1 Establish an IPsec VPN connection between Android client and mGuard device

Document-ID: 108394_en_00

Document-Description: AH DE MGUARD ANDROID SUPPORT

Make sure you always use the latest documentation.

It can be downloaded using the following link phoenixcontact.net/products.

Contents of this document

This document describes the required steps to configure a VPN connection between the mGuard server and an Android client (tablet PC or mobile phone with Android OS version 6.0).

1.1 Introduction

The Android device acts as a remote client that initiates the IPsec VPN connection. The mGuard acts as the local server and configures and provides the local network for the clients via the XAuth/Mode Config extension.

The VPN connections require the installation of X.509 certificates and keys both on the Android client and the mGuard device.

For general information on how to configure VPN connections, please refer to the "Software Reference Manual – mGuard Firmware", available online or in the PHOENIX CONTACT Webshop at: phoenixcontact.net/products. For further information regarding the Android client, please refer to the corresponding manufacturer's web page.

Settings and user interfaces may look different on different Android devices. They depend on the manufacturer‘s implementation. The present document was created on the basis of the following device: *SAMSUNG SM-T580* with installed Android version 6.0.1.

1.1.1 Requirements

- mGuard device with installed firmware 8.5 or later
- Android device with installed firmware version 6.0
- All required and signed certificates

How to obtain X.509 certificates?

For further information about certificate management please refer to the application note X.509 CERTIFICATES, available in the PHOENIX CONTACT Webshop at: phoenixcontact.net/products.

1.2 Manage certificates

To establish an IPsec VPN connection between an Android client and the mGuard server, the devices need to authenticate each other via X.509 certificates.

Table 1-1 Required certificates

Device	Required certificate	Format
mGuard	CA Certificate	**PEM / CER**
	mGuard Machine Certificate (signed by CA)	**PKCS#12**
Android client	mGuard Machine Certificate (signed by CA)	**PEM / CER**
	Android Client Certificate (signed by CA)	**PKCS#12**

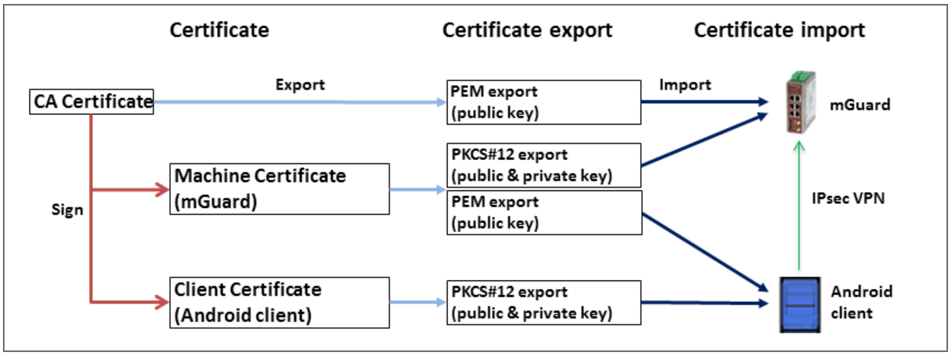


Figure 1-1 Certificate handling for connections initiated by Android clients

The terms “Machine Certificate” and “Client Certificate” signify an X.509 certificate and it‘s corresponding private key by which the machine/client identifies itself to it‘s peers.

1.2.1 Required certificates on the mGuard device

The following certificates need to be installed on the mGuard device.

mGuard Machine Certificate (PKCS#12)

The **Android client** verifies the mGuard on the basis of the mGuard Machine Certificate. The mGuard Machine Certificate must therefore be installed on the Android client.

1.2.2 Required certificates on the Android client

The following certificates need to be installed on the Android device (see page 2).

1. **mGuard Machine Certificate (PEM/CER)**

The Android client verifies the mGuard server on the basis of the mGuard Machine Certificate.

2. **Android Client Certificate (PKCS#12)**

The mGuard verifies the Android client on the basis of the Android Client Certificate signed by the CA. The signing CA Certificate must therefore be installed on the mGuard.

