SIEMENS

Ingenuity for life

Layer 2 VPN mit SCALANCE SC64x-2C

SCALANCE SC64x-2C

https://support.industry.siemens.com/cs/ww/en/view/109792357

Siemens Industry Online Support

This entry is from the Siemens Industry Online Support. The general terms of use (http://www.siemens.com/terms_of_use) apply.

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 only form one element of such a concept.
Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.
Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

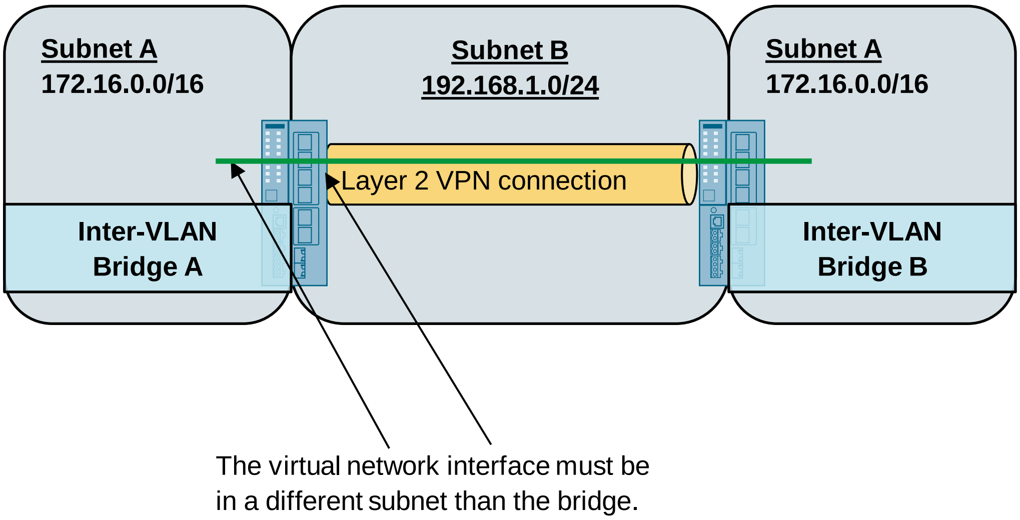
Table of content

1 OpenVPN

OpenVPN can be used to set up virtual private networks (VPN). The SCALANCE SC64x-2C can establish a Layer 2 VPN connection to a remote network as an OpenVPN client.
The Layer 2 VPN connection is established via a virtual network interface, the so-called TAP device. The TAP device is connected to the actual network via a network bridge (inter-VLAN bridge), in other words, the Layer 2 VPN connection must always be assigned to a bridge and cannot be used directly on a VLAN. With the SCALANCE SC64x-2C, a maximum of 6 VLANS can be assigned to the bridge.

In this example, an inter-VLAN bridge is created to which a VLAN is added.

Figure 1-1



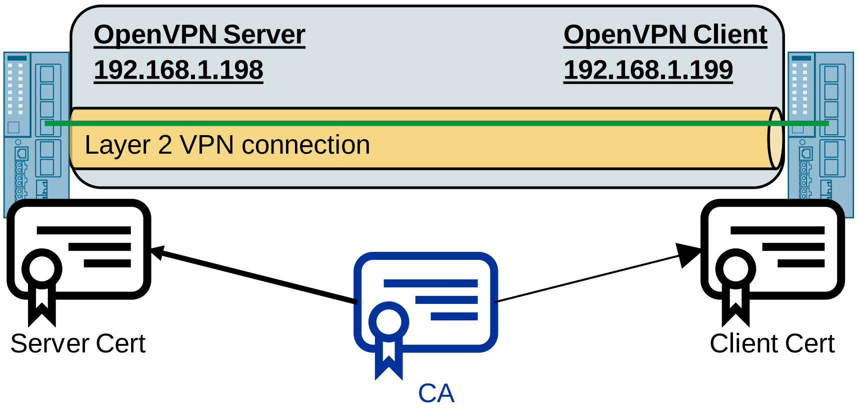
Authentication procedure

OpenVPN server and client need a CA certificate and device certificate to establish the Layer 2 VPN connection. You can also use a user name and password for authentication.

The certificates are created and signed in the TIA Portal, for example.

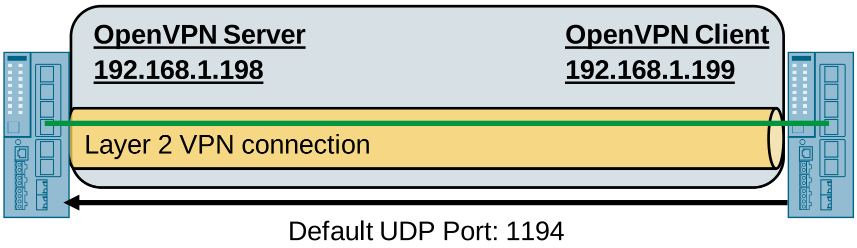
The use of certificates is an asymmetric cryptosystem. Each node (device) has a secret private key and a public key of the partner. The private key makes it possible to authenticate and generate digital signatures.

Figure 1-2



The OpenVPN client establishes the S7 connection to the OpenVPN server. With OpenVPN you can set the transport protocol TCP or UDP as well as the port used.

Figure 1-3

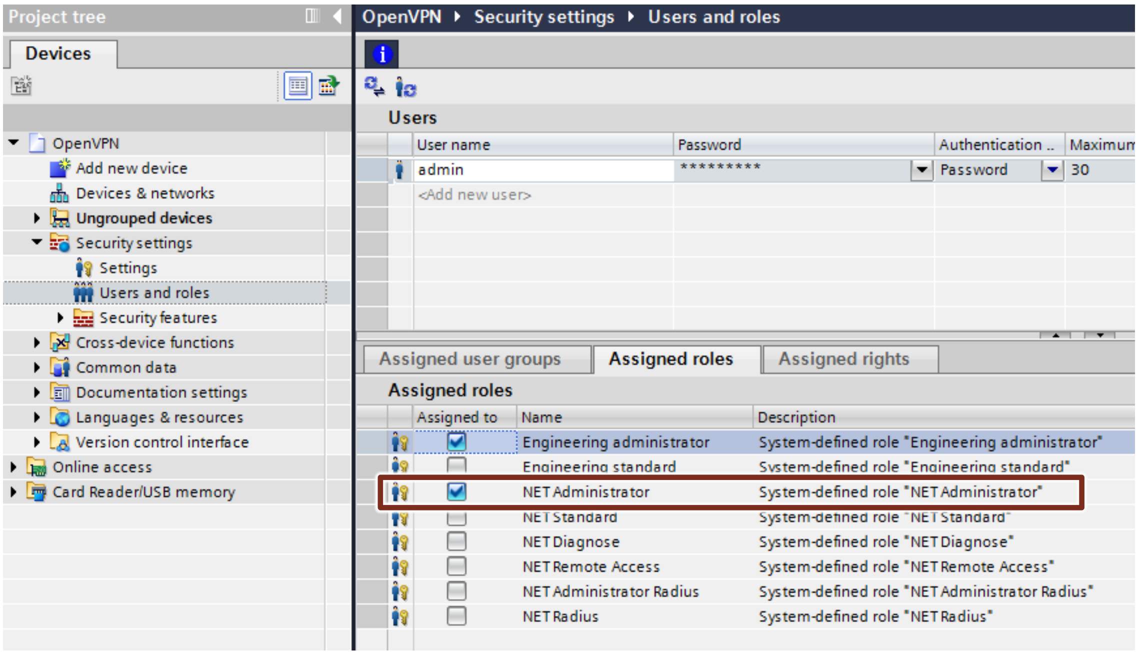


2 Create and Export Certificates

2.1 Requirements

- The STEP 7 project is protected with user name and password because security functions are used.
- The "NET Administrator" role is enabled in the Security settings for the user.
- SCALANCE SC64x-2C firmware V2.1.1 or higher.

Figure 2-1



Users

User name	Password	Authentication ..	Maximum
admin	*********	Password	30
<Add new user>			

Assigned roles

Assigned to	Name	Description
☑	Engineering administrator	System-defined role "Engineering administrator"
□	Engineering standard	System-defined role "Engineering standard"
☑	NET Administrator	System-defined role "NET Administrator"
□	NET Standard	System-defined role "NET Standard"
□	NET Diagnose	System-defined role "NET Diagnose"
□	NET Remote Access	System-defined role "NET Remote Access"
□	NET Administrator Radius	System-defined role "NET Administrator Radius"
□	NET Radius	System-defined role "NET Radius"

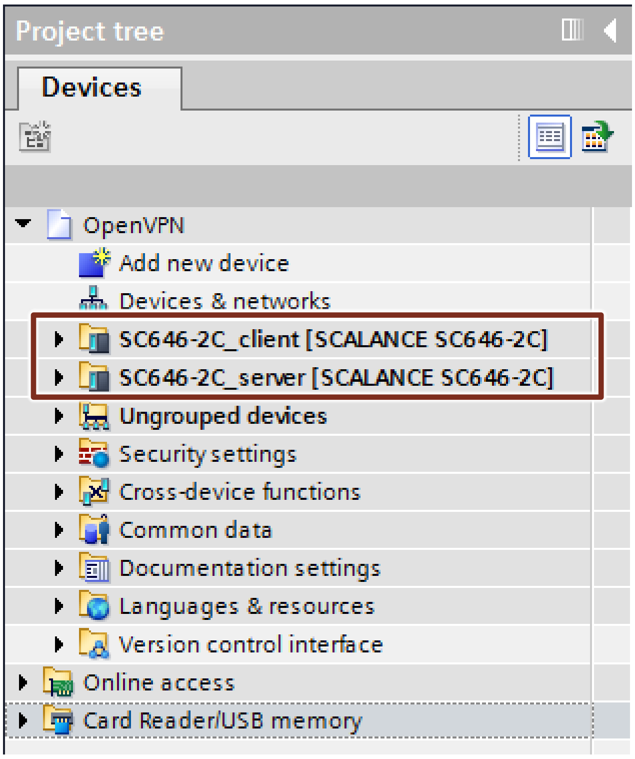
2.2 Add device

1. In the project tree you double-click the "Devices & networks" item. The "Devices & networks" editor opens.
2. Open the Network view in the "Devices & networks" editor.
3. Use drag and drop to add two SCALANCE SC64x-2C devices from the Hardware Catalog to the Network view.

Result

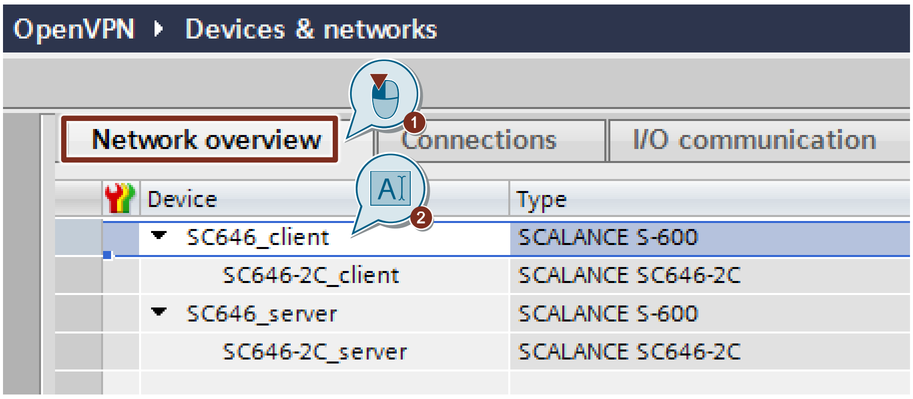
Two SCALANCE SC64x-2C devices are added to the STEP 7 project.

Figure 2-2



2.3 Change the Station Name

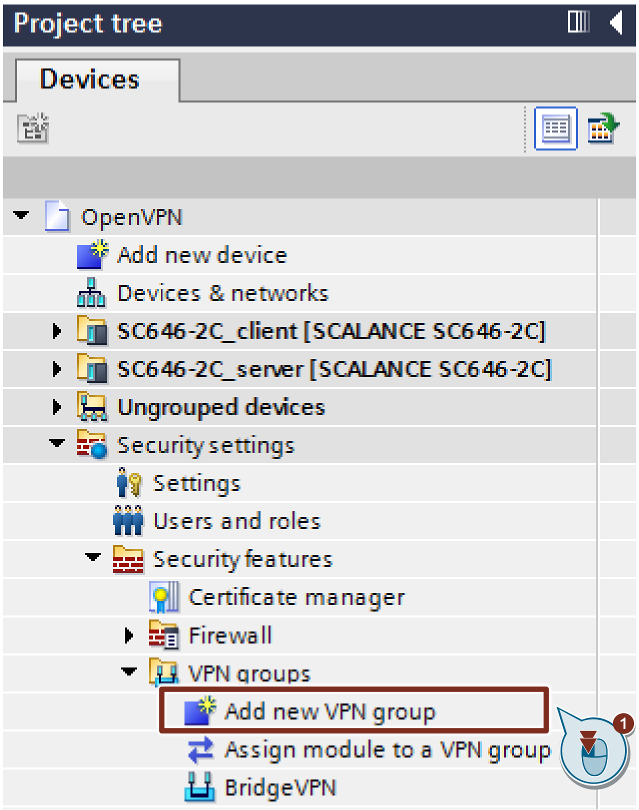
1. In the table area of the Network view you open the "Network overview" tab.
2. Change the station name of the SCALANCE SC64x-2C to keep VPN server and VPN client apart.



Device	Type
▼ SC646_client	SCALANCE S-600
SC646-2C_client	SCALANCE SC646-2C
▼ SC646_server	SCALANCE S-600
SC646-2C_server	SCALANCE SC646-2C

2.4 Add VPN Group

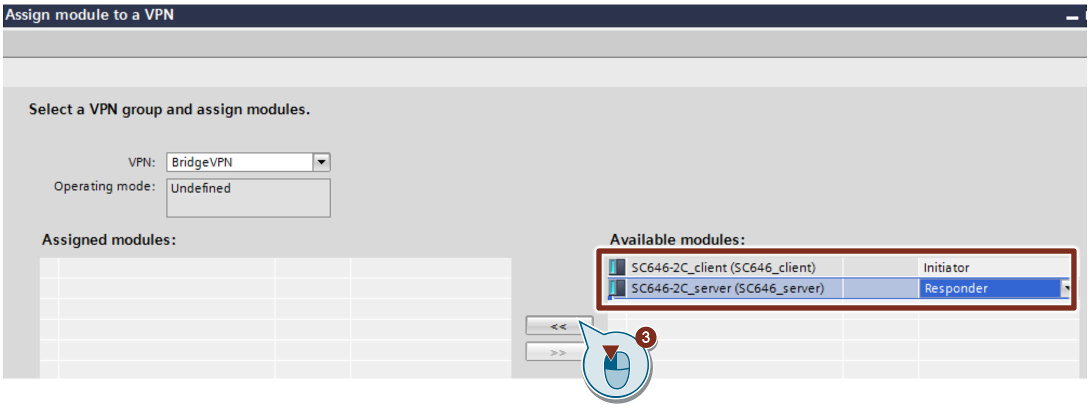
1. Go to "Security settings > Security features > VPN groups" in the Project tree and double-click the "Add new VPN group" command. A new VPN group is added, "BridgeVPN", for example.



- ▼ OpenVPN
  - Add new device
  - Devices & networks
  - ▸ SC646-2C_client [SCALANCE SC646-2C]
  - ▸ SC646-2C_server [SCALANCE SC646-2C]
  - ▸ Ungrouped devices
  - ▼ Security settings
    - Settings
    - Users and roles
    - ▼ Security features
      - Certificate manager
      - ▸ Firewall
      - ▼ VPN groups
        - Add new VPN group
        - Assign module to a VPN group
        - BridgeVPN

2. Double-click the VPN group "BridgeVPN". The "Assign module to a VPN" dialog opens.

3. Assign the available "SCALANCE SC64x-2C" modules to the VPN group.
   - VPN client: Initiator
   - VPN server: Responder



Assign module to a VPN

Select a VPN group and assign modules.

