TC Router 4G LTE and mGuard Secure VPN Client VPN Configuration Guide





1 Description

This application note describes how you can establish a VPN connection from the mGuard Secure VPN Client to the TC Router 4G LTE. This requires the use of certificates.

You need the following:

Name	Order No.	Description
MGUARD SECURE VPN CLIENT LIC	<u>2702579</u>	License for mGuard Secure VPN Client
TC Router 3002T-4G	2702528 (EU) 2702532 (VZW) 2702533 (ATT)	4G LTE cellular modem.
SIM Card with public/static IP address	Contact cellular provider	Active SIM card with public/static IP address that enables the TC Router to connect to the Internet.



WARNING:

This application note does **not** replace the device-specific documents. Please follow the safety notes in the associated package slips, data sheets, and user manuals.



Make sure you always use the latest documentation. It can be downloaded at phoenixcontact.net/products.

Table of Contents

1	0	Description	1
2	(Certificates	3
3	(Configuring the router	3
	3.1	Mobile communication router	3
4	(Configuring the mGuard Secure VPN Client	6
	4.1	Installation	6
	4.2	Uploading a certificate	6
	4.3	Creating a profile	6
	4.4	Testing the connection	9

2 Certificates

Learn how to create certificates in the "Quick Reference Guide for creating certificates" at <u>phoenixcontact.com/product/2314008</u>.

Certificates required

For a VPN tunnel in connection with the mGuard Secure Client, you require three certificates: a private certificate from each side and a public certificate from the client loaded in the VPN server.

- Machine certificate.p12#
- Client certificate.p12#
- Client certificate.crt

3 Configuring the router

3.1 Mobile communication router



Figure 1

i

System overview with mobile router

Ensure that the TC Router has an active data plan with a public/static IP address. Please check with your cellular provider to learn more about the data plan associated with the SIM card

- Power up the TC Router and connect to the Internet
 - Refer to the TC Router user manual for setup instructions
- Open the web-based management. Log in with your username and password.
 - Default IP address: 192.168.0.1
 - o Default username: admin
 - o Default password: admin
- Switch to the "VPN >> IPsec >> Certificates" subfolder.
- Load the Client certificate.crt and Machine certificate.p12# into the TC Router
- Confirm with "Apply"





IPsec certificates

- Switch to the "VPN >> IPsec >> Connections" subfolder.
- Enter a name for the VPN connection.
- Confirm with "Apply".
- Under the "Settings" main item, click on the "Edit" button.

TC ROUTER 3002T-4G ATT	IPsec conne	ctions					
27 02 533	Monitor DynDNS			No 🔻			
11110	Check interva	Check interval			600 sec.		
1811	IKE logging le	evel		0 •			
11:1	Enabled	Name		Settings	IKE	Firewall	
	Yes •	mGSVC to TC Router VPN		Edit	Edit	Edit	
- A	No 🔻	vpn2		Edit	Edit	Edit	
1.1	No •	vpn3		Edit	Edit	Edit	
		Apply					
Device information							
 Status 							
 Local network 							
Wireless network							
 Device services 							
Network security							
VPN							
 IPsec 							
Connections Certificates							
OpenVPN							
* I/O							
System							
Basic setup							
🗅 Logout	-						



- Activate the VPN tunnel.
- Select the certificates.
- Enter the network area of the local network. Enter the fixed IP address of the client. The example shows the network area 192.168.0.0/24 and for the client 192.168.9.1/32.
- Enable remote masquerading
- Confirm with "Apply".

TC ROUTER 3002T-4G ATT	IPsec connection settings				
27 02 533	Name	mGSVC to TC Router VPN			
	VPN	O Disabled ® Enabled			
10 20	Authentication	X.509 remote certificate			
**	Remote certificate	Client_Certificate.crt •			
6. A	Local certificate	Machine_Certificate.p12 *			
1 . /	Remote ID				
	Local ID				
Device information	Uritual remote address	192.168.9.2			
+ Status	Address remote network	192.168.9.1/32			
Local network	Address local network	192.168.0.0/24			
Wireless network	Connection NAT	Remote masquerading *			
 Device services 	NAT to local network	192.168.0.0			
 Network security 					
 VPN 	Remote connection	Accept *			
 IPsec 	Autoreset	60 min.			
Connections Certificates	IKE	â selv			
OpenVPN	Appry				
+ I/O	Reloading strongSwan IPsec co	onfiguration			
+ System					
Basic setup					
C Logout	*				

Figure 4

IPsec connection settings

- Click on "IKE"
- Take the settings from the figure below.

