

mGuard Secure Cloud Starting Guide

Table of Contents

Z
2
3
4
5
0
7
0
2
4





Introduction

The Phoenix Contact mGuard Secure Cloud is an industrial VPN cloud service that gives technicians the ability to access remote machines via the Internet. The mSC service is not tied to recurring charges at all, it's a free service with the only requirement to use mGuard devices at the machine and the supported software (mentioned below).

Brief overview of the steps required to utilize the secure cloud:

- Purchase the required Phoenix Contact mGuard hardware
- Register on the Phoenix Contact Secure Cloud webpage: <u>https://us.cloud.mguard.com</u>
- You will receive account credentials, from the cloud administrator, via an e-mail
- Use the credentials you received (account ID, user name, and password) to access the account page
- Add machines (remote devices) to the Machines section of your account and service techs to the service workstations section
- Request configurations for the hardware and software that the Machines and Service technicians are using these are created automatically
- Save the configurations files and load them onto the hardware and/or software

Terminology

The terms used in this guide parallels the terminology used by the cloud website. We hope this diagram will help explain the structure of the service.

- Service: a technician/ engineer accessing remote machines is referred as Service Workstations
 - Supported Service Clients:
 - Laptop running Shrewsoft or mGuard Secure VPN Client
 - iOS device (iPad or iPhone)
 - Any commercial mGuard HW
- Machines: Machines are groups of remote devices which the service technicians want to access to support, troubleshoot, control, etc. These machine is reference as Service Targets (Machines)
 - Supported Service Clients:
 - Any mGuard hardware. For more information visit www.phoenixcontact.com/mguard

Service Targets (Machines)	Service Workstations	Administration	Logbook	Preferences

Figure 1 – mGuard Secure Cloud Main Menu



Architecture

Leveraging the power of the cloud and maximizing your flexibility enable Phoenix Contact to be your IT department – hosting a state-of-the-art data center with a central mGuard that connects you to your remote devices over secure tunnels. Our Automatic VPN Wizard in the Secure Cloud, based on your input, will build the tunnel configurations for you, for an immediate download. The bottom line is this: We are standing by, ready to connect and support your end customers.

The mGuard Secure Cloud forms a powerful infrastructure in the cloud, securely interconnecting service staff with machines and plants via the Internet. The mGuard VPN technology uses the IPsec security protocol with AES-256 encryption. The mGuard guarantees the confidentiality, authenticity and integrity of all information and data transmitted between the service staff and the machines.



Service Workstations	Service Target (Machines)
Unlimited technicians and engineers can be added to the mSC for free	Unlimited machines and locations can be added
Unique Service VPNs are required in order for them to cooperate in machines at the same time	An mGuard hardware device is required to connect each machine to the mSC
The VPN needed for your techs can be software or hardware based	No need to change your machine's network IP scheme
Many users can connect to the same remote machine at the same time	The mSC will route your traffic as if you were locally connected to the machine
Many users can connect to several remote machines at the same time	The machine subnet networks supported are /24 or 255.255.255.0
One user can't connect to several machines at the same time	No need to have configured default gateway in all your remote devices



Registration

To get started, you must first register at the following web location:

https://us.cloud.mguard.com/

- 1. When at the registration page, click on the SIGN UP link and complete the registration form.
 - a. Note that through this step you will need to enter the real IP address of the machine network (PLCs, HMIs, etc.) you will like to reach remotely. If you have more than one network, please proceed registration and then email the mSC admin team portal@phoenixcon.com with a network addition request.



You will then receive an email from the mGuard Secure Cloud administrator. The email will contain instructions and your Account credentials. You will then use the following credentials to access your mGuard Secure Cloud account:

- Account ID
- User (Normally your email address)
- Password (Created at registration)



Service Workstations - VPN Builder

The following is a walkthrough guide showing the steps required to request the service VPN to all technicians and support engineers in the account.

Requesting Service VPN Configurations to the account

Service technicians are added to the **Service Workstation** section of your account page. Note that you can name the service workstations as the technician by first and/or last name, by computer number or other functions. The service workstation name in the website is not tied to the user signing in.

To add a Service technician:

- 1. Access the account webpage
- 2. Select the Service Workstations Tab
- 3. Click on the blue circle/plus icon
- 4. Enter the workstation name and click the OK option (bottom)

Account: PHO17000US I User: dschaffer@	secure cloud public phoenixcon.com I Role: admin	Language: English 🗸 🛛	Contact Hel	2.5.0-pre00 p & Support I Log out
Routing	Service Targets (Machines) Service Workstations	Administration Logbook	Preferences	
Service VPN tunnel offline > no secure con	nection initiated >no secure remote access to service	target (machine)		
active VPNs all Service Workstation	s			
Add new workstation				
Bob's iPad	*			
Notice:				
• = mandatory field	\frown			
Cancel	ОК)		
© Copyrigh	t 2011-2016 Phoenix Contact Cyber Security AG I Data pri	vacy I Evaluation License Agreeme	ent I Legal Notice	

- 5. Next, click on the all Service Workstations tab
- 6. Click on the drop-down arrow next to the workstation
- 7. Select the New Contact you just created
- 8. Click on the VPN Builder button.



Account: PHO17000US I User: ds	chaffer@phoenixcon.com Role: admin	I d ^{public}	Language: En	glish 🗸 I	Contact	Help & Support	2.5.0-pre00
Routing	Service Targets (Machines)	Service Workstations	Administration	Logbook	Preferences		
Service VPN tunnel offline > no se	orkstations	mote access to service ta	arget (machine)				
Workstations							
1 I Bob's iPad	I no user	1	not connected	I VPN: of	flie I		≡

A new window will open where you will see the parameters page. Here you first select the VPN client desired for your service technician configuration. The options are:

