mGuard Secure Cloud Starting Guide

Table of Contents

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

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

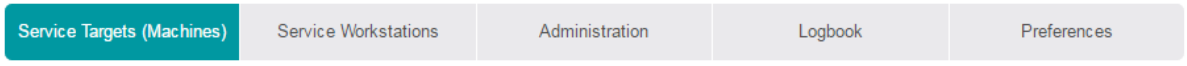
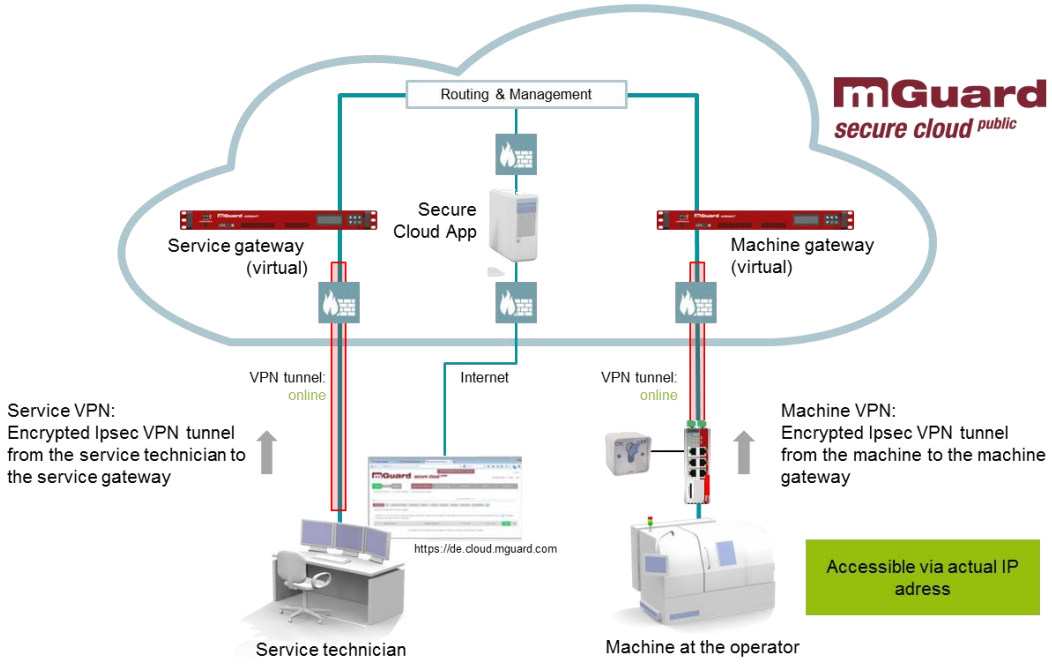


Figure 1 – mGuard Secure Cloud Main Menu

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.



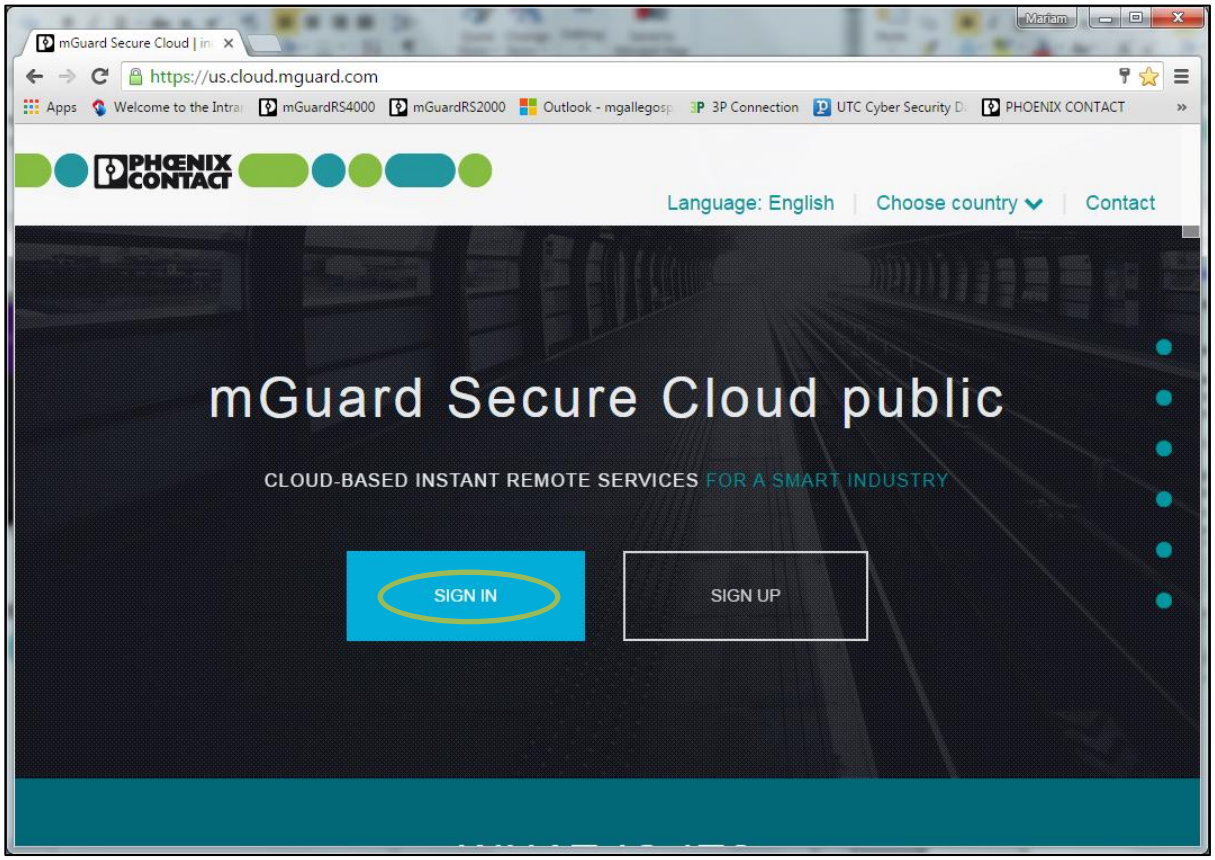
Service Workstations	Service Target (Machines)
Unlimited technicians and engineers can be added to the mSC for free	Unlimited machines and locations can be added in the mSC for free
Unique Service VPNs are required in order for them to cooperate in machines at the same time	An mGuard hardware device 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

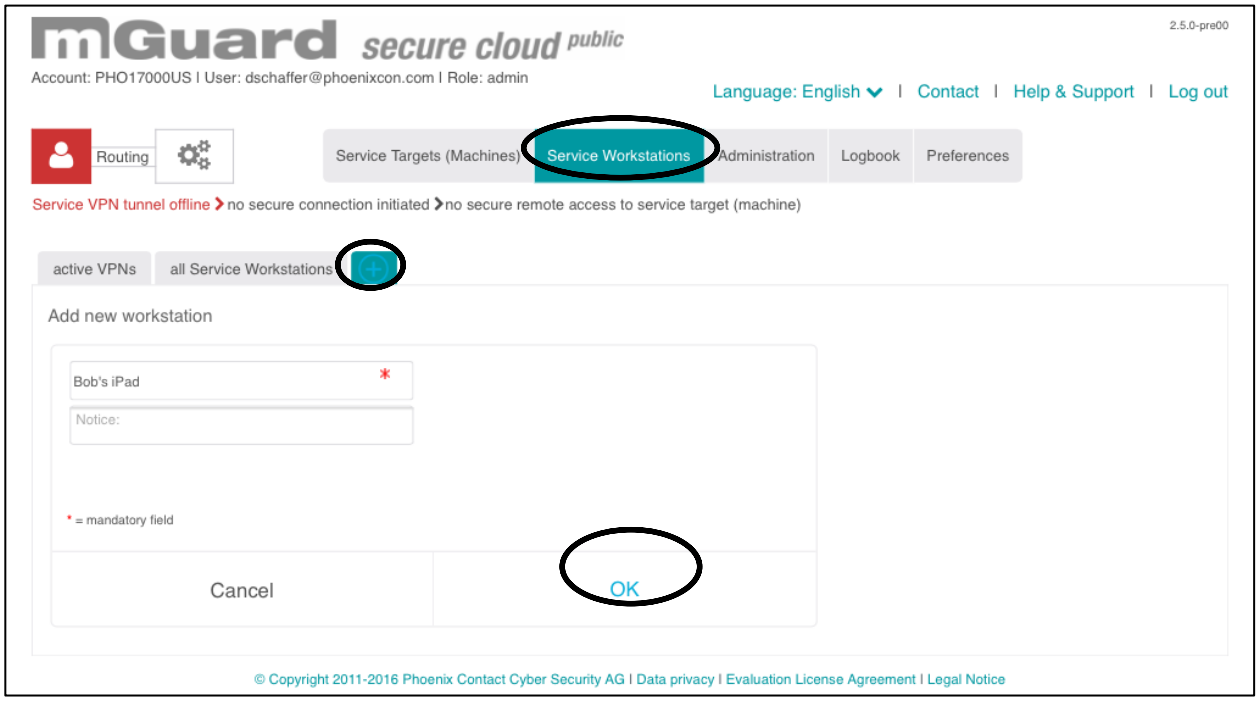
The following is a walkthrough guide showing the steps required to request the service VPN to all technicians and support engineers in the account.

Requesting Service VPN Configurations to the account

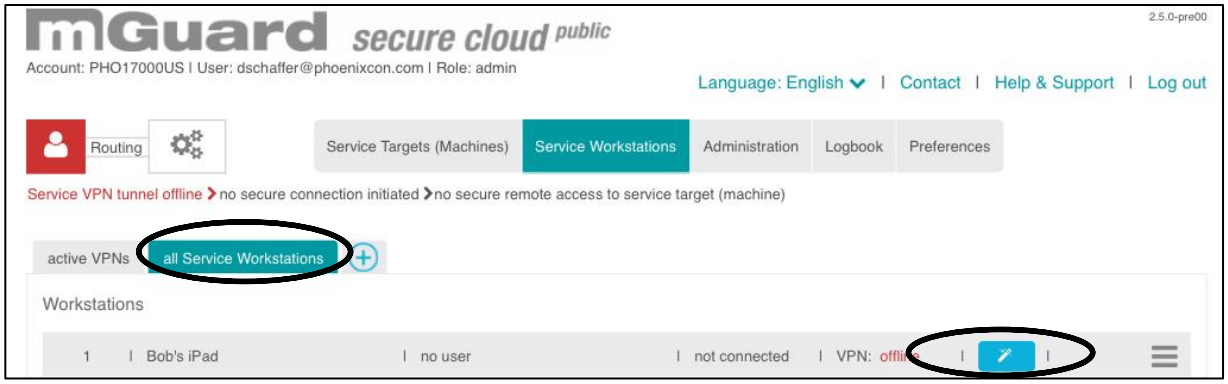
Service technicians are added to the **Service Workstation** section of your account page. Note that you can name the service workstations as the technician by first and/or last name, by computer number or other functions. The service workstation name in the website is not tied to the user signing in.

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)



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.



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. Download the 30-day-free-trial of the mGuard Secure VPN Client here

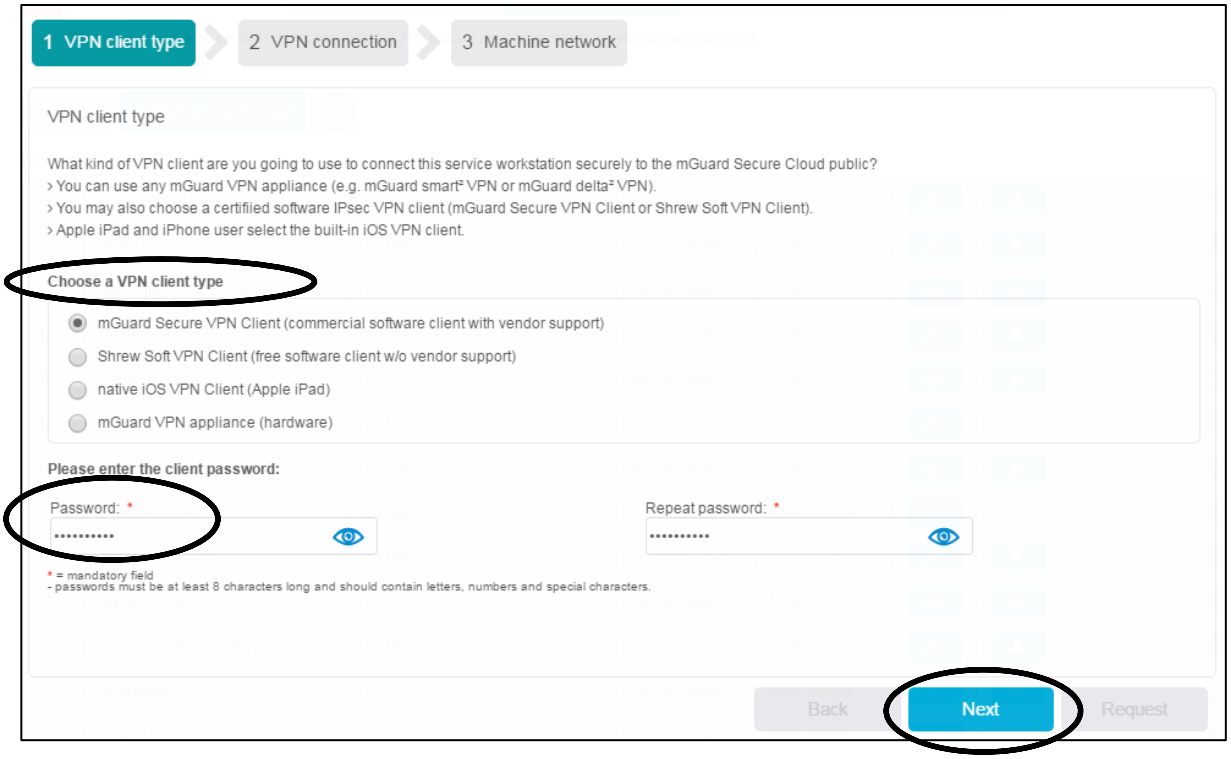
- **Shrewsoft VPN Client:** Shrewsoft is a free, third party open source VPN client that can be used to tunnel into the mSC. It is great for basic connections, but it doesn't support Proxies or using alternate VPN ports. Download the free Shrewsoft VPN here

- **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.