VPN: BridgeVPN

Operating mode: Undefined

Assigned modules:

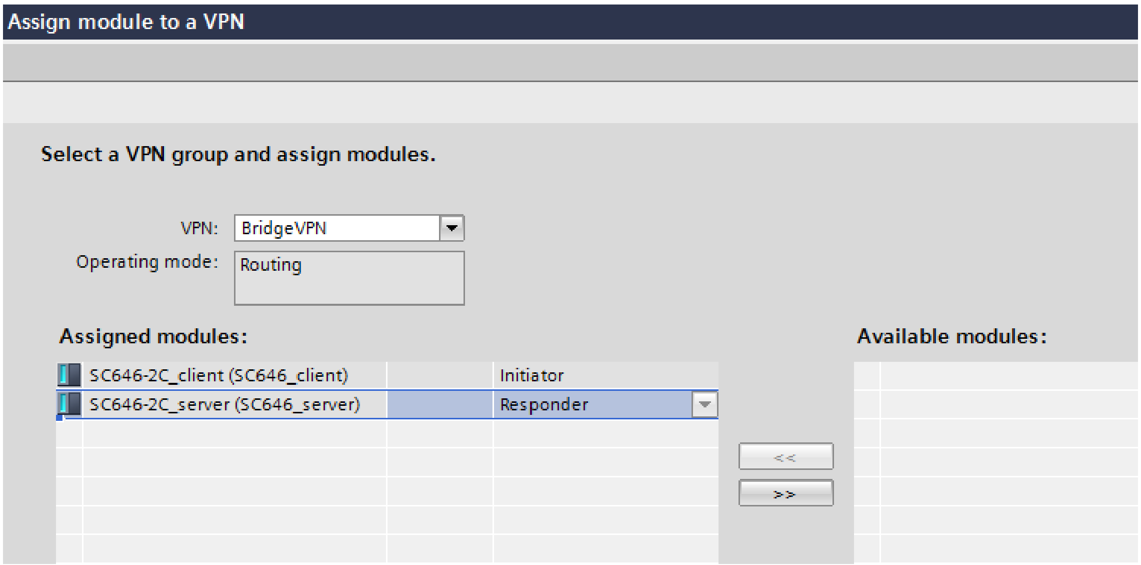
Available modules:

SC646-2C_client (SC646_client)	Initiator
SC646-2C_server (SC646_server)	Responder

Result

The "SCALANCE SC64x-2C" modules are displayed in the "Assigned modules" area.

Figure 2-3



Assign module to a VPN

Select a VPN group and assign modules.

VPN: BridgeVPN

Operating mode: Routing

Assigned modules:

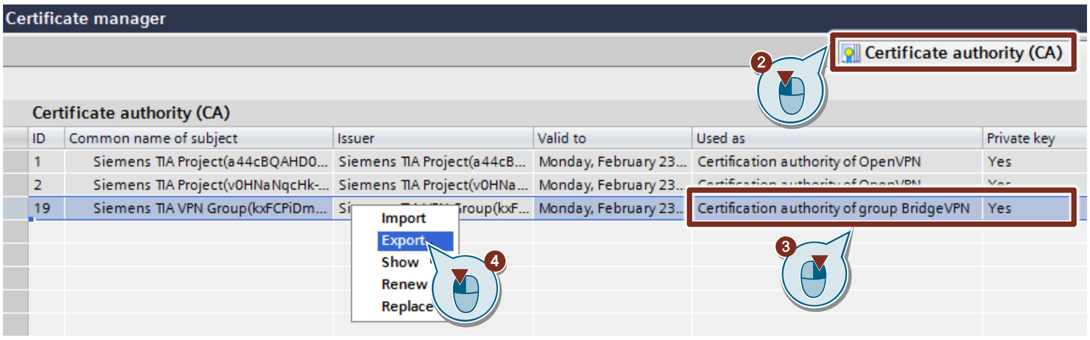
SC646-2C_client (SC646_client)	Initiator
SC646-2C_server (SC646_server)	Responder

Available modules:

2.5 Export Certificates

2.5.1 Export CA Certificate of the VPN Group

1. In the Project tree, go to "Security settings > Security features" and double-click the "Certificate manager" item. The Certificate manager opens.
2. In the Certificate manager you open the "Certificate authority (CA)" tab.
3. Right-click the CA certificate of the VPN group. The pop-up menu opens.
4. Select the "Export" item.

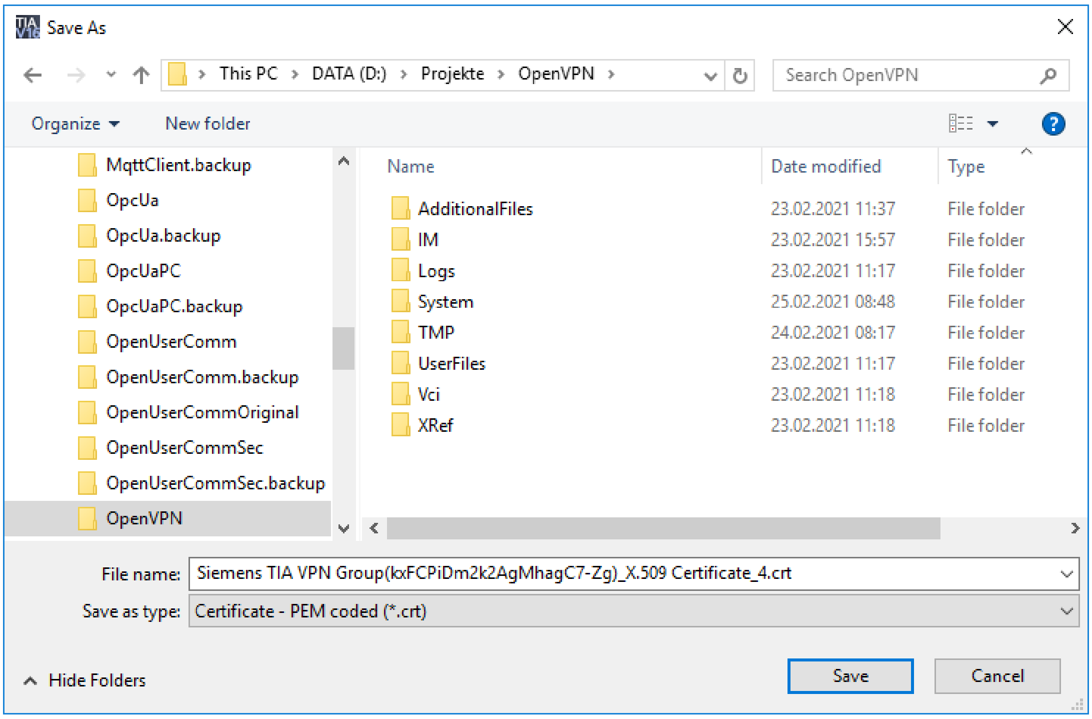


Certificate manager

Certificate authority (CA)

ID	Common name of subject	Issuer	Valid to	Used as	Private key
1	Siemens TIA Project(a44cBQAHD0...	Siemens TIA Project(a44cB...	Monday, February 23...	Certification authority of OpenVPN	Yes
2	Siemens TIA Project(v0HNaNqcHk-...	Siemens TIA Project(v0HNa...	Monday, February 23...	Certification authority of OpenVPN	Yes
19	Siemens TIA VPN Group(kxFCPiDm...	Si roup(kxF...	Monday, February 23...	Certification authority of group BridgeVPN	Yes

5. Save the certificate as the type "PEM coded (*.crt)". The private code of the certification authority (CA) is not exported as well.



MqttClient.backup
OpcUa
OpcUa.backup
OpcUaPC
OpcUaPC.backup
OpenUserComm
OpenUserComm.backup
OpenUserCommOriginal
OpenUserCommSec
OpenUserCommSec.backup
OpenVPN

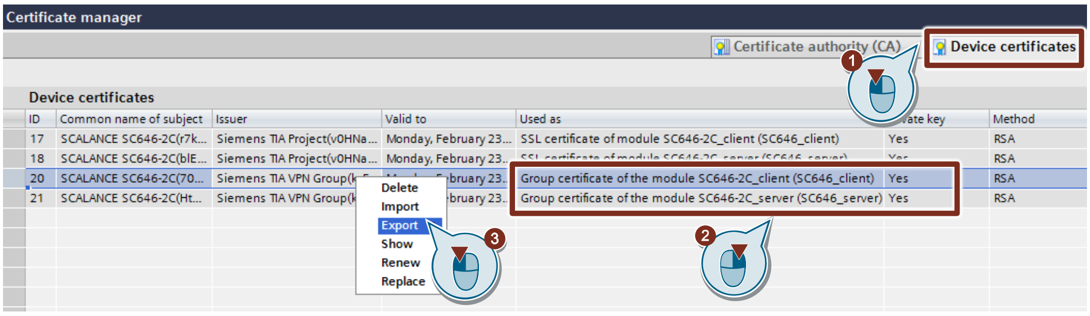
Name	Date modified	Type
AdditionalFiles	23.02.2021 11:37	File folder
IM	23.02.2021 15:57	File folder
Logs	23.02.2021 11:17	File folder
System	25.02.2021 08:48	File folder
TMP	24.02.2021 08:17	File folder
UserFiles	23.02.2021 11:17	File folder
Vci	23.02.2021 11:18	File folder
XRef	23.02.2021 11:18	File folder

File name: Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg)_X.509 Certificate_4.crt

Save as type: Certificate - PEM coded (*.crt)

2.5.2 Export Device Certificates

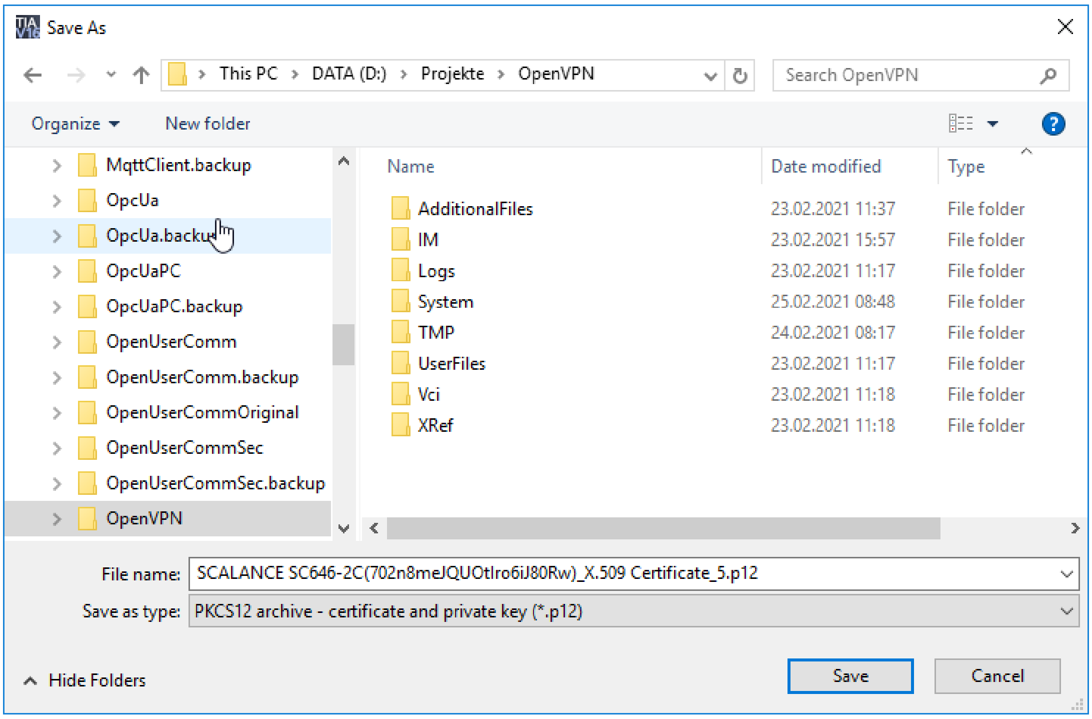
1. In the Certificate manager you open the "Device certificates" tab.
2. Right-click the device certificate of the SCALANCE SC64x-2C. The pop-up menu opens.
3. Select the "Export" item.



Device certificates

ID	Common name of subject	Issuer	Valid to	Used as	…ate key	Method
17	SCALANCE SC646-2C(r7k…	Siemens TIA Project(v0HNa…	Monday, February 23…	SSL certificate of module SC646-2C_client (SC646_client)	Yes	RSA
18	SCALANCE SC646-2C(blE…	Siemens TIA Project(v0HNa…	Monday, February 23…	SSL certificate of module SC646-2C_server (SC646_server)	Yes	RSA
20	SCALANCE SC646-2C(70…	Siemens TIA VPN Group(k…	…bruary 23…	Group certificate of the module SC646-2C_client (SC646_client)	Yes	RSA
21	SCALANCE SC646-2C(Ht…	Siemens TIA VPN Group(k…	…bruary 23…	Group certificate of the module SC646-2C_server (SC646_server)	Yes	RSA

4. Save the certificate as the type "PKCS12 archive – certificate and private key (*.p12)". The device certificate is exported with a private key. It is necessary to protect the private key with a password.



Name	Date modified	Type
AdditionalFiles	23.02.2021 11:37	File folder
IM	23.02.2021 15:57	File folder
Logs	23.02.2021 11:17	File folder
System	25.02.2021 08:48	File folder
TMP	24.02.2021 08:17	File folder
UserFiles	23.02.2021 11:17	File folder
Vci	23.02.2021 11:18	File folder
XRef	23.02.2021 11:18	File folder

File name: SCALANCE SC646-2C(702n8meJQUOtlro6iJ80Rw)_X.509 Certificate_5.p12

Save as type: PKCS12 archive - certificate and private key (*.p12)

Result

You have exported and saved 3 certificates:

- CA certificate of the VPN Group
- Device certificate of the VPN client (*.p12)
- Device certificate of the VPN server (*.p12)

NOTE If you do not have TIA Portal available, in PCS 7 for example, you can create and export the certificates in the Security Configuration Tool (SCT).

Instructions for this are available at this link:

https://support.industry.siemens.com/cs/ww/en/view/109792637

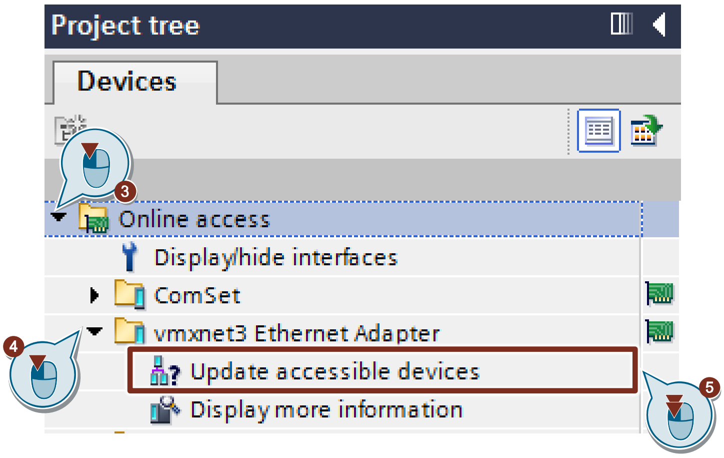
3 Configure SCALANCE SC64x-2C

3.1 Requirements

The SCALANCE SC64x-2Cs (VPN client and VPN server) are reset to the factory settings.

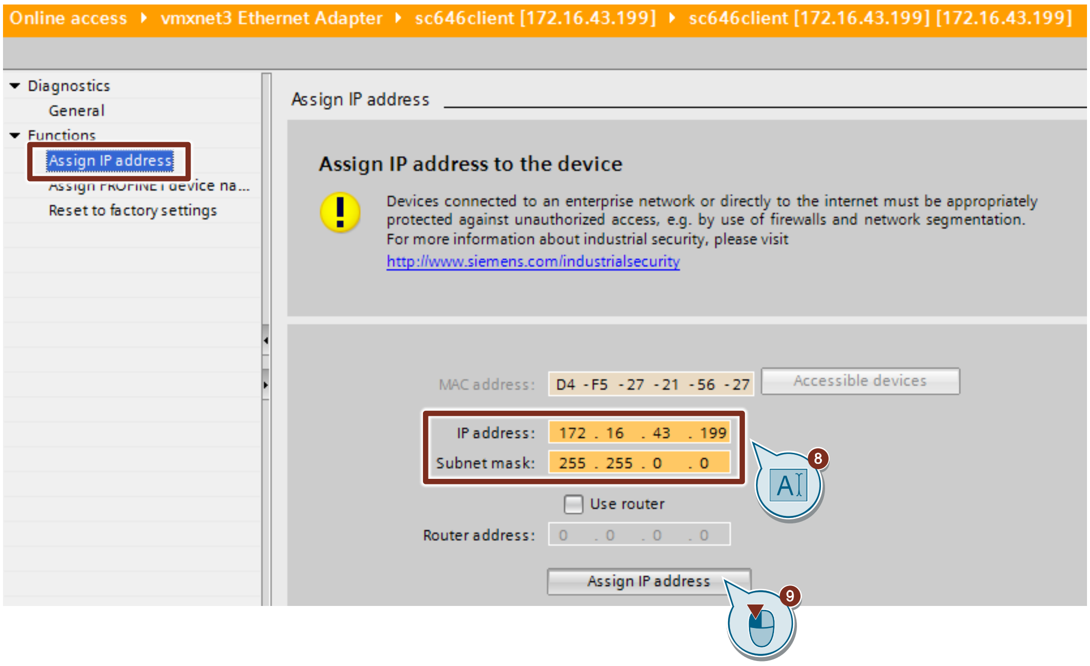
3.2 Assign IP Address to the SCALANCE SC64x-2C

1. Connect the Engineering PC on which TIA Portal is installed to the internal interface of the SCALANCE SC64x-2C.
2. Open TIA Portal.
3. In the Project tree you click the arrow on the left of the "Online access" item. All the available interfaces of the Engineering PC are displayed.
4. Click the arrow on the left of the interface via which the Engineering PC is connected to the internal interface of the SCALANCE SC64x-2C.
5. Double-click the "Update accessible devices" command. The SCALANCE SC64x-2C is displayed with the MAC address.