- mGuard Secure VPN Client: The new mGSVC is a Phoenix Contact IPsec client compatible with all mGuard firmware and developed for the use with the mSC. It is compatible with both basic and advanced situations and supports going through a Proxy and using alternate VPN ports. <u>Download the 30-day-free-trial of the mGuard Secure VPN Client here</u>
- Shrewsoft VPN Client: Shrewsoft is a free, third party open source VPN client that can be used to tunnel into the mSC. It is great for basic connections, but it doesn't support Proxies or using alternate VPN ports. <u>Download the free Shrewsoft VPN here</u>
- Native iOS VPN: All Apple mobile devices (iPad and iPhones) running iOS firmware are now capable of connecting to our mSC server and reach remote devices' webpages by using the native VPN client. The service VPN builder contains the new automated iOS client option to generate this configuration profile automatically, including the certificates. After the configuration for iOS is downloaded, the settings app opens automatically, allowing easy installation of the profile.
- **mGuard Hardware:** If desired, any commercial or industrial mGuard devices can also be used for the service VPN tech.
- 9. Select the desired option and then type your own password for the service VPN authentication.
- 10. Click Next

|--|--|

VPN client type				
What kind of VPN client are you going to use to conne	ct this service workstation secu	irely to the mGuard S	Secure Cloud public?	
You can use any mGuard VPN appliance (e.g. mGua	rd smart ^a VPN or mGuard delta	² VPN).	(DNL Olicest)	
• rou may also choose a certified software IPSec VPN • Apple iPad and iPhone user select the built-in iOS V	r chent (mGuard Securé VPN C PN client.	nem or Shrew Soft V	PN Glient).	
I Adam I no us	er			
Choose a VPN client type				
mGuard Secure VPN Client (commercial softw	are client with vendor support)			
Shrew Soft VPN Client (free software client w/	vendor support)			
native iOS VPN Client (Apple iPad)	er			
mGuard VPN appliance (hardware)				
Please enter the client password:				
Password: *		Repeat passw	ord: *	
= mandatory field				
passwords must be at least 8 characters long and should con	tain letters, numbers and special ch	aracters.		

If you selected the mGuard Secure VPN Client or the mGuard Hardware continue with next step, if not continue in step 12.

11. Select the desired port. IPsec VPN uses ports UDP 500/4500, if you know your network is blocking these ports going outbound use the VPN Path Finder option via port TCP 443.

/PN connection mode (UDP/TCF	P configuration)		
The mGuard Secure VPN Client can u: and 500 must be opened for outbound carried firewall friendly via secure TCF be used.	ise different ports to establish a I IPsec traffic (also through firev P port 443 (HTTPS), if a standar	VPN connection to a destination device. When usin valls, proxies, etc.). When choosing VPN Path Find d IPsec connection via port 500 cannot be establish	ng standard IPsec ports, the UDP ports 4500 er, IPsec traffic will be encapsulated and ned. An interconnected proxy server can also
Connect through			
the standard IPsec ports of UDP	500 and 4500		
(the VPN Path Finder (secure HT	TP portTCP 443 which also su	pports going through a network proxy)	
the VPN Path Finder (secure HT) If a proxy should be used, please confi	TP port TCP 443 which also sup figure the proxy settings in the n	pports going through a network proxy) nGuard Secure VPN Client ('Configuration -> Proxy	for VPN Path Finder').
the VPN Path Finder (secure HT f a proxy should be used, please confi	TP port TCP 443 which also sup figure the proxy settings in the n	pports going through a network proxy) nGuard Secure VPN Client ('Configuration -> Proxy	for VPN Path Finder').
 the VPN Path Finder (secure HT if a proxy should be used, please confi 	TP port TCP 443 which also sup	pports going through a network proxy) nGuard Secure VPN Client ('Configuration -> Proxy	for VPN Path Finder').
the VPN Path Finder (secure HT if a proxy should be used, please confi if a proxy should be used please confi if a p	TP port TCP 443 which also sup figure the proxy settings in the n	pports going through a network proxy) nGuard Secure VPN Client ('Configuration -> Proxy	for VPN Path Finder').
the VPN Path Finder (secure HT if a proxy should be used, please conf.	TP port TCP 443 which also sup figure the proxy settings in the n	pports going through a network proxy) nGuard Secure VPN Client ("Configuration -> Proxy	for VPN Path Finder').
the VPN Path Finder (secure HT	TP port TCP 443 which also sup figure the proxy settings in the n	pports going through a network proxy) nGuard Secure VPN Client ('Configuration -> Proxy	for VPN Path Finder').
the VPN Path Finder (secure HT if a proxy should be used, please conf if a proxy should be used, please conf	TP port TCP 443 which also sup figure the proxy settings in the n	pports going through a network proxy) nGuard Secure VPN Client ('Configuration -> Proxy	for VPN Path Finder').



- 12. Enter the IP address of the remote network your service technician will use to access the end machine.
- 13. Click Request to submit the information to the mGuard Secure Cloud

VPN-Builder I Request VPN configuration (service: Bob's iPad)	(
VPN client type > 2 VPN connection > 3 Machine network	
achine network	
ease enter the destination network, which you want to reach through your VPN connection, for example, IP address of the network: 192.168.1.0 and similar stars 255.255.0.	
we that the IP address of the network must be a private IP address, i.e. within the following subnets: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	
address of the network: *	
12.168.1.0	
etmask: WAN port LAN port Machine: 192.168.1.20	
13.255.255.0 Machine network:	
Tanoadoy heid 255.255.255.0	

The configurations are provided automatically and you can now choose to download the VPN configuration at this time.

Routing	VPN Builde	Language: Eng	iguration		pport i Log (
Service VPN tunnel offline > no secure con	/PN configuration successfu				
	You can now download the o	illy generated. onfiguration for your service work	station client.	- 1	
active VPNs all Service Workstation				- 1	
Workstations	Send via e-mail				
1 I Bob's iPad	O Download			- 1	≡
2 I Dan iPad					₹ Ξ
3 I Dan NCP					* =
4 I Kickoff iPad		I not connected			▲
5 I Mari ipad	i the user	Download	1 VPN: offline		▲
6 I Test Chris					▲
© Convrigh		Close			



You can follow the next videos in order to upload each configuration into the specific software:

mGuard Secure VPN Client

Shrewsoft VPN Client

<u>iOS VPN</u>

mGuard Hardware (using .atv file)

mGuard Hardware (using ECS file)



Service Targets (Machine) - VPN Builder

The following is a walkthrough guide showing the steps required to request a Machine VPN in order to connect your industrial devices to your account.

