SIEMENS

Preface

Configure timeout for VPN connection 1

Timeout for VPN connections

Getting Started

07/2020
C79000-G8976-C575-02

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-C575-02
℗ 06/2020 Subject to change

Copyright © Siemens AG 2020.
All rights reserved

Preface

Information on timeout

Purpose

Using an example, a timeout is configured for the VPN tunnel.

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

The designation . . .	stands for . . .
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

Preface **3**

1 Configure timeout for VPN connection **9**

1.1 Introduction 9

1.2 Configuring a VPN connection on the SINEMA RC Server 11

1.3 Configuring VPN connection on the device 12

1.4 Establishing the VPN connection 14

Index **15**

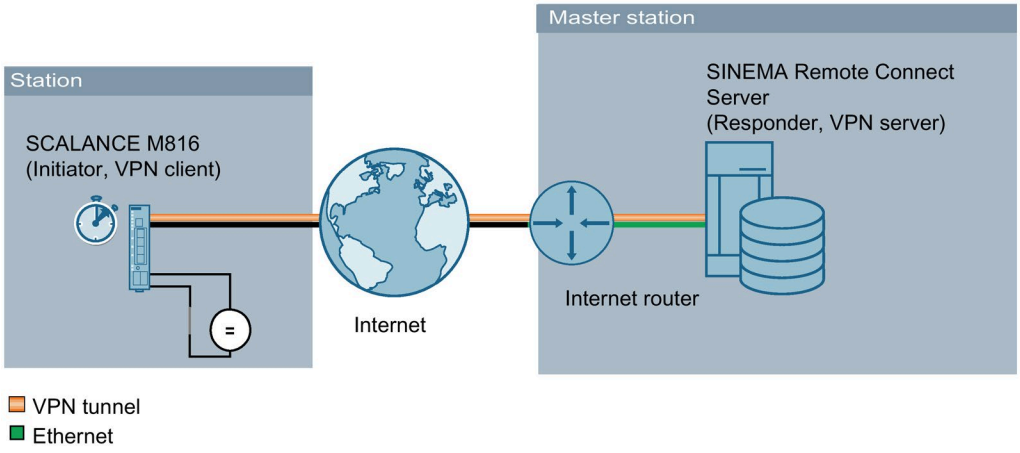
Configure timeout for VPN connection

1

1.1 Introduction

It is possible to automatically disconnect an existing VPN connection (IPsec, OpenVPN, and SINEMA RC) after a defined time without any activity. In the example configuration, the VPN tunnel to the SINEMA RC Server is set up via the digital input. A pushbutton is connected to the digital input of the M816. When the pushbutton is closed, a voltage is present at the digital input, the DI LED lights up, the event "VPN tunnel" is triggered, and the VPN connection to the SINEMA RC Server is established.

The VPN connection is automatically disconnected after 30 minutes of inactivity even though the signal 1 (TRUE/HIGH) is present at the digital input. To set up a VPN tunnel to the SINEMA RC Server again, the digital input is opened and closed. You can also configure the timeout in case of inactivity via OpenVPN and IPsec for VPN connections.



Required devices/components

Master station

- 1 x PC on which the SINEMA RC Server is installed.
- 1 x PC for configuring the SINEMA RC Server
- 1 x DSL port with static WAN IP address and a DSL router.

Station

- 1 x M816 (additional option: a suitably installed standard rail with fittings)
- 1 x DSL port with dynamic WAN IP address
- 1 x 24 V power supply with cable connector and terminal block plug
- 1 x PC for configuration
- The required network cables, TP cables (twisted pair) complying with the IE FC RJ45 standard for Industrial Ethernet.

Note

You can also use another SCALANCE M-800 or SC-600 device. The configuration described below relates explicitly to the components mentioned in the Section "Required devices/components".