6. Click the arrow on the left of the SCALANCE SC64x-2C.
7. Double-click the "Online & diagnostics" command. The "Online & Diagnostics" dialog opens.

8. Enter the required parameters under "Functions > Assign IP address":
   - IP address: 172.16.43,199
   - Subnet mask: 255,255.0.0
9. Click the "Assign IP address" button.



Online access ▸ vmxnet3 Ethernet Adapter ▸ sc646client [172.16.43.199] ▸ sc646client [172.16.43.199] [172.16.43.199]

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: D4 -F5 -27 -21 -56 -27

Accessible devices

IP address: 172 . 16 . 43 . 199

Subnet mask: 255 . 255 . 0 . 0

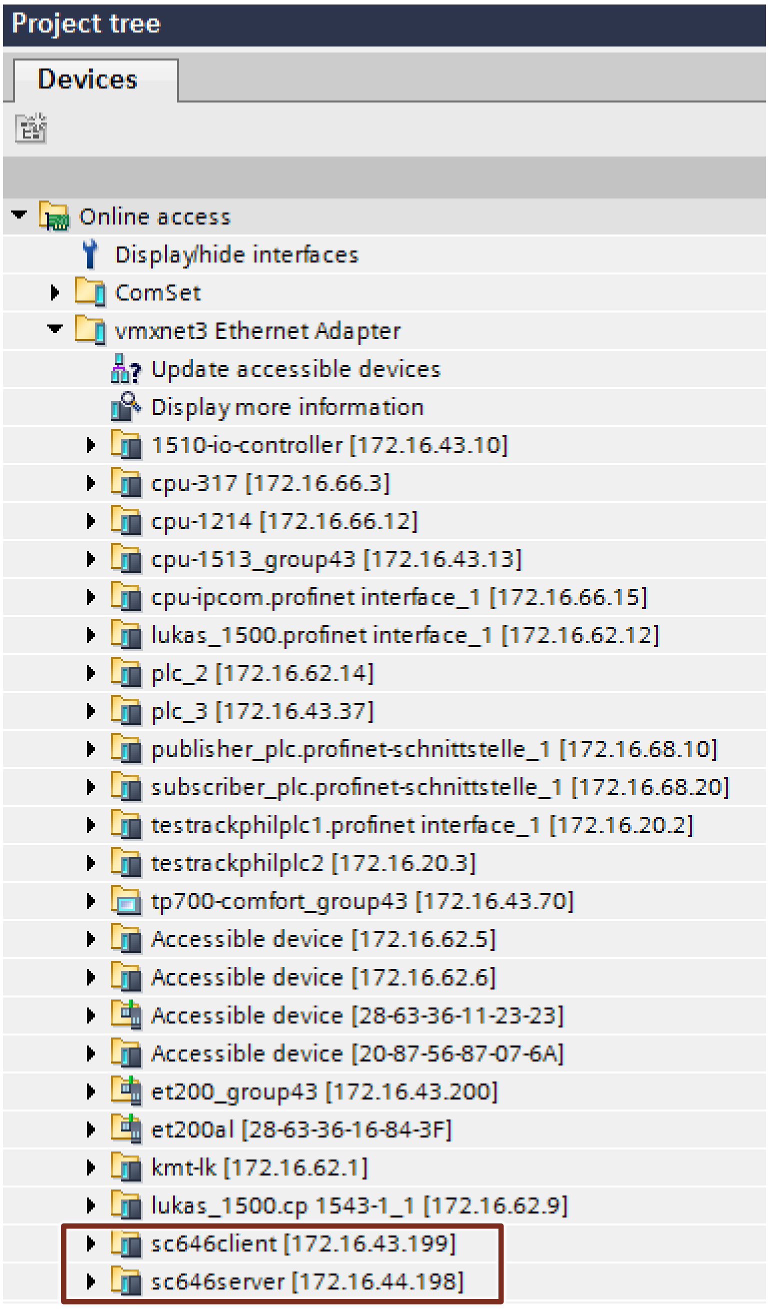
□ Use router

Router address: 0 . 0 . 0 . 0

Result

If the parameters have been successfully transferred to the SCALANCE SC64x-2C, the SCALANCE SC64x-2C can be reached via the assigned IP address.

Figure 3-1



Project tree

Devices

- Online access
  - Display/hide interfaces
  - ComSet
  - vmxnet3 Ethernet Adapter
    - Update accessible devices
    - Display more information
    - 1510-io-controller [172.16.43.10]
    - cpu-317 [172.16.66.3]
    - cpu-1214 [172.16.66.12]
    - cpu-1513_group43 [172.16.43.13]
    - cpu-ipcom.profinet interface_1 [172.16.66.15]
    - lukas_1500.profinet interface_1 [172.16.62.12]
    - plc_2 [172.16.62.14]
    - plc_3 [172.16.43.37]
    - publisher_plc.profinet-schnittstelle_1 [172.16.68.10]
    - subscriber_plc.profinet-schnittstelle_1 [172.16.68.20]
    - testrackphilplc1.profinet interface_1 [172.16.20.2]
    - testrackphilplc2 [172.16.20.3]
    - tp700-comfort_group43 [172.16.43.70]
    - Accessible device [172.16.62.5]
    - Accessible device [172.16.62.6]
    - Accessible device [28-63-36-11-23-23]
    - Accessible device [20-87-56-87-07-6A]
    - et200_group43 [172.16.43.200]
    - et200al [28-63-36-16-84-3F]
    - kmt-lk [172.16.62.1]
    - lukas_1500.cp 1543-1_1 [172.16.62.9]
    - sc646client [172.16.43.199]
    - sc646server [172.16.44.198]

3.3 Configure VPN client

3.3.1 Requirements

You configure the SCALANCE SC64x-2C via the Web Based Management (WBM). The following requirements must be met to access the WBM of the SCALANCE SC64x-2C via a web browser.

- The Engineering PC is connected to the internal interface of the SCALANCE SC64x-2C.
- The SCALANCE SC64x-2C has an IP address that is in the same subnet as the IP address of the Engineering PC.

3.3.2 Start Web Based Management (WBM)

Enter the IP address or the URL of the SCALANCE SC64x-2C in the address field of the web browser.

HTTPS access is enabled by default. If you access the device via HTTP, the address is automatically redirected to HTTPS.

NOTE **Security certificate information**

Since the device can only be administered via encrypted access, it is delivered with a self-signed certificate. In the case of certificates with signatures that the operating system does not know, a security message is generated. You can display the certificate.

A message about the security certificate is displayed. Acknowledge this message and continue loading the page.

Result

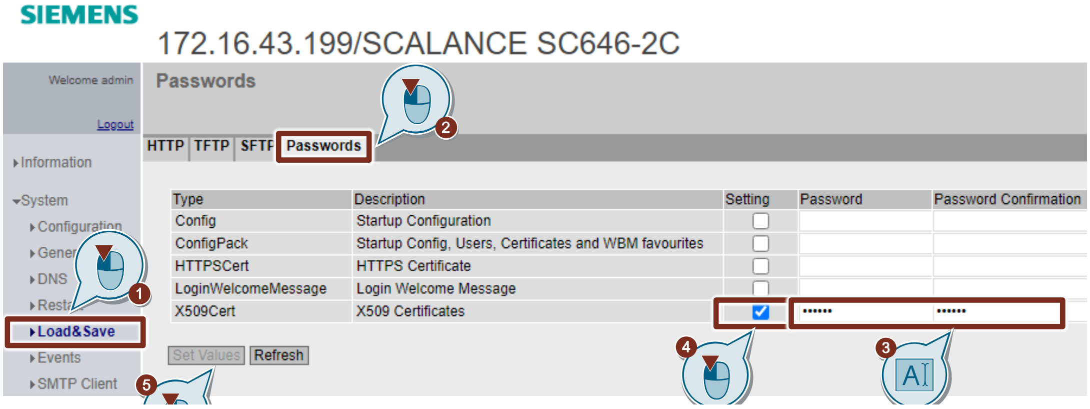
The WBM login page appears.

If you want to access the WBM via an HTTP connection, go to "System > Configuration" for "HTTP Services" and select "Redirect HTTP to HTTPS".

3.3.3 Import Certificates

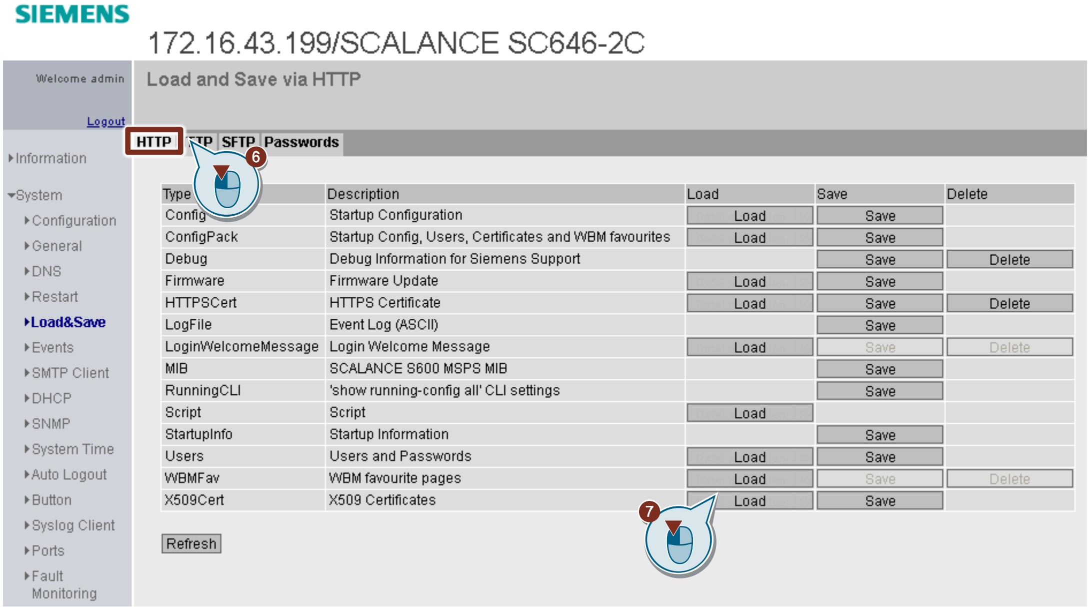
Import

1. In the WBM, you navigate to "System > Load&Save".
2. Open the "Passwords" tab.
3. For X509 Certificates you enter the password for the private key of the device certificate (*.p12).
4. Activate the checkbox in the "Setting" column for X509 certificates.
5. Click the "Set Values" button.



Type	Description	Setting	Password	Password Confirmation
Config	Startup Configuration	☐		
ConfigPack	Startup Config, Users, Certificates and WBM favourites	☐		
HTTPSCert	HTTPS Certificate	☐		
LoginWelcomeMessage	Login Welcome Message	☐		
X509Cert	X509 Certificates	☑	••••••	••••••

6. Open the "HTTP" tab.
7. Click the "Load" button for X509 Certificates.

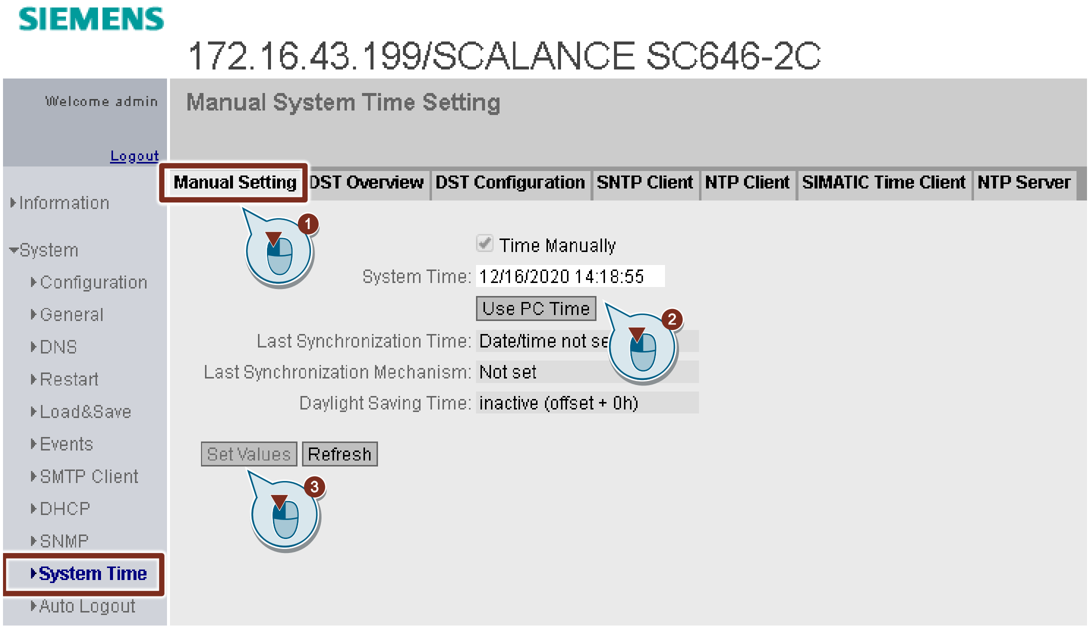


Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users, Certificates and WBM favourites	Load	Save	
Debug	Debug Information for Siemens Support		Save	Delete
Firmware	Firmware Update	Load	Save	
HTTPSCert	HTTPS Certificate	Load	Save	Delete
LogFile	Event Log (ASCII)		Save	
LoginWelcomeMessage	Login Welcome Message	Load	Save	Delete
MIB	SCALANCE S600 MSPS MIB		Save	
RunningCLI	'show running-config all' CLI settings		Save	
Script	Script	Load		
StartupInfo	Startup Information		Save	
Users	Users and Passwords	Load	Save	
WBMFav	WBM favourite pages	Load	Save	Delete
X509Cert	X509 Certificates	Load	Save	

NOTE Load the CA certificate of the certification authority (*.crt) and the device certificate of the VPN client (*.p12).

Set the system time

1. Set the system time manually or set up NTP time synchronization.
   To set the system time manually, you go to "System > System Time" and open the "Manual Setting" tab.
2. Click the "Use PC Time" button.
3. Click the "Set Values" button.



172.16.43.199/SCALANCE SC646-2C

Manual System Time Setting

☑ Time Manually

System Time: 12/16/2020 14:18:55

Last Synchronization Time: Date/time not se

Last Synchronization Mechanism: Not set

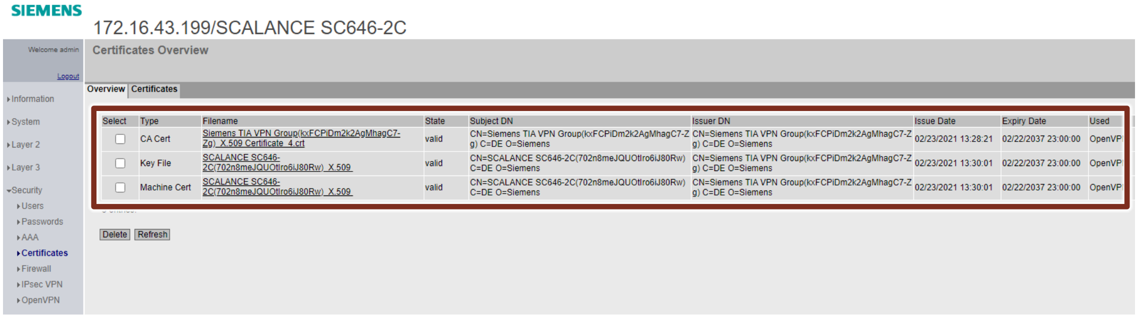
Daylight Saving Time: inactive (offset + 0h)

Result

Go to "Security > Certificates" and open the "Overview" tab. The following certificates are shown as valid here.