Requesting Machine VPN Configurations to the account

Your machines are added to the **Service Targets (Machines)** section of your account page. First you must add an Operator/Location tab then, under each location specify the individual remote machine. Note that you can name the Operator/Location as you like (project number, machine model, etc.) also, we recommend you use a unique and distinctive name for each remote machine. The machine names in the website are not tied to the user signing in or IP addresses of the mGuard devices.

To add a new Operator / Location:

- 14. Access the account webpage
- 15. Select the Service Targets (Machines) Tab
- 16. Click the swipe button to show all the operator/locations

MGuard secure cloud public					2.5.0
Account: PHO17100US User: mgallegos@phoenixcon.com Role: admin	age: English 🗸	Conta	act Help	& Support	ს Log out
Routing 🗱 Service Targets (Machines) Pervice Workstations	Administration	Logbook	Preferences		
Service VPN tunnel offline > no secure connection initiated > no secure remote access to service tar	get (machine)				
show operator/locat	ons: All 0-9 A-B (C-D E-F G-	H I-J K-L M-N	0-P Q-R S-T U	J-V W-X Y-Z
active VPNs					
active VPN connections to Service Targets					
On this tab, you can see all Service Targets like facilities and machines currently connected with immediately shows the current status of the VPN connections.	the mGuard Secure	Cloud publi	c via secure VPN	. Reloading this pa	ige via

17. Click on the blue circle/plus icon

18. Enter the Operator/Location name and click the OK option

active VPNs	CenterPoint Demo	LMS	PHC	399 Training	PxC HQ	Wireless Radio	
Add new ope	erator/location						\sim
Harrisburg	j, PA	*		Contact pers	ion:		
Street, ho	Street, house number:			Phone numb			
Zip code:				Fax:			
City:				E-mail addre	ISS:		
Country:				Notice:			
* = mandatory	Cancel				6	ĸ	
	Cancer				Ľ	ノ	

You have now created a single operator location and should see a new tab, in this example called

"Harrisburg, PA".



Next, you will need to add machines to this group. To do this:

- 19. Click on the newly created tab ("Harrisburg, PA" in this example).
- 20. Click on the blue circle/plus icon located under the location tab

Account PHO17100US User: mgallegos	@phoenixcon.com Role:	oud ^{public} admin			
Routing	Service Targets (Machi	nes) Service Wo	rkstations	Administ	ration
Service VPN tunnel offline > no secure con	nnection initiated >no secu	ire remote access to se	rvice target (ma	achine)	
	\frown				
active VPNs CenterPoint Demo	Harrisburg, PA LMS	PHC 399 Training	PxC HQ	Wireless Radio	$\bigcirc \oplus$
Harrisburg, PA					
1					

- 21. Enter a name to identify this machine (or VPN device). You may also add reference information.
- 22. Click OK

Add ne	ew machine
Machine name: *	Location:
Demo Machinery	
Type.	Positioning data (Lat, Long):
Serial number:	Inventory number:
Build year:	Cost center:
Monufacturar	Activation
Supplier:	Software:
68 2011-2018 PHOENIX C	NDACI Data privacy Legal Natice
Manufacturing number.	Notice:
Delivery day:	
* = mandstory field	
Cancel	OK



- 23. You will see the newly created machine device (following this example it's called "Demo Machinery")
- 24. Click on the VPN Builder button.

Account: PHO17	TOOUS User: mgallego	s@phoenixcon.con	e clou n Role: adm	in public				
Routing	\$	Service Targets	s (Machines)	Service Wor	kstations	Administ	tration	
Service VPN tunr	nel offline > no secure c	onnection initiated)	no secure re	emote access to ser	vice target (m	achine)		
active VPNs	CenterPoint Demo	Harrisburg, PA	LMS F	PHC 399 Training	PxC HQ	Wireless Radio	$\bigcirc \bigcirc$	
Harrisburg, F	PA							
1 Demo	Machinery	I	SN:	VPN: none	I s	tart 🚺		

A new window will open where you will see the parameters page. Here you first select the VPN mode desired for your hardware configuration. The options are:

- **Stealth:** In stealth mode, the mGuard behaves as a bridge (or switch) and will make a transparent connection between the internal and external ports. This means that the machine's network connected to its LAN port is integrated in the corporate network connected to its WAN port. If selected, the Secure Cloud administrator will still need a management IP address for accessing the mGuard's web interface.





 Router: In router mode, the mGuard will route between two different networks, the external (WAN) and internal (LAN). The device network connected to the LAN port is different from the corporate network connected to its WAN port.



- **Mobile (3G) or Ethernet plus 3G:** There is available hardware that can be used to connect the mGuard to our mSC server through the cellular network.
- 25. Select the mGuard mode

26. Click Next

	VPN Builder	Request VPN configu	uration (machine: Dem	o Machinery)		
1 mGuard mode	2 VPN connection		4 External network	5 Interna	al network	6 Misc.
mGuard operation mode						
The mGuard can operate in > if the machine is designed > if the end customer networ > if the machine is connected > Choose Ethernet plus 3G if	different modes: to fit into the existing networ c and the machine network a l via a mobile connection <i>M</i> c a mobile connection is use	k the <i>Stealth</i> mode (which be are different, the <i>Router</i> mode obile (3G) should be used. d as a fallback for an etherne	haves transparently to the net should be used to connect b t connection.	work) should be us oth networks.	ed.	
Choose a mode						
Stealth	: office					
Router Arbite (20))					
 Mobile (3G) Ethernet plus 3G 						
	/					
				Back	Next	

- 27. Select the desired port. IPsec VPN uses ports UDP 500/4500, if you know your network is blocking these ports outbound use the option via port TCP 443.
- 28. Click Next

