the factory setting and you download the configuration via the TIA Portal, the password and the user name may be changed during downloading. The new user matches the project administrator with which you are logged in to the TIA Portal at this time.

Example:

You are logged in with the project administrator "Device_Admin" and the password "TIAPortal0815!" in the TIA Portal.

The device is in the factory setting and you download the configuration for the first time from the TIA Portal. You must log in with the following credentials when loading: User: admin Password: admin

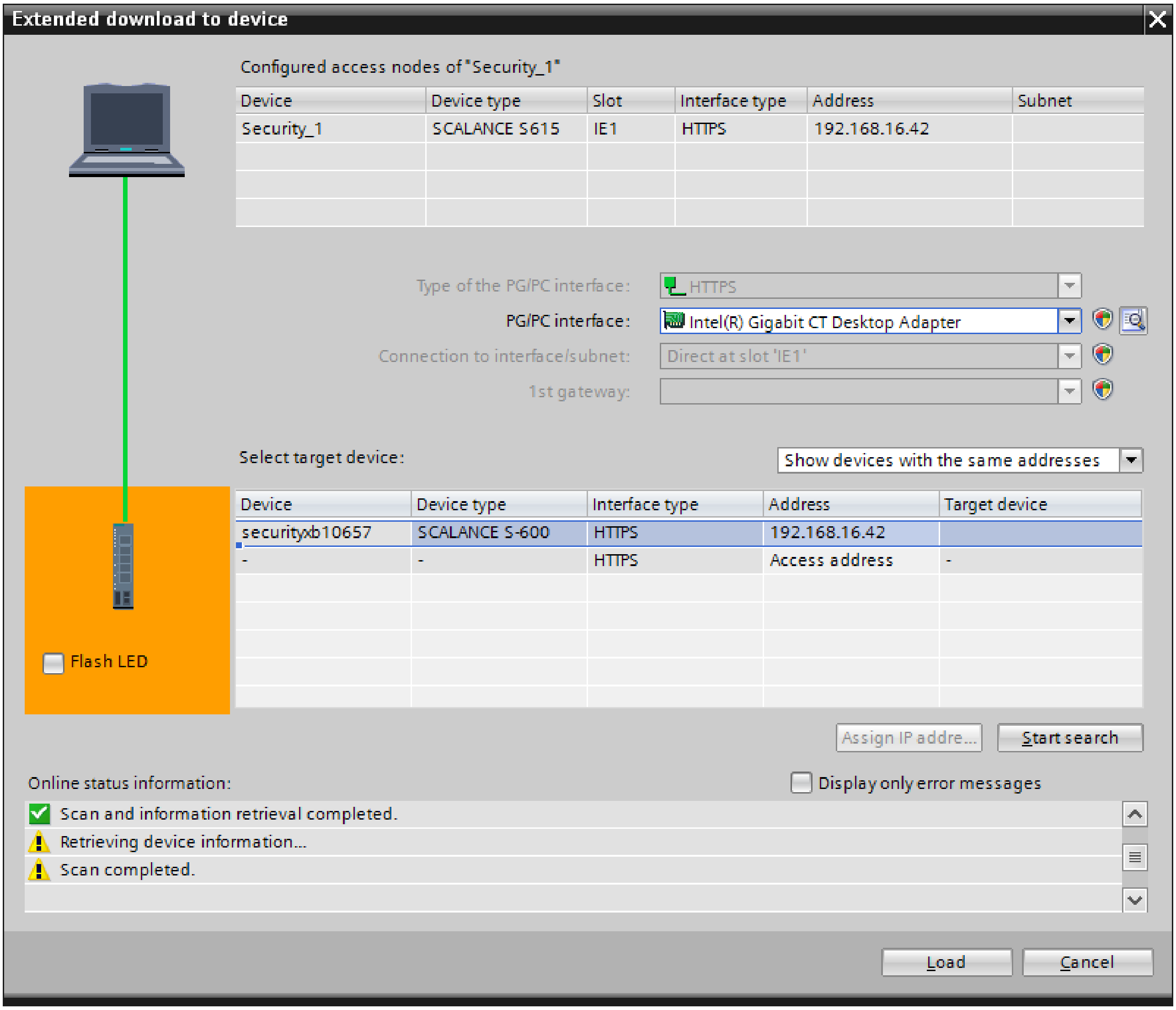
The password and the user name are changed during the download. To log in to the device, you must use these credentials from now on.