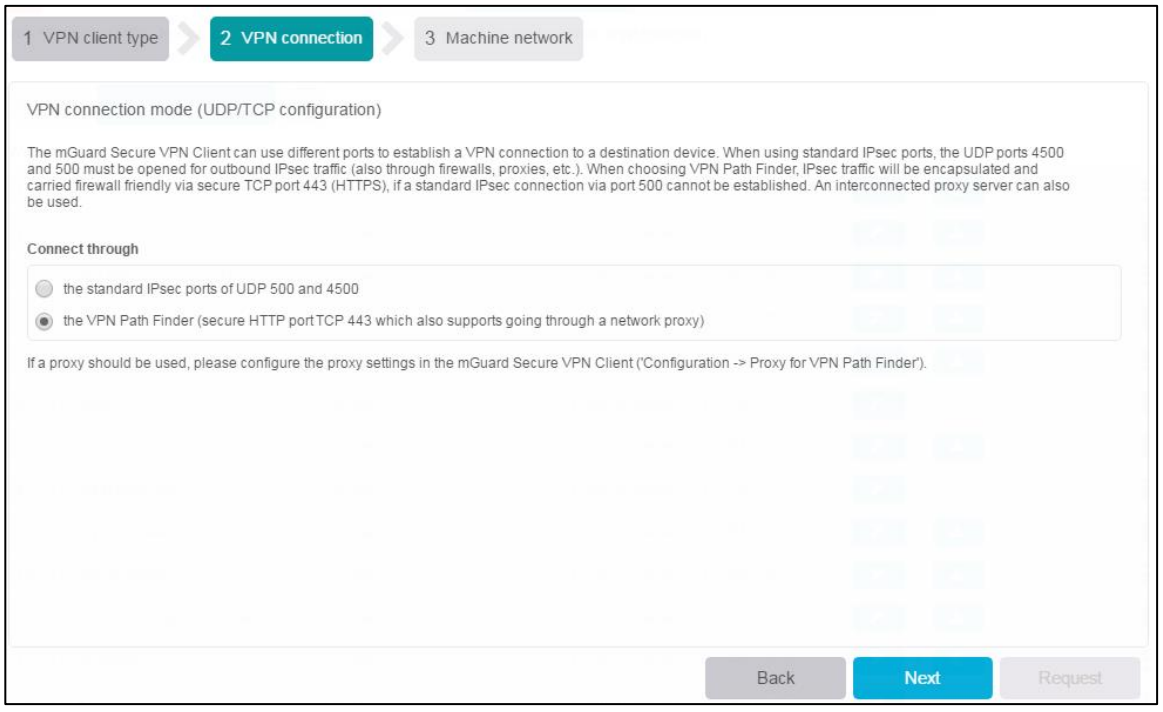
9. Select the desired option and then type your own password for the service VPN authentication.

10. Click Next

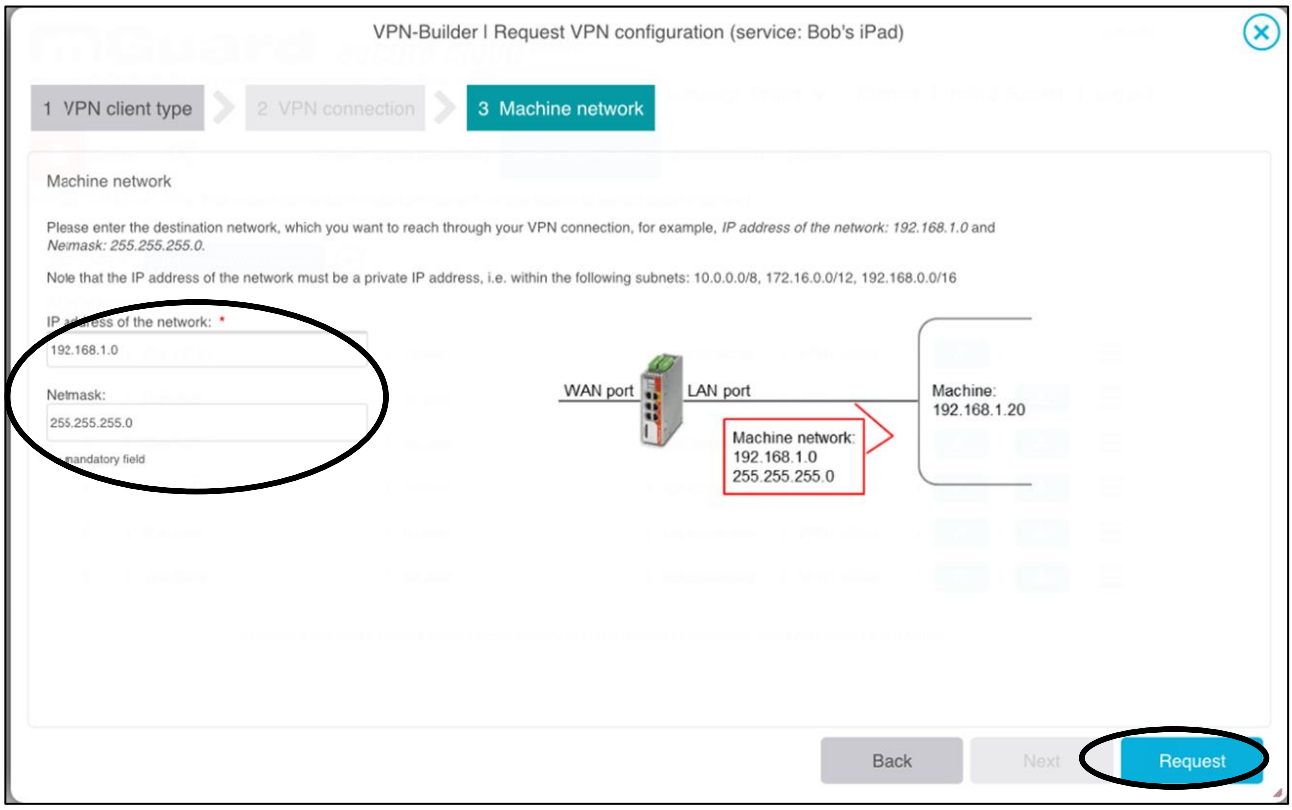


If you selected the mGuard Secure VPN Client or the mGuard Hardware continue with next step, if not continue in step 12.

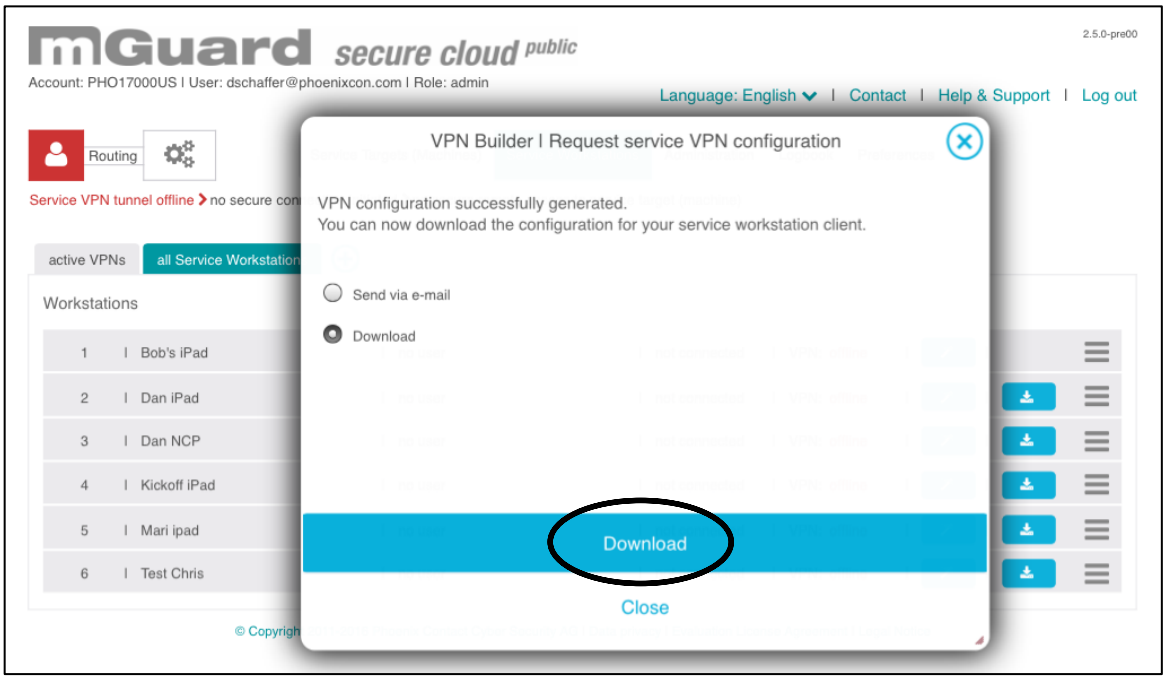
11. Select the desired port. IPsec VPN uses ports UDP 500/4500, if you know your network is blocking these ports going outbound use the VPN Path Finder option via port TCP 443.



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



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



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

mGuard Secure VPN Client

Shrewsoft VPN Client

iOS VPN

mGuard Hardware (using .atv file)

mGuard Hardware (using ECS file)

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

Service Targets (Machine) - VPN Builder

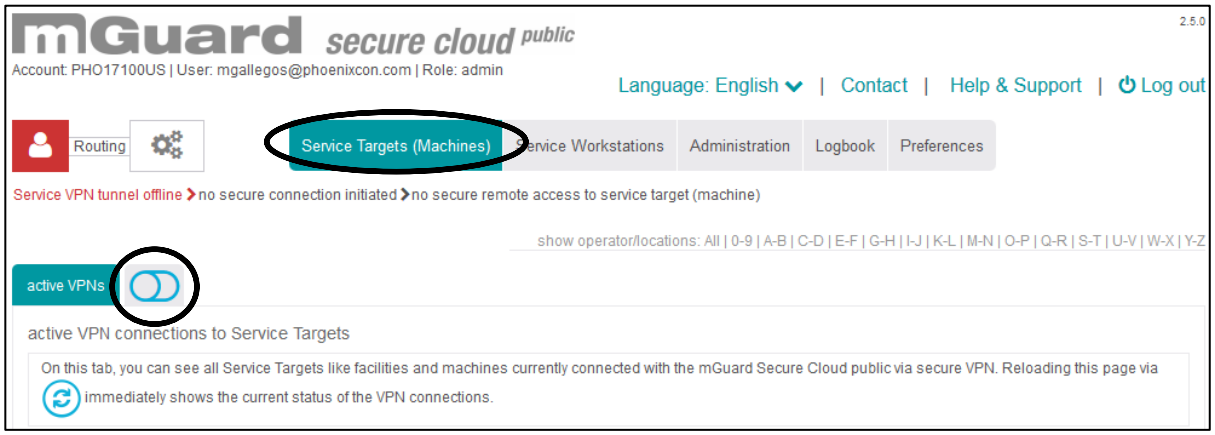
The following is a walkthrough guide showing the steps required to request a Machine VPN in order to connect your industrial devices to your account.

Requesting Machine VPN Configurations to the account

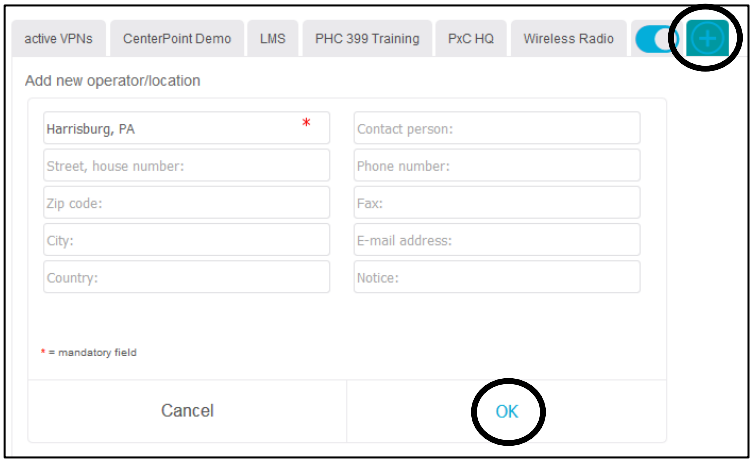
Your machines are added to the **Service Targets (Machines)** section of your account page. First you must add an Operator/Location tab then, under each location specify the individual remote machine. Note that you can name the Operator/Location as you like (project number, machine model, etc.) also, 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



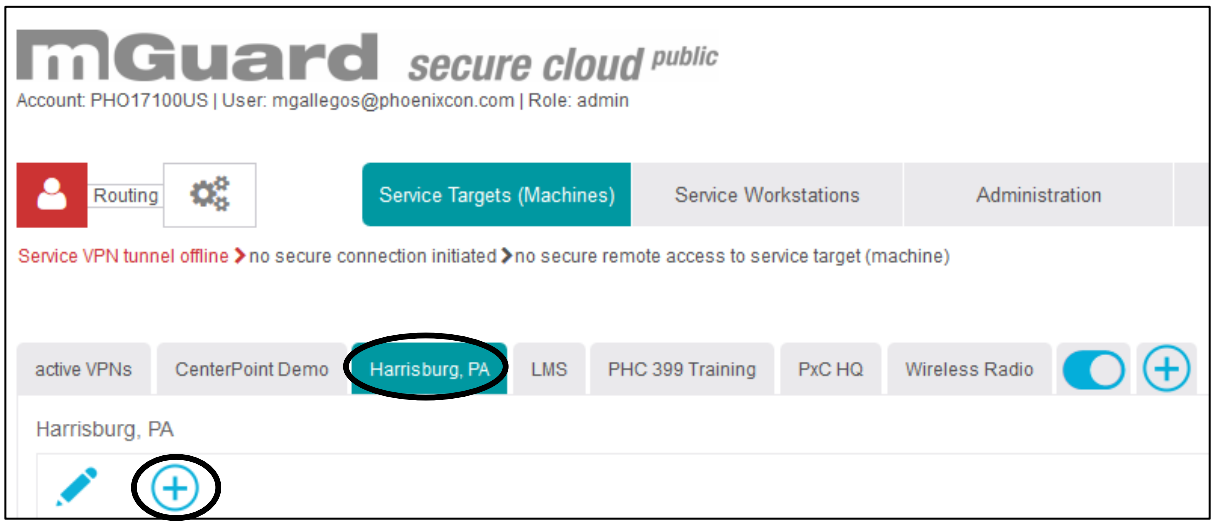
17. Click on the blue circle/plus icon
18. Enter the Operator/Location name and click the OK option



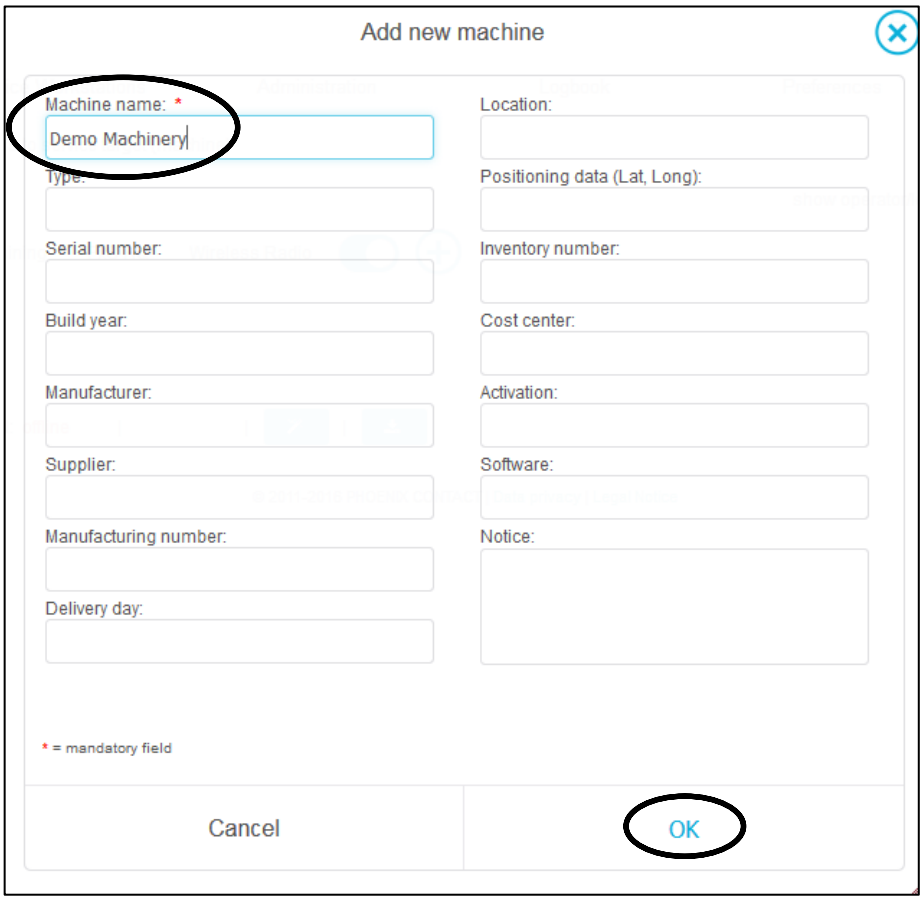
You have now created a single operator location and should see a new tab, in this example called "Harrisburg, PA".