	VPN Builder Request VPN cor	nfiguration (machine: Demo M	achinery)	glish 🗸 👔
1 mGuard mode	2 VPN connection 3 Mobile (3G)	4 External network	5 Internal network 6 M	Misc.
VPN connection mode (UD	P/TCP configuration)			
An mGuard VPN appliance car > When using standard IPsec p > When choosing secure HTTF encapsulation). An interconne	1 use different ports to establish a connection to a 20rts, the UDP ports 4500 and 500 must be opener 2 port TCP 443, IPsec traffic will be encapsulated a cted proxy server can also be used.	destination device: d for outbound IPsec traffic (also throug ind carried firewall friendly via standard	jh firewalls, proxies, etc.). TCP port 443 (TCP	
Connect through				
the standard IPsec ports	of UDP 500 and 4500			
the secure HTTP port TC	P 443 (this also supports going through a network	k proxy)		

29. If using a 3G mGuard follow procedure below. If not jump to step 17.

- a. Select the cellular provider (AT&T, Verizon or Generic) from the drop down box and type the APN for the SIM if needed.
- b. Click Next

Mobile (3G) configuration (optional)	
Select the Decider Type	Initiate VPN connection via SMS token
Provider Type:	Token:
Verizon CDMA (US)	vpn/start <token> vpn/stop <token></token></token>
Configuration 1. SIM Card	Configuration 2. SIM Card
SIM PIN for first SIM card:	SIM PIN for second SIM card:
APN (Access Point Name) for first SIM card:	APN (Access Point Name) for second SIM card:
Use PPP Admenacation.	Use PPP Authentication:
no	no 💌

PHOENIX CONTACT • PO. Box 4100 • Harrisburg, PA 17111-0100 Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625 E-mail: info@phoenixcontact.com • Website: www.phoenixcontact.com



- 30. Configure the external (WAN) network of the mGuard
 - a. Type the DNS configuration if available
 - b. Chose if your mGuard device will be receiving a WAN IP address through the DHCP server or statically assigned by you
 - c. Click Next

Vi N Duidei Request Vi N conligui	ration (machine: Demo Machinery)
1 mGuard mode 2 VPN connection 3 Mobile (3G)	4 External network 5 Internal network 6 Misc.
External network DNS configuration (optional) Enter the DNS Server Address used by the mGuard. IP address of DNS server (optional): Configuration external IP address Select the external IP address mode of the machine side mGuard VPN appliance:	External network: static IP or dynamic (DHCP) WAN port UAN port LAN port Machine network: 192.168.1.00 LAN port Machine network: 192.168.1.20
Choung Static IP address (DRCP) Ineans the insulat VPN appliance requires a fixed IP : Operand Static IP address (DRCP) Static IP address	address in the customer LAN.

- 31. Configure the Internal (LAN) network of the mGuard by typing the unique / reserved IP address
- 32. Click Next

Internal network The mGuard IP address (LAN port) machine network.	together with the Netma	isk of internal network is ti	e reserved IP of the	mGuard VPN appliar	nce in your	
Note that the IP address (LAN port): * 192.168.1.1 Netmask of internal network: * 255.255.255.0		External network static IP or dynamic (DHCP)	IN port	ternal network: 22 168 1 10 55 255 255 0 1 achine network: 25 265 10 55 255 255.0	Acchine:	



33. The last step is to select some miscellaneous items like the VPN extension file you will like to use to upload the configuration into the mGuard device

	VPN Bui	lder Request VPI	N configurati	on (machine: De	emo Machii	nery)		
1 mGuard mode	2 VPN connection	1 3 Mobile	(3G)	4 External networ	к 5	Internal n	etwork	6 Misc.
Misc.								
Choose the format of the VPI - type <i>atv</i> to upload the config - type <i>ecs</i> to activate the conf	N configuration for your guration via the mGuar figuration via external co	r machine connection: d web interface onfiguration memory (e.	.g. SD card, USE	stick)				
Format of the mGuard config	guration file:	\mathbf{b}						
Please enter the serial numl	ber of the mGuard VPN	appliance to configure	(optional):					
mGuard serial number:								
Shall the vpn connection be i	initiated via a key switc	h (Service-IO)?						
no	•							

The configurations are provided automatically and you can now choose to download the VPN configuration at this time.

PxC HQ	VPN Builder Request VPN machine configuration	×
You can no	N configuration successfully generated w download the configuration for your machine VPN client.	
	▲ Download file	
	Close	

You can follow the next videos in order to upload each configuration into the specific software:

mGuard Hardware (using .atv file)

mGuard Hardware (using ECS file)



Starting the VPN Client

The following is a walkthrough guide showing the steps required start your service VPN

Starting Shrewsoft client

To start your Shrewsoft VPN you must have downloaded the Shrewsoft software client from <u>www.shrew.net/download</u> and requested the mGuard Service VPN for Shrewsoft configuration from the cloud (Check Service VPN Builder steps).

1. Locate the Shrewsoft start icon and start the software client



2. Double-click on the new connection icon. You will then see the VPN Connect window

ile Edit View Help		
Sopport Add Modify	Delete	
	Host Name	Authentication
	· · ·	Addiencectori
6 PHO17000US.vpn	service-gw1.us.mguar	mutual-rsa
PHO17000US_SS_John Fi	4.49.121.19	mutual-rsa
B PHO17000US_SS_Toenni	service-gw1.us.mguar	mutual-rsa
🖲 pxcmguard2.dnsalias.net	pxcmguard2.dnsalias	mutual-rsa
🖰 SDTech1	pxcmguard2.dnsalias	mutual-rsa
🖰 SDTech2	pxcmguard2.dnsalias	mutual-rsa
🖰 SDTech3	pxcmguard2.dnsalias	mutual-rsa
🖰 SDTech4	pxcmguard2.dnsalias	mutual-rsa
B SDTech5	pxcmguard2.dnsalias	mutual-rsa
B SHR97000US_Tech_Shre	4.49.121.19	mutual-rsa
B To Sierra Portal	4.49.121.19 mutual-rsa	
B TRA80200US_S1.vpn	service-gw1.us.mguar	mutual-rsa
🖲 Voith - Benjamin	10.1.10.253	mutual-rsa
NPN configuration Terry	4.49.121.19	mutual-rsa

- 3. Click the Connect button. You will then be prompted to enter the pre-configured password (This is the password you entered when requesting the VPN through the Service VPN Builder).
- 4. Click OK



S VPN C C	onnect - PHO17000US
config la attache peer co iskamp esp pro client co local id remote server o client co	vaded for site 'PH017000US.vpn' d to key daemon nfigured proposal configured posal configured sonfigured d configured ert configured ert configured
	Connect Exit
Passwo	rd for PHO17000US_S_Mari
	Cike Cancel

Starting the mGuard Secure VPN Client

To start your mGSVC you must have downloaded the software client from

<u>https://www.phoenixcontact.com/msc</u> and requested the mGSVC VPN configuration from the cloud (Check Service VPN Builder steps).