- CA certificate
- Key file
- Device certificate

Figure 3-2



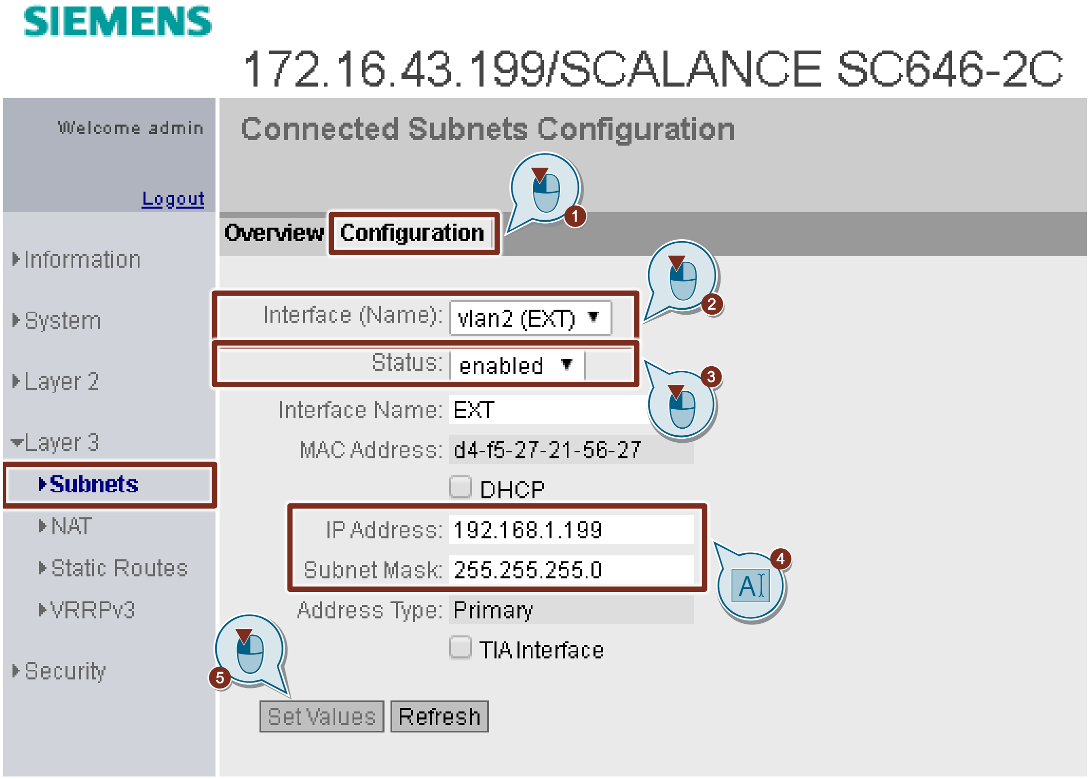
Certificates Overview

Select	Type	Filename	State	Subject DN	Issuer DN	Issue Date	Expiry Date	Used
□	CA Cert	Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg)_X.509 Certificate_4.crt	valid	CN=Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg) C=DE O=Siemens	CN=Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg) C=DE O=Siemens	02/23/2021 13:28:21	02/22/2037 23:00:00	OpenVP
□	Key File	SCALANCE SC646-2C(702n8meJQUOtlro6iJ80Rw)_X.509	valid	CN=SCALANCE SC646-2C(702n8meJQUOtlro6iJ80Rw) C=DE O=Siemens	CN=Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg) C=DE O=Siemens	02/23/2021 13:30:01	02/22/2037 23:00:00	OpenVP
□	Machine Cert	SCALANCE SC646-2C(702n8meJQUOtlro6iJ80Rw)_X.509	valid	CN=SCALANCE SC646-2C(702n8meJQUOtlro6iJ80Rw) C=DE O=Siemens	CN=Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg) C=DE O=Siemens	02/23/2021 13:30:01	02/22/2037 23:00:00	OpenVP

3.3.4 Configure the External Interface

The VPN tunnel is set up on the external interface. Configure the external interface according to the following instructions.

1. Go to "Layer 3 > Subnets" and open the "Configuration" tab.
2. Select the "vlan2 (EXT)" interface.
3. Select the "enabled" status.
4. Enter the required parameters for the external interface:
   - IP address: 192.168.1.199
   - Subnet mask: 255.255.255.0
5. Click the "Set Values" button.



Connected Subnets Configuration

Interface (Name): vlan2 (EXT)

Status: enabled

Interface Name: EXT

MAC Address: d4-f5-27-21-56-27

□ DHCP

IP Address: 192.168.1.199

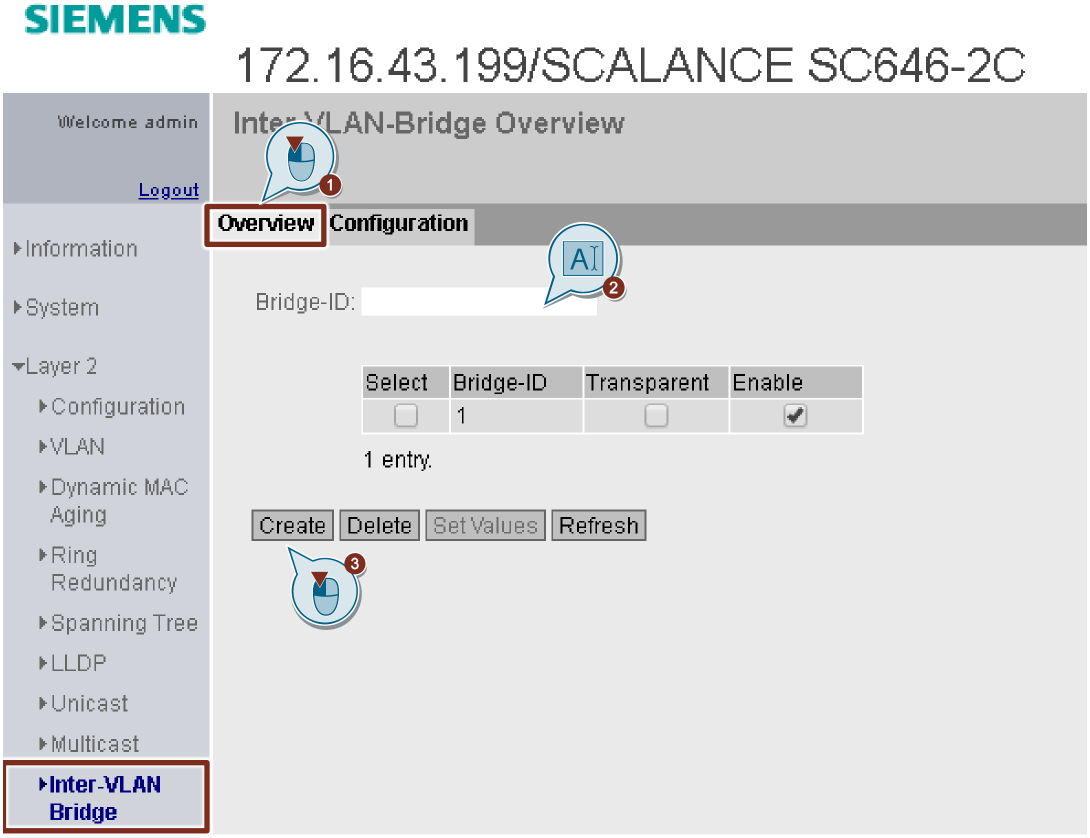
Subnet Mask: 255.255.255.0

Address Type: Primary

□ TIA Interface

3.3.5 Configure a Bridge

1. Go to "Layer 2 > Inter-VLAN Bridge" and open the "Overview" tab.
2. Enter a bridge ID, "1", for example.
3. Click the "Create" button. Bridge ID "1" is created.

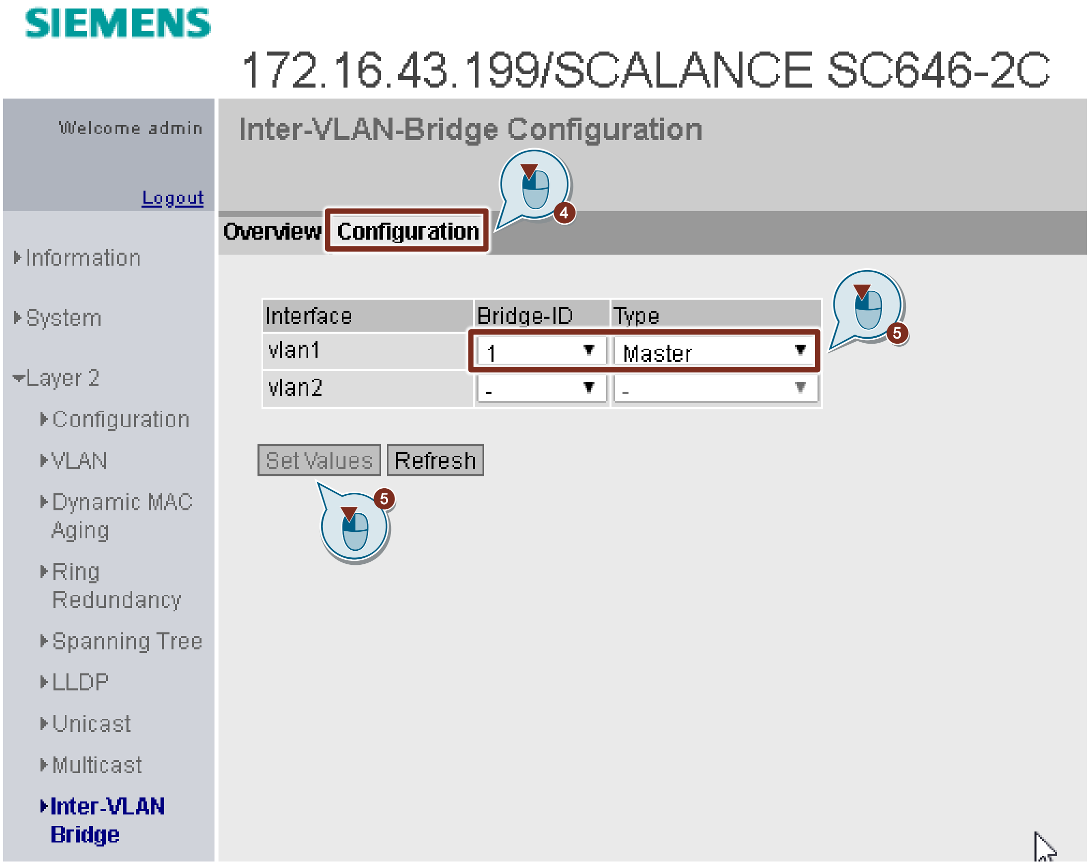


Bridge-ID:

Select	Bridge-ID	Transparent	Enable
□	1	□	☑

1 entry.

4. Open the "Configuration" tab.
5. Assign the vlan1 as master to the bridge ID "1" so that the vlan1 can be reached via the VPN tunnel.
6. Click the "Set Values" button.

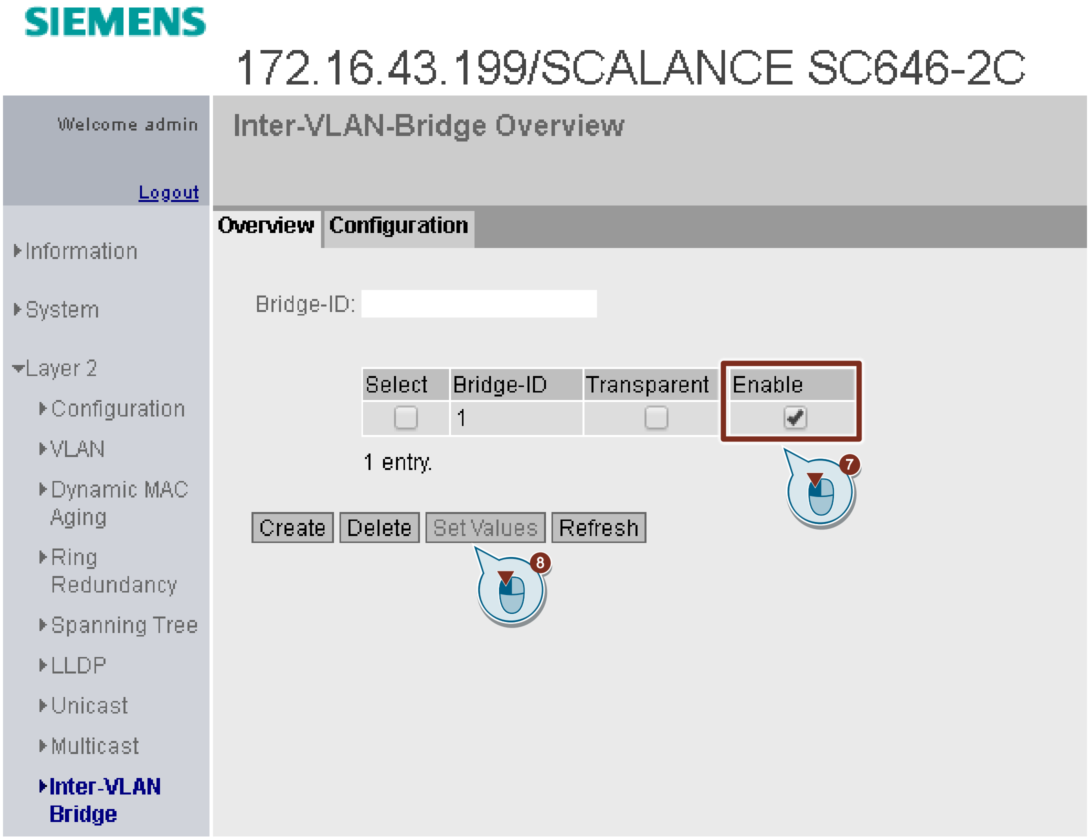


172.16.43.199/SCALANCE SC646-2C

Inter-VLAN-Bridge Configuration

Interface	Bridge-ID	Type
vlan1	1	Master
vlan2	-	-

7. In the "Overview" tab you enable Bridge ID "1".
8. Click the "Set Values" button.



Inter-VLAN-Bridge Overview

Bridge-ID:

Select	Bridge-ID	Transparent	Enable
□	1	□	☑

1 entry.