TC ROUTER 3002T-4G ATT	IPsec - Internet key exchange settings				
27 02 533	Name	mGSVC to TC Router VPN			
	IKE protocol	IKEv1 only ▼			
	Dhaco 1 ISAKMD SA				
1 lea	ISAKMP SA encryption	AFS-256 ¥			
	ISAKMP SA hash	SHA-2/SHA-1 (all)			
3	ISAKMP SA lifetime	3600 sec.			
1					
	Phase 2 IPsec SA				
	IPsec SA encryption	AES-256 •			
 Device information 	IPsec SA hash	SHA-2/SHA-1 (all) 🔻			
🛨 Status	IPsec SA lifetime	28800 sec.			
🛨 Local network					
 Wireless network 	Perfect forward secrecy (PFS)	Yes V			
Device services	DH/PFS group	2/modp1024 •			
+ Network security	Rekey	Yes •			
- VPN	Dead peer detection	Yes •			
- IPsec	DPD delay	30 sec.			
Connections	DPD timeout	120 sec.			
Certificates					
+ OpenVPN	Settings	Apply			
• I/O					
+ System					
Basic setup					
🗅 Logout	v				

Figure 5

IPsec – Internet key exchange settings

The settings for the TC Router are now complete

In the "Status >> IPsec status" stub-folder you can monitor the status of the VPN tunnel.



Figure 6

IPsec connection status menu

4 Configuring the mGuard Secure VPN Client

4.1 Installation

 Install the mGuard Secure VPN Client as described in the corresponding data sheet (see <u>phoenixcontact.com/ product/2702579</u>).

4.2 Uploading a certificate

- Start the mGuard Secure VPN Client software
- Navigate to "Configuration >> Certificates"
- Select "Add" and name the certificate "Client Certificate"
- In the "User Certificate" tab, select the "from PKCS#12 file" option.
- Upload the previously created Client Certificate.p12#

Certificates							×
<u>N</u> ame:	Name: Client Certificate						
User Cer	User Certificate PIN Policy Certificate Renewal Computer Certificate						
Certifi	ica <u>t</u> e:			from PKCS#12 fi	le		~
Select	Certific	ate:	I	1			
PKCS#	12 <u>F</u> iler	name:	-	C:\Users\dhoysa	n\Onel	Drive - PHOE	NIX CC
	Enabl	le Certificate	Selec	tion			
c	ertificat	te Path:					
PIN	l reques	it at each co	nnect	ion			
				Help		OK	Cancel
Certificates X							
Certificates							×
Certificates <u>N</u> ame:	Client	Certificate					×
Certificates <u>N</u> ame: User Cer	Client	Certificate PIN Policy	Certi	ficate Renewal	Comp	uter Certifica	×
Certificates <u>N</u> ame: User Cer Certifi	Client tificate ica <u>t</u> e:	Certificate PIN Policy	Certi	ficate Renewal from PKCS#12 fi	Comp	uter Certifica	× ate
Certificates <u>N</u> ame: User Cer Certifi Se <u>l</u> ect	Client tificate ica <u>t</u> e: Certific	Certificate PIN Policy ate:	Certi	ficate Renewal from PKCS#12 fi	Comp	uter Certifica	Ate
Certificates <u>N</u> ame: User Cer Certifi Select PKCS#	Client tificate ica <u>t</u> e: Certific 12 <u>F</u> iler	Certificate PIN Policy ate: name:	Certi	ficate Renewal from PKCS#12 fi 1 C:\Users\dhoysa	Comp le	uter Certifica Drive - PHOEI	
Certificates <u>N</u> ame: User Cer Certifi Select PKCS#	Client tificate ica <u>t</u> e: Certific 12 <u>F</u> iler	Certificate PIN Policy ate: name: le Certificate	Certi	ficate Renewal from PKCS#12 fi I C:\Users\dhoysa tion	Comp le n\Onel	uter Certifica Drive - PHOEI	x ate
Certificates <u>N</u> ame: User Cer Certifi Select PKCS#	Client tificate ca <u>t</u> e: Certific 12 <u>F</u> iler Enabl	Certificate PIN Policy ate: name: le Certificate te Path:	Certi Certi	ficate Renewal from PKCS#12 fi I C:\Users\dhoysa tion	Comp le n\Onel	uter Certifica Drive - PHOEI	ate
Certificates <u>N</u> ame: User Cert Certifi Select PKCS# C DIME DIME DIME DIME DIME DIME DIME DIME	Client tificate ca <u>t</u> e: 12 <u>F</u> iler Enabl <u>e</u> rtificat	Certificate PIN Policy ate: hame: le Certificate te Path: it at each co	Certi [] Selec	ficate Renewal from PKCS#12 fi i C:\Users\dhoysa tion	Comp le	uter Certifica Drive - PHOEI	ste