User: Device_Admin and password: TIAPortal0815!

Procedure

The configuration is loaded via HTTPS protocol to the SCALANCE S615.

1. Select the SCALANCE S615 in the project tree.
2. In the shortcut menu, select the command "Download to device > Hardware configuration". The "Extended download to device" dialog opens.
3. Set the type and the PG/PC interface.
4. To start the search, click "Start search".



Configured access nodes of "Security_1"

Device	Device type	Slot	Interface type	Address	Subnet
Security_1	SCALANCE S615	IE1	HTTPS	192.168.16.42	

Type of the PG/PC interface: HTTPS

PG/PC interface: Intel(R) Gigabit CT Desktop Adapter

Connection to interface/subnet: Direct at slot 'IE1'

1st gateway:

Select target device: Show devices with the same addresses

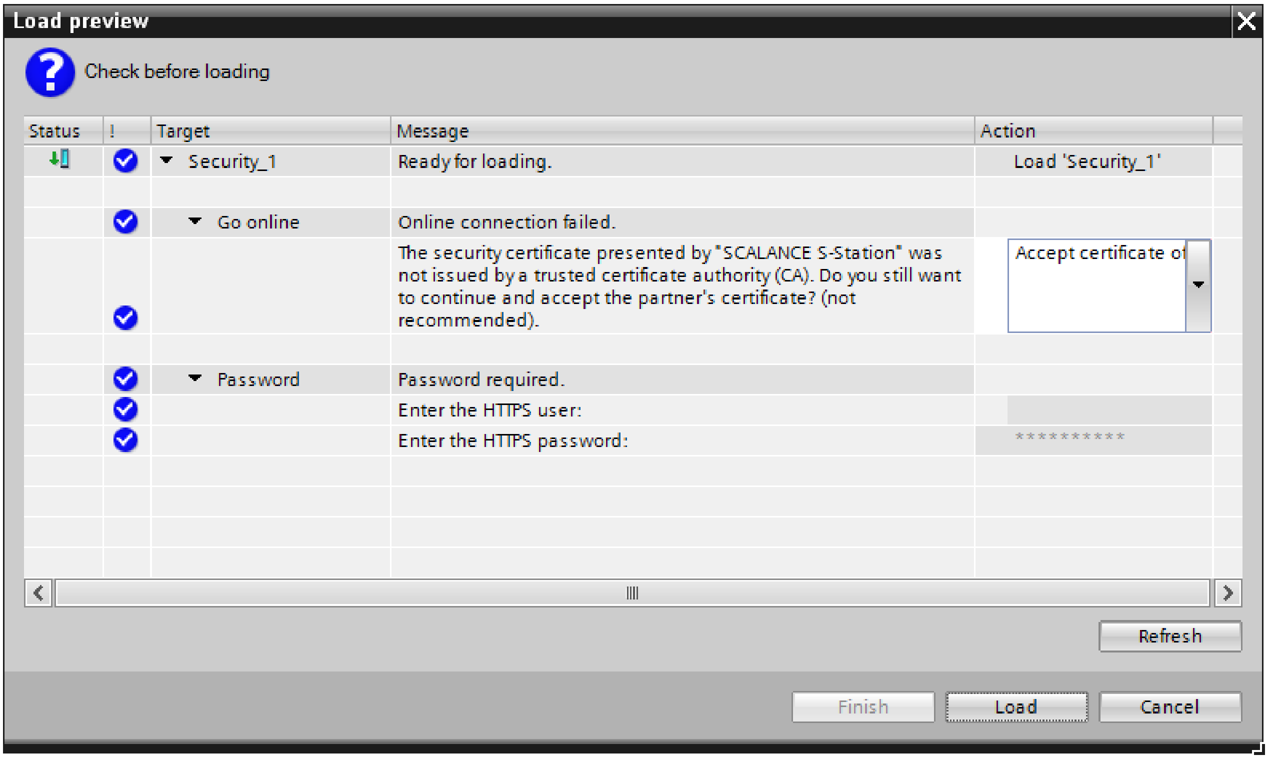
Device	Device type	Interface type	Address	Target device
securityxb10657	SCALANCE S-600	HTTPS	192.168.16.42	
-	-	HTTPS	Access address	-