1. Locate the mGSVC start icon and start the software client



2. With the mGSVC window open, click/swipe the connection button



PHOENIX CONTACT • P.O. Box 4100 • Harrisburg, PA 17111-0100 Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625 E-mail: info@phoenixcontact.com • Website: www.phoenixcontact.com



- 3. You will then be prompted to enter the pre-configured PIN or password (This is the password you entered when requesting the VPN through the Service VPN Builder).
- 4. Click OK
- 5. Confirm the established connection

	🛞 mGuard Secure VPN Client
	Connection Configuration View Help
Enter PIN	Connection Profile: Connection:
Please enter the PIN of your certificate!	PH01/1000552560645
PIN:	Connection established.
<u>O</u> K <u>C</u> ancel	mGuard

No matter the service VPN software used, your mGuard Secure Cloud status bar should look like the image below after the VPN is authenticated succesully.

	Account: PHO17100US User: mgallegos	@phoenixcon.com Role: admin	public	
\langle	Routing	Service Targets (Machines)	Service Workstations	
	Service VPN tunnel online > no secure con	nnection initiated >no secure rem	note access to service target (ma	chine)



Taking to your end devices

The following is a walkthrough guide showing the steps required to start the VPN to your machine and talking to your end devices.

1. Make sure the Service Target (Machine) and the Service Workstation are both connected to the cloud and have the online status (both circled in the image below)

Account PHO17100US User	mgallegos@phoenixcon.con	re cloud n Role: admin	l public				
Routing	Service Targets	s (Machines)	Service Wo	rkstations	Adminis	tration	Logbook
Service VPN tunnel online >n	secure connection initiated and the secure connection initiated an	no secure remo	ote access to se	vice target (ma PxC HQ	chine) Wireless Radio		()
active VPN connections	to Service Targets						
On this tab, you can see a	II Service Targets like facilities	s and machines	currently connec	ted with the mG	Guard Secure Clou	d public via se	ecure VPN. Reloading this pag
1 Harrisburg, PA	1	Demo Machiner	у	I	SN:	VPN: onl	ine Start

2. To link the service workstation to the machine, click on the Start button.

Account PHO17100US	User: mgallego	s@phoenixcon.com	e clo	ud ^{public} Imin					
A Routing	e e	Service Targets	(Machine	es) Service Wo	rkstations	Administ	tration	Log	book
Service VPN tunnel onli	ne 🕽 no secure co	onnection initiated >	no secure	e remote access to se	rvice target (ma	ichine)			
active VPNs Cen	terPoint Demo	Harrisburg, PA	LMS	PHC 399 Training	PxC HQ	Wireless Radio		Ð	
active VPN connect	tions to Service	e Targets							
On this tab, you car	i see all Service T	argets like facilities	and mach	nines currently connec	ted with the mG	Guard Secure Cloue	d public via se	cure VPN. Reloa	ding this pag
1 Harrisburg, F	PA	1	Demo Mac	chinery	I	SN:	VPN: onlin	ne St	art

- 3. After a cloud has established a successful connection between the service technician and the machine, you will see the following status indicators on your account page:
 - The Service, Routing, and Machine status icons at the top of the page will all turn green.
 - The Start button has changed to a Stop button.

INSPIRING INNOVATIONS

Account: PH0171	OUS User: mgallego	s@phoenixcon.com	e clou n Role: adr	nin public				
- Routing		Service Targets	(Machines	s) Service Wo	rkstations	Adminis	tration	Logbook
Service VPN tunn	el online > secure conr	ection initiated >Ha	arrisburg, P/	A / Demo Machinery				
active VPNs	CenterPoint Demo	Harrisburg, PA	LMS	PHC 399 Training	PxC HQ	Wireless Radio		-)
active VPN co	onnections to Servic	e Targets						
On this tab, y	ou can see all Service 1	fargets like facilities	and machi	nes currently connec	ted with the mo	Guard Secure Clou	d public via sec	cure VPN. Reloading thi
1 Harris	burg, PA	T	Demo Mach	ninery		SN:	VPN: onlir	ne I Stop

The service technician can now access the mGuard machine and all other end-devices via the mGuard Secure Cloud connection.

Administrator: C:\WINDOWS\system32\cmd.exe
C:\Users\mcoladon>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data: Reply from 192.168.1.1: bytes=32 time=1ms TTL=62 Reply from 192.168.1.1: bytes=32 time=1ms TTL=62 Reply from 192.168.1.1: bytes=32 time=1ms TTL=62 Reply from 192.168.1.1: bytes=32 time=1ms TTL=62
Ping statistics for 192.168.1.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\Users\mcoladon>

When the users are ready to disconnect from the machine, click on the Stop button. Note that clicking in another Start button in a second machine will stop the original tunnel and connect you to the last machine chosen.



Extra: Additional Users

Additional users can be added to the account. These users will then be able to access the Secure Cloud account page where they can start tunnel connections, or add and remove Service workstations, etc.

If an added technician is given the role of admin, they will then have all the privileges that the main admin has. That means that user with Admin roles can create new workstations and machine locations, as well as, request VPN configurations. Unlike an added technician is given the role of user, they will only have the rights to start the VPN tunnels to the remote machines in order to access them.