Figure 7 mGSVC certificate upload

4.3 Creating a profile

- In the main menu, select "Configuration >> Profiles".
- Add a new profile

Profiles				-		×
Available Profiles						
Group:						
Show All Profiles				\sim	Group	
Profile Name 🔺				Defa	ult	
Add / Import	Edit	Сору	Delete		Export	
		Hel	p (DK	Canc	el

Figure 8

Add mGSVC configuration profile

- Select the manual configuration
- Enter a profile name

×
MGuard
up to 39 alphanumeric field.

Figure 9

Profile name

- Select the previously uploaded certificate
- Click next

New Profile Wizard	×
Certificate Usage Should a certificate be used for authentication?	MGuard
For strong authentication a certificate can be used. Thi the VPN gateway at beginning of the connection. Secure Client Monitor's menu item Configuration: Certi configuration of which certificate the client is going to No Certificate for Authentication © Certificate for Authentication	s certificate will be checked by ficates allows for the use.
Client Certificate	~
< Bac	k Next > Cancel

Figure 10 Certi

Certificate Configuration

- In "Gateway", enter the public/static IP address address of the remote station. In this example the address is 166.130.95.55
- Click next

New Profi	le Wizard X
VPN G To whic establis	ateway Parameters ch VPN gateway should the connection be shed?
Enter ti 212.10. Using E authen establis	he DNS name (e.g. vpnserver.domain.com) or the official IP address (e.g. 17.29) of the VPN gateway you want to connect to. Extended Authentication (XAUTH) you can enter the user ID and password for the tication. If no authentication data are entered they will be requested when shing the connection. Gateway (funnel Endpoint):
	166.130.95.55
22	Extended Authentication (XAUTH)
	User ID:
	Password: Password (confirm):
	< Back Next > Cancel

Figure 11

Gateway (Tunnel Endpoint)

- Apply the IPsec parameters shown below:
 - o Main mode
 - o DH2 (modp1024)

New Profil	e Wizard	×
IPsec C Configu	Configuration ure the basic IPsec parameters	MGuard
The bas "autom In the e defined	ic IPsec parameters can be specified here. atic mode" which are pre-defined (default) event that uniquely defined IKE- / IPsec pol I and assigned using the policy editor und	The IPsec negotiations will use proposals. icies are to be used, these can then be ler IPsec General Settings.
	main mode	~
	PFS Group:	
	DH2 (modp1024)	~
		< Back Next > Cancel

Figure 12 IPsec Configuration

• Leave the ASN1 Distinguished Name ID field blank. This should only be used in configurations requiring a Pre-shared key instead of certificates

New Profil	le Wizard				×
Pre-sh Commo	ared Key on Secret for A	uthentication		MGu	lard
Enter ti	he appropriate	value for the IKE ID ac	cording to the s	elected ID type.	
8	Local Identit Type: ID:	y (IKE) ASN1 Distinguished I	Name		~
			< Back	Next >	Cancel

Figure 13 Pre-shared Key

• Enter the VPN client IP address. In the example in the system overview, the IP address is 192.168.9.1

New Profil	le Wizard	×
IPsec C Assigni	Configuration - IP Addresses ng the IP address to the client	mGuard
Specify the clie Further	which IP address the client is going to us nt's IP address is dynamically assigned by more, define where the DNS / WINS serve	e. By selecting "Use IKE Config Mode" the VPN gateway. rs (if used) can be found.
	IP Address <u>A</u> ssignment Manual IP Address IP Address	~
	192.168.9.1] DNS / WINS Servers DNS Server: 0.0.0.0	WINS Server: 0.0.0.0
		< Back Next > Cancel



IPsec Configuration – Client IP Address

• Enter the network area of the remote station. In the example in the system overview, the network area is 192.168.0.0/24



NOTE: Malfunction

The logical network on the PC and on the remote station must be located in different network areas. Otherwise problems may arise when routing. - Select different network areas.

