

6 Establish an IPsec VPN connection between iOS client and mGuard device



Document-ID: 108393_en_02
 Document-Description: AH DE MGUARD IOS SUPPORT
 © PHOENIX CONTACT 2022-10-27



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 iOS client (iPad or iPhone with iOS version 8.0 or later).

6.1	Introduction	125
6.2	Manage certificates	126
6.3	Configure VPN connections	132
6.4	Start VPN connections on the iOS client	136
6.5	Check VPN connections on the mGuard	137

6.1 Introduction

The iOS 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 iOS 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](https://phoenixcontact.net/products) or in the PHOENIX CONTACT Webshop at: phoenixcontact.net/products. For further information regarding the iOS client, please refer to the corresponding manufacturer's web page.

6.1.1 Requirements

- mGuard device with installed firmware 8.5 or later
- iOS device with installed firmware version 8.0 or later
- All required and signed certificates



How to obtain X.509 certificates?

For further information about certificate management please refer to the application note "AH EN MGUARD APPNOTES", available in the PHOENIX CONTACT Webshop at: phoenixcontact.net/products.

6.2 Manage certificates

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

Table 6-1 Required certificates

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

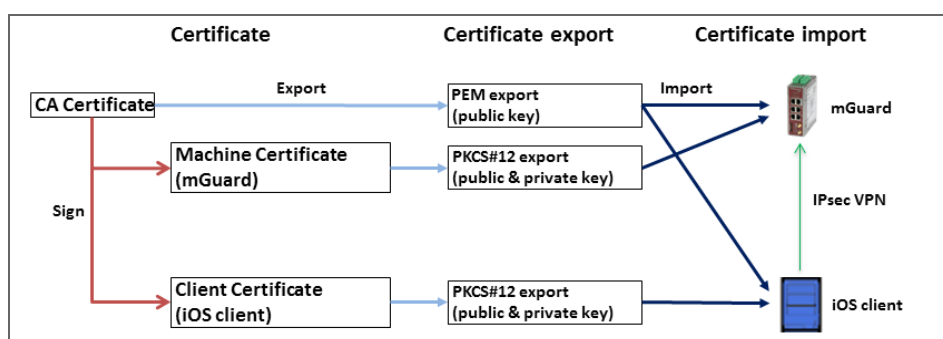


Figure 6-1 Certificate handling for connections initiated by iOS clients



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.

6.2.1 Required certificates on the mGuard device

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

1. CA Certificate (PEM / CER)

The mGuard verifies the iOS client on the basis of the iOS Client Certificate signed by the CA Certificate.

2. mGuard Machine Certificate (PKCS#12)

The iOS client verifies the mGuard on the basis of the mGuard Machine Certificate signed by the CA Certificate. The CA Certificate must therefore be installed on the iOS client.



NOTE: The network address of the mGuard device must be added in the certificate

When creating the mGuard Machine Certificate, the IP address (or hostname/DNS name) that the iOS client uses to establish a VPN connection with the mGuard device (usually the external server IP address of the mGuard device) must be entered in two places:

- **commonName (CN)** --> see Figure 6-2 and Figure 6-3
- **X509v3 Subject Alternative Name** --> see Figure 6-4

Network » Interfaces

General External Internal DMZ Secondary External

Network Status ?

External IP address	76.126.21.44
Current default route	10.1.0.254
Used DNS servers	10.7.53.53

Network Mode

Network mode	Router
Router mode	Static

Network » Interfaces

General **External** Internal DMZ Secondary External

External Networks ?

Seq. +	IP address	Netmask	Use VLAN	VLAN ID
1	76.126.21.44	255.255.255.0	<input type="checkbox"/>	1

Additional External Routes

Figure 6-2 (Example) Network settings on the mGuard: external IP address highlighted

Authentication » Certificates

Certificate Settings **Machine Certificates** CA Certificates Remote Certificates CRL

Machine Certificates

Seq. +	Short name	Certificate details
1 + ✕	76.126.21.44	<div> Download PKCS#12 Password Upload </div> <p>Subject: CN= 76.126.21.44,O=Phoenix-Contact CS,L=Berlin,ST=Germany,C=DE</p> <p>Issuer: CN=CA mGuard,O=Phoenix-Contact CS,L=Berlin,ST=Germany,C=DE</p> <p>Valid from: Oct 15 12:22:01 2015 GMT</p> <p>Valid until: Oct 14 12:19:50 2016 GMT</p> <p>Fingerprint MD5: 93:13:61:BA:AC:E2:5F:8D:D1:D9:B3:66:14:10:13:CC</p>