To add additional users to the account, do the following:

- 1. When in the mGuard Secure Cloud account page, click on the Administration tab
- 2. Next, click on the User administrator tab
- 3. Click the New User option at the top of the page

MGuard	secure cloud public	Language: English 🗸	Contact Help & Support 也Lo	2.5.0 og out
Routing 🗱	Service Targets (Machines) Service Wo	orkstation Administration Logboo	ook Preferences	
Service VPN tunnel offline > no secure conne	action initiated ≯no secure remote access to	service target (machine)		
User administration Access permission	ns VPN connections Account data	Master data Info & Downloads	Release Notes	
User administration				
New User				

You will then see the new user registration form appear below the New User button.

4. Complete the form and then click the Apply user option



User name (valid e-mail address): *	Password: *
jdoe@phoenixcon.com	
Last name: *	Repeat password: *
Doe	
First name: *	User State:
John	Enabled •
Role: *	
Admin	Ŧ
* = mandatory field - passwords must be at least 8 characters long and si	hould contain letters, numbers and special characters.
Cancel	OK
0411001	



Extra: iOS Procedure

The mGuard Secure Cloud 2.5 firmware gives your technicians the ability to access remote machines via iOS devices like iPads and iPhones. The following is a walkthrough guide showing the steps required to utilize the secure cloud through an iPhone or iPad device:

Adding Service Technicians to an account

Service technicians are added to the **Service Workstation** section of your account page. Note that you can name the service workstations as the technician by first and/or last name, by computer number or other functions. The service workstation name in the website is not tied to the user signing in.

To add a Service technician:

- 35. Access the account webpage
- 36. Select the Service Workstations Tab
- 37. Click on the blue circle/plus icon
- 38. Enter the workstation name and click the OK option (bottom)

হ		9:41 AM					∦ 28% 🗉
: > 📖 🗌		77.245.33.75			Ċ	: 1	+ 🗇
mGu	ard (mGuard-Portal-GW)	\otimes		mGuard Se	ecure Cloud se	rvice	
DOUNT: PHO17000US I User: c	Incompared secure clo	ud ^{public}	Language: Eng	glish 🗸 I	Contact	Help & Suppo	2.5.0-pre00
Routing	Service Targets (Machines)	Service Workstations	Administration	Logbook	Preferences		
rvice VPN tunnel offline > no s	secure connection initiated >no secure r	remote access to service ta	get (machine)				
active VPNs all Service V	Vorkstations						
Add new workstation	Ŭ						
Bob's iPad	*						
Notice:							
* = mandatory field							
Can	cel	(ок)					

- 39. Next, click on the all Service Workstations tab (Figure 2)
- 40. Click on the drop-down arrow next to the workstation
- 41. Select the New Contact you just created
- 42. Click on the VPN Builder button.



iPad ᅙ		9:41 AM					* 28% 💷
$\langle \rangle$	₽ 77.245.33.75				Ċ	Û	+
mGuard (mGua	rd-Portal-GW)	\otimes		mGuard Sec	cure Cloud serv	ice	
M Guard	secure clou	I d ^{public}					2.5.0-pre00
Account: PHO17000US I User: dschaffer@	phoenixcon.com Role: admin		Language: En	glish 🗸 I	Contact I H	lelp & Supp	oort I Log out
Routing	Service Targets (Machines)	Service Workstations	Administration	Logbook	Preferences		
Service VPN tunnel offline > no secure cor	nection initiated >no secure ren	note access to service	target (machine)				
active VPNs all Service Workstation	ns 🕂						
Workstations	-						
1 I Bob's iPad	I no user		I not connected	I VPN: of	fline	/	> ≡

A new window will open where you will see the parameters page (Figure 3). Here you first select the VPN client desired for your service technician configuration, in this case the iOS VPN Client. Then type your own password for the service VPN authentication, you will need this password on step 13. Make sure you choose a strong one.

			9:42 /	AM					X	2
< > []			₿ 77.245	5.33.75			¢	Û	+	
	mGuard (mGuard-Portal-G	N)		\otimes		mGuard Secure	Cloud service			
1 VPN client type	2 VPN conne		3 Machine ne	etwork						
VPN client type										
What kind of VPN clien via <i>mGuard VPN applia</i> You may also use a cer	t are you going to use for this ances like mGuard smart ² or tifiied software IPsec VPN cl	s service worksta mGuard delta ² . ient like the <i>mGu</i>	ation? Your worksta uard Secure VPN (ation can be s Client.	securely conne	cted to the mGua	ard Secure Clou	d public		
Choose a VPN client t	vpe									
mGuard Secure	VPN Client (commercial sof	tware client with	vendor support)							
Shrew Soft VPN	Client (free software client	w/o vendor supp	ort)							
iOS VPN-Client	(Apple iPad)									
mGuard VPN a	ppliance (hardware)									
Please enter the clien	t password:									
Password: *					Repeat pas	sword: *				
						•		\odot		



- 43. Enter the IP address of the remote network your service technician will use to access the end machine.
- 44. Click Request to submit the information to the mGuard Secure Cloud

id 🗟		9:43 AM				*	28%
< > 📖 📃		₿ 77.245.33.75		¢	Û	+	Ć
	mGuard (mGuard-Portal-GW)) mG	uard Secure Cloud service	0		
mGua	VPN-Builder I R	lequest VPN configura	tion (service: Bob's iPad)			
1 VPN client type	2 VPN connection 🔰 3 N	Machine network					
Machine network							
Please enter the destination ne Neimask: 255.255.255.0.	twork, which you want to reach through yo	our VPN connection, for exam	ple, IP address of the network: 1	92.168.1.0 and			
Note that the IP address of the	network must be a private IP address, i.e.	within the following subnets:	10.0.0.0/8, 172.16.0.0/12, 192.16	68.0.0/16			
IP address of the network: *							
192.168.1.0		1770					
Natmask		WAN port	AN port	Machine:			
255.255.255.0				192.168.1.20			
- nandaton/field			Machine network:	1 A			
= mandatory field			255.255.255.0				
						_	
				and the second			

You can now choose to download the iOS VPN configuration at this time (recommended if steps 1-8 were done in iOS device), or select send via-email to the iOS device itself.