If you enable the "Transparent" option, the Inter-VLAN bridge and the associated VLANs are switched to Transparent mode when the bridge is activated. Ports belonging to the bridge become transparent ports. This means:

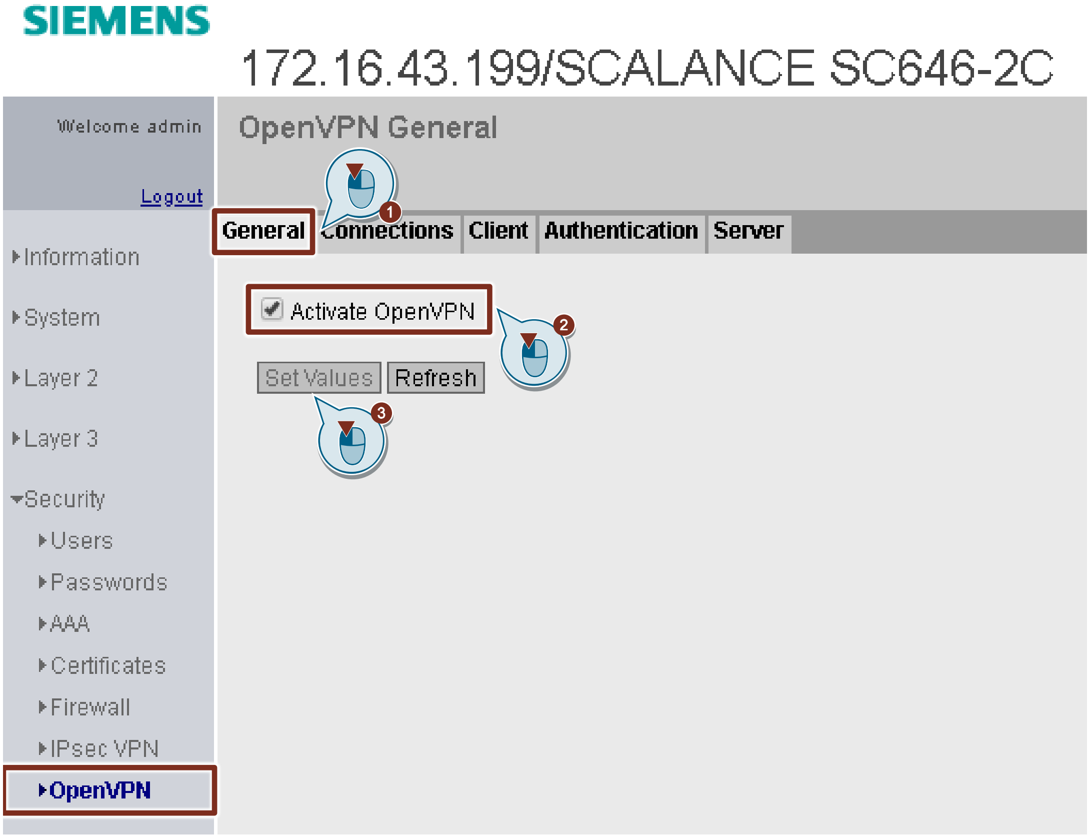
- Tagged messages received at these ports are not evaluated and are forwarded to all other ports of the Inter-VLAN Bridge with unchanged tag. No messages are forwarded from ports that do not belong to the Inter-VLAN Bridge to ports that do belong to the Inter-VLAN Bridge.
- Untagged messages received at these ports are forwarded to all other ports of the Inter-VLAN Bridge likewise untagged.

If you disable the option, the VLAN tags are evaluated.

3.3.6 Configure an OpenVPN Tunnel

OpenVPN aktivieren

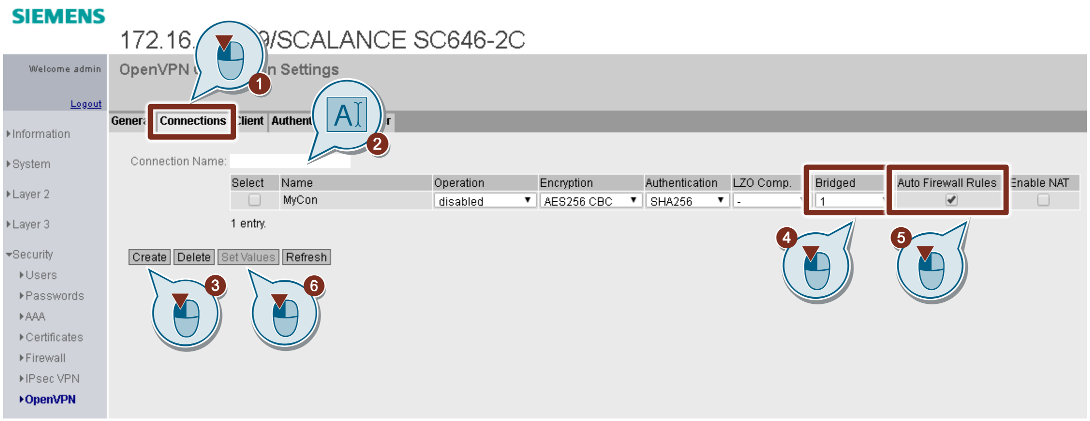
1. Go to "Security > OpenVPN" and open the "General" tab.
2. Enable the "Activate OpenVPN" function.
3. Click the "Set Values" button.



☑ Activate OpenVPN

Create an connection

1. Open the "Connections" tab to create a connection.
2. Enter a connection name, "MyCon", for example.
3. Click the "Create" button.
4. In the "Bridge" column you select the Bridge ID "1" to assign the Bridge ID "1" to the "MyCon" connection.
5. In the "Auto Firewall Rules" column you check the checkbox. This allows Layer 3 traffic and IP traffic through the tunnel.
6. Click the "Set Values" button.



Connection Name:

Select	Name	Operation	Encryption	Authentication	LZO Comp.	Bridged	Auto Firewall Rules	Enable NAT
☐	MyCon	disabled	AES256 CBC	SHA256	-	1	☑	☐

1 entry.

NOTE To change the OpenVPN connection settings, "Operation" must be set to "disabled".

Result

Go to "Security > Firewall" and open the "Predefined MAC Rules" tab.

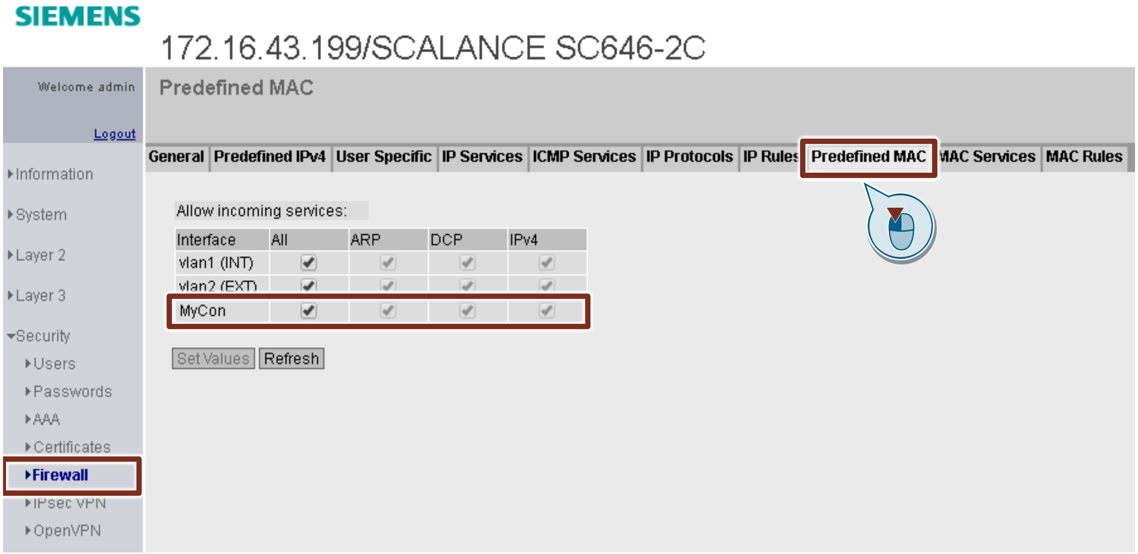
The "MyCon" connection is added automatically and permits the following services by default in the Layer 2 firewall:

- ARP
- DCP
- IPv4

Other services have to be permitted explicitly in the "MAC Rules" tab.

NOTE With the default setting, the services "ARP" and "DCP" as well as any IP traffic via the VPN tunnel are permitted.

Figure 3-3

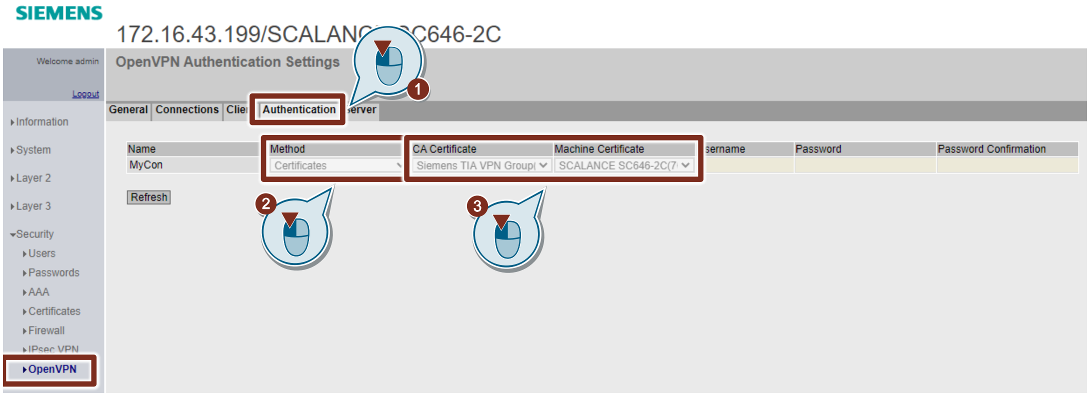


Allow incoming services:

Interface	All	ARP	DCP	IPv4
vlan1 (INT)	☑	☑	☑	☑
vlan2 (EXT)	☑	☑	☑	☑
MyCon	☑	☑	☑	☑

Define the authentication procedure

1. Go to "Security > OpenVPN" and open the "Authentication" tab.
2. Select the "Certificates" method.
3. Select the imported certificates in the following columns:
   - CA certificate
   - Device certificate
4. Click the "Set Values" button.



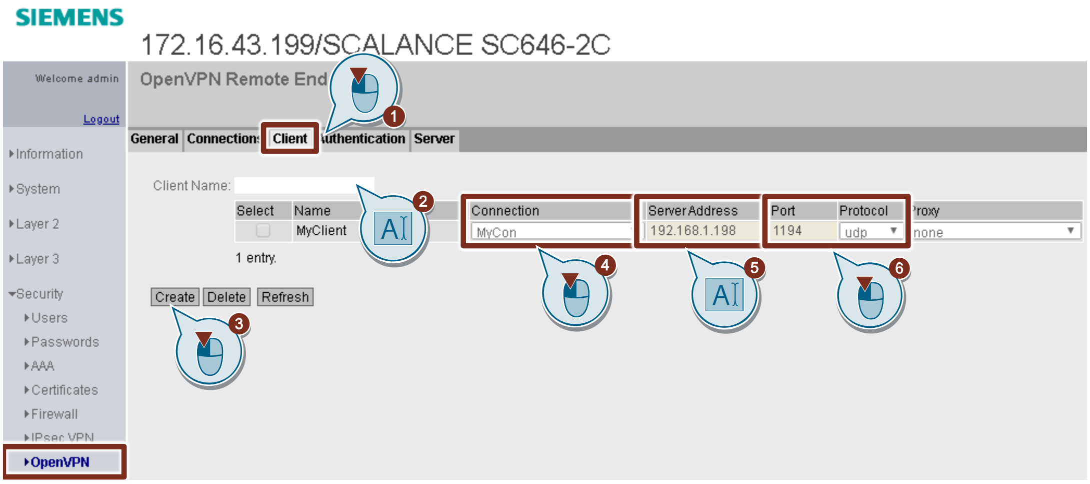
OpenVPN Authentication Settings

Name	Method	CA Certificate	Machine Certificate	sername	Password	Password Confirmation
MyCon	Certificates	Siemens TIA VPN Group(	SCALANCE SC646-2C(7			

NOTE User name and password are also used for authentication. All VPN clients of the VPN server must use the same user name and password.

Settings for VPN client

1. Go to "Security > OpenVPN" and open the "Client" tab.
2. Enter a client name, "MyClient", for example.
3. Click the "Create" button.
4. In the "Connection" column you select the "MyCon" connection.
5. Enter the IP address of the VPN server, 192,168.1,198, for example.
6. Select the protocol and enter the port.
   - Protocol: "udp"
   - Port: 1194 (default)
7. Click the "Set Values" button.



SIEMENS

172.16.43.199/SCALANCE SC646-2C

OpenVPN Remote End

Client Name:

Select	Name	Connection	Server Address	Port	Protocol	Proxy
□	MyClient	MyCon	192.168.1.198	1194	udp	none

1 entry.

3.4 Configure VPN Server

3.4.1 Requirements

The requirements listed in section 3.3.1 must be fulfilled.

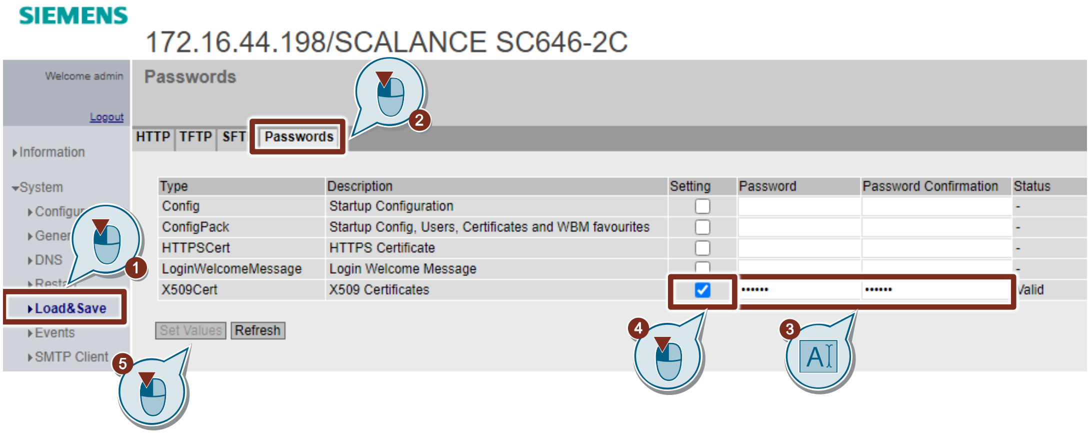
3.4.2 Start Web Based Management (WBM)

Section 3.3.2 describes how to start the WBM.

3.4.3 Import Certificates

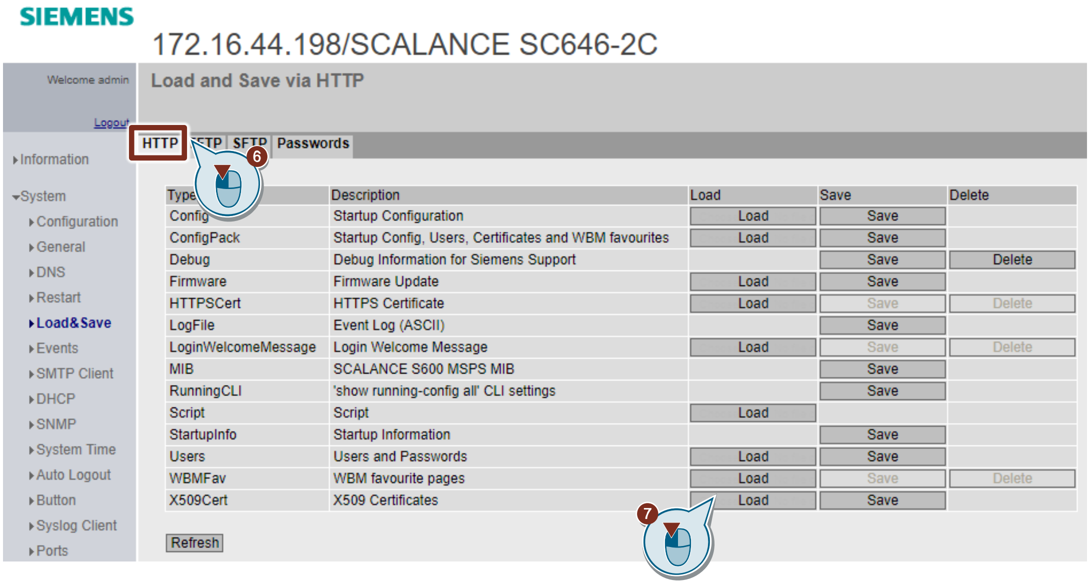
Import

1. In the WBM, you navigate to "System > Load&Save".
2. Open the "Passwords" tab.
3. For X509 Certificates you enter the password for the private key of the device certificate (*.p12).
4. Check the checkbox in the "Setting" column for X509 certificates.
5. Click the "Set Values" button.