1.2.3 Install certificates on the mGuard device

Machine Certificate

To upload the mGuard Machine Certificate to the mGuard, proceed as follows:

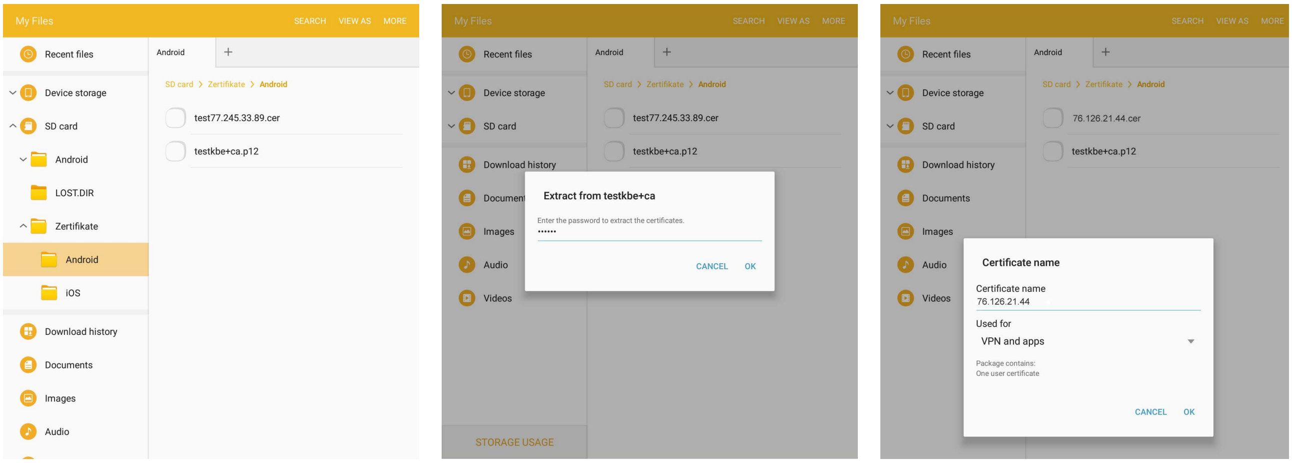
1. Select the menu **Authentication >> Certificates >> Machine Certificates**.
2. Click the icon ⊕ to create a new table row.
3. Click the icon 🗀 .
4. Choose the Machine Certificate (PKCS#12 file) and click “Open”.
5. Enter the password, that has been used to protect the private key of the certificate.
6. Click the button “Upload”.
   ► The uploaded certificate appears in the certificates list.
7. Click “Apply” to save the settings.
   ► The mGuard Machine Certificate has been uploaded and can be used for authentication towards the Android client (see “Configure the mGuard” , Tab “Authentication”).

CA Certificate

To upload the CA Certificate to the mGuard, proceed as follows:

1. Select the menu **Authentication >> Certificates >> CA Certificates**.
2. Click the icon ⊕ to create a new table row.
3. Click the icon 🗀 .
4. Choose the CA Certificate (PEM or CER file) and click “Open”.
5. Click the button “Upload”.
   ► The uploaded certificate appears in the certificates list.
6. Click “Apply” to save the settings.
   ► The CA Certificate has been uploaded and can be used to authenticate the Android client certificate (see “Configure the mGuard” , Tab “Authentication”).

1.2.4 Install certificates on the Android client



Extract from testkbe+ca

Enter the password to extract the certificates.

••••••

CANCEL OK

Certificate name

Certificate name: 76.126.21.44

Used for: VPN and apps

Package contains:
One user certificate

CANCEL OK

To install the **Android Client Certificate** (PKCS#12 file with signing CA certificate) and the **mGuard Machine Certificate** (PEM / CER file) on the Android client, proceed as follows:

1. To use the VPN feature on the Android device, you must set the screen lock type pattern, PIN, or password.
2. Make the certificate files available on the Android client.
3. Open the PKCS#12 file (**.p12)* to extract and install the Android Client and signing CA Certificates.
   ► The screen “Extract from <certificate name>” appears.

   If the screen does not appear and the device displays the content of the file instead, download the file to the storage of your device or make it available via SD card. Open the file from the corresponding directory.

4. Enter the password and click “OK”.
   ► The screen “Certificate name” appears.
5. Optional: Assign a new name to the certificate to easily locate the certificate in the certificate list.
6. Click “OK” to finish the installation of the Android Client and signing CA Certificate.
   ► The installed certificates appear in the user certificates list (Apps >> Settings >> Lock screen and security >> Other security settings >> User certificates).
7. Open the PEM or CER file (**.pem* / **.cer*) to install the mGuard Machine Certificate.
   ► The screen “Certificate name” appears.