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

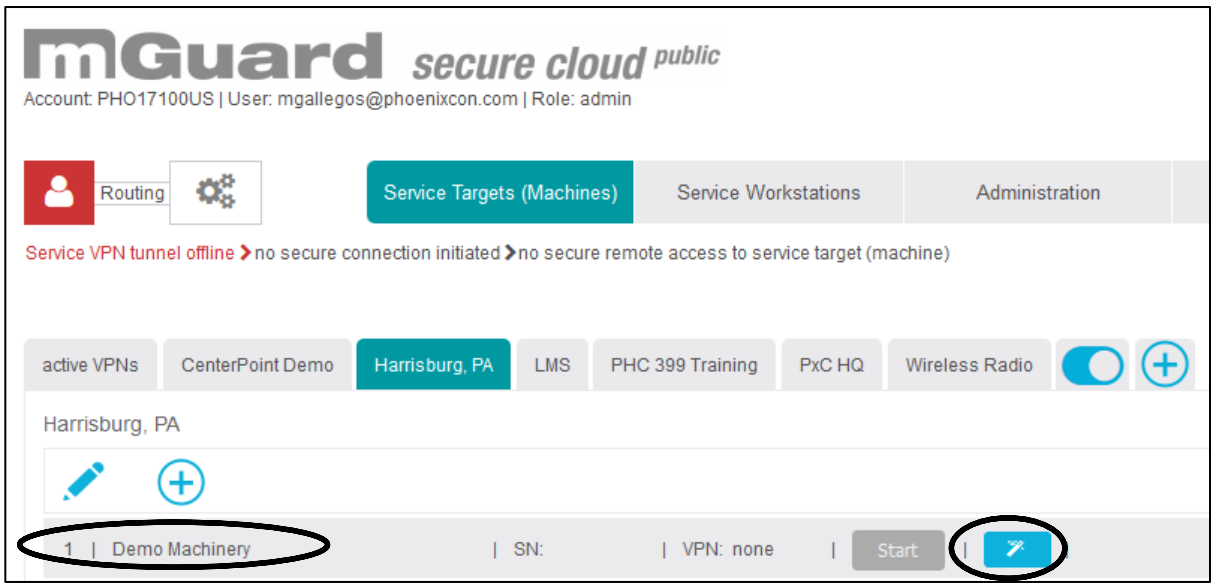
19. Click on the newly created tab (“Harrisburg, PA” in this example).
20. Click on the blue circle/plus icon located under the location tab



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

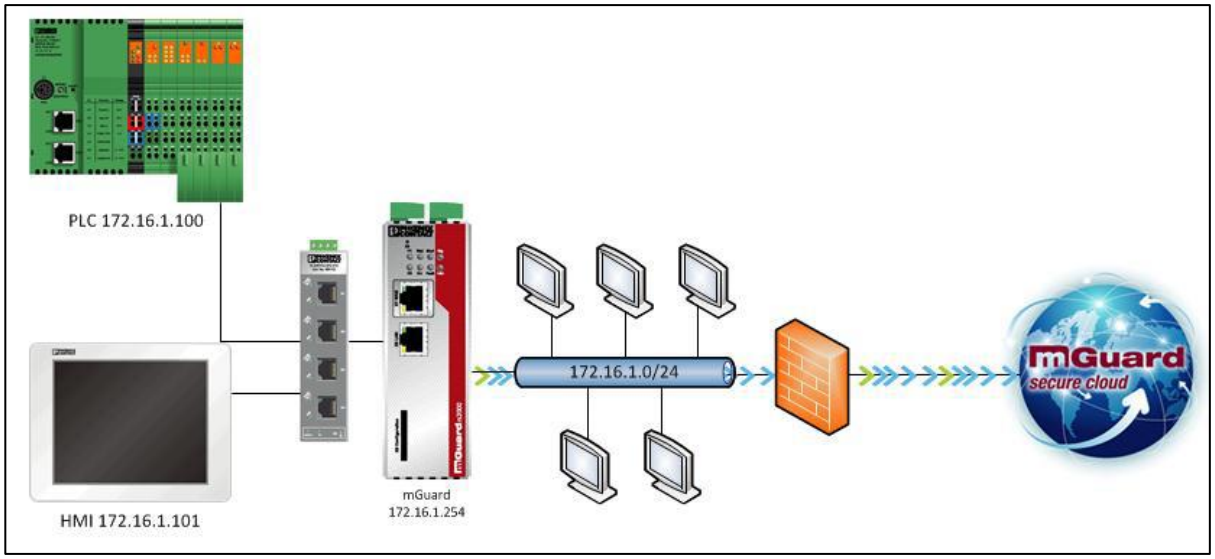


23. You will see the newly created machine device (following this example it's called "Demo Machinery")
24. Click on the VPN Builder button.

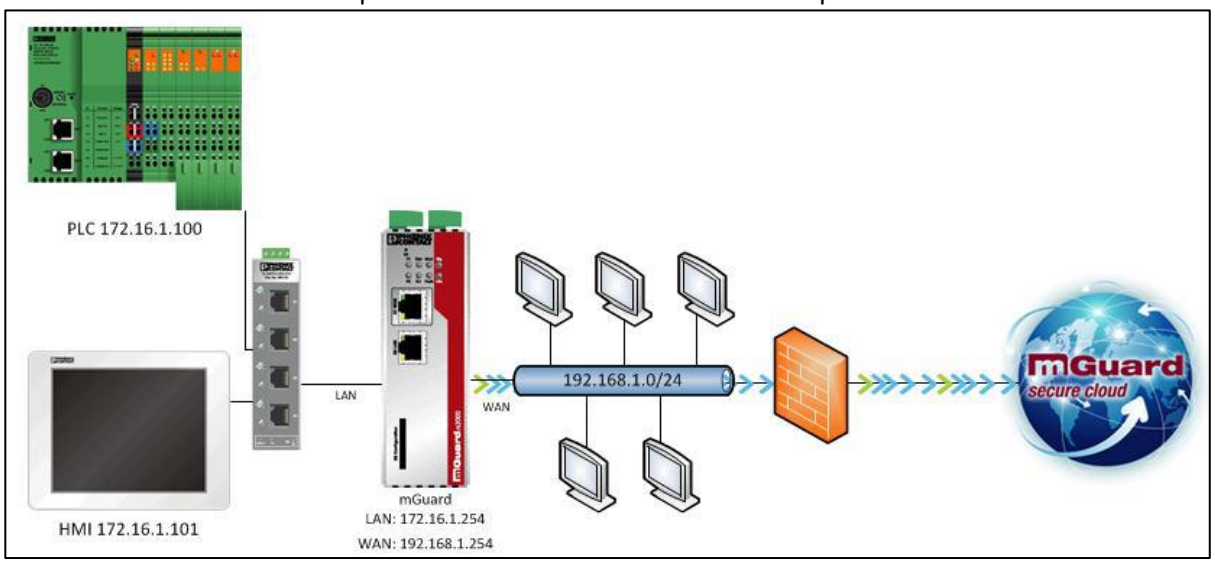


A new window will open where you will see the parameters page. Here you first select the VPN mode desired for your hardware configuration. The options are:

- **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.

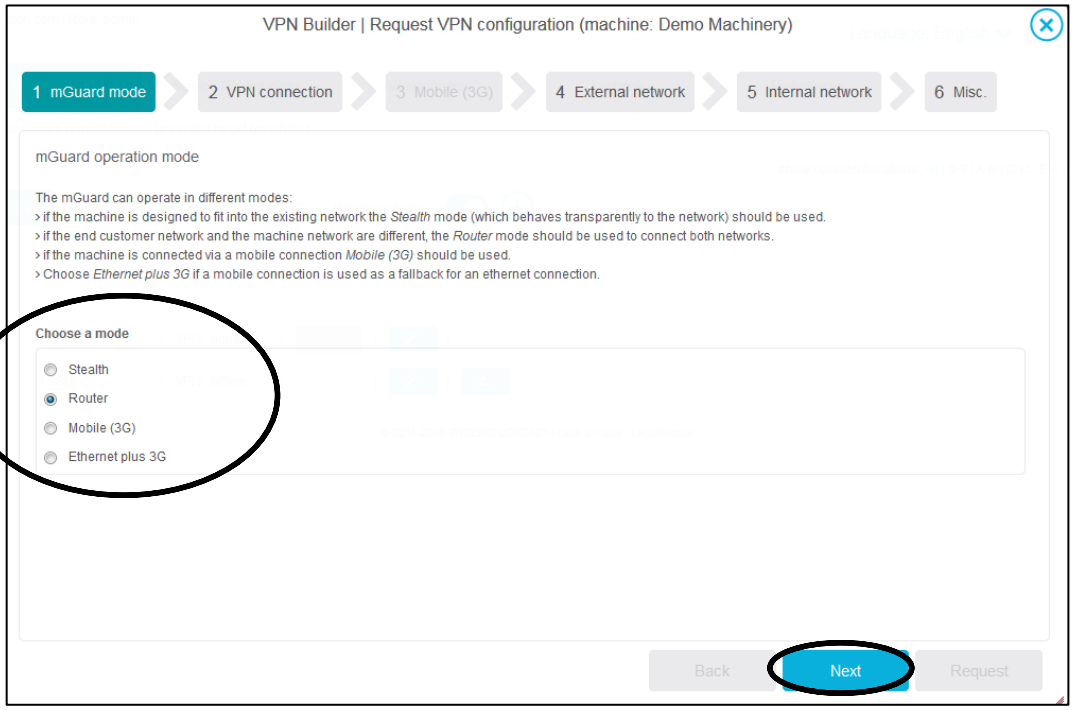


- **Router:** In router mode, the mGuard will route between two different networks, the external (WAN) and internal (LAN). The device network connected to the LAN port is different from the corporate network connected to its WAN port.

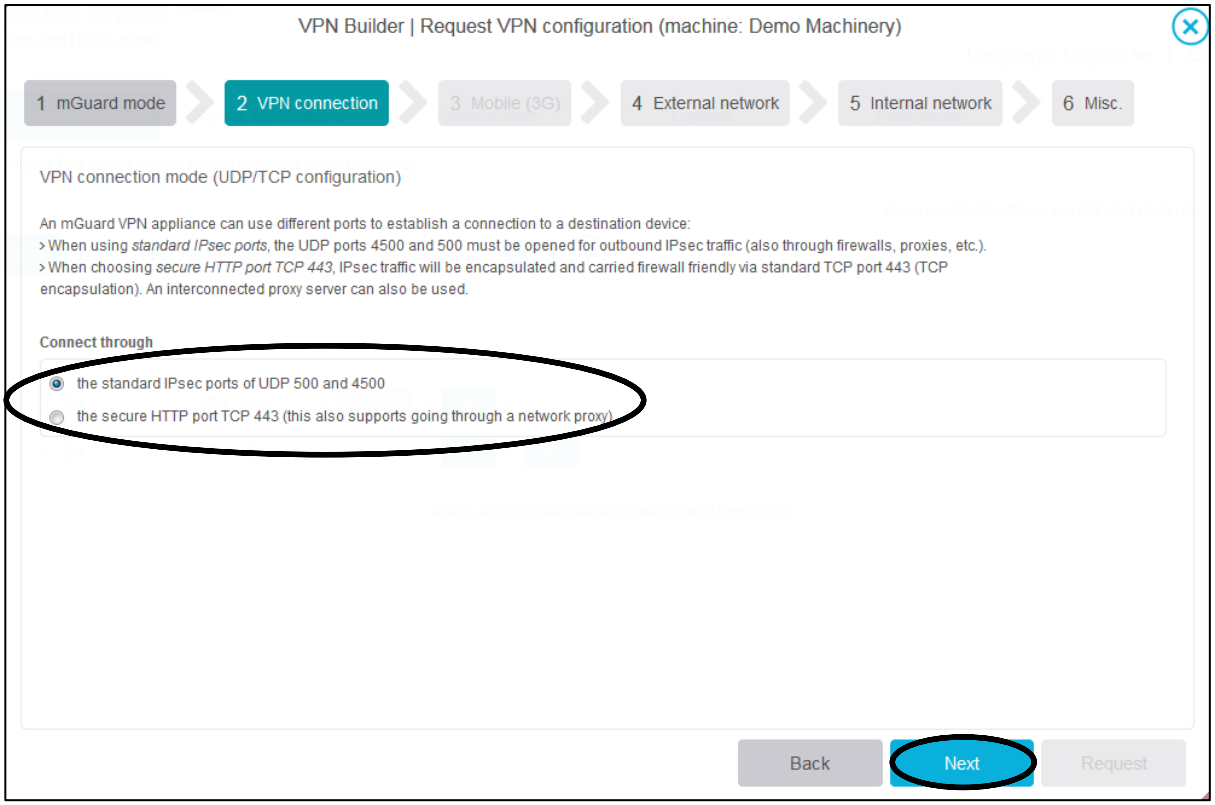


- **Mobile (3G) or Ethernet plus 3G:** There is available hardware that can be used to connect the mGuard to our mSC server through the cellular network.