Type	Description	Setting	Password	Password Confirmation	Status
Config	Startup Configuration	□			-
ConfigPack	Startup Config, Users, Certificates and WBM favourites	□			-
HTTPSCert	HTTPS Certificate	□			-
LoginWelcomeMessage	Login Welcome Message	□			-
X509Cert	X509 Certificates	☑	••••••	••••••	Valid

6. Open the "HTTP" tab.
7. Click the "Load" button for X509 Certificates.



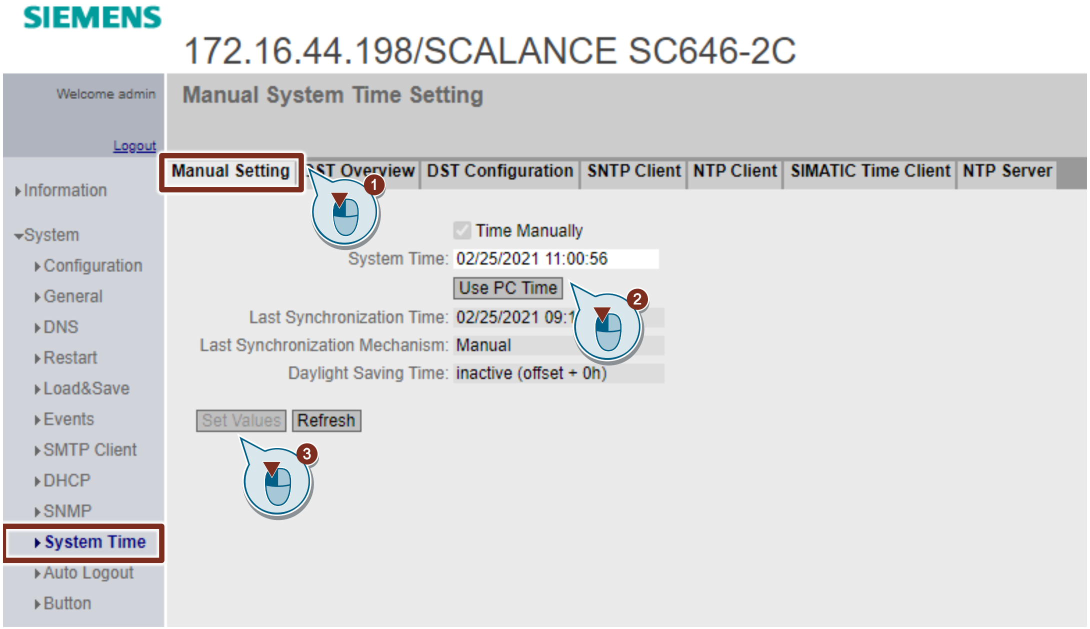
Load and Save via HTTP

Type	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users, Certificates and WBM favourites	Load	Save	
Debug	Debug Information for Siemens Support		Save	Delete
Firmware	Firmware Update	Load	Save	
HTTPSCert	HTTPS Certificate	Load	Save	Delete
LogFile	Event Log (ASCII)		Save	
LoginWelcomeMessage	Login Welcome Message	Load	Save	Delete
MIB	SCALANCE S600 MSPS MIB		Save	
RunningCLI	'show running-config all' CLI settings		Save	
Script	Script	Load		
StartupInfo	Startup Information		Save	
Users	Users and Passwords	Load	Save	
WBMFav	WBM favourite pages	Load	Save	Delete
X509Cert	X509 Certificates	Load	Save	

NOTE Load the CA certificate of the certification authority (*.crt) and the device certificate of the VPN server (*.p12).

Set the system time

1. Set the system time manually or set up NTP time synchronization.
   To set the system time manually, you go to "System > System Time" and open the "Manual Setting" tab.
2. Click the "Use PC Time" button.
3. Click the "Set Values" button.



Manual System Time Setting

☑ Time Manually

System Time: 02/25/2021 11:00:56

Last Synchronization Time: 02/25/2021 09:1

Last Synchronization Mechanism: Manual

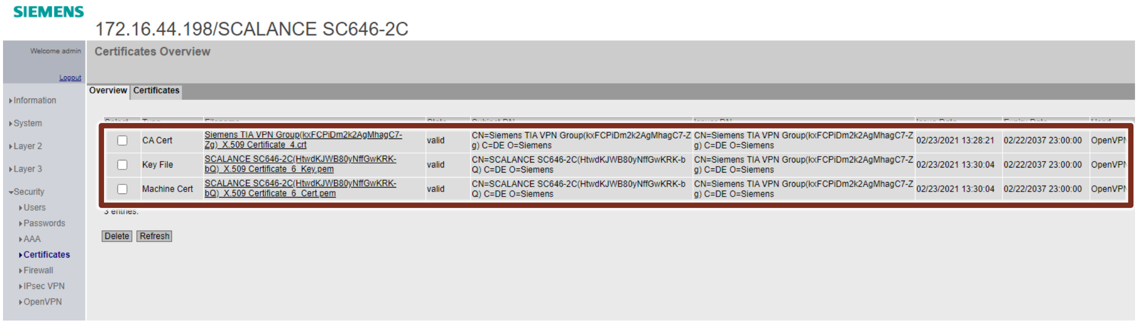
Daylight Saving Time: inactive (offset + 0h)

Result

Go to "Security > Certificates" and open the "Overview" tab. The following certificates are shown as valid here.

- CA certificate
- Key file
- Device certificate

Figure 3-4



Certificates Overview

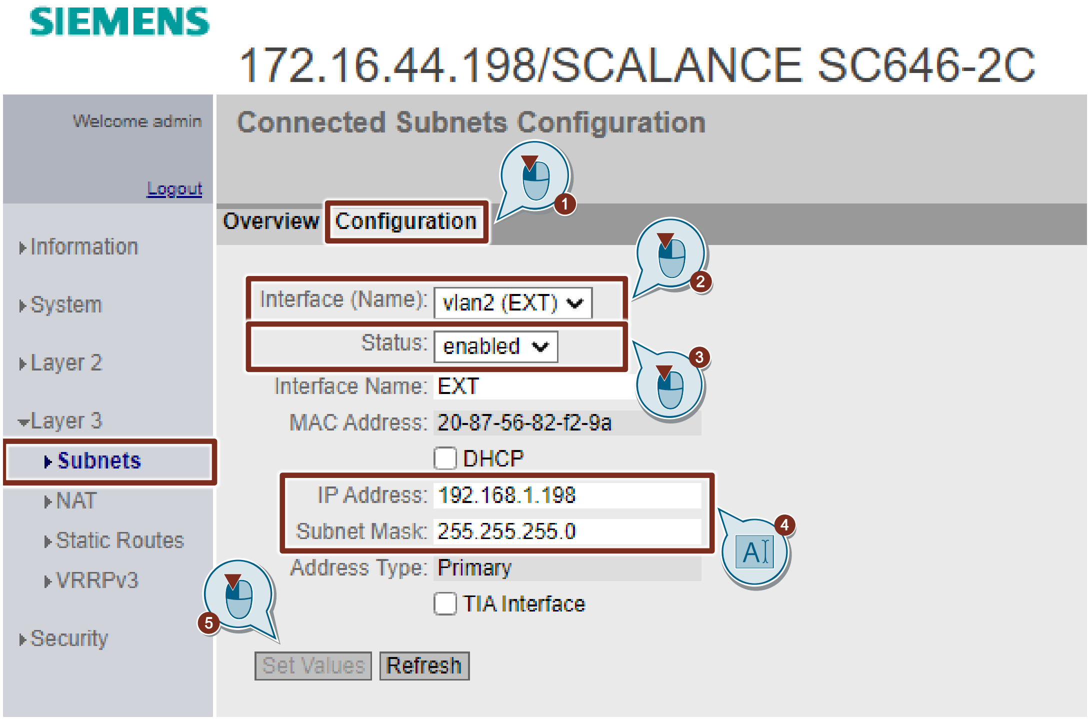
□	CA Cert	Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg)_X.509 Certificate_4.crt	valid	CN=Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg) C=DE O=Siemens	CN=Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg) C=DE O=Siemens	02/23/2021 13:28:21	02/22/2037 23:00:00	OpenVPN
□	Key File	SCALANCE SC646-2C(HtwdKJWB80yNffGwKRK-bQ)_X.509 Certificate_6_Key.pem	valid	CN=SCALANCE SC646-2C(HtwdKJWB80yNffGwKRK-bQ) C=DE O=Siemens	CN=Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg) C=DE O=Siemens	02/23/2021 13:30:04	02/22/2037 23:00:00	OpenVPN
□	Machine Cert	SCALANCE SC646-2C(HtwdKJWB80yNffGwKRK-bQ)_X.509 Certificate_6_Cert.pem	valid	CN=SCALANCE SC646-2C(HtwdKJWB80yNffGwKRK-bQ) C=DE O=Siemens	CN=Siemens TIA VPN Group(kxFCPiDm2k2AgMhagC7-Zg) C=DE O=Siemens	02/23/2021 13:30:04	02/22/2037 23:00:00	OpenVPN

3 entries.

3.4.4 Configure the External Interface

The VPN tunnel is set up on the external interface. Configure the external interface according to the following instructions.

1. Go to "Layer 3 > Subnets" and open the "Configuration" tab.
2. Select the "vlan2 (EXT)" interface.
3. Select the "enabled" status.
4. Enter the required parameters for the external interface:
   - IP address: 192.168.1.198
   - Subnet mask: 255.255.255.0
5. Click the "Set Values" button.



Connected Subnets Configuration

Interface (Name): vlan2 (EXT)

Status: enabled

Interface Name: EXT

MAC Address: 20-87-56-82-f2-9a

□ DHCP

IP Address: 192.168.1.198

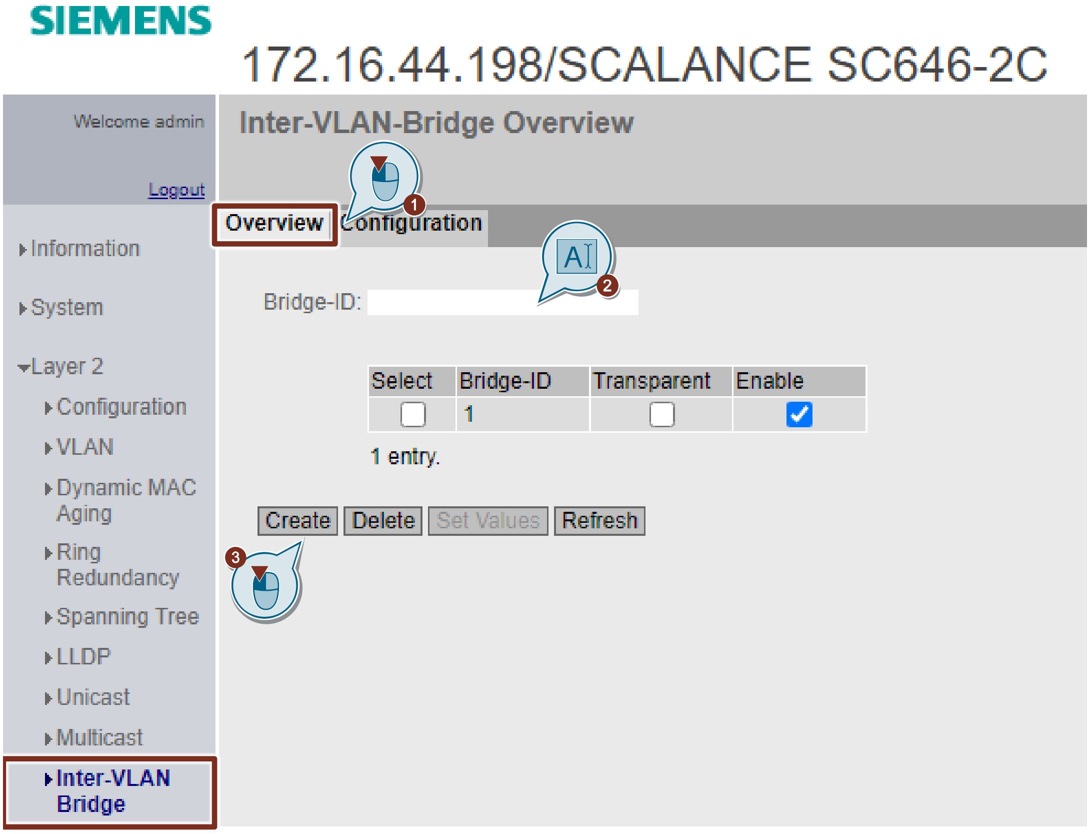
Subnet Mask: 255.255.255.0

Address Type: Primary

□ TIA Interface

3.4.5 Configure a Bridge

1. Go to "Layer 2 > Inter-VLAN Bridge" and open the "Overview" tab.
2. Enter a bridge ID, "1", for example.
3. Click the "Create" button. Bridge ID "1" is created.

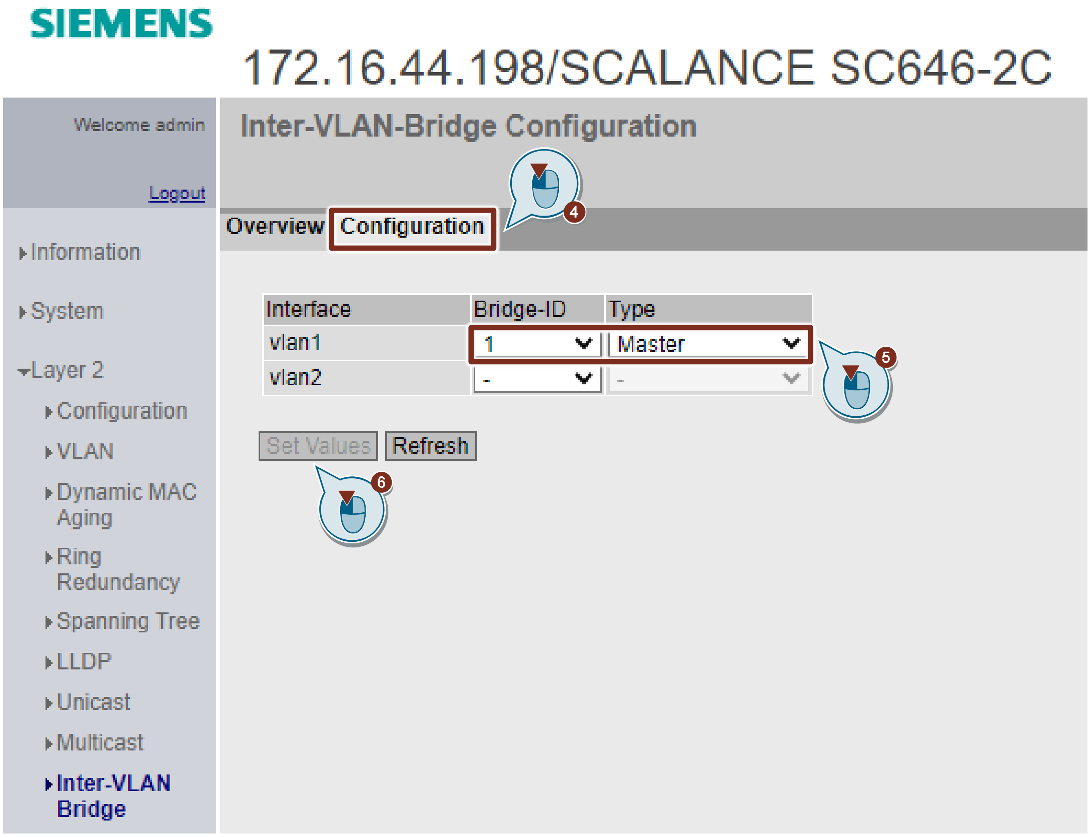


Bridge-ID:

Select	Bridge-ID	Transparent	Enable
☐	1	☐	☑

1 entry.

4. Open the "Configuration" tab.
5. Assign the vlan1 as master to the bridge ID "1" so that the vlan1 can be reached via the VPN tunnel.
6. Click the "Set Values" button.