Figure 6-3 Machine Certificate: CN = mGuard's external IP address or DNS name

X Certificate and Key management

Create x509 Certificate

Source Subject **Extensions** Key usage Netscape Advanced

X509v3 Basic Constraints

Type: End Entity
Path length:

Key Identifier

☐ Subject Key Identifier
☐ Authority Key Identifier

Validity

Not before: 2017-07-13 07:59 GMT
Not after: 2018-07-10 14:44 GMT

Time range

2 Years
☐ Midnight ☐ Local time ☐ No well-defined expiration

X509v3 Subject Alternative Name ✓ IP: 76.125.21.44 **Edit**

X509v3 Issuer Alternative Name **Edit**

X509v3 CRL Distribution Points **Edit**

Authority Information Access: OCSP **Edit**

Cancel **OK**

Figure 6-4 Machine Certificate: Example (XCA) – X509v3 Subject Alternative Name

6.2.2 Required certificates on the iOS client

The following certificates need to be installed on the iOS device (see page 126).

1. CA Certificate (PEM/CER)

The iOS client verifies the mGuard server on the basis of the mGuard Machine Certificate signed by the CA.

2. iOS Client Certificate (PKCS#12)

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





Because the iOS client ignores the keychain of the PKCS#12 file, the signing CA Certificate must therefore be separately installed on the mGuard.

6.2.3 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 >> Certificate" (Tab "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 iOS client (see "Configure mGuard", Tab "Authentication").

CA Certificate

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

1. Select the menu "Authentication >> Certificate" (Tab "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 iOS client certificate (see "Configure mGuard", Tab "Authentication").

6.2.4 Install certificates on the iOS client

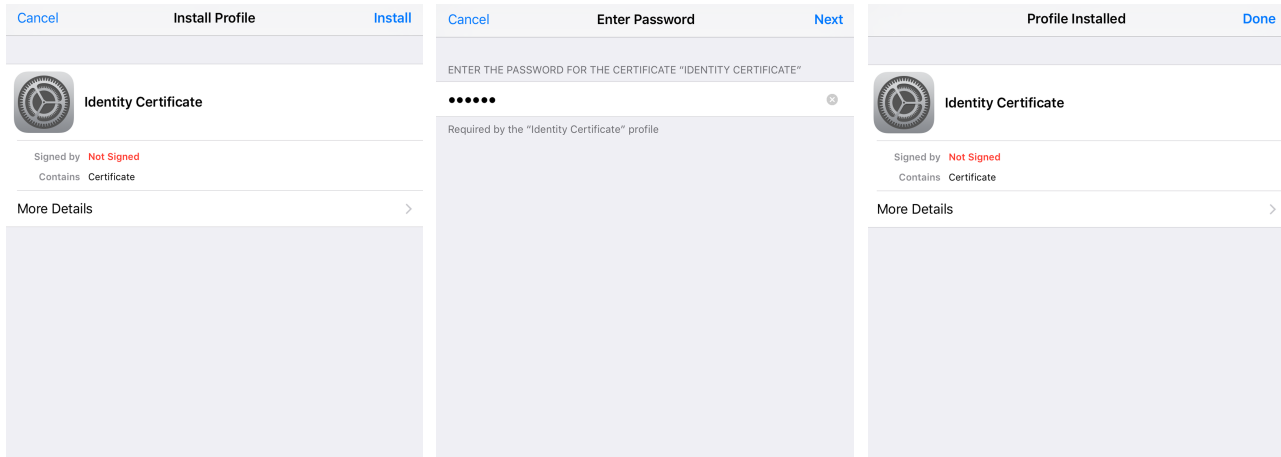


Figure 6-5 Installation of client certificates



Figure 6-6 Installed certificates in the certificate list

To install the iOS Client Certificate or the CA Certificate on the iOS client, proceed as follows:

1. Make the certificate file available on the iOS client.
2. Open the file.
 - The screen “Install Profile” appears.
3. Click twice on “Install”.
 - If the certificate has been secured with a secret key (PKCS#12 files), the screen “Enter Password” appears.
4. In this case, enter the password.
5. Click “Next”.
 - The screen “Profile Installed” appears.
6. Click “Done” to finish the installation of the certificate.
 - The installed certificate appears in the certificate list.