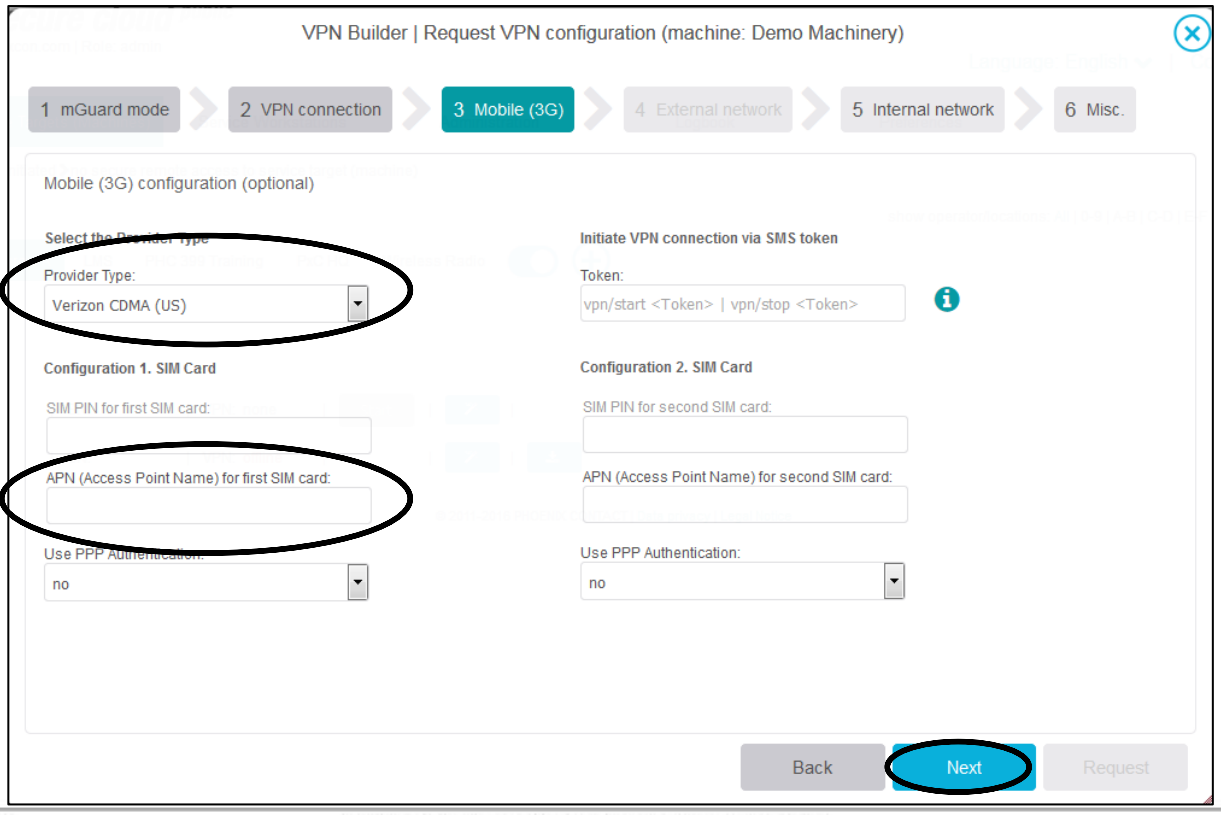
25. Select the mGuard mode
26. Click Next



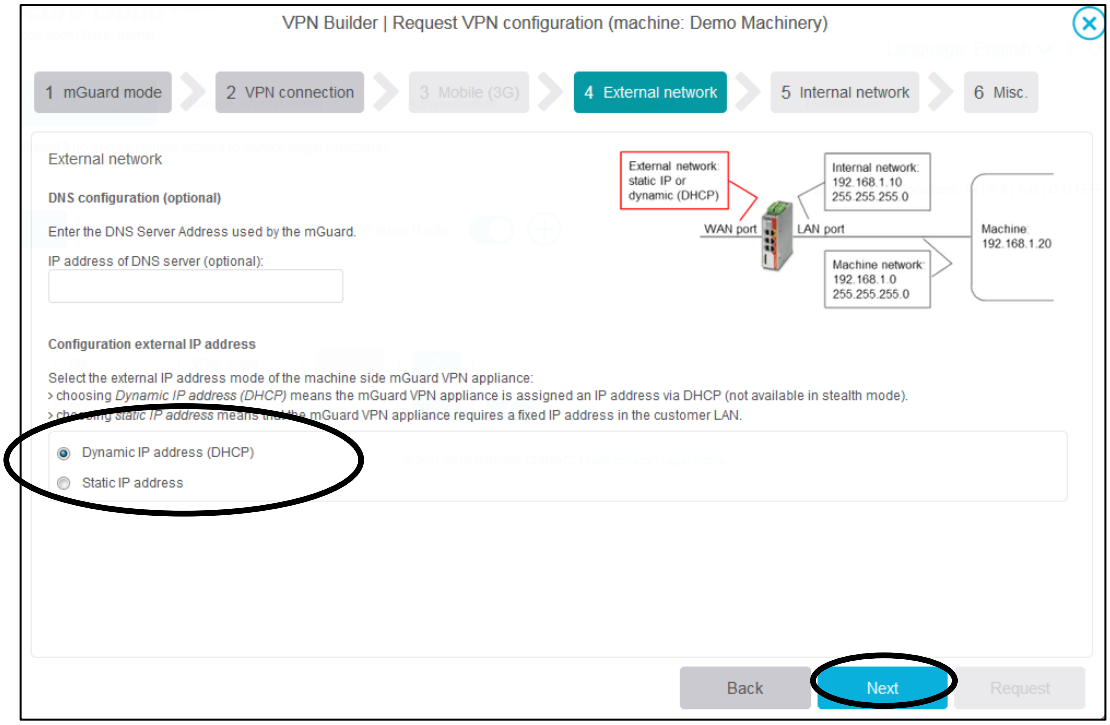
27. Select the desired port. IPsec VPN uses ports UDP 500/4500, if you know your network is blocking these ports outbound use the option via port TCP 443.
28. Click Next



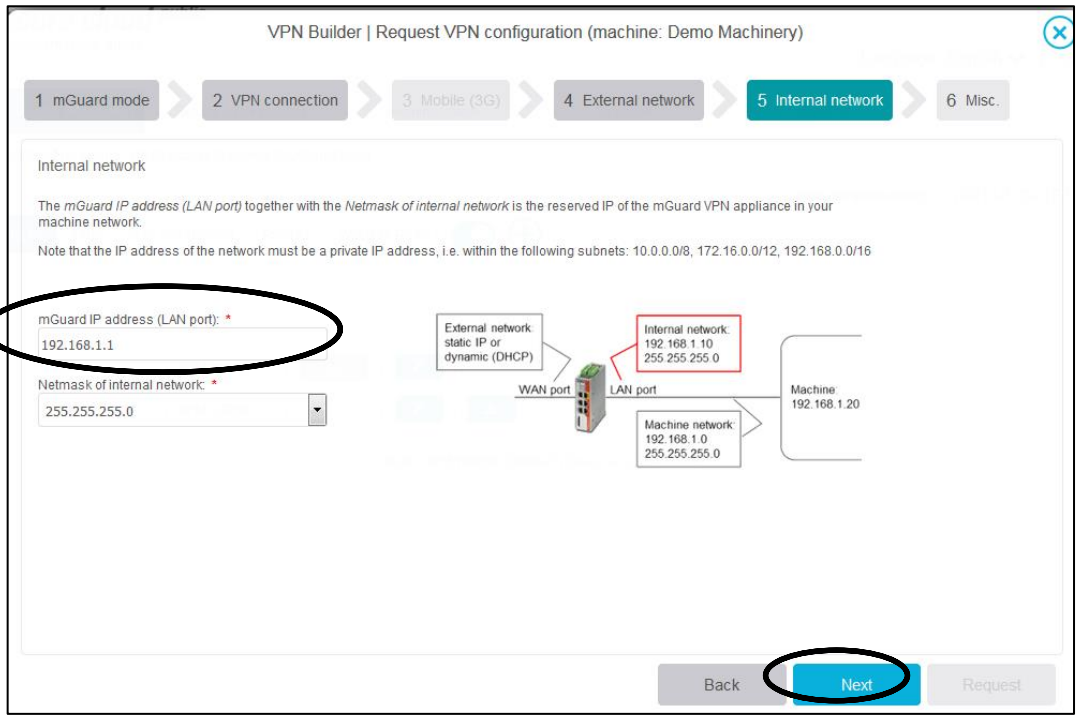
29. If using a 3G mGuard follow procedure below. If not jump to step 17.
    a. Select the cellular provider (AT&T, Verizon or Generic) from the drop down box and type the APN for the SIM if needed.
    b. Click Next



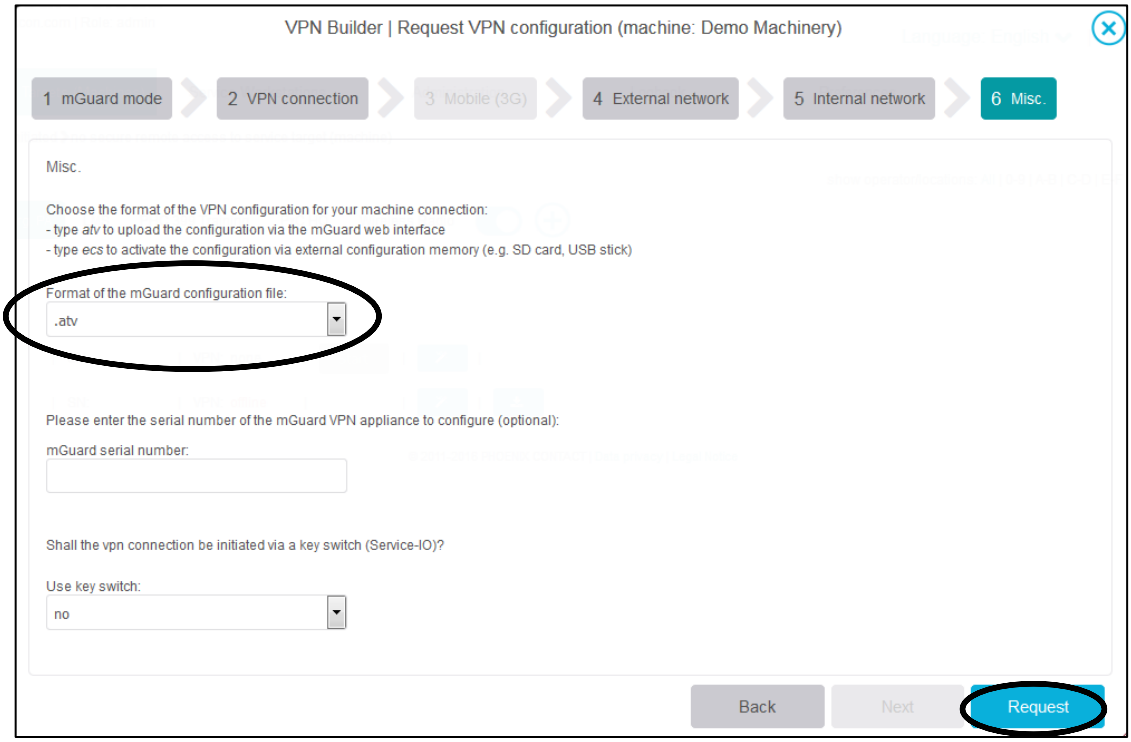
30. Configure the external (WAN) network of the mGuard
    a. Type the DNS configuration if available
    b. Chose if your mGuard device will be receiving a WAN IP address through the DHCP server or statically assigned by you
    c. Click Next



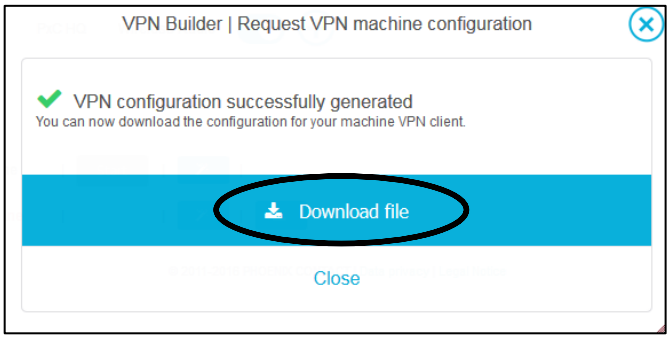
31. Configure the Internal (LAN) network of the mGuard by typing the unique / reserved IP address
32. Click Next



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
34. Click Request



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



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

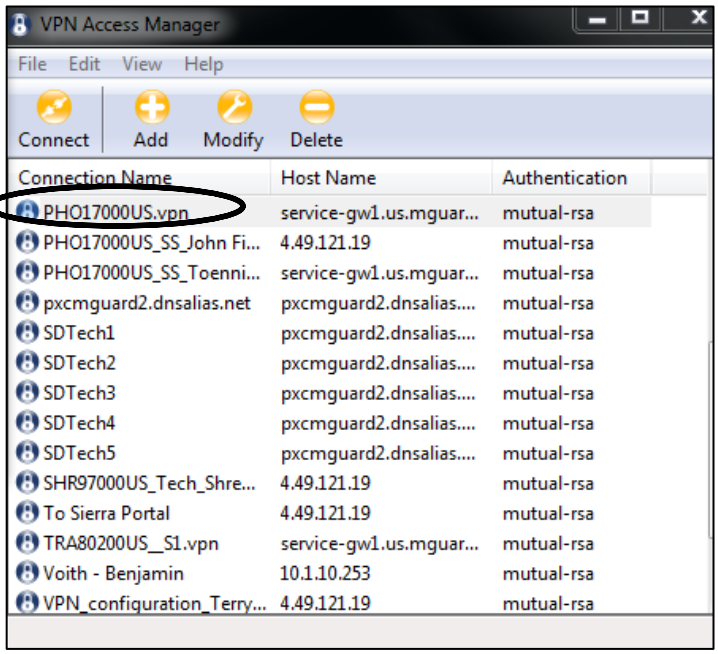
The following is a walkthrough guide showing the steps required start your service VPN

Starting Shrewsoft client

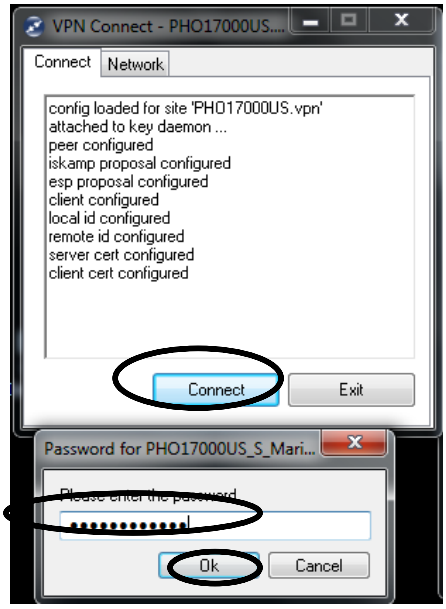
To start your Shrewsoft VPN you must have downloaded the Shrewsoft software client from www.shrew.net/download and requested the mGuard Service VPN for Shrewsoft configuration from the cloud (Check Service VPN Builder steps).