iPad ᅙ		9:43 AM				* 28% 💷
$\langle \rangle$		₽ 77.245.33.75		¢	Û	$+$ \Box
mGuard (mGuard	I-Portal-GW)	\otimes	mGuard Secure 0	Cloud service		
M Guard	secure clou	d ^{public}				2.5.0-pre00
Account: PHO17000US I User: dschaffer@p	hoenixcon.com I Role: admin	Langu	uage: English 🗸 I Con	tact Help &	& Suppo	ort I Log out
Routing	VPN Bui	der I Request service V	PN configuration	\mathbf{x}		
Service VPN tunnel offline > no secure con	VPN configuration succes You can now download th	sfully generated. e configuration for your ser	vice workstation client.		L	
active VPNs all Service Workstation	\frown				н.	
Workstations	Send via e-mail					
1 I Bob's iPad	Download					\equiv
2 I Dan iPad					*	
3 I Dan NCP					*	
4 I Kickoff iPad		I not con			*	
5 I Mari ipad	1 no usor	Download			1	
6 I Test Chris					*	
© Copyrigh		Close				

Installation procedure of VPN configuration in iPhone/iPad

After you received the configuration by email in the iOS device, or click in the download link (shown in Figure 5) the system will automatically send you to the General settings – Install Profiles page. It is fairly simple to perform the VPN profile installation, just follow the instructions in the device and type the corresponding passwords when prompted.



iPad ᅙ			12:18 PM		∦ 42% 💽
	Settings		🗙 General	Profiles & Device Manage	ement
		Cancel	Install Profile		
↔	Airplane Mode				
(?	Wi-Fi	рно	17000USS768		
*	Bluetooth	mSC	Public		
VPN	VPN	Signed by Not S	igned		
		Contains VPN	ce VPN Profile for mSC Public		
	Notifications	2 Cer	tificates		
8	Control Center	More Details		>	
٦	Do Not Disturb				
Ø	General				
AA	Display & Brightness				
	Wallpaper				
()	Sounds				
	Touch ID & Passcode				

- 45. Perform the installation of the profile (should be showing your account ID in the configuration name)
- 46. Type the iOS device passcode (the one you use to unlock the device)



iPad 🤶				9:44 AM			∦ 28% ■
	Settings		🗙 General		Pro	ofile	
				Install Profile			
✐	Airplane Mode			Fata Davad	- Carred		
?	Wi-Fi p	Summing the	-	Enter Passcoo	e Cancel		
*	Bluetooth						
		Signed		Enter your passco	de		
	Notifications	Descrip	the second		-)	
8	Control Center	Cont	ains				
C	Do Not Disturb	More D	etail:				
			1	2 _{АВС}	3 Def		
AA	Display & Brightness		4	5	6		
	Wallpaper		дні 7	JKL 8	MNO Q		
=))	Sounds		PQRS	TUV	WXYZ		
A	Passcode			0			
	Privacy						
	iCloud						

47. After the device passcode is authenticated, click Next

iPad 奈				9:44 AM		* 28% 💷
	Settings		< General		Profile	
		Cancel		Consent	Next	
≻	Airplane Mode					/
?	Wi-Fi p	MESSAG	E FROM "MSC PUBLIC"			
*	Bluetooth	Service \	/PN profile for mSC I	Public will be installed		
	Notifications					
8	Control Center					
C	Do Not Disturb					
Ø						
AA	Display & Brightness					
	Wallpaper					
(())	Sounds					
A	Passcode					
	Privacy					
	iCloud					

48. Click Install twice



iPad ᅙ		9:44 AM				* 28% 💷	
	Settings		〈 General		Profile		
	Airplane Mode	Cancel		Warning	Install	\supset	
~	Wi-Fi p	ROOT CE	RTIFICATE				
*	Bluetooth	Installing trusted c	the certificate "P ertificates on you	HO17000US-CA" wil r iPad.	I add it to the list of		
G	Notifications	VPN					
8	Control Center	The netw monitore	ork traffic of your d by a VPN serve	iPad may be secure r.	d, filtered, or		
C	Do Not Disturb	UNSIGNE	D PROFILE				
Ø		The profi	le is not signed.				
AA	Display & Brightness						
*	Wallpaper						
()	Sounds						
	Passcode						
	Privacy						
	iCloud						

iPad 🤶			(9:44 AM		* 28% 💷
	Settings		< General		Profile	
		Cancel	Ŵ	arning	Install	
	Airplane Mode					
?	Wi-Fi p	ROOT CE	RTIFICATE			
*	Bluetooth	Installing trusted c	the certificate "PHO17 ertificates on your iPac	7000US-CA" will add I.	d it to the list of	
	Notifications	VPN				
8	Control Center	The netw monitore	ork traffic of your iPad	may be secured, fil	tered, or	
C	Do Not Disturb		Insta	all Profile		
		UNSIGNE	Cancel	Install		
Ø		The profi	le is not signed.			
AA	Display & Brightness					
*	Wallpaper					
	Sounds					
A	Passcode					
	Privacy					
	iCloud					

- 49. Enter the password that you created for the VPN configuration (this is the password typed in Figure 3, after step 6 doing the VPN Builder feature for iOS)
- 50. Click Next



iPad ᅙ				9:45 AM		* 28% 💷
	Settings		〈 General		Profile	
		Cancel	Ente	r Password	Next	
\rightarrow	Airplane Mode					
?	Wi-Fi	ENTER TH	HE PASSWORD FOR THE C	ERTIFICATE "PHOTOSOO	USS778.P12"	
*	Bluetooth	•••••	••••			
		muired	by the "PHO17000USS778"	profile		
	Notifications					
8	Control Center					
C	Do Not Disturb					
Ø	General					
AA	Display & Brightness					
	Wallpaper					
=))	Sounds					
A	Passcode					
	Privacy					
	iCloud					

51. Click Done

iPad 🤶		9:4	5 AM	∦ 28% ■
	Settings	General	Profile	
		Profile	Installed Done	
	Airplane Mode			
?	Wi-Fi p	And the second s		
*	Bluetooth	mSC Public		
VPN	VPN	Signed by Not Signed		
		Description Service VPN Profile for mSC	Public	
6	Notifications	Contains VPN Settings 2 Certificates		
B	Control Center	More Details	>	
C	Do Not Disturb			
Ø				
A	Display & Brightness			
*	Wallpaper			
	Sounds			
8	Passcode			
C	Privacy			

52. Make sure your mGuard Secure Cloud VPN profile is selected (Settings / VPN) and the swipe the VPN switch to enable it

iPad ᅙ	Settings		iPad 후 IPB Settings	
<mark>⊳</mark>	Airplane Mode	\bigcirc	Airplane Mode	\bigcirc
?	Wi-Fi	pxcguest	🛜 Wi-Fi	pxcguest
*	Bluetooth	On	8 Bluetooth	On
VPN	VPN		VPN VPN	

Now that the VPN is enabled and established, go back to the mGuard Secure Cloud through Safari. If you are already familiar using the mSC, your service indicator will be green allowing you to "START" a machine connection. If you aren't sure how to start the tunnel to your remote machine continue following the next steps.