6.3 Configure VPN connections

6.3.1 Configure mGuard

The IPsec VPN connection between the iOS 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.

The screenshot displays the 'IPsec ModeCfg' configuration page. It has four tabs: General, Authentication, Firewall, and IKE Options. The 'General' tab is active, showing the 'Mode Configuration' section. This section includes dropdown menus for 'Mode configuration' (set to 'Server') and 'Local' (set to 'From table below'). Below these is a table with two columns: 'Seq.' and 'Network'. The table contains one row with 'Seq.' 1 and 'Network' 172.16.100.0/24. Below the table are fields for 'Remote' (set to 'From the pool below'), 'Remote IP network pool' (172.16.101.0/24), and 'Tranches of size (network size between 0 and 32)' (32).

Figure 6-7 mGuard VPN configuration – Mode Configuration

6.3.1.1 Tab “General”

To configure a VPN connection to an iOS 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 iOS 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 iOS client will be sent over the VPN connection.
 - **From table below:** Only traffic to the *Networks* listed in the *table below* will be sent over the VPN connection. On iOS clients, traffic to networks not listed in the *table below* will bypass the VPN connection.
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.

6.3.1.2 Tab “Authentication”

Figure 6-8 mGuard VPN configuration – Authentication

The VPN connection between an iOS 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 126).

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**.



The *Common Name (CN)* and *Subject Alternative Name* of the certificate must match the IP address (or host name/DNS name) of the mGuard device that the iOS client uses to establish a VPN connection with the mGuard device (see Section 6.2.1).



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

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

6.3.1.3 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.

6.3.1.4 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

6.3.2 Configure iOS client

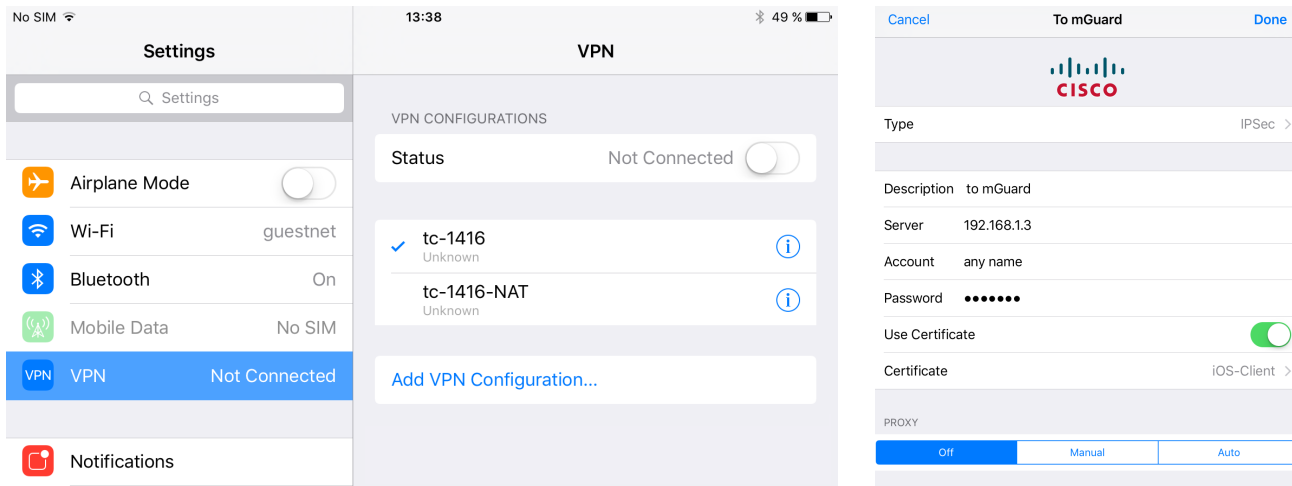


Figure 6-9 iOS client: VPN configuration

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

1. Select the menu “Settings >> VPN”.
2. Click “Add VPN Configuration...”.
3. Click “Type”.
4. Select “IPSec” and click “Back”.
5. Fill out the following input fields:
 - Description: A descriptive name for the connection
 - Server: The external IP address or the DNS name of the mGuard server



This IP address or host name/DNS name must match the *Common Name* (CN) and *Subject Alternative Name* of the mGuard Machine Certificate (see Section 6.2.1).