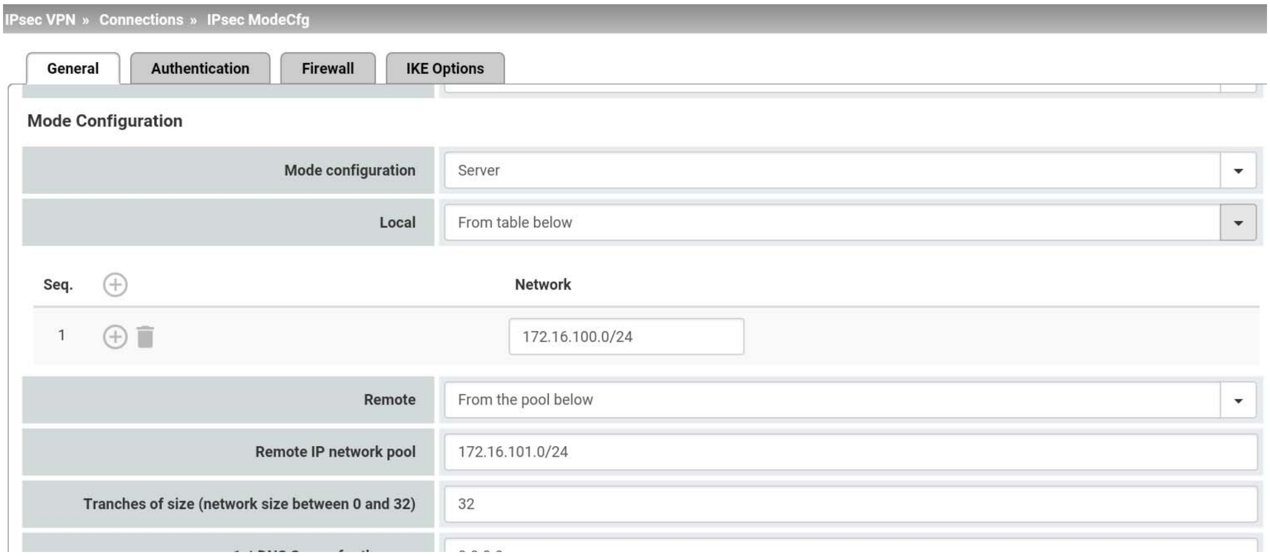
   If the screen does not appear and the device displays the content of the file instead, download the file to the storage of your device or make it available via SD card. Open the file from the corresponding directory.

8. Click “OK” to finish the installation of the mGuard Machine Certificate.
   ► The installed certificate appears in the user certificates list (Apps >> Settings >> Lock screen and security >> Other security settings >> User certificates).

1.3 Configure VPN connections

1.3.1 Configure the mGuard

The IPsec VPN connection between the Android client and the mGuard will be established using the XAuth/Mode Config extension. The configuration of the iOS client will be configured by the mGuard and communicated to the iOS client.



Mode Configuration

Mode configuration	Server
Local	From table below

Seq.	Network
1	172.16.100.0/24

Remote	From the pool below
Remote IP network pool	172.16.101.0/24
Tranches of size (network size between 0 and 32)	32

Figure 1-2 mGuard VPN configuration – Mode Configuration

1.3.1.1 Tab "General"

To configure a VPN connection to an Android client on the mGuard, proceed as follows:

1. Select the menu "IPsec VPN >> Connections".
2. Click the icon ⊕ to create a new table row.
3. Click the icon ✎ "Edit row".
   ► The tab "General" appears.
4. Enter a descriptive name for the connection and change further settings optionally.

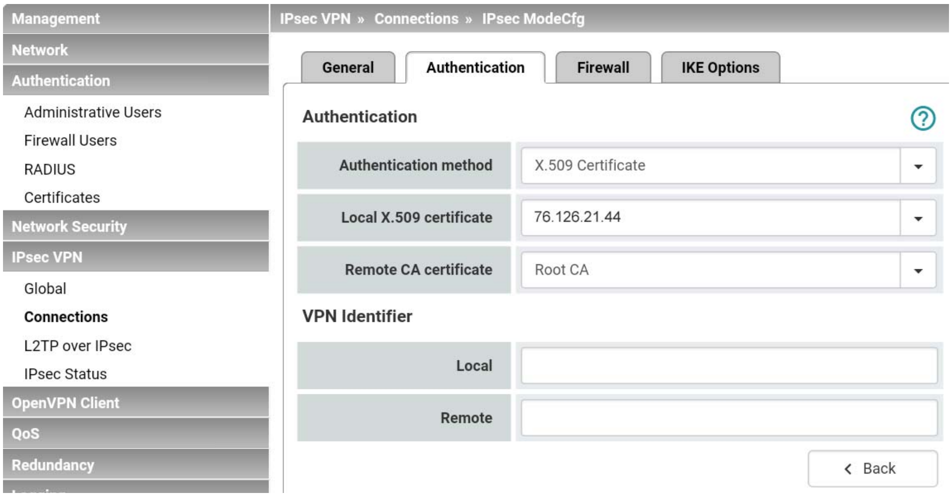
> Verify that the input field "Address of the remote site's VPN gateway" contains the value "**%any**" and "Connection startup" is set to "**Wait**" (default values).