Online status information:

✓ Scan and information retrieval completed.
⚠ Retrieving device information...
⚠ Scan completed.

5. When the device is found, the SCALANCE S615 shows up in the table as the target device.
6. Select the SCALANCE S615 in the table and click "Load".
7. The load preview opens. Accept the certificate.

8. For "HTTPS user" and "HTTPS password", enter the data of the WBM user. When you log in for the first time or following a reset to factory settings, enter the user "admin" preset in the factory and the password "admin", see note under "Logging on at the device".



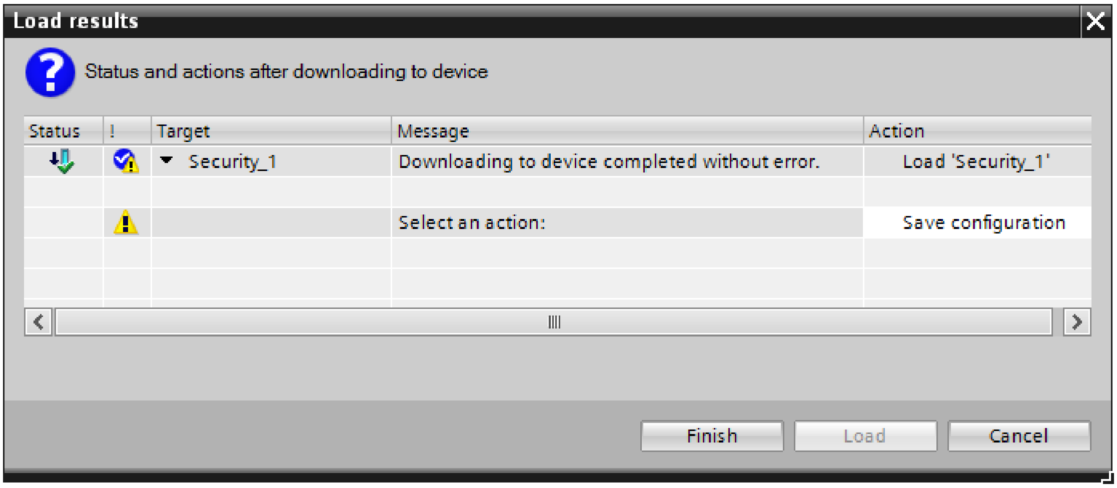
Load preview

Check before loading

Status	!	Target	Message	Action
	✓	Security_1	Ready for loading.	Load 'Security_1'
	✓	Go online	Online connection failed.	
	✓		The security certificate presented by "SCALANCE S-Station" was not issued by a trusted certificate authority (CA). Do you still want to continue and accept the partner's certificate? (not recommended).	Accept certificate of
	✓	Password	Password required.	
	✓		Enter the HTTPS user:	
	✓		Enter the HTTPS password:	**********

9. Click the "Load" button.

Loading is performed and the "Load results" dialog is displayed.



Load results

Status and actions after downloading to device

Status	!	Target	Message	Action
	✓	Security_1	Downloading to device completed without error.	Load 'Security_1'
	⚠		Select an action:	Save configuration

10. If the loading is completed error-free, select "Save configuration" in "Action".

    Click the "Finish" button.

Result

The configuration is loaded to the device and is used after restarting the device.