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



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

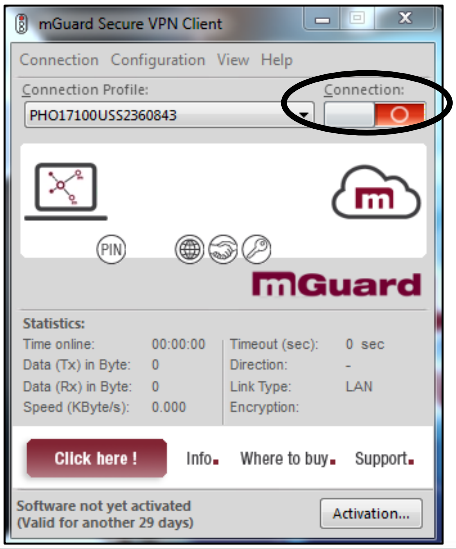


Starting the mGuard Secure VPN Client

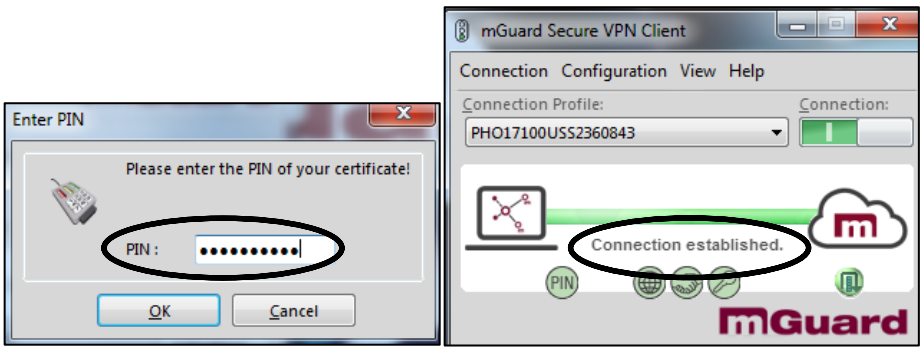
To start your mGSVC you must have downloaded the software client from https://www.phoenixcontact.com/msc and requested the mGSVC VPN configuration from the cloud (Check Service VPN Builder steps).

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

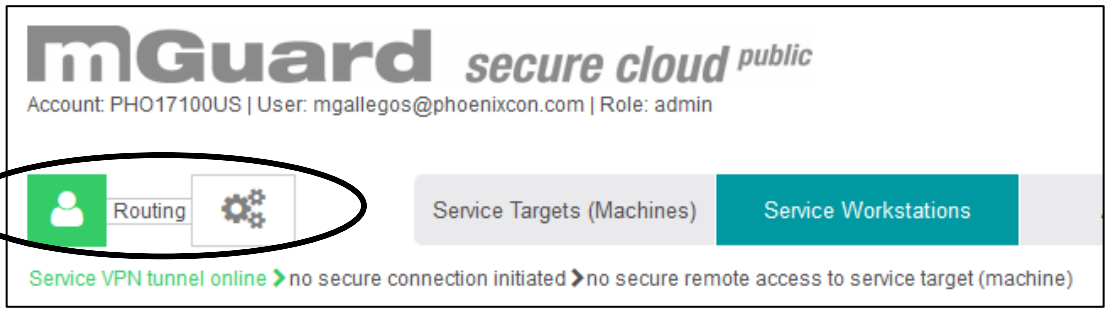
2. With the mGSVC window open, click/swipe the connection button



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



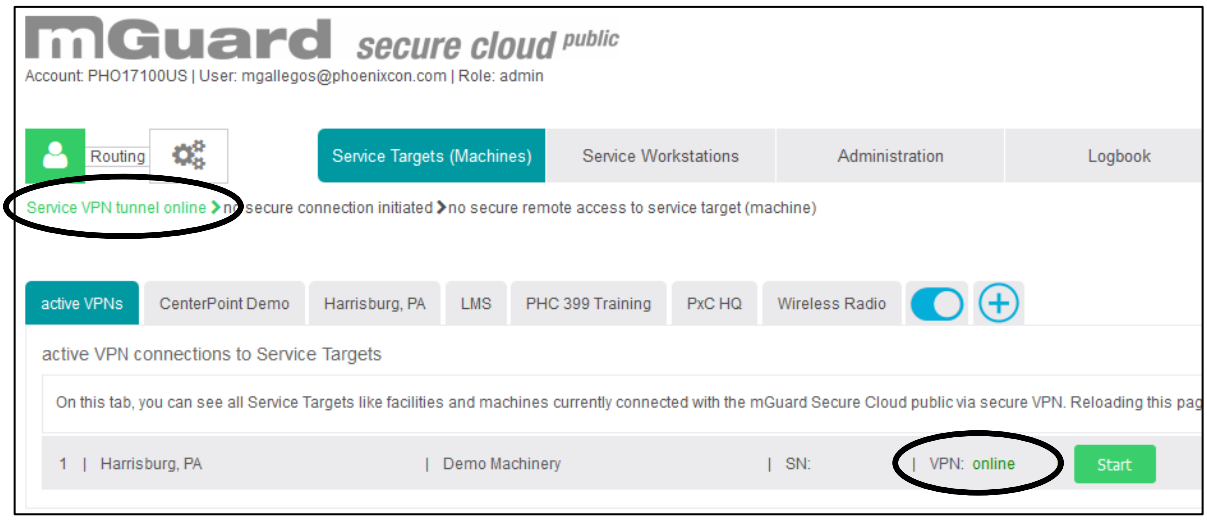
No matter the service VPN software used, your mGuard Secure Cloud status bar should look like the image below after the VPN is authenticated succesully.



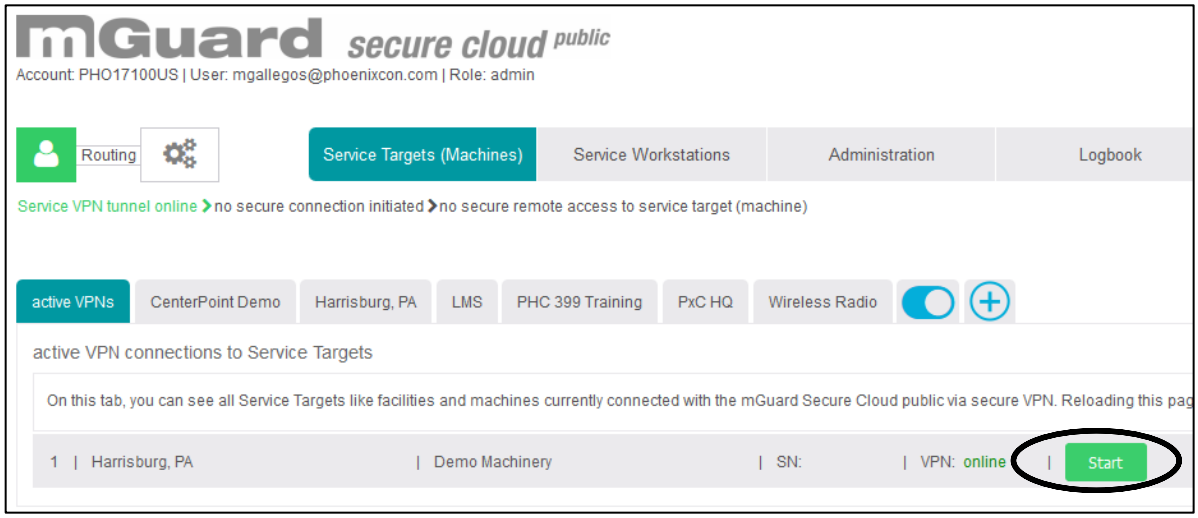
Taking to your end devices

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

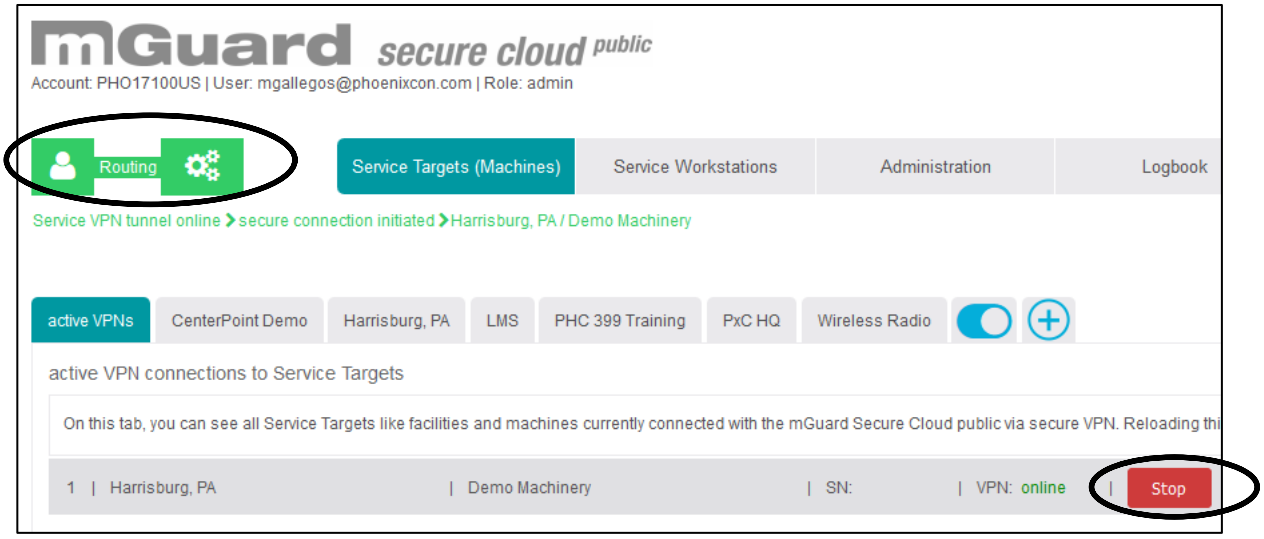
1. Make sure the Service Target (Machine) and the Service Workstation are both connected to the cloud and have the online status (both circled in the image below)



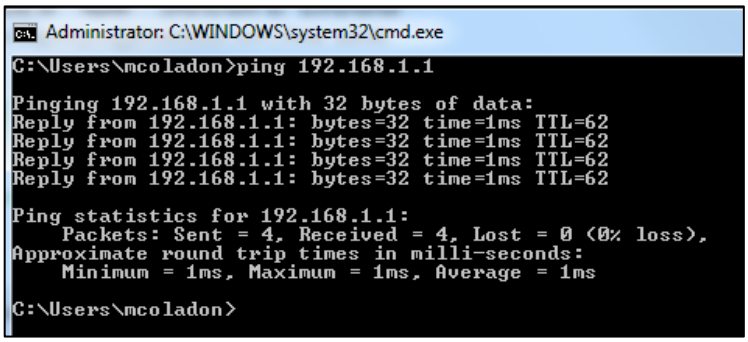
2. To link the service workstation to the machine, click on the Start button.



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.



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



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.

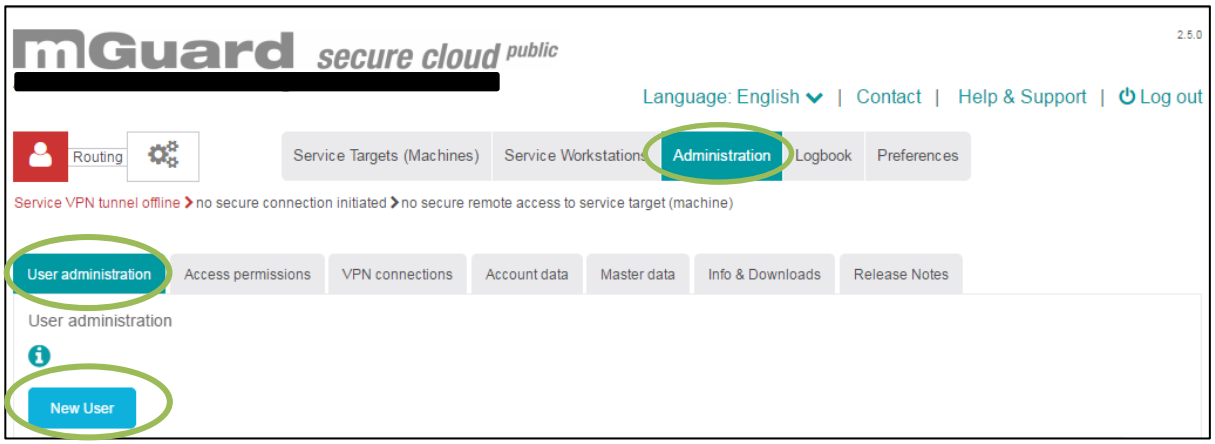
Extra: Additional Users

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.