5. In section **Mode Configuration** select Mode configuration **Server**.
6. **Local**: Enter the local network(s) on the server side (mGuard) that shall be accessible by the Android client via VPN connection.
   – **Fixed**: The *Local IP network* must be set to 0.0.0.0/0. In this case, all traffic from the Android client will be sent over the VPN connection.
   – **From table below**: Only traffic to the *Networks* listed in the *table below* will be send over the VPN connection.

> Android clients do not fully support this feature. Traffic from Android clients to networks not defined in the *table below* **will be blocked!**

7. **Remote**: Define the network pool (**From the pool below**) from which the mGuard allocates a variable tranche (**Tranches of size**) to be used by the remote client‘s network.

1.3.1.2 Tab “Authentication”



Authentication

Authentication method	X.509 Certificate
Local X.509 certificate	76.126.21.44
Remote CA certificate	Root CA

VPN Identifier

Local	
Remote	

Figure 1-3 mGuard VPN configuration – Authentication

The VPN connection between an Android client and the mGuard must be authorized by X.509 certificates, that have to be installed on the corresponding devices (see “Manage certificates” on page 2).

To assign the required certificates to a VPN connection, proceed as follows:

1. Select the menu “IPsec VPN >> Connections”.
2. Edit the desired VPN connection (Tab “Authentication”).
3. Select the **Authentication method** “X.509 Certificate”.
4. As the *Local X.509 certificate* select the **mGuard Machine Certificate**.

> **Only for connections from iOS clients:** The CN of the certificate must correspond with the external IP address or DNS name of the mGuard server.

> The certificate must have been signed by the CA Certificate that has been installed on the Android client.

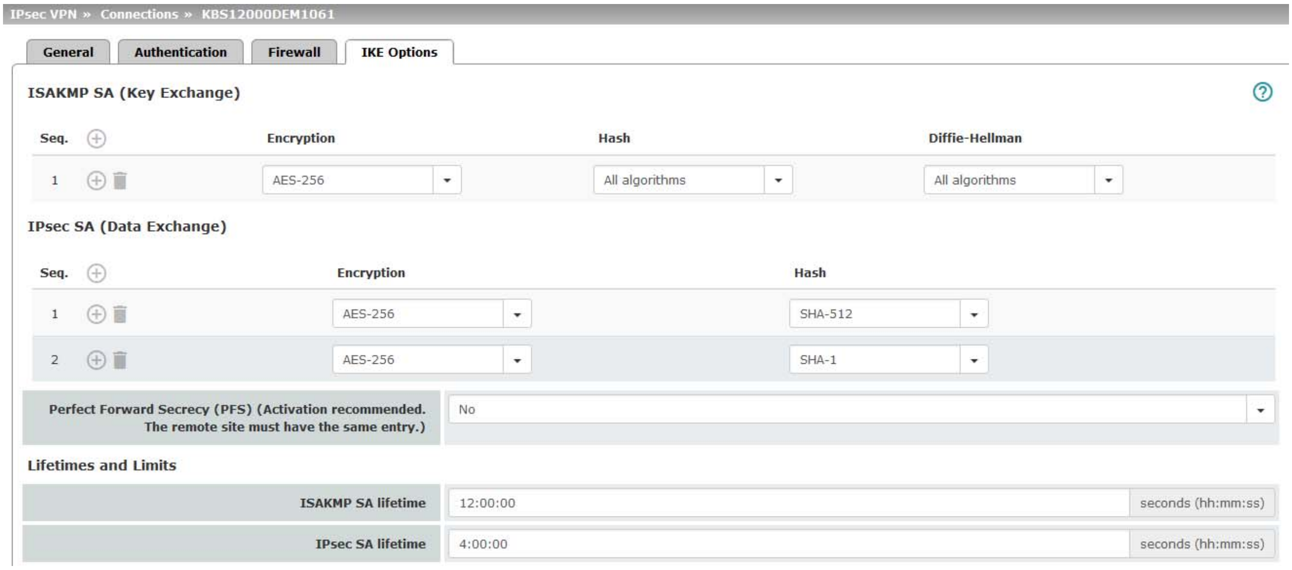
5. As the *Remote CA certificate* select the *CA Certificate* that has been used to sign the **iOS Client Certificate** and the **Android Client Certificate**.
6. Click “Apply” to save the settings.
   ► The VPN connection will be established after being initiated by the Android client.