1.4 Logging on via user-specific firewall

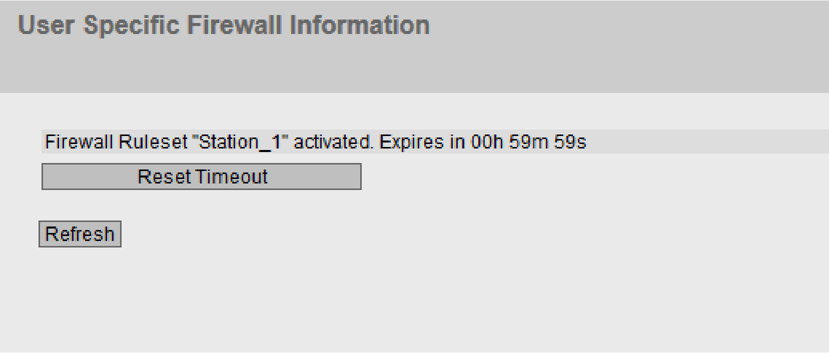
The service technician logs on with the "Maintenance" user and then logs on to the Web server of the CPU.

Requirement

- The Web server CPU can be reached and a corresponding user has been created. You can find additional information on this under the following entry IDs:
  - 59191792 (https://support.industry.siemens.com/cs/ww/de/view/59191792/en): SIMATIC S7-1500, ET 200MP automation system
  - 59193560 (https://support.industry.siemens.com/cs/de/de/view/59193560/en): SIMATIC S7-1500, ET 200SP, ET 200pro Webserver

Procedure

1. In the login window, click "Switch to firewall login".
2. Log in as the "Maintenance" user. After successful login, the WBM page "User Specific Firewall Information" opens.

