PHOENIX CONTACT
INSPIRING INNOVATIONS

FAQ

mGuard Secure Cloud (mSC) FAQs

1. **What is the mGuard Secure Cloud?**
The mGuard Secure Cloud (mSC) is a secure remote connectivity service from Phoenix Contact . The mSC offers OEMs and machine builders an easy, cost-effective and secure method of supporting their machines and systems through the public infrastructure, regardless of where they are. It is a highly secure, web-based method giving instant connectivity to machines and plants around the world.

2. **How does the mGuard Secure Cloud work?**
The mGuard Secure Cloud uses virtual private network (VPN) technology following the IPsec standard. Phoenix Contact's mGuard Secure Cloud receives the connections from both technicians and mGuard hardware connected to the machines. This mGuard technology allows communication from both ends to take place in a secure and convenient environment through the Internet.

3. **Where is the mGuard Secure Cloud hosted?**
The mGuard Secure Cloud is hosted in Phoenix Contact's data center. The central mGuards managing the connections are housed in this state-of-the-art facility with 24/7/365 monitoring, connecting you to your remote devices over a secure tunnel. This enables Phoenix Contact to be your IT department, implementing the most cost-effective, high-performing and reliable VPN solution.

4. **How secure is the mGuard Secure Cloud?**
Phoenix Contact implements several layers of security within the mSC infrastructure. On the technician side, the service uses an optional two-factor method, requiring a one-time PIN emailed during the logon process for authentication to the mSC account. Additionally, the technician needs to establish a valid VPN connection from his/her workstation to the mSC. That is both the session and VPN tunnel are required to connect to a remote mGuard. The mGuard Secure Cloud also supports X509 certificates that give the uniqueness and confidentiality to each VPN tunnel. In addition to these layers, we also utilize the trusted FL mGuard stateful firewall and IPsec VPN technology. The mGuard guarantees confidentiality, authenticity and integrity of all information and data transmitted between the service staff and the machines.

5. **How is my data protected by the mGuard Secure Cloud?**
The mGuard Secure Cloud uses IPsec Virtual Private Network (VPN), an accepted and highly secure IETF standard for remote connectivity. The mSC uses the AES standard with 256 bit encryption (AES-256), which is approved by the US government for securing "Top Secret" data. Additionally, the SHA-1 algorithm is used to ensure the data integrity when the encrypted packets are traveling over the Internet.

6. **How does the mGuard Secure Cloud guarantee that nobody but me will be able to connect to my machines?**
Each FL mGuard that is connected to your machine will have a unique, built-in configuration that is used exclusively to talk to the mGuard Secure Cloud. Users aren't allowed to see, probe, or otherwise communicate with devices or technicians in other accounts. Unique certificates in each device ensure an authentication mechanism to our servers, similar authentication methods are used within the technicians for them to be able to communicate only with specified mGuard device(s). Along with the authentication, the FL mGuard offers a stateful firewall that protects your machine from any unauthorized access outside the VPN.

7. **Do I need to reconfigure my firewall to enable incoming VPN ports?**
The mGuard devices (at machine or office) are initiating the IPsec VPN tunnel to the mGuard Secure Cloud and use only outgoing ports. There is no need to open incoming ports in your corporate firewall to be able to use our servers. In addition, IPsec VPN standard uses ports (UDP 500/4500) but with the mGuard technology we can use TCP port 443, which is almost always open outbound.

8. **The mGuard is connected to the end customer's network. Does this mean they have local access to my machine?**
The FL mGuard can be configured for both situations. If you don't want your end customer to have access to your machine, the mGuard can block all local traffic from the end customer's network and allow only the VPN traffic to pass through. However, the mGuard is also capable of being set up to allow end customer traffic to access your machine. This is easily accomplished with 1:1 NAT rules or by using port-forwarding, both standard features of all mGuard hardware. Should more granular firewall rules be needed to allow only certain end customer traffic through to your machine, the RS4000 hardware variants provide that capability.

FAQ

9. **My end customer's IT department is worried that I will be in their network 24/7. Is there an easy way for them to activate/deactivate the tunnels?**
   With the FL mGuard, it is possible to enable and disable the tunnel with a contact closure on the mGuard hardware. Make sure you request the special feature configured for this case.

10. **What else do I need from my end customer network to be able to connect the machine to the mGuard Secure Cloud?**
    The mGuard will use the end customer's network to connect to the servers. So, the same settings as a PC connected to the network (IP address, subnet mask and a default gateway, plus any proxy settings) will be needed. The mGuard can also be a