1.3.1.3 Tab“Firewall”

The VPN firewall restricts the access through the VPN tunnel. You may configure the VPN firewall if required.

> By default, **any incoming** and **outgoing** traffic will be accepted**.**

1.3.1.4 Tab “IKE Options”



IPsec VPN » Connections » KBS12000DEM1061

General | Authentication | Firewall | IKE Options

ISAKMP SA (Key Exchange)

Seq.	Encryption	Hash	Diffie-Hellman
1	AES-256	All algorithms	All algorithms

IPsec SA (Data Exchange)

Seq.	Encryption	Hash
1	AES-256	SHA-512
2	AES-256	SHA-1

Perfect Forward Secrecy (PFS) (Activation recommended. The remote site must have the same entry.)	No

Lifetimes and Limits

ISAKMP SA lifetime	12:00:00	seconds (hh:mm:ss)
IPsec SA lifetime	4:00:00	seconds (hh:mm:ss)

It is necessary to change the default IKE options:

1. Select the menu “IPsec VPN >> Connections”.
2. Edit the desired VPN connection (Tab “IKE Options”).
3. Configure the following settings and leave all other settings on default.

ISAKMP SA (Key Exchange)

– Encryption: AES-256
– Hash: All algorithms
– Diffie-Hellman: All algorithms

IPsec SA (Data exchange)

- Click the icon ⊕ to create two table rows and use the following settings:
  – (Row 1) Encryption: AES-256 | Hash: SHA-512
  – (Row 2) Encryption: AES-256 | Hash: SHA-1

Perfect Forward Secrecy (PFS)

– The PFS must be set to **No**.
(Even if set to **No**, iOS clients will still be able to use PFS.)

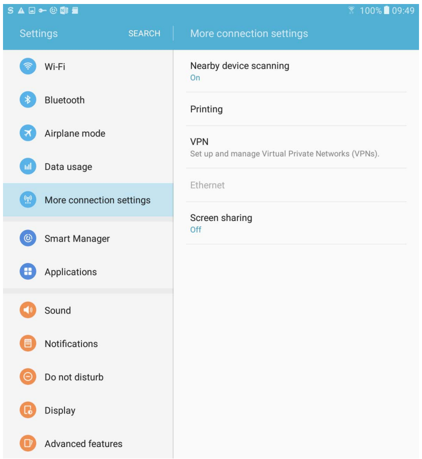
ISAKMP SA lifetime

– 12:00:00 (hh:mm:ss)

IPsec SA lifetime

– 04:00:00 (hh:mm:ss)

1.3.2 Configure the Android client



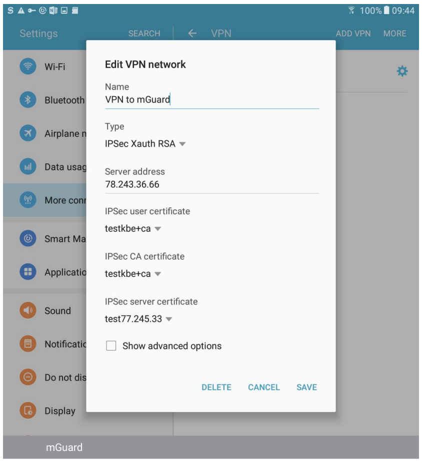
Nearby device scanning
On

Printing

VPN
Set up and manage Virtual Private Networks (VPNs).