IPsec C Define f through	onfiguration - Split Tunne the remote IP networks to b n the IPsec tunnel.	eling De reached	Guard
Enter th used 0.0	e remote IP networks the to 0.0.0/0 for the standard rou	unnel should be used for. Withou te over VPN.	t entries will be
	Remote Networks	Remote IP Net Masks	Add
J	192.168.0.0	255.255.255.0	Edit
			Delete

Figure 15 IPsec Configuration – Remote Network

• Close the wizard with "Finish"

- From the VPN Client main menu, select "Configuration >> Profiles"
- Select the Remote Connection profile and choose edit

Profiles				-		×
Available Profiles						
Group:						
Remote Connection			×	/	Group	
Profile Name 🔺				Defau	ilt	
Remote Connection						
Add / Import	Edit	Сору	Delete		Export	
		Help	ОК		Cance	el

Figure 16 Edit

Edit the configuration

 Select "Line Management" from the menu and set the Inactivity timeout to 0 seconds to prevent any timeout issues.

Profile Settings Remote Connection		×
Basic Settings Li	ine Management	
Line Management Extended Authentifation IPsec General Settings Advanced IPsec Options Identities Local Network Remote Network Certificate Check	Cognection Mode: Cognection Mode: Inactivity Timeout (seq: Jactivity	
	Help OK Cancel	



• Select "IPsec General Settings" from the menu, and set IKE Policy and IPsec Policy to "All algorithm"

Profile Settings Remote Connec	tion			×
Basic Settings	IPsec Ge	eneral Settings		
Line Management Extended Authentication IPsec General Settings		<u>G</u> ateway (Tunnel En 166.130.95.55	lpoint):	
Advanced IPsec Options	Policies			
Local Network	i i i i i i i i i i i i i i i i i i i	Exch. <u>M</u> ode:	main mode	~
Remote Network	π	[KE Policy:	All algorithm	~
Certificate Check		IKE DH Group:	DH2 (modp1024)	~
		IPsec Policy:	All algorithm	~
		PFS Group:	DH2 (modp1024)	~
			Policy Lifetimes	Policy Editor
			Help OK	Cancel

Figure 18

IKE Policy and IPsec Policy

Exit the menu. The VPN Client software setup is now complete

4.4 Testing the connection

- In the main menu, select your profile.
- Activate the connection by clicking the connection slider



Figure 19 Testing the connection

 The VPN client will prompt you for a PIN. This is the password associated to the p12 certificate. Enter this password to establish the connection



Figure 20 Entering the password

The connection is established when all four circles and the tunnel turn green as shown below.

mGuard Secure	VPN Client	:	_		×
Connection Confi	guration V	iew H	elp		
Connection Profile:			<u>c</u>	onnecti	on:
Remote Connectio	on		~ [
×.	connection	establi	ished.		D
(PIN)		30)		
\bigcirc			mG	ua	rd
Statistics:					
Data (Tx) in Byte:	0	Time o	nline:	00:00:	42
Data (Rx) in Byte:	0	Timeou	ut (sec):	58 se	с
Speed (KByte/s):	0.000	Encryp	otion:	AES C	BC 256
Click here !	Info.	Whe	re to buy	Sup	port
Figure 21	Connectio	on esta	blished		

 Verify the tunnel has been established by logging into the TC Router and navigating to "Status >> IPsec status". A successful connection will show two green check marks

TC ROUTER 3002T-4G ATT	IPsec status						
27 02 533	Active IPsec connections						
1777 D	Name	Remote host	ISAKMP SA	IPsec SA			
1411 1	mGSVC to TC Router VPN	192.30.227.251	1	1			
Device information Status							
Radio							
Network connections							
OnenVRN status							
I/O status							
Routing table							
DHCP leases							
- System into							
Local network							
 Wireless network 							
 Device services 							
 Network security 							
VPN							
 I/O 							
	*						



Connection verification

Congratulations, you have successfully established a VPN tunnel between the mGuard Secure VPN Client software on your laptop to a TC Router over the cellular network.