- Account: The Authentication of VPN peers relies on certificates. Thus the account name and password will be **ignored by the mGuard**. To avoid ongoing requests, enter some random text.
 - Password: The password will be **ignored by the mGuard**. Enter random text.
 - Use Certificate: To select a certificate, activate the switch.
6. Click “Certificate”.
 - ▶ A list with all installed certificates appears.
 7. Select the appropriate client certificate and click “Back”.
 8. Click “Done” to save the configuration.
 - ▶ The VPN configuration has been saved and is ready to be started.

6.4 Start VPN connections on the iOS client

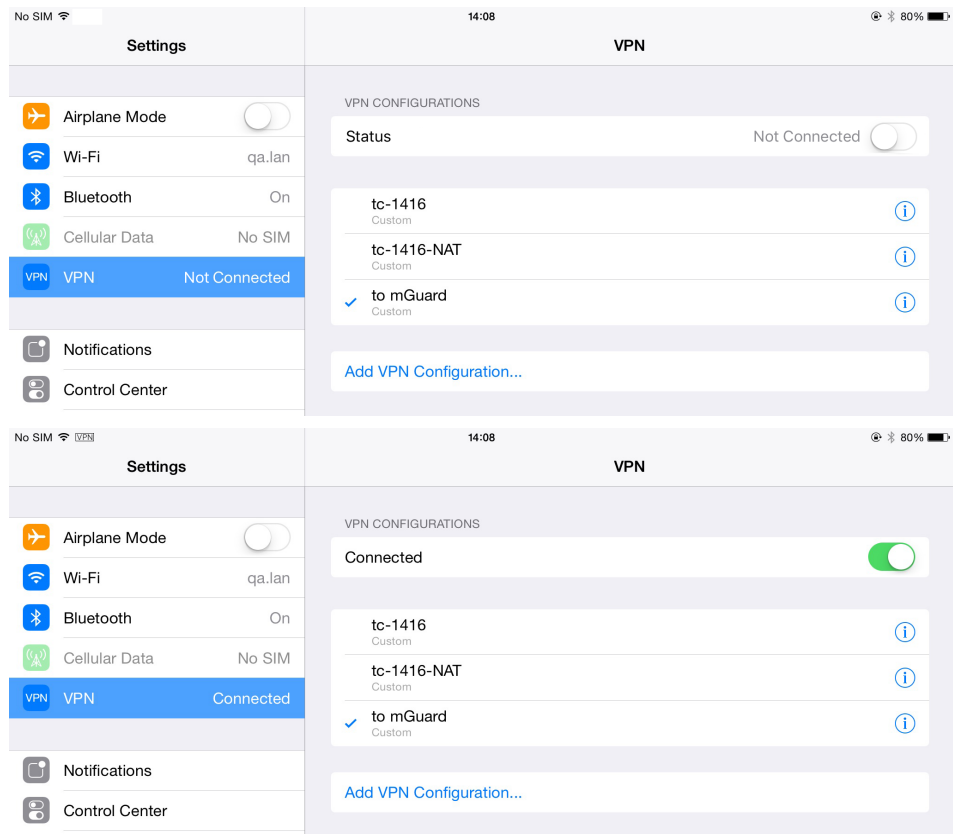


Figure 6-10 Start VPN connection on the iOS client

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

1. Select the menu "Settings >> VPN".
2. Click on the name of the appropriate VPN connection.
3. In the area "Status", click the Button "Not Connected".
 - The VPN connection will be established and the status changes from "Not Connected" to "Connected".



If the connection fails, click the Info icon of the VPN connection to check for errors in the configuration or check your internet connection.

6.5 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	aes-256;(sha1 sha2-512);modp-(1024 1536 2048 3072 4096 6144 8192)
	Remote	%any:500 / (none)	
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	main-r3 replace in 7h 58m 14s (active) aes-256;(sha1 sha2-512);modp-(1024 1536 2048 3072 4096 6144 8192)
	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	
IPsec SA		IPsec ModeCfg: 172.16.100.0/24...172.16.101.1/32	<div>quick-r2 replace in 58m 14s (active)</div> <div>aes-256;(sha1 sha2-512)</div> <div>quick-r2 replace in 23m 49s</div> <div>aes-256;(sha1 sha2-512)</div> <div style="display: flex; align-items: center; gap: 5px;"> </div>

Figure 6-11 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”.