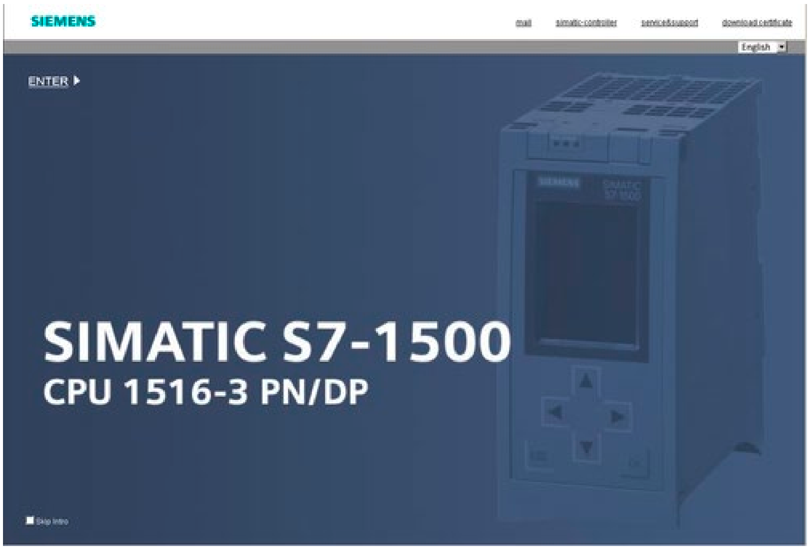
   User Specific Firewall Information

   Firewall Ruleset "Station_1" activated. Expires in 00h 59m 59s

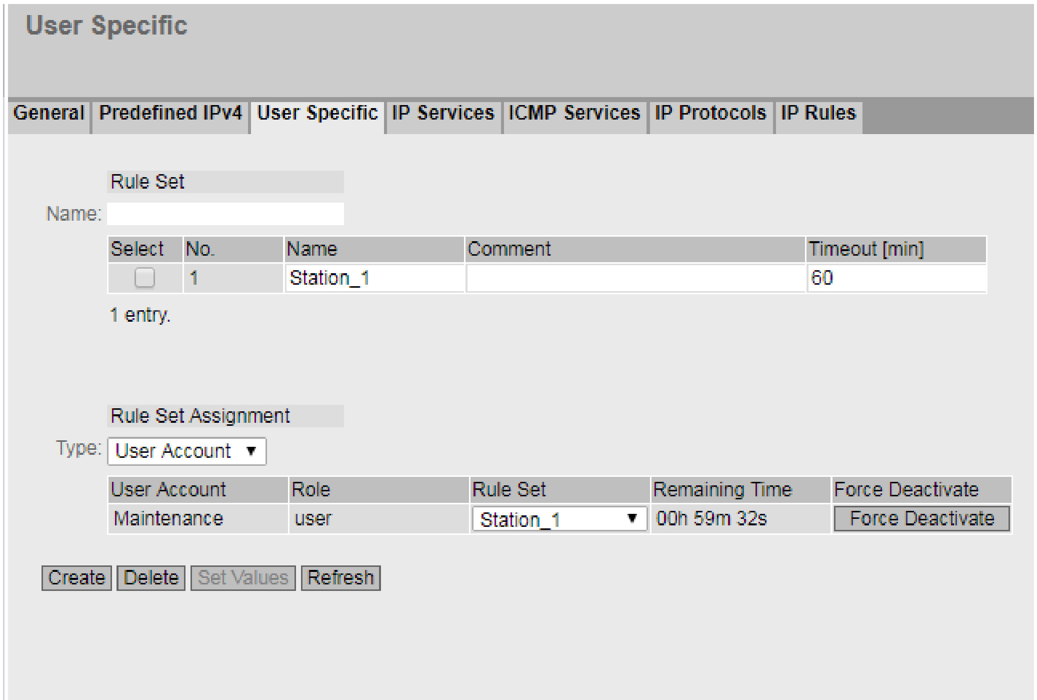
   This WBM page must always remain open.
3. Enter the IP address of the CPU, e.g. https://192.168.100.43, in the address bar of the Web browser.

Result

The Intro page is called after successful login to the Web server of the CPU.



The remaining time is shown to the device administrator on the "User Specific" tab. If necessary, the device administrator can log off the active user using the "Force Deactivate" button.



User Specific

Rule Set

Name:

Select	No.	Name	Comment	Timeout [min]
□	1	Station_1		60

1 entry.

Rule Set Assignment

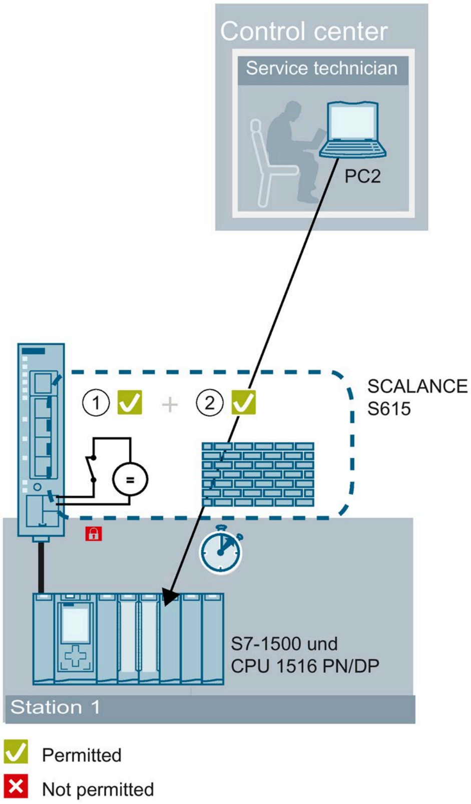
Type: User Account ▼

User Account	Role	Rule Set	Remaining Time	Force Deactivate
Maintenance	user	Station_1 ▼	00h 59m 32s	Force Deactivate

2 Access with user data and digital input

2.1 Introduction

The user login to the user-defined firewall can be combined with an event. In this example configuration, the event is "Digital input". A pushbutton is connected to the digital input of the S615. When the pushbutton is closed, a voltage is present at the digital input, the DI LED lights up and the event "Digital input" (condition ①) is triggered. The "Maintenance" user now logs on with his/her user data (condition ②) to the user-defined firewall. When conditions ① and ② are met, the WBM page "User Specific Firewall Information" opens and executes the ruleset "Station_1". When the digital input is open, the user receives a corresponding error message during login.