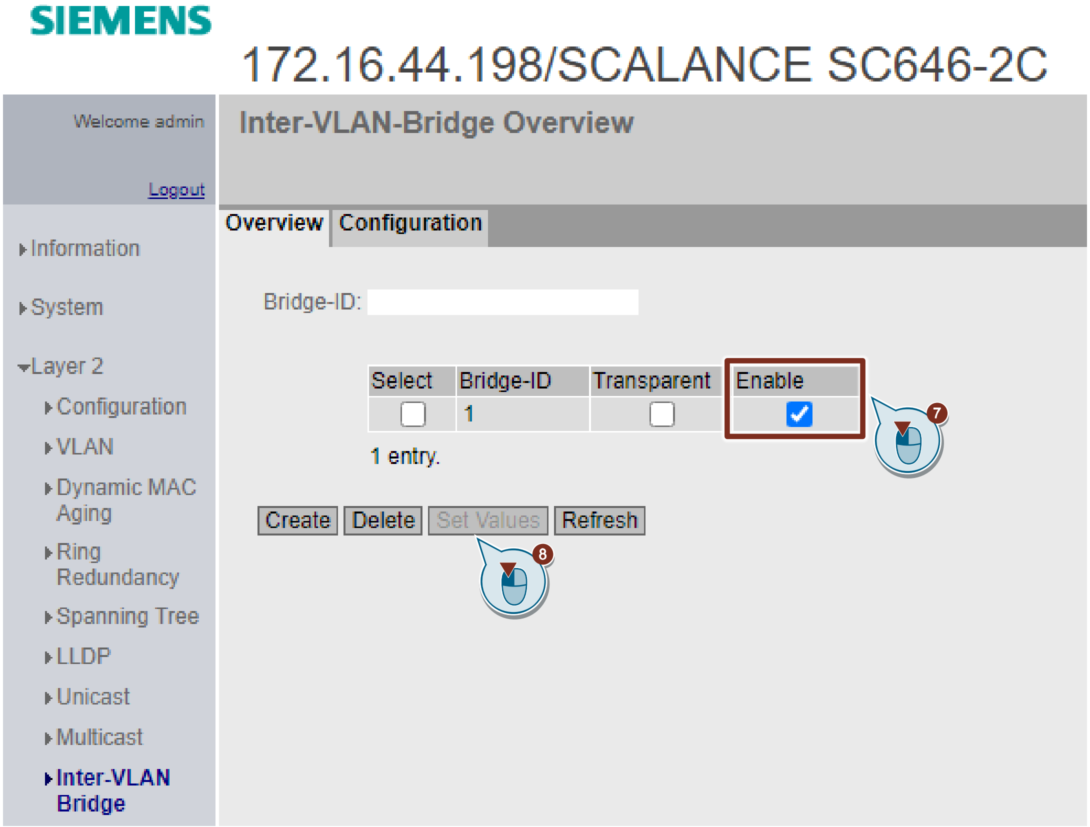


172.16.44.198/SCALANCE SC646-2C

Inter-VLAN-Bridge Configuration

Interface	Bridge-ID	Type
vlan1	1	Master
vlan2	-	-

7. In the "Overview" tab you enable Bridge ID "1".
8. Click the "Set Values" button.



Bridge-ID:

Select	Bridge-ID	Transparent	Enable
□	1	□	☑

1 entry.

If you enable the "Transparent" option, the Inter-VLAN bridge and the associated VLANs are switched to Transparent mode when the bridge is activated. Ports belonging to the bridge become transparent ports. This means:

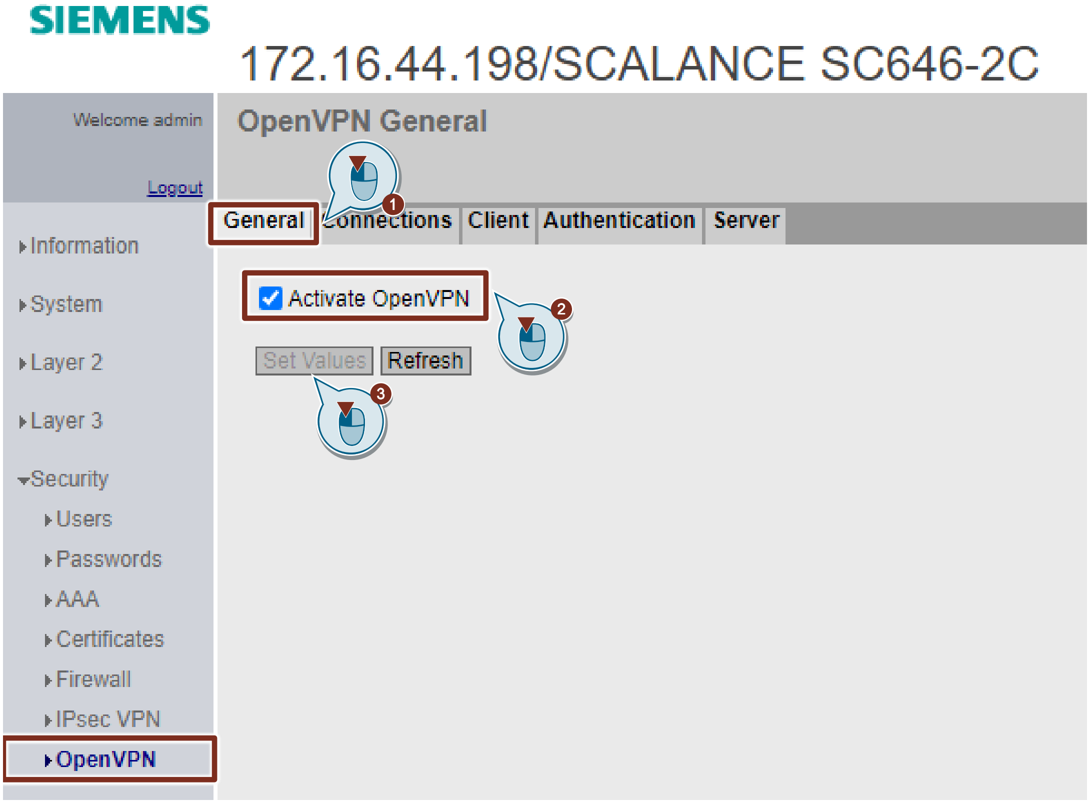
- Tagged messages received at these ports are not evaluated and are forwarded to all other ports of the Inter-VLAN Bridge with unchanged tag. No messages are forwarded from ports that do not belong to the Inter-VLAN Bridge to ports that do belong to the Inter-VLAN Bridge.
- Untagged messages received at these ports are forwarded to all other ports of the Inter-VLAN Bridge likewise untagged.

If you disable the option, the VLAN tags are evaluated.

3.4.6 Configure an OpenVPN-Tunnel

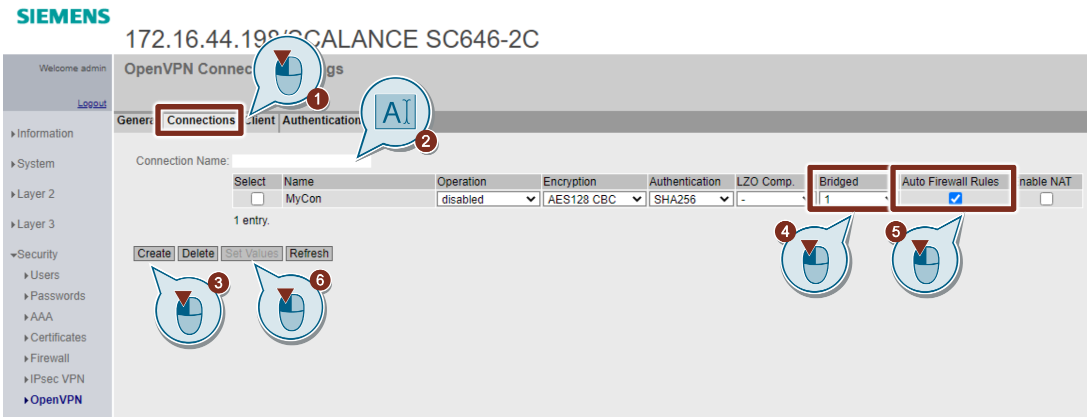
Activate OpenVPN

1. Go to "Security > OpenVPN" and open the "General" tab.
2. Enable the "Activate OpenVPN" function.
3. Click the "Set Values" button.



Create a connection

1. Open the "Connections" tab to create a connection.
2. Enter a connection name, "MyCon", for example.
3. Click the "Create" button.
4. In the "Bridge" column you select the Bridge ID "1" to assign the Bridge ID "1" to the "MyCon" connection.
5. In the "Auto Firewall Rules" column you check the checkbox. This allows Layer 3 traffic and IP traffic through the tunnel.
6. Click the "Set Values" button.



172.16.44.19 SCALANCE SC646-2C

OpenVPN Connec gs

Connection Name:

Select	Name	Operation	Encryption	Authentication	LZO Comp.	Bridged	Auto Firewall Rules	nable NAT
□	MyCon	disabled	AES128 CBC	SHA256	-	1	☑	□

1 entry.

NOTE To change the OpenVPN connection settings, "Operation" must be set to "disabled".

Result

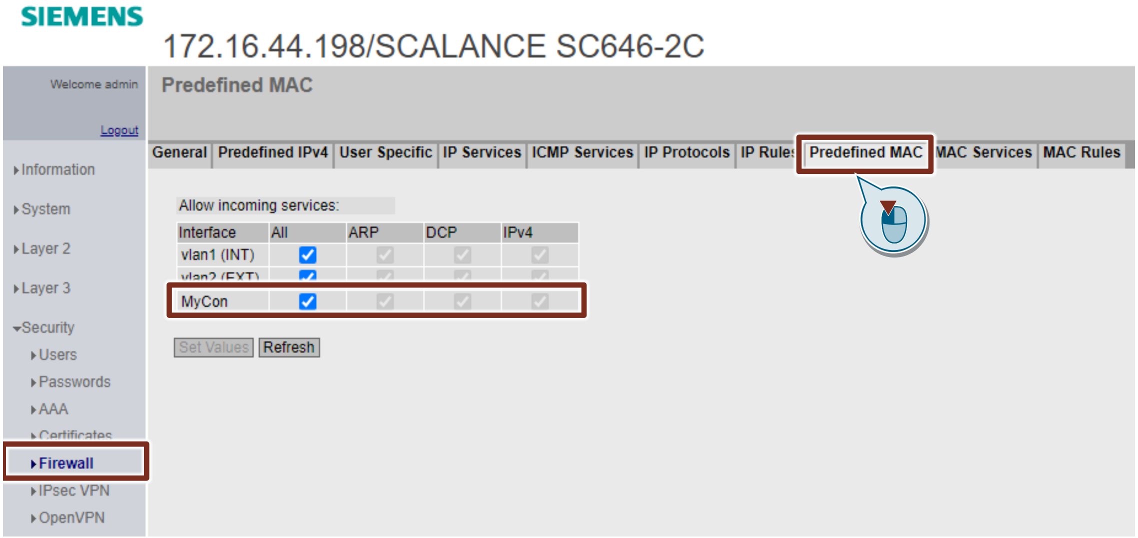
Go to "Security > Firewall" and open the "Predefined MAC Rules" tab.

The "MyCon" connection is added automatically and permits the following services by default in the Layer 2 firewall:

- ARP
- DCP
- IPv4
- Other services have to be permitted explicitly in the "MAC Rules" tab.

NOTE With the default setting, the services "ARP" and "DCP" as well as any IP traffic via the VPN tunnel are permitted.

Figure 3-5



172.16.44.198/SCALANCE SC646-2C

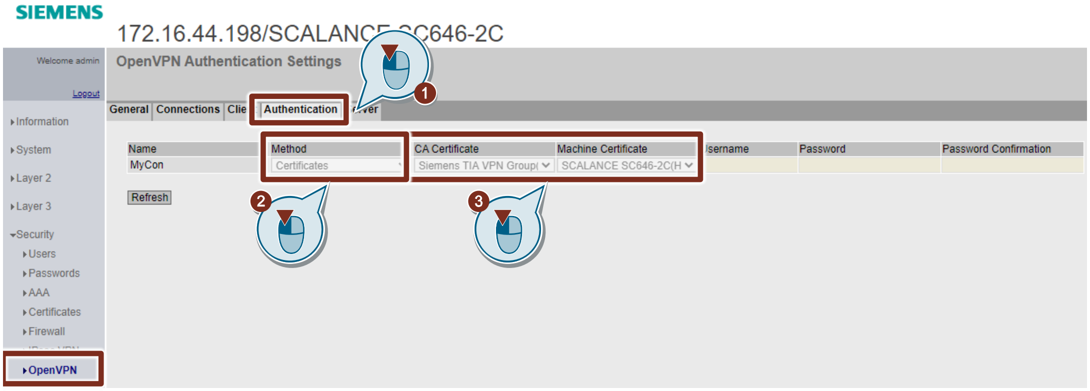
Predefined MAC

Allow incoming services:

Interface	All	ARP	DCP	IPv4
vlan1 (INT)	☑	☑	☑	☑
vlan2 (EXT)	☑	☑	☑	☑
MyCon	☑	☑	☑	☑

Define the authentication procedure

1. Go to "Security > OpenVPN" and open the "Authentication" tab.
2. Select the "Certificates" method.
3. Select the imported certificates in the following columns:
   - CA certificate
   - Device certificate
4. Click the "Set Values" button.



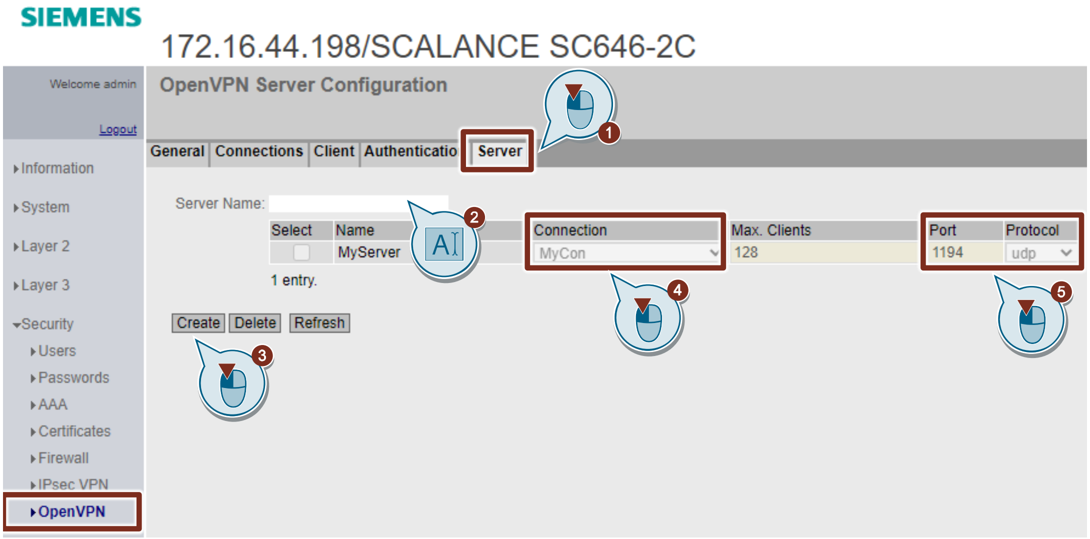
OpenVPN Authentication Settings

Name	Method	CA Certificate	Machine Certificate	sername	Password	Password Confirmation
MyCon	Certificates	Siemens TIA VPN Group(	SCALANCE SC646-2C(H			

NOTE User name and password are also used for authentication.

Settings for VPN server

1. Go to "Security > OpenVPN" and open the "Server" tab.
2. Enter a server name, "MyServer", for example.
3. Click the "Create" button.
4. In the "Connection" column you select the "MyCon" connection.
5. Select the protocol and enter the port.
   - Protocol: "udp"
   - Port: 1194 (default)
6. Click the "Set Values" button.



172.16.44.198/SCALANCE SC646-2C

OpenVPN Server Configuration

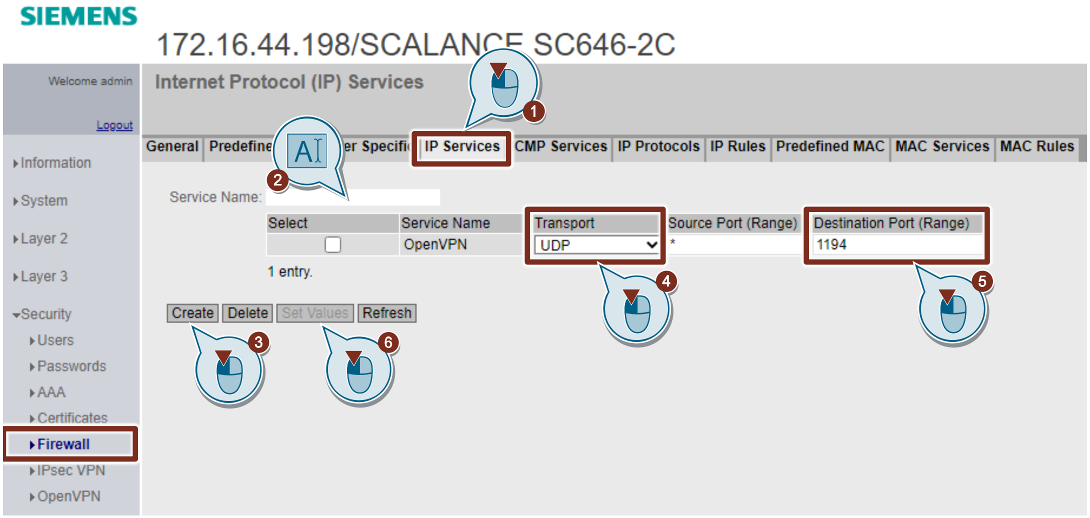
Server Name:

Select	Name	Connection	Max. Clients	Port	Protocol
□	MyServer	MyCon	128	1194	udp

1 entry.