Starting the Secure Cloud tunnel between the Service technician and a Machine

After the Machine device (mGuard/3G modem) and the Service device (in this case the iOS) have both tunneled into the Secure Cloud server, you must connect the Service technician to the Machine via your Secure Cloud account page.

Note: The iPad/iPhone device used to access the cloud account must also have enabled the VPN client (Step 16).

- 53. Access you mGuard Secure Cloud account and click on the Service Workstations tab. If the service technician device is truly connected to the cloud you should see two indicators:
 - The Service tab, as shown in the following diagram, will be green
 - The Workstation which has made the service technician connection to the cloud will have an online status

	INSPIRING INNOVATIONS	

iPad 🗢 VPN		9:46 AM			∦ 26% 🛙	
$\langle \rangle$		₽ 77.245.33.75		Ç	Ô + Ó]
	mGuard (mGuard-Portal-GW)	\otimes	mGuard Se	cure Cloud service		
Account: PHO17000US I Us	ser: dschaffer@phoenixcon.com I Role: admin	<i>Id^{, public}</i>	anguage: English 🗸 I	Contact Help 8	2.5.0-pre00 & Support I Log out	D t
Routing 🗱	Service Targets (Machines)	Service Workstations	Administration Logbook	Preferences		
Service VPN tunnel online >	no secure connection initiated > no secure re	mote access to service targe	et (machine)			
active VPN connection	ns to Service Workstations					
On this tab, you can see immediately shows you	e all Service Workstations currently connected the current status of the VPN connections.	with the service gateway of	the mGuard Secure Cloud v	ia VPN. Reloading this	s page via 🧭	
1 I Bob's iPac	d I dschaffer@phc	enixcon.com I no	ot connected VPN: on	line	≡	
	© Copyright 2011-2016 Phoenix Contact Cyt	er Security AG I Data privacy I	Evaluation License Agreemen	t I Legal Notice		

- 54. Next, click on the Service Targets (Machines) tab (Figure 15). You will see that you have an active Machine (online). The account page is confirming that the machine device (mGuard/3G modem) is currently connected to the cloud.
- 55. To link the service workstation to the machine, click on the Start button.

iPad 🗢 VPN	9:	46 AM					* 26% 💷		
$\langle \rangle$	₽ 77.2	245.33.75			¢	Û	+		
	mGuard (mGuard-Portal-GW)	\otimes	mGuar	rd Secure Cloud	activeconne	ctions			
Account: PHO17000US I	User: dschaffer@phoenixcon.com I Role: admin	c	Language: Engli	ish ✔ I Con	ntact I Help	& Suppo	2.5.0-pre00		
Routing	Service Targets (Machines) Pervice W	/orkstations	Administration	Logbook Pre	eferences				
Service VPN tunnel online > no secure connection initiated > no secure remote access to service target (machine)									
	show operator	r/location: All	0-9 A-B C-D E-	FIG-HII-JIK-I	LIM-NIO-PI	Q-RIS-TI	U-V I W-X I Y-Z		
active VPNs									
active VPN connecti	ons to Service Targets								
On this tab, you can s via 😂 immediately s	see all Service Targets like facilities and machines currently c shows the current status of the VPN connections.	connected wit	h the mGuard Secure	e Cloud public v	ia secure VPN.	. Reloading	this page		
1 I Kickoff D	Demo I Demo unit		I SN:	I VPN	N: online	Start			
© Copyright 2011-2016 Phoenix Contact Cyber Security AG I Data privacy I Evaluation License Agreement I Legal Notice									

After a cloud has established a successful connection between the service technician and the

machine, you will see the following status indicators on your account page:



- The Service, Routing, and Machine tabs at the top of the page will all turn green.
- The VPN status is online.
 - The Start button has changed to a Stop button.

iPad 🗢 VPN		9:46 AM						*	26% 💷
$\langle \rangle$	₽ 77.245.33.75			Ç	Û	+			
Account: PHO17000US I User: dschaf	d secure cloud	public	Language: I	English 🗸	I Contact I	Help	& Suppo	2. ort I Lo	5.0-pre00
Routing 🔅	Service Targets (Machines) Ser	rvice Workstations	Administration	Logbook	Preferences				
Service VPN tunnel online > secure co	nnection initiated > Kickoff Demo / Der	mo unit v operator/location:	All 0-9 A-B C-E) E-F G-H	-J K-L M-N	O-P C)-RIS-TI	U-VIW-	-X Y-Z
active VPNs									
active VPN connections to Service	vice Targets								
On this tab, you can see all Servic via immediately shows the cu	e Targets like facilities and machines c rrent status of the VPN connections.	currently connected	with the mGuard S	ecure Cloud	public via secur	re VPN. I	Reloading	this pag	e
1 I Kickoff Demo	I Demo unit		I SN	:	I VPN: online	e I	Stop		

The service technician can now access the machine device via the mGuard Secure Cloud connection.

When the users are ready to disconnect from the machine, click on the Stop button. Note that clicking another Start button in a second machine will stop the original tunnel and connect you to the last machine chosen.

Note: Remember there are more mGuard videos in the Phoenix Contact YouTube Channel. If you have any questions email the mSC admins at <u>portal@phoenixcon.com</u>