Settings used

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

	Name	Interface	IP address
Master station LAN	SINEMA RC Server (VPN server)	LAN port	192.168.20.250
		WAN port	255.255.255.0 The WAN IP address via which the SINEMA RC Server can be reached is the WAN IP address of the router in this example. 192.168.184.20 Default gateway is the LAN IP address of the router 192.168.20.2
	PC (not shown in figure)	LAN port	192.168.20.20 255.255.255.0
	Router 1	LAN port	192.168.20.2 255.255.255.0
		WAN port	Static IP address assigned by the provider, e.g. 192.168.184.20
Station LAN	M816 (VPN client)	LAN port P1 (vlan1)	192.168.10.1 255.255.255.0
		WAN port (ppp0)	Dynamic IP address from the provider
	PC (not shown in figure)	LAN port	192.168.10.20 255.255.255.0

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.

1.2 Configuring a VPN connection on the SINEMA RC Server

Configure SCALANCE M816-1 as device

1. In the navigation area, click "Remote connections > Devices". Click "Create" to create a new device.
2. Configure the device with the following settings.

Name of the device	The following characters are permitted: a-z, A-Z, 0-9 and _. The space character is not allowed. "conn" cannot be used as a name.
Password Confirm password	The password must be made up of uppercase and lowercase letters, numbers and special characters. This password is required again later when configuring the SCALANCE S615.
Type	SCALANCE S615 / M804PB / M826 / M816
VPN protocol	OpenVPN
Type of connection	Digital Input
Request VPN address	Is enabled.
Participant group	Add vpn_user_group.

3. Click "Quick Finish".

Determine device ID and export certificate

1. Click on the symbol in "Actions" to open the device information.
2. Write down the entry for "Device ID", or copy the entry and save the value to a text file in your local directory.
3. Click on the symbol in "Export CA" and save the certificate to a local directory on the PC.
4. Close the dialog with "Exit dialog".

1.3 Configuring VPN connection on the device

Requirement

- The correct time is set on the devices.

  Note

  Manual time setting - reaction after interrupting the power supply

  Note that the time is reset to the factory setting if the power supply is interrupted. On return of the power, you need to set the system time again. As a result, certificates can lose their validity.

  Synchronization using a time server

  Synchronization of the system time using a public time server creates additional data traffic on the connection. This may result in additional costs, depending on your subscriber contract.

- A valid KEY-PLUG is plugged into the device.

Loading a certificate

1. In the navigation area, select "System > Load & Save" and the "HTTP" tab in the content area.
2. Click the "Load" button next to "X509Cert".

   With this certificate, the SCALANCE M816 verifies the SINEMA RC Server during the initialization of the VPN tunnel.

Configuring a VPN connection to the SINEMA RC Server

1. Wire the digital input.

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

   Note

   Notes on device

   Please note the safety instructions in the operating instructions.

2. In the navigation area, select "System > Events".
3. In the "VPN tunnel" column, enable the event "Digital Input".
4. Click on "Set Values".
5. In the navigation area, select "System > SINEMA RC".

6. Configure the SINEMA RC Server with the following settings:

SINEMA RC Address	The WAN IP address via which the SINEMA RC Server can be reached is the WAN IP address of the router in this example.
Verification type	The password must be made up of uppercase and lowercase letters, numbers and special characters.
CA certificate	The loaded CA certificate
Device ID	"Device ID" value that the SCALANCE M816 has received in the SINEMA RC Server.
Device Password Device Password Confirmation	The password that you have configured for access.
Auto Firewall/NAT Rules	Enabled. Corresponding rules are created automatically.
Type of connection	Digital Input
Timeout [min]	30 The VPN tunnel is automatically disconnected after 30 minutes of inactivity.