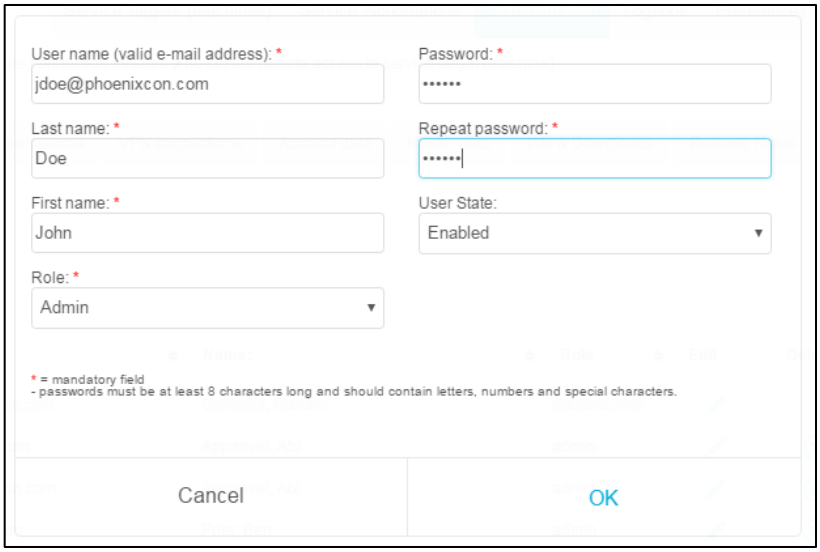
To add additional users to the account, do the following:

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



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): *
jdoe@phoenixcon.com
Password: *
Last name: *
Doe
Repeat password: *
First name: *
John
User State:
Enabled
Role: *
Admin
* = mandatory field
- passwords must be at least 8 characters long and should contain letters, numbers and special characters.
Cancel
OK

Extra: iOS Procedure

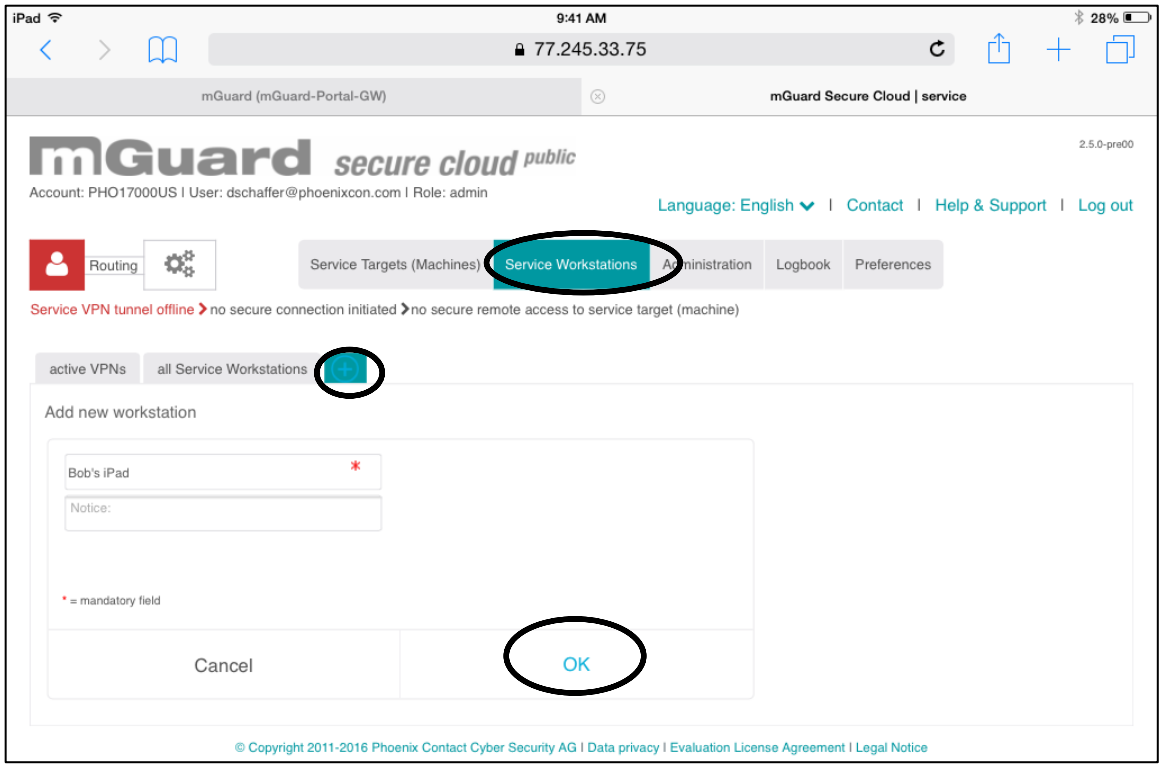
The mGuard Secure Cloud 2.5 firmware gives your technicians the ability to access remote machines via iOS devices like iPads and iPhones. The following is a walkthrough guide showing the steps required to utilize the secure cloud through an iPhone or iPad device:

Adding Service Technicians to an account

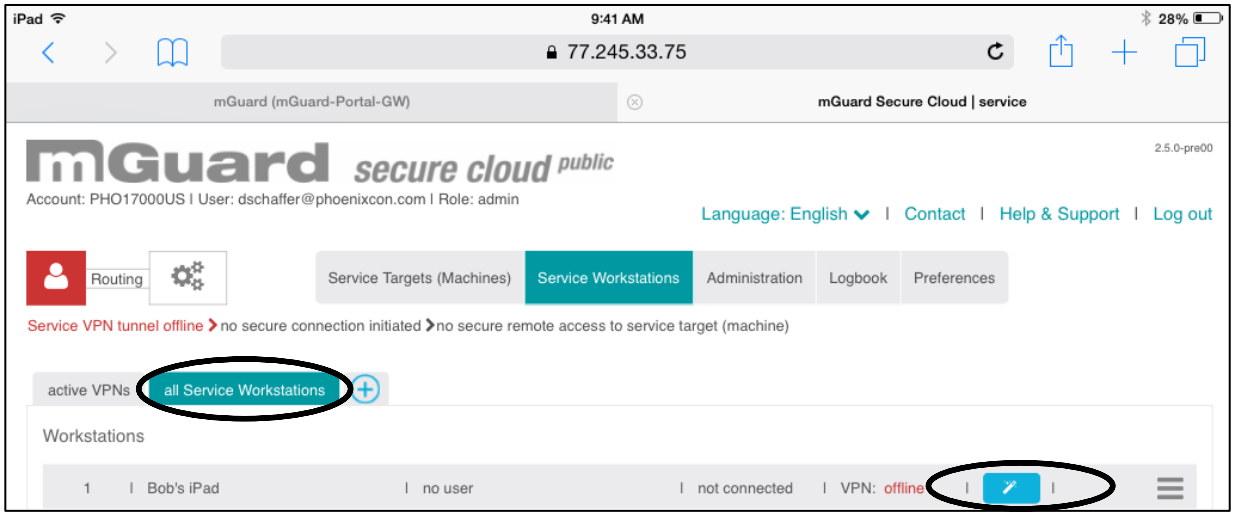
Service technicians are added to the **Service Workstation** section of your account page. Note that you can name the service workstations as the technician by first and/or last name, by computer number or other functions. The service workstation name in the website is not tied to the user signing in.

To add a Service technician:

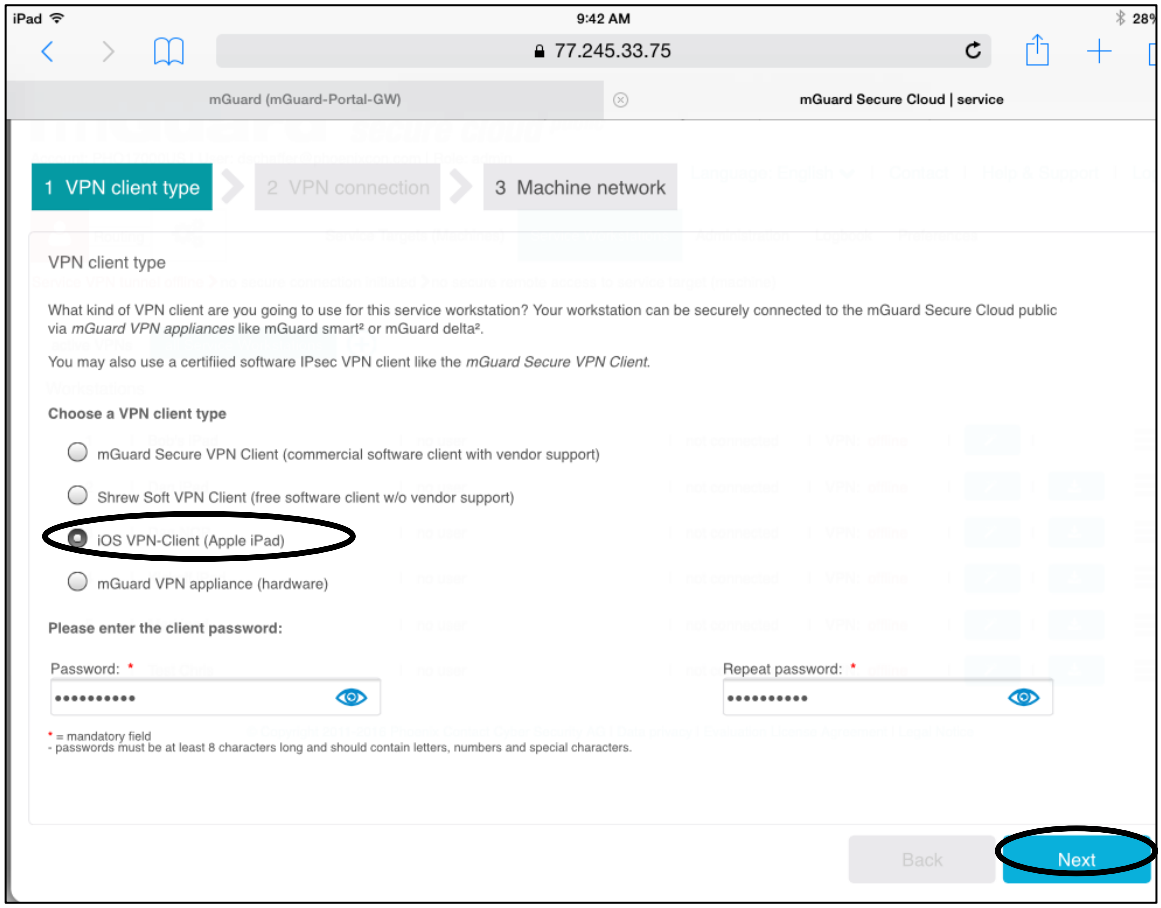
35. Access the account webpage
36. Select the Service Workstations Tab
37. Click on the blue circle/plus icon
38. Enter the workstation name and click the OK option (bottom)



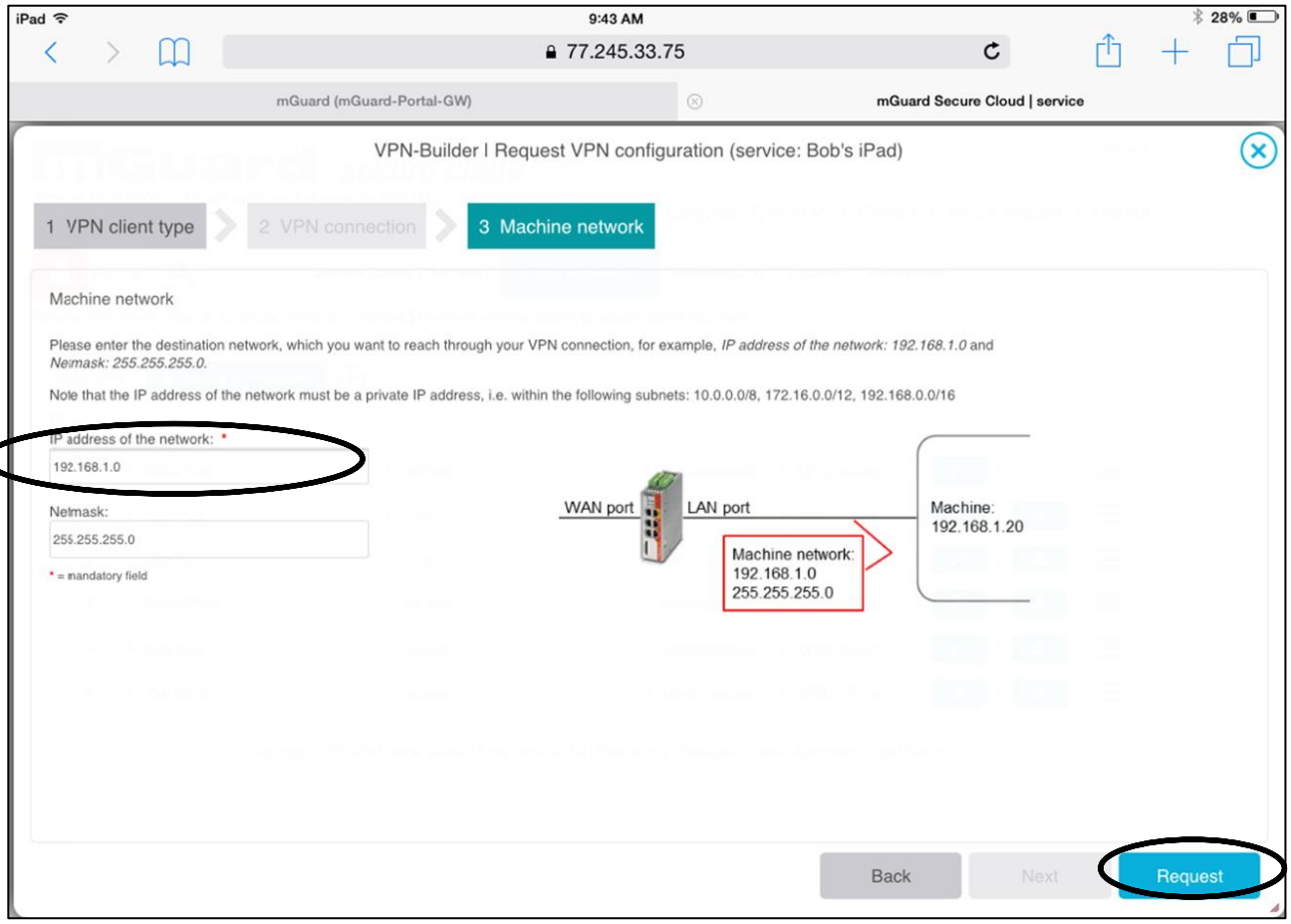
39. Next, click on the all Service Workstations tab (Figure 2)
40. Click on the drop-down arrow next to the workstation
41. Select the New Contact you just created
42. Click on the **VPN Builder** button.



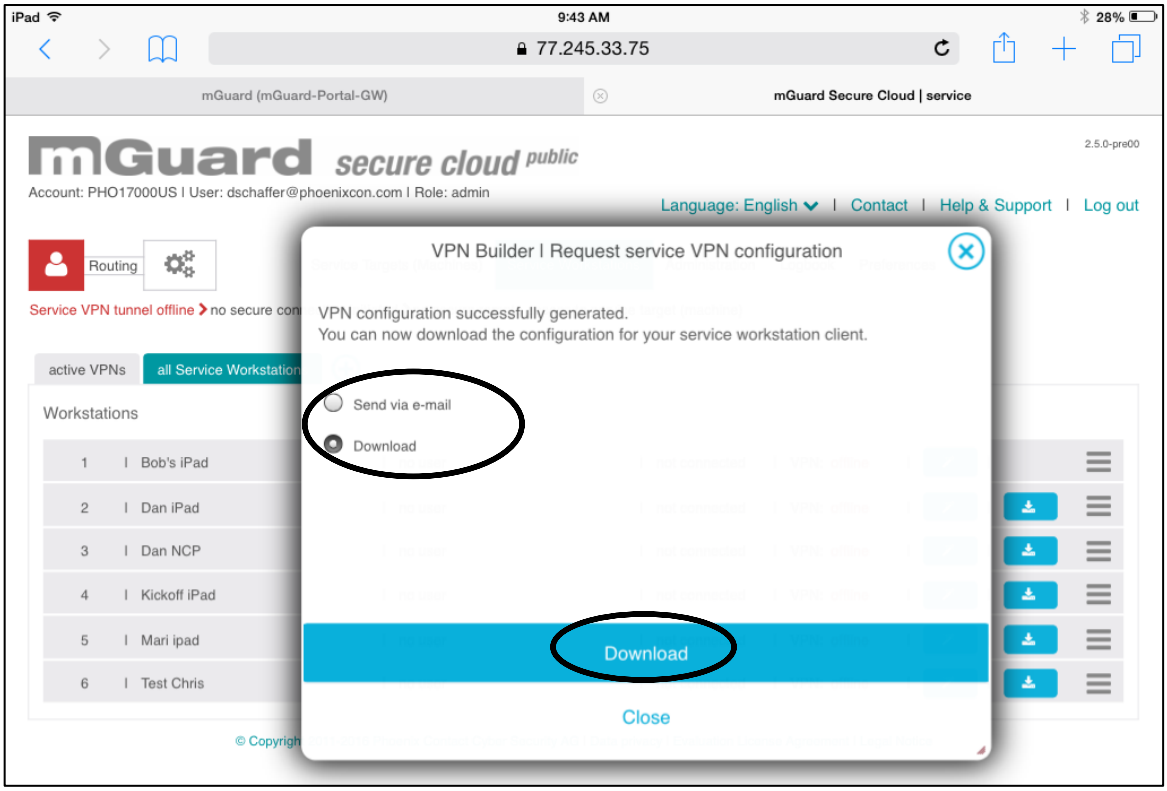
A new window will open where you will see the parameters page (Figure 3). Here you first select the VPN client desired for your service technician configuration, in this case the iOS VPN Client. Then type your own password for the service VPN authentication, you will need this password on step 13. Make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