Create IP service

1. Go to "Security > Firewall" and open the "IP Services" tab.
2. Enter a name for the service, "OpenVPN", for example.
3. Click the "Create" button.
4. Configure the service according to the VPN settings. In the "Transport" column, select the "UDP" protocol.
5. In the "Destination Port (Range)" column, select port "1194".
6. Click the "Set Values" button.



172.16.44.198/SCALANCE SC646-2C

Internet Protocol (IP) Services

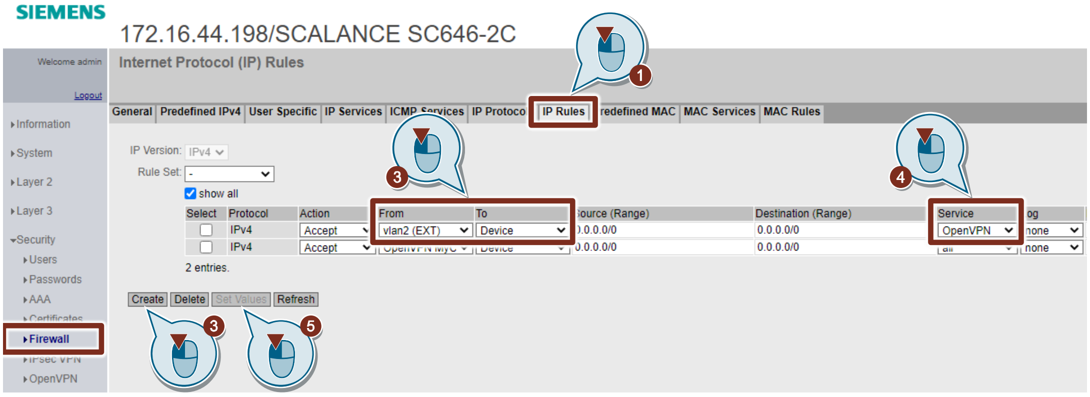
Service Name:

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)
□	OpenVPN	UDP	*	1194

1 entry.

Create IP rule

1. Go to "Security > Firewall" and open the "IP Rules" tab.
2. Click the "Create" button to create a new IP rule.
3. Create an IP rule that permits access from "vlan2 (EXT)" to "Device".
4. In the "Service" column, select the previously created IP service "OpenVPN”.
5. In the "Action" column, select the "Accept" item.
6. Click the "Set Values" button.



Internet Protocol (IP) Rules

IP Version: IPv4

Rule Set: -

☑ show all

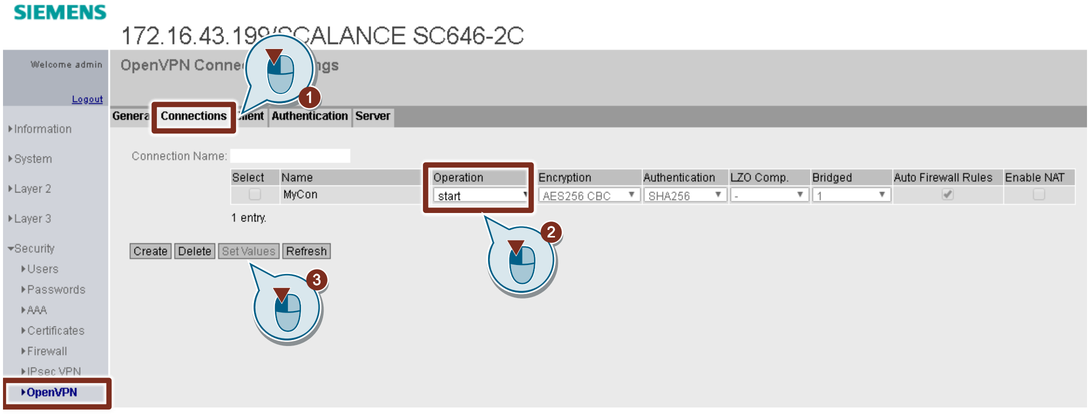
Select	Protocol	Action	From	To	ource (Range)	Destination (Range)	Service	og
□	IPv4	Accept	vlan2 (EXT)	Device	).0.0.0/0	0.0.0.0/0	OpenVPN	none
□	IPv4	Accept	OpenVPN MyC	Device	).0.0.0/0	0.0.0.0/0	all	none

2 entries.

3.5 Start OpenVPN Connection

Start OpenVPN connection in the VPN client

1. In the VPN client, go to "Security > OpenVPN" and open the "Connections" tab.
2. In the "Operation" column, select the "start" item.
3. Click the "Set Values" button.



OpenVPN Conne ngs

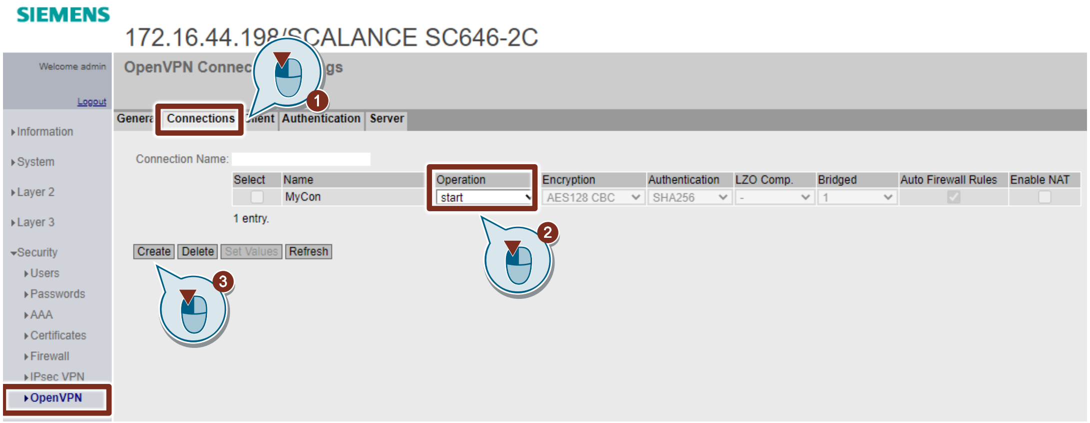
Connection Name:

Select	Name	Operation	Encryption	Authentication	LZO Comp.	Bridged	Auto Firewall Rules	Enable NAT
□	MyCon	start	AES256 CBC	SHA256	-	1	☑	□

1 entry.

Start OpenVPN connection in the VPN server

1. In the VPN server, go to "Security > OpenVPN" and open the "Connections" tab.
2. In the "Operation" column, select the "start" item.
3. Click the "Set Values" button.



Connection Name:

Select	Name	Operation	Encryption	Authentication	LZO Comp.	Bridged	Auto Firewall Rules	Enable NAT
□	MyCon	start	AES128 CBC	SHA256	-	1	☑	□

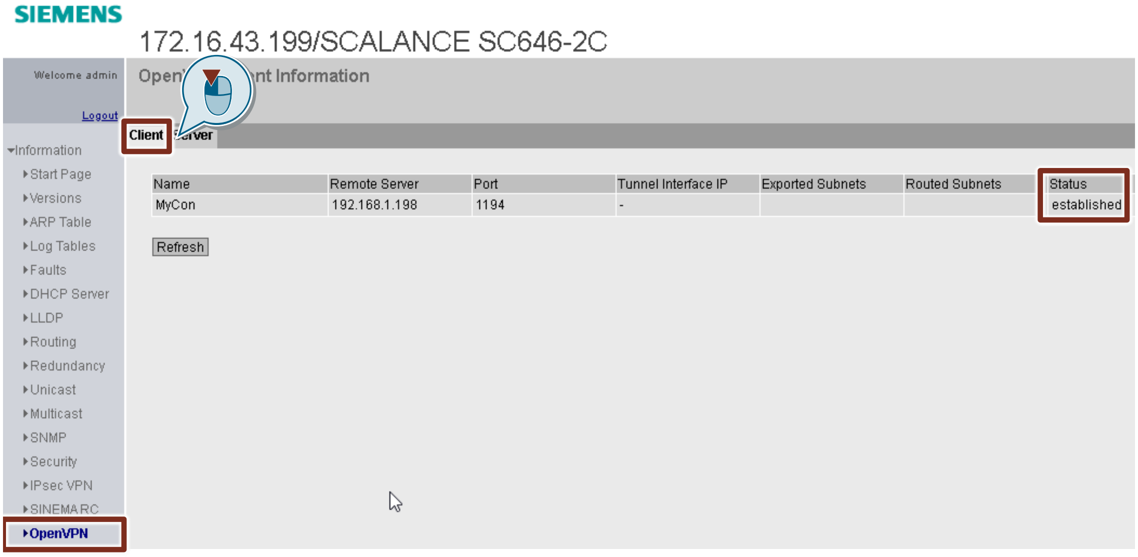
1 entry.

Result

In the VPN client, go to "Information > OpenVPN" and open the "Client" tab.

The status of the OpenVPN tunnel is displayed. The OpenVPN tunnel is established.

Figure 3-6

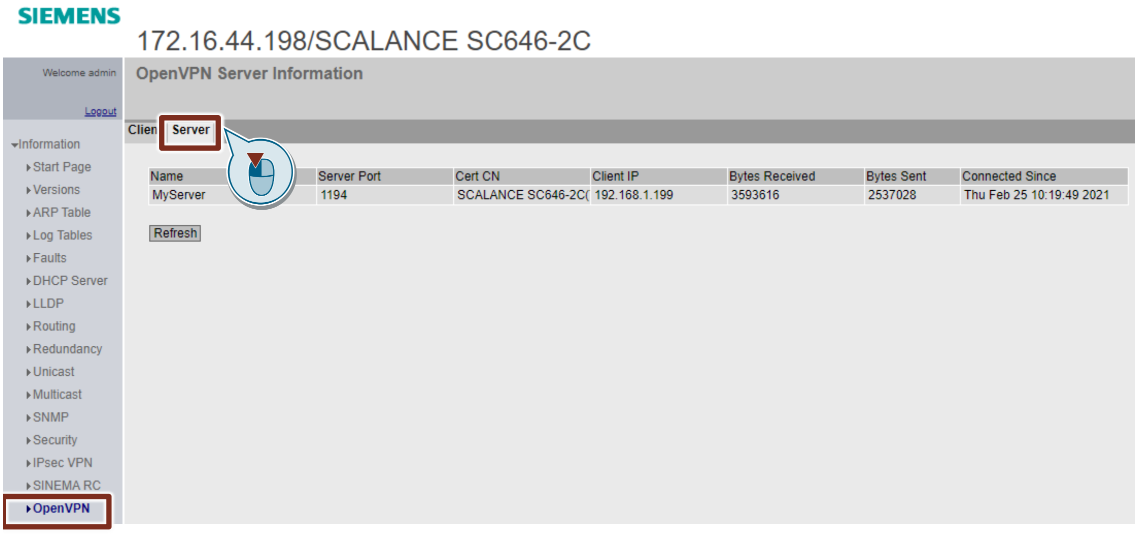


Name	Remote Server	Port	Tunnel Interface IP	Exported Subnets	Routed Subnets	Status
MyCon	192.168.1.198	1194	-			established

In the VPN server, go to "Information > OpenVPN" and open the "Server" tab.

The OpenVPN connection is displayed.

Figure 3-7



172.16.44.198/SCALANCE SC646-2C

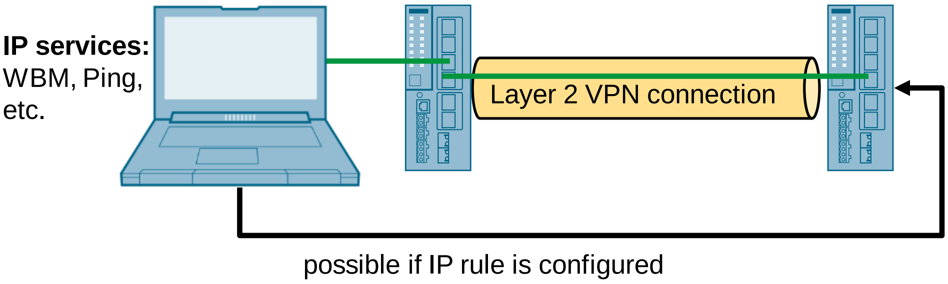
OpenVPN Server Information

Name	Server Port	Cert CN	Client IP	Bytes Received	Bytes Sent	Connected Since
MyServer	1194	SCALANCE SC646-2C(	192.168.1.199	3593616	2537028	Thu Feb 25 10:19:49 2021

3.6 Further Informationen

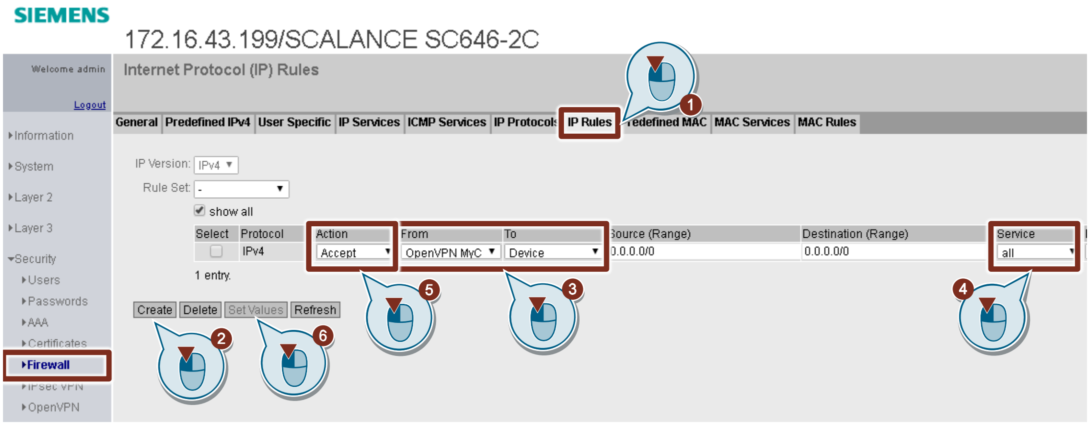
Create IP rule to access the internal IP-address of the tunnel partner

Figure 3-8



If the internal IP address of the tunnel partner is to be accessible, to access the WBM or ping, for example, it is necessary to create an IP rule.

1. In the VPN client, go to "Security > Firewall" and open the "IP Rules" tab.
2. Click the "Create" button to create a new IP rule.
3. Create an IP rule that permits access from the OpenVPN connection to "Device".
4. In the "Service" column, select the "all" item.
5. In the "Action" column, select the "Accept" item.
6. Click the "Set Values" button.



172.16.43.199/SCALANCE SC646-2C

Internet Protocol (IP) Rules

IP Version: IPv4

Rule Set: -

☑ show all

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service
□	IPv4	Accept	OpenVPN MyC	Device	0.0.0.0/0	0.0.0.0/0	all

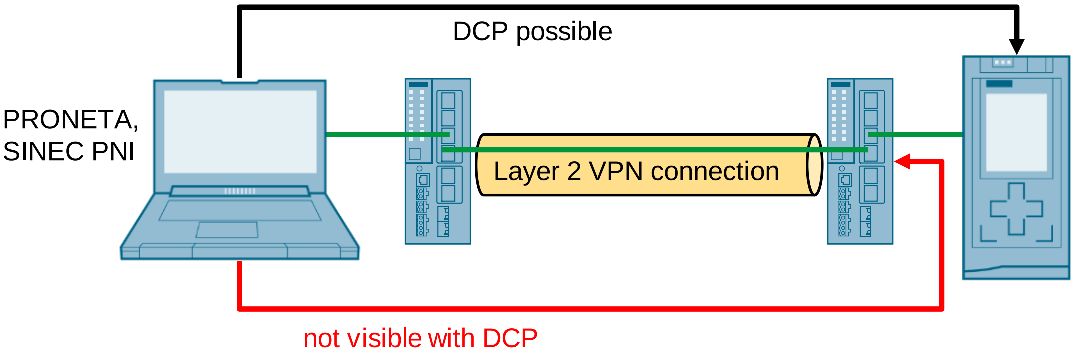
1 entry.

NOTE Create the IP rule in the VPN client and in the VPN server.

Visibility via DCP (Discovery and Configuration Protocol)

The internal interface of the tunnel partner is not visible via DCP (Discovery and Configuration Protocol). The devices connected to the internal interface of the tunnel partner are visible via DCP.

Figure 3-9


DCP possible
PRONETA,
SINEC PNI
Layer 2 VPN connection
not visible with DCP