Requirement

- The "Maintenance" user and the ruleset have been created, see "Access via user-specific firewall (Page 9)".
- Firmware version 6.2

Steps in configuration

The following steps are required for the configuration:

1. Configuring digital input (Page 33)
2. Logging on via user-specific firewall (Page 35)

2.2 Configuring digital input

Wiring digital input

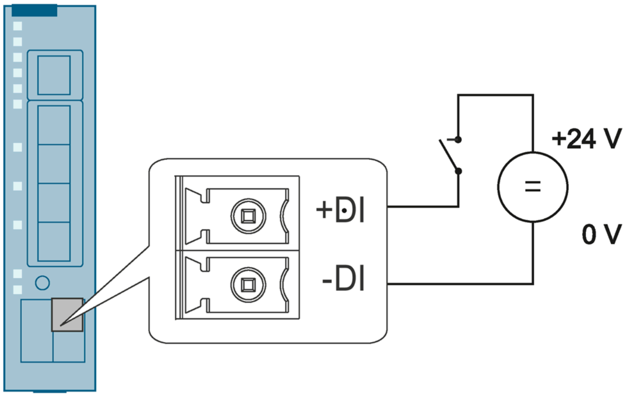
Note

Notes on device

Please note the safety instructions in the operating instructions.

1. Wire the digital input.

   You can find additional information on the terminals in the operating instructions.



CAUTION

Damage due to voltage being too high or too low

The voltage at the digital input/output must not exceed 30 V DC and not fall below -30 V DC; otherwise, the digital input/output will be destroyed.

Note

Interference pulse

To avoid evaluating an interference pulse, the pulse for the signal 1 (TRUE / HIGH) must be at least 200 ms.

Setting parameters in the WBM

Configuring "Digital Input" event

1. Click on "System" > "Events" in the navigation area and on the "Configuration" tab in the content area.
2. Enable the "Digital Input" event in the "Firewall" column.
3. Click the "Set Values" button.

Combining user login with event

1. Click on "Security" > "Firewall" in the navigation area and on the "User Specific" tab in the content area.
2. For "Combined" select the entry "Digital Input".
3. Click the "Set Values" button.

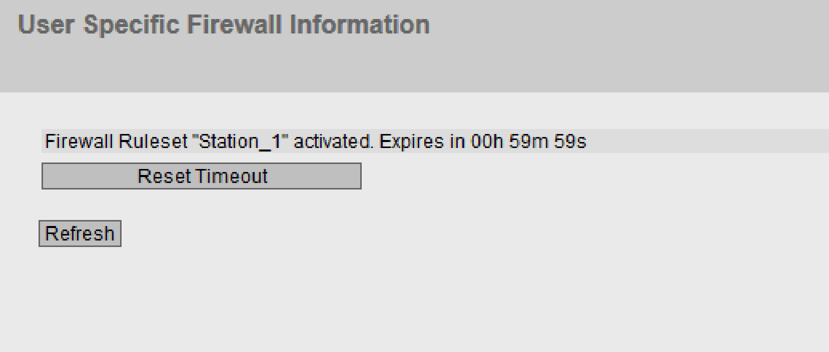
2.3 Logging on via user-specific firewall

When the "Digital Input" event is executed, the service technician logs in with the "Maintenance" user. Afterwards, the technician can log in to the CPU web server.

Procedure

1. Close the pushbutton.

   When the pushbutton closes, voltage is applied to the digital input (Signal 1 - TRUE / HIGH) and the LED of the digital input lights up. Signal 1 triggers the "Firewall" event on the device that controls the login to the user-specific firewall. You will find information on connecting and the maximum current load in the operating instructions of the devices.
2. In the login window, click "Switch to firewall login".
3. Log in as the "Maintenance" user. After successful login, the WBM page "User Specific Firewall Information" opens.