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

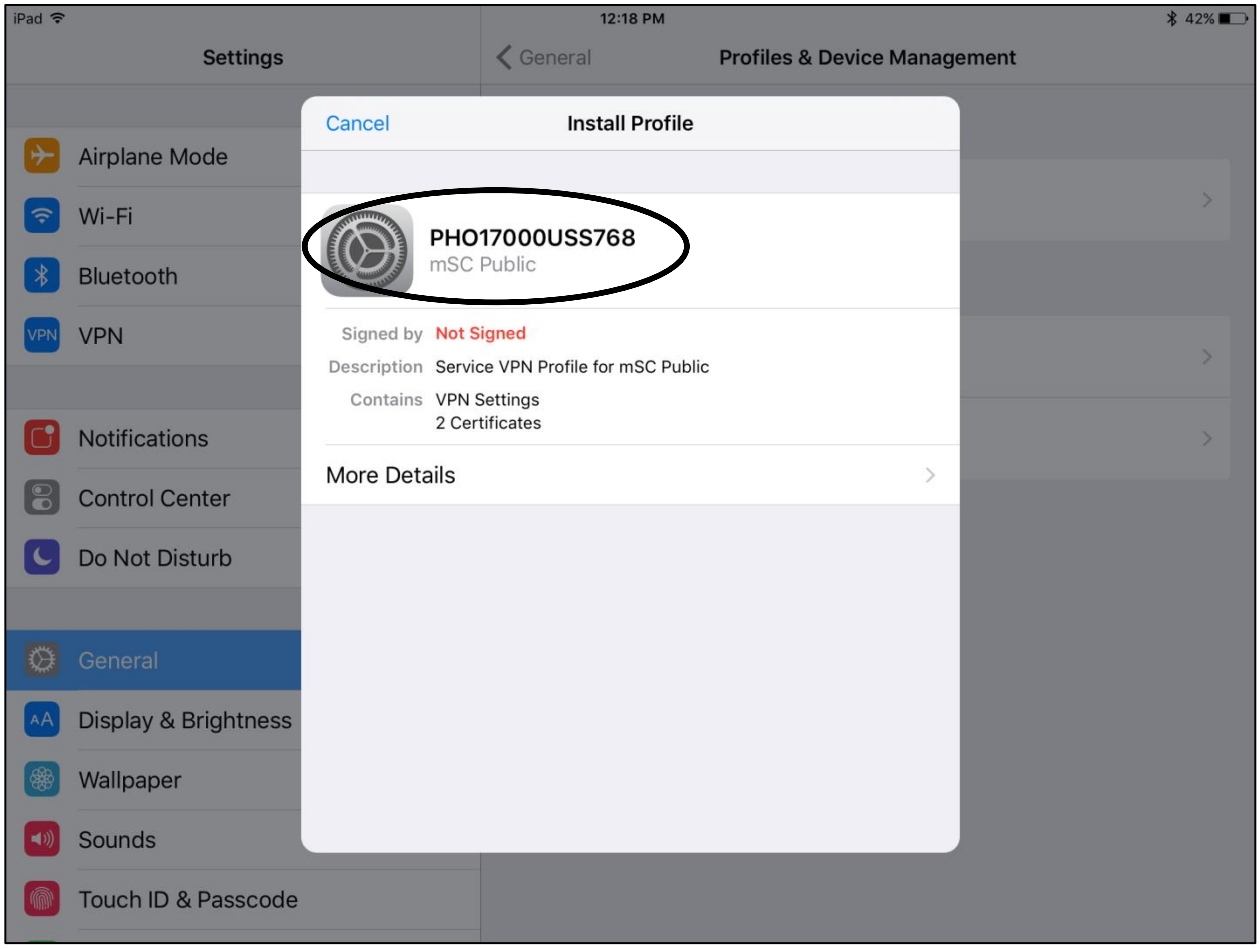


You can now choose to download the iOS VPN configuration at this time (recommended if steps 1-8 were done in iOS device), or select send via-email to the iOS device itself.

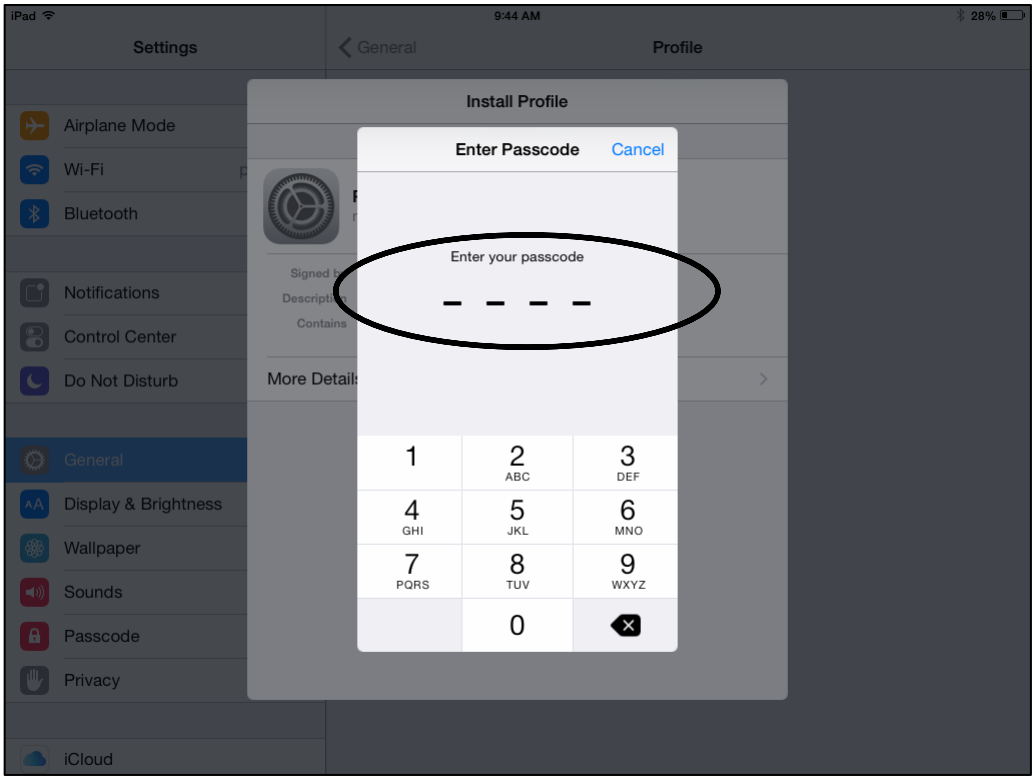


Installation procedure of VPN configuration in iPhone/iPad

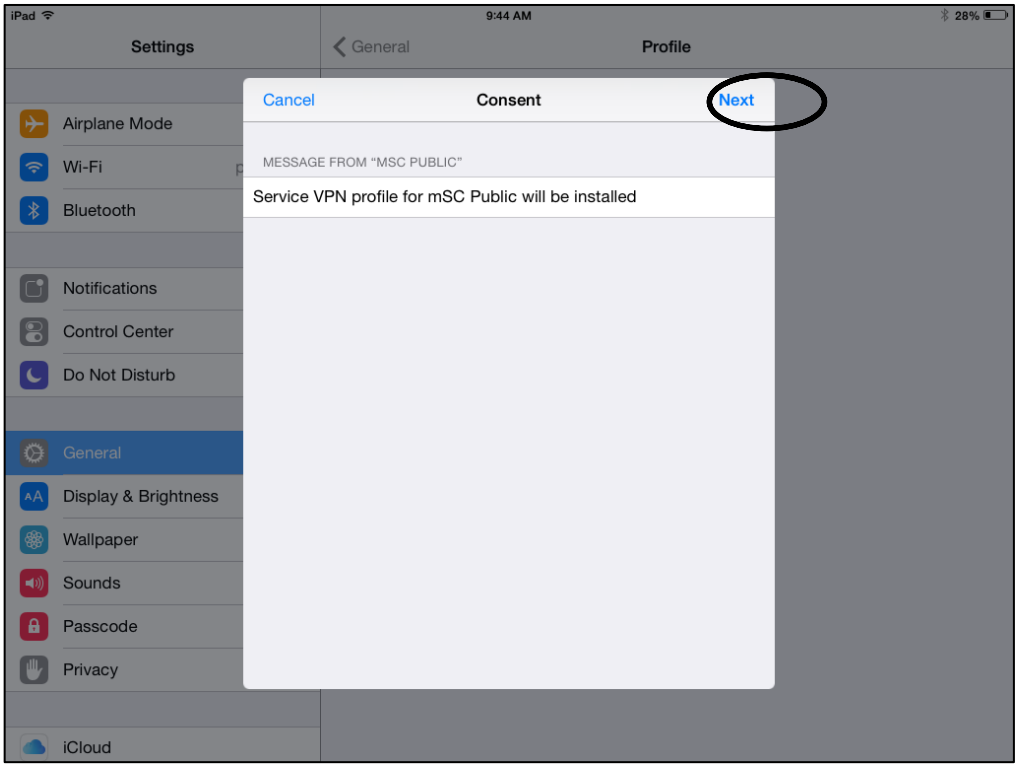
After you received the configuration by email in the iOS device, or click in the download link (shown in Figure 5) the system will automatically send you to the General settings – Install Profiles page. It is fairly simple to perform the VPN profile installation, just follow the instructions in the device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



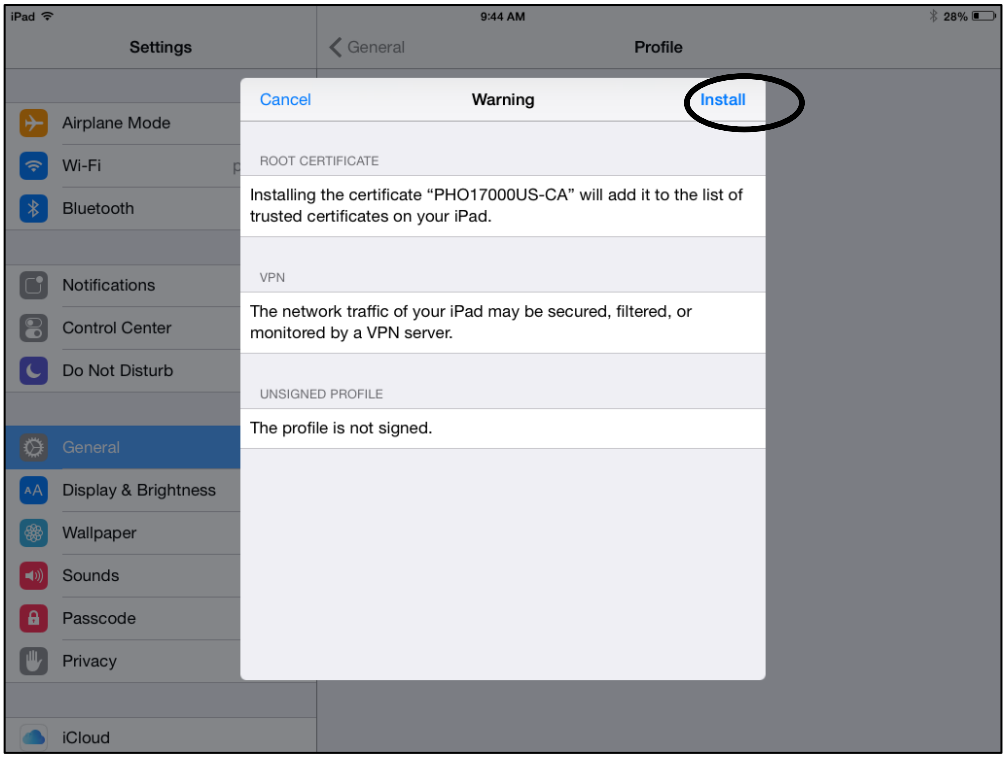
45. Perform the installation of the profile (should be showing your account ID in the configuration name)
46. Type the iOS device passcode (the one you use to unlock the device)