7. Click on "Set Values".

1.4 Establishing the VPN connection

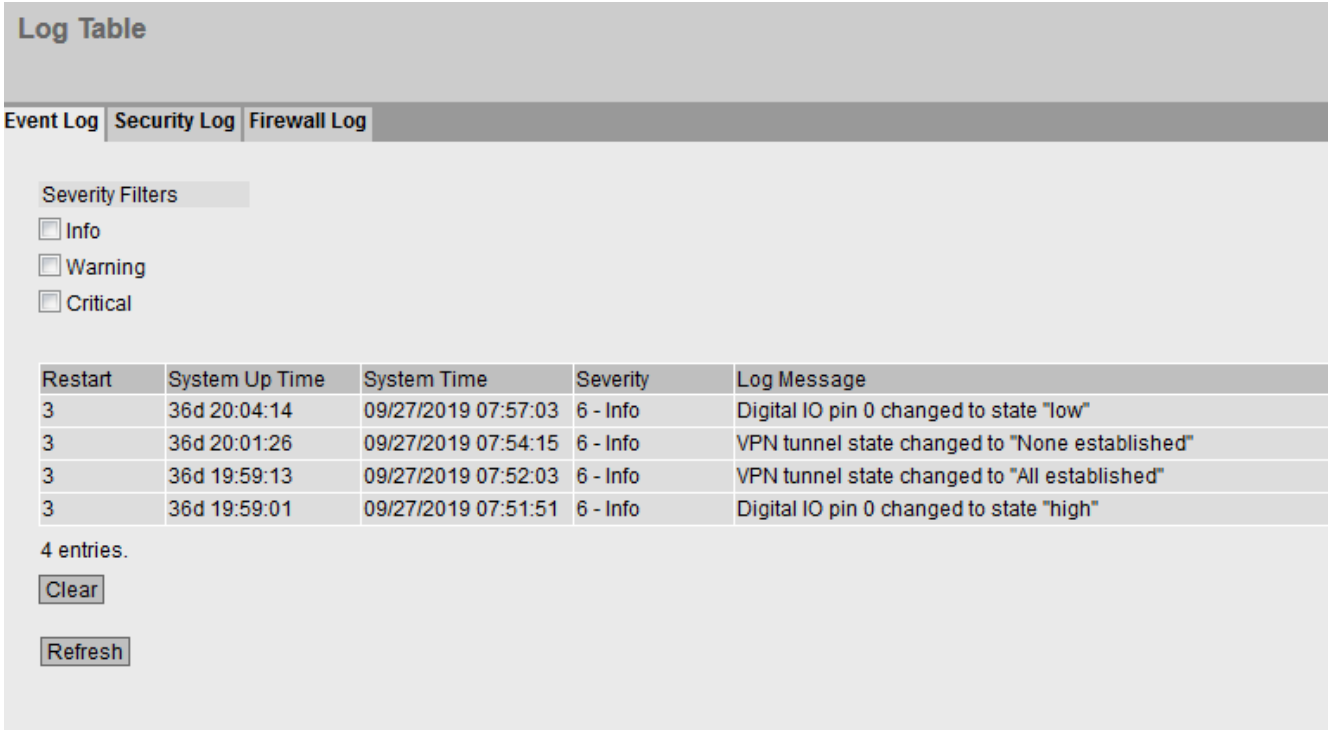
Procedure

1. In the navigation area, select "System > SINEMA RC".
2. Enable the SINEMA RC and click on "Set Values".
3. Close the pushbutton.

Result

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 "VPN tunnel" event on the device that controls the connection setup to the SINEMA RC Server. You will find information on connecting and the maximum current load in the operating instructions of the devices.

The VPN connection is automatically disconnected after 30 minutes of inactivity even though the signal 1 (TRUE/HIGH) is present at the digital input. This is logged under "Information > Event Log".



To re-establish the connection to the SINEMA RC Server, open the digital input and close it again.

You can also configure the timeout in case of inactivity via OpenVPN and IPsec for VPN connections.

Index

G

Glossary, 6

S

Service & Support, 5
SIMATIC NET glossary, 6

T

Training, 5