   User Specific Firewall Information

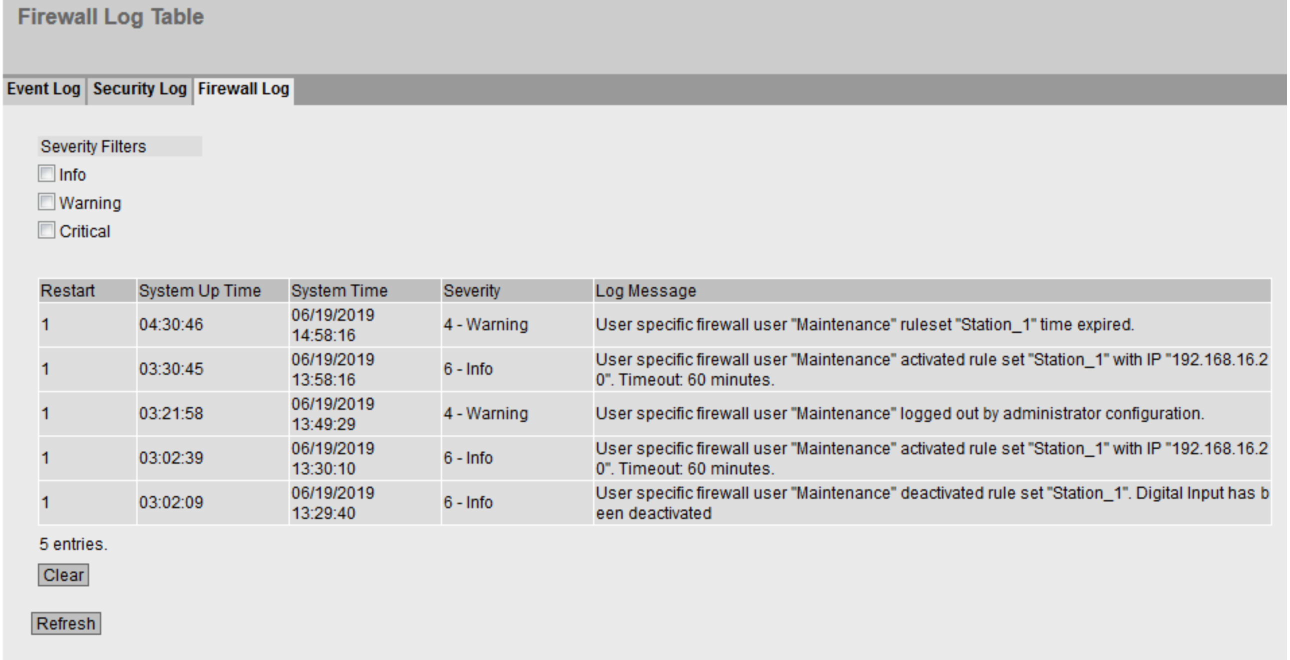
   Firewall Ruleset "Station_1" activated. Expires in 00h 59m 59s

   This WBM page must always remain open.
4. Enter the IP address of the CPU, e.g. https://192.168.100.43, in the address bar of the Web browser.

Result

The remaining time is shown to the device administrator in the "User Specific" tab. If necessary, the device administrator can log off the active user using the "Force Deactivate" button. The user is logged off when a voltage is applied to the button.

The corresponding messages are displayed in "Information > Log Tables > Firewall Log".



Severity Filters

□ Info
□ Warning
□ Critical

Restart	System Up Time	System Time	Severity	Log Message
1	04:30:46	06/19/2019 14:58:16	4 - Warning	User specific firewall user "Maintenance" ruleset "Station_1" time expired.
1	03:30:45	06/19/2019 13:58:16	6 - Info	User specific firewall user "Maintenance" activated rule set "Station_1" with IP "192.168.16.20". Timeout: 60 minutes.
1	03:21:58	06/19/2019 13:49:29	4 - Warning	User specific firewall user "Maintenance" logged out by administrator configuration.
1	03:02:39	06/19/2019 13:30:10	6 - Info	User specific firewall user "Maintenance" activated rule set "Station_1" with IP "192.168.16.20". Timeout: 60 minutes.
1	03:02:09	06/19/2019 13:29:40	6 - Info	User specific firewall user "Maintenance" deactivated rule set "Station_1". Digital Input has been deactivated

5 entries.

Index