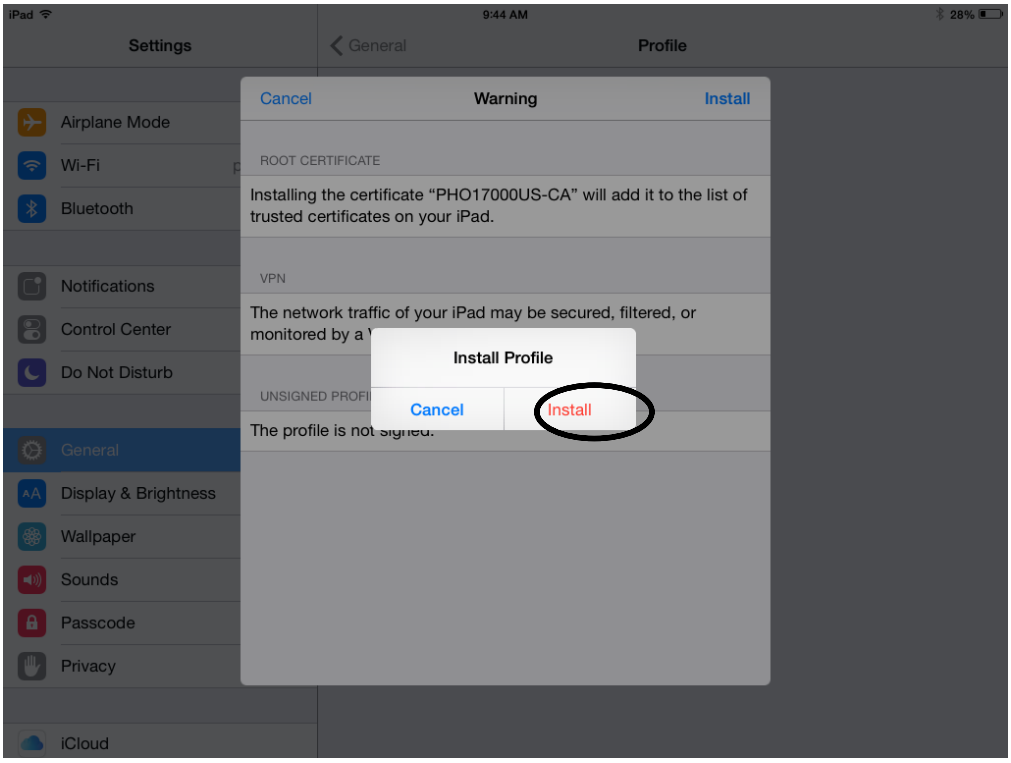


47. After the device passcode is authenticated, click Next

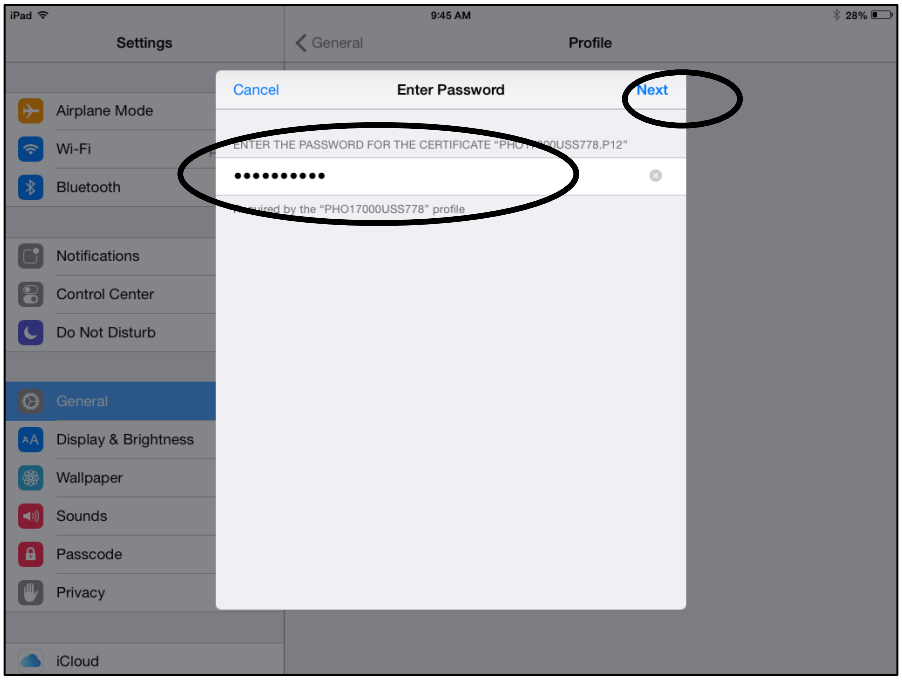


48. Click Install twice

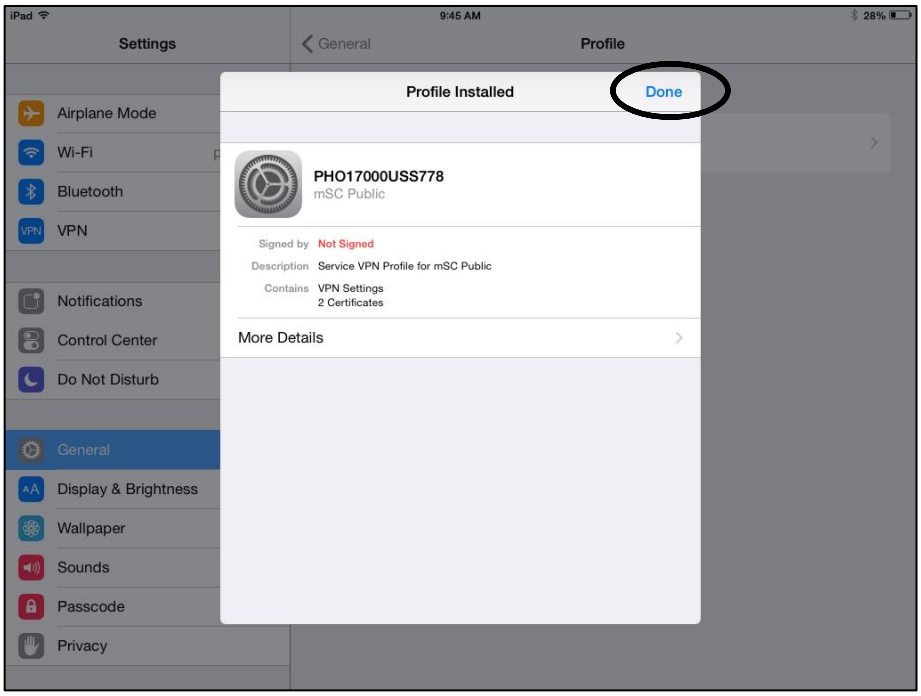




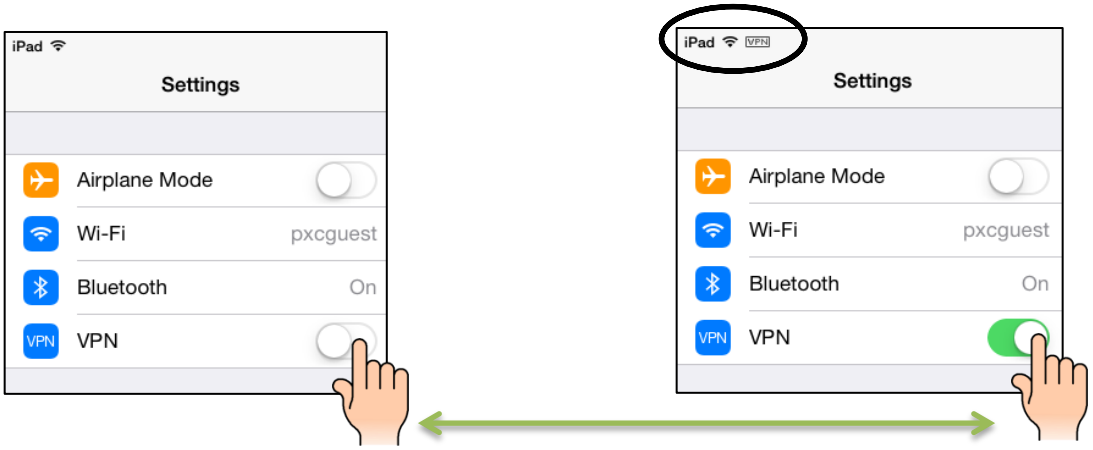
49. Enter the password that you created for the VPN configuration (this is the password typed in Figure 3, after step 6 doing the VPN Builder feature for iOS)
50. Click Next



51. Click Done



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



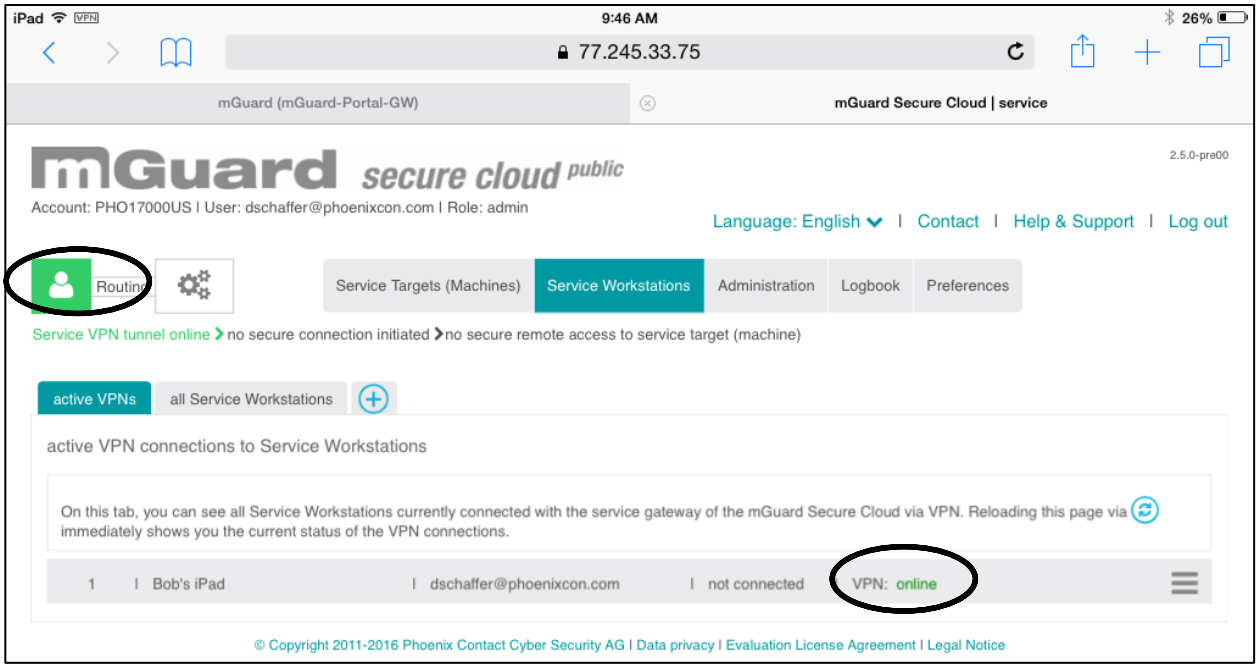
Now that the VPN is enabled and established, go back to the mGuard Secure Cloud through Safari. If you are already familiar using the mSC, your service indicator will be green allowing you to "START" a machine connection. If you aren't sure how to start the tunnel to your remote machine continue following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

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

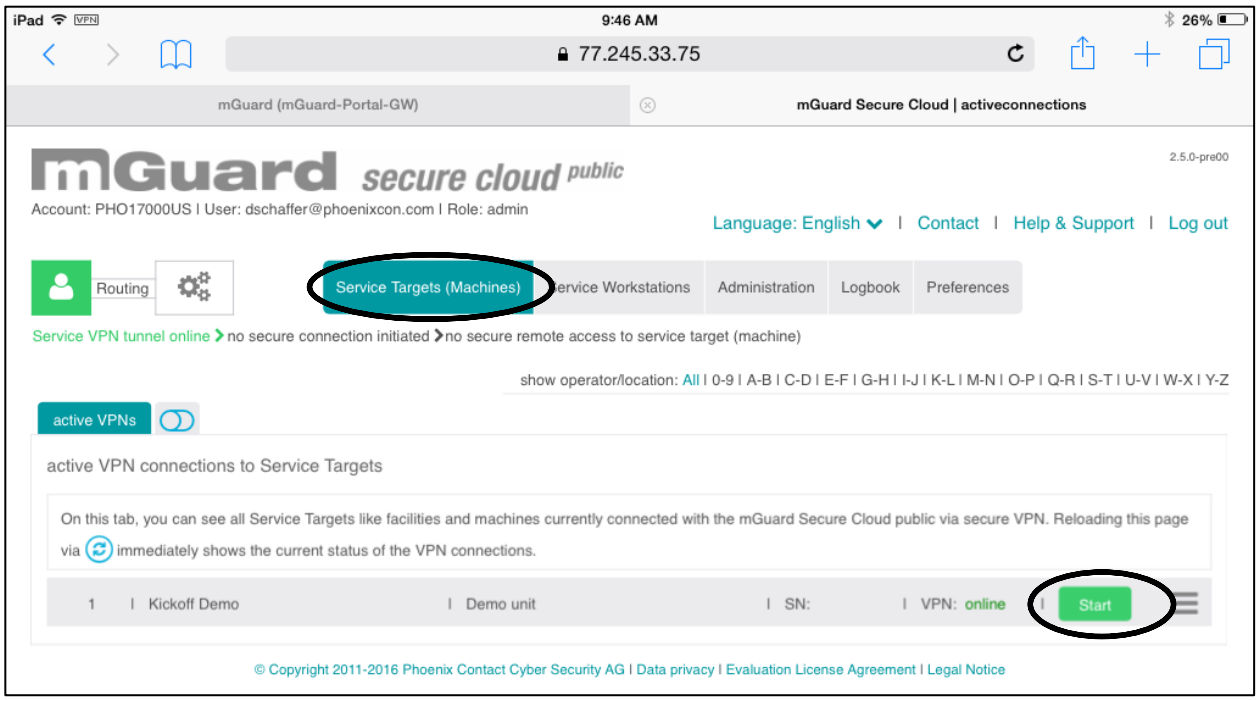
After the Machine device (mGuard/3G modem) and the Service device (in this case the iOS) have both tunneled into the Secure Cloud server, you must connect the Service technician to the Machine via your Secure Cloud account page.

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

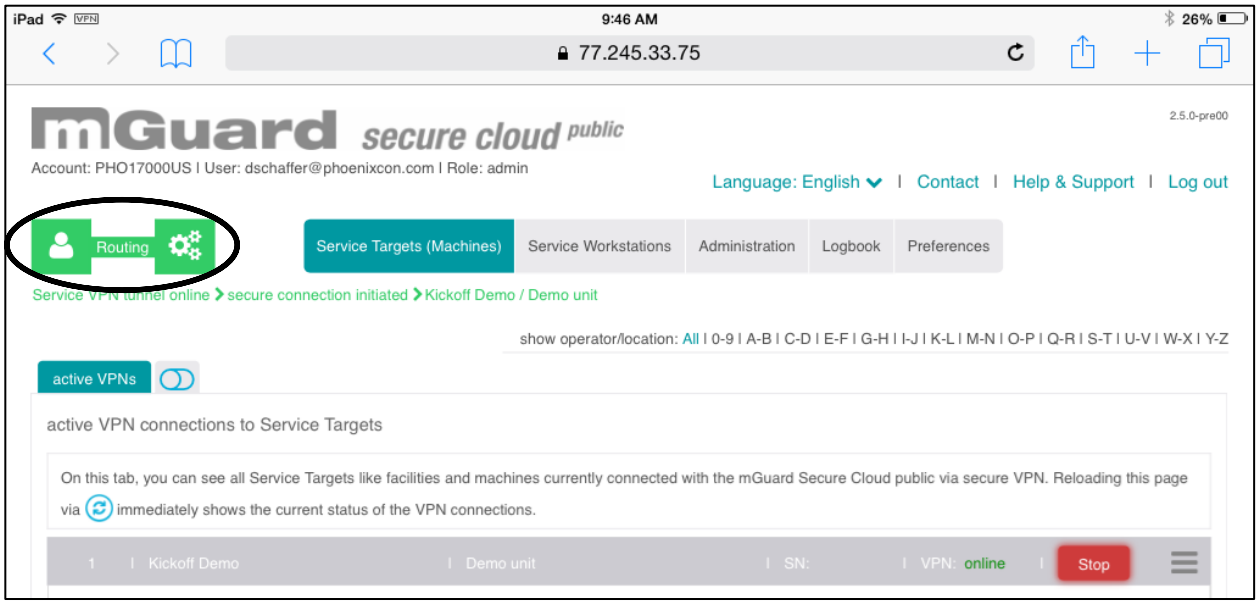


54. Next, click on the Service Targets (Machines) tab (Figure 15). You will see that you have an active Machine (online). The account page is confirming that the machine device (mGuard/3G modem) is currently connected to the cloud.
55. To link the service workstation to the machine, click on the Start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



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.



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 portal@phoenixcon.com