Ethernet

Screen sharing
Off



Edit VPN network

Name
VPN to mGuard

Type
IPSec Xauth RSA

Server address
78.243.36.66

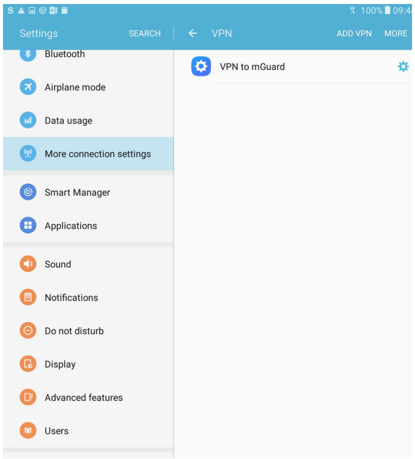
IPSec user certificate
testkbe+ca

IPSec CA certificate
testkbe+ca

IPSec server certificate
test77.245.33

□ Show advanced options

DELETE CANCEL SAVE

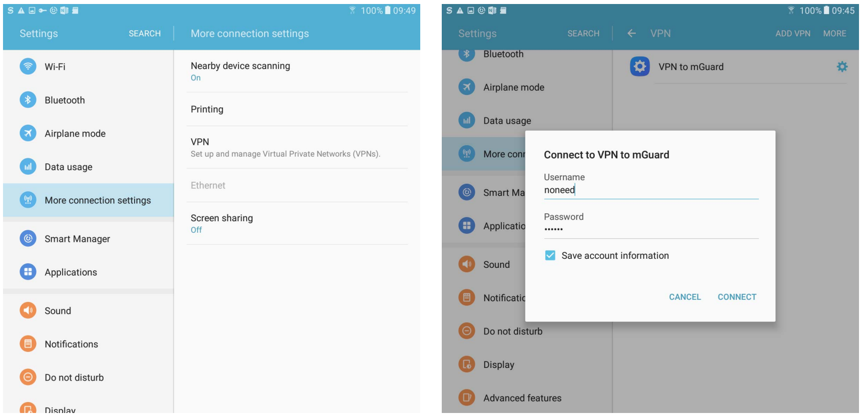


VPN to mGuard

To configure an IPsec VPN connection on the Android client, proceed as follows:

1. Select the menu “Settings >> More connection settings >> VPN”.
2. Click “ADD VPN” or “+”.
   ► The screen “Edit VPN network” appears.
3. Configure the following settings:
   – Name: A descriptive name for the connection
   – Type: IPSec Xauth RSA
   – Server address: The external IP address or the DNS name of the mGuard server
   – IPSec user certificate: Select the name you have assigned to the Android Client Certificate from the PKCS#12 file.
   – IPSec CA certificate: Select the name you have assigned to the Android Client Certificate from the PKCS#12 file.
   – IPSec Server certificate: Select the name you have assigned to the mGuard Machine Certificate of the mGuard server (VPN gateway).
4. Click “Save” to save the configuration.
   ► The VPN configuration has been saved and is ready to be started.

1.4 Start VPN connections on the Android client



Connect to VPN to mGuard

Username
noneed

Password
······

☑ Save account information

CANCEL CONNECT

Figure 1-4 Start VPN connection on the Android client

To start an IPsec VPN connection on the Android client, proceed as follows:

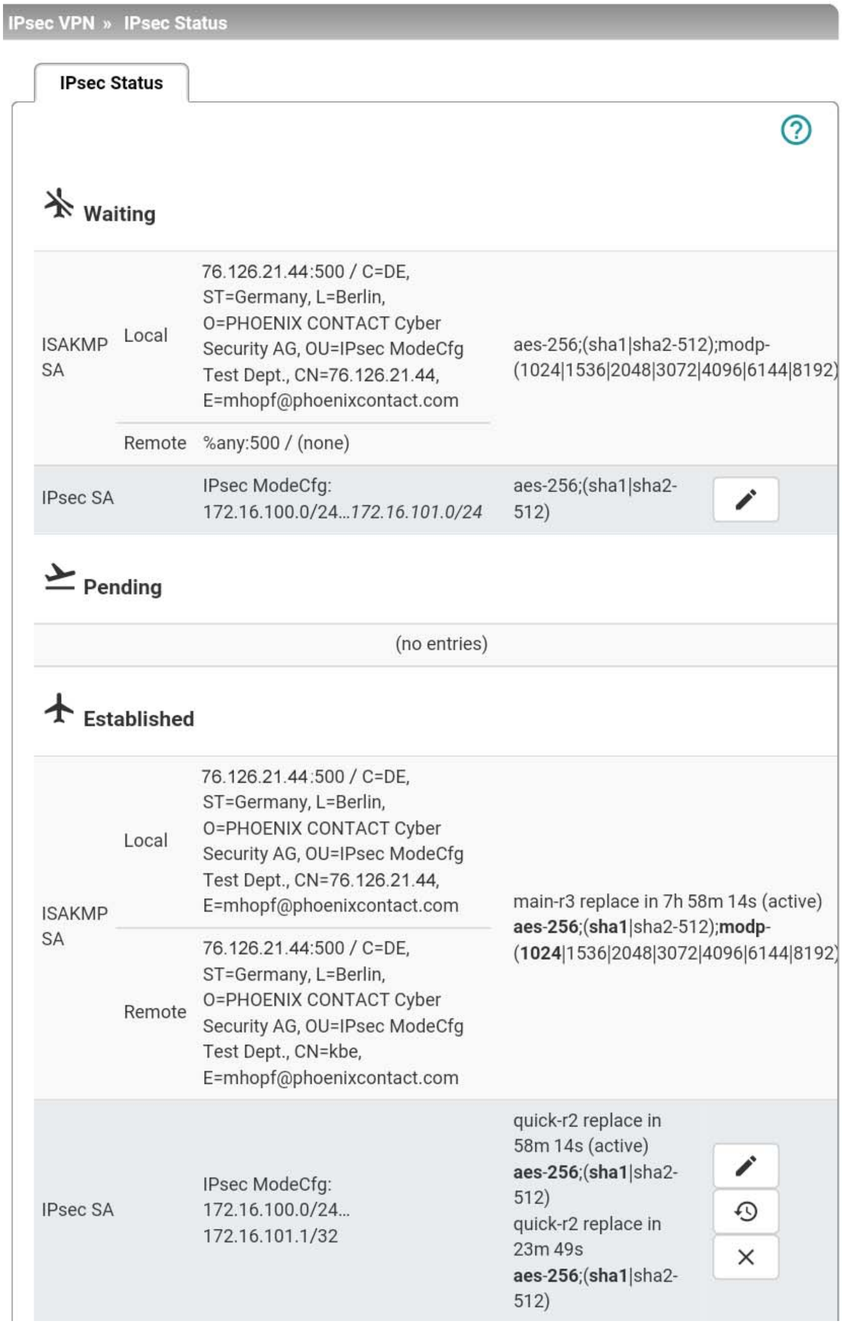
1. Select the menu “Apps >> Settings >> More connection settings >> VPN”.
2. Click on the name of the appropriate VPN connection.
   - ► The screen “Connect to <connection name>” appears.

> The username and password for Xauth will be ignored by the mGuard. Enter some random text and save the account information.

3. Click “CONNECT” to start the connection.
   - ► The VPN connection will be established and the status changes from “Not Connected” to “Connecting...” to “Connected”.

> If the connection fails, click the “gear” symbol of the VPN connection to check for errors in the configuration or check your internet connection.

1.5 Check VPN connections on the mGuard



IPsec VPN » IPsec Status

IPsec Status

Waiting

ISAKMP SA

Local: 76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=76.126.21.44, E=mhopf@phoenixcontact.com

Remote: %any:500 / (none)

aes-256;(sha1|sha2-512);modp-(1024|1536|2048|3072|4096|6144|8192)

IPsec SA

IPsec ModeCfg: 172.16.100.0/24...*172.16.101.0/24*

aes-256;(sha1|sha2-512)

Pending

(no entries)

Established

ISAKMP SA

Local: 76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=76.126.21.44, E=mhopf@phoenixcontact.com

Remote: 76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=kbe, E=mhopf@phoenixcontact.com

main-r3 replace in 7h 58m 14s (active)
aes-256;(**sha1**|sha2-512);**modp**-(**1024**|1536|2048|3072|4096|6144|8192)

IPsec SA

IPsec ModeCfg: 172.16.100.0/24... 172.16.101.1/32

quick-r2 replace in 58m 14s (active)
aes-256;(**sha1**|sha2-512)
quick-r2 replace in 23m 49s
aes-256;(**sha1**|sha2-512)

Figure 1-5 IPsec VPN status

To check the status of an IPsec VPN connection, proceed as follows:

- Select the menu “IPsec VPN >> IPsec Status”.
  - ► An established IPsec VPN connection appears in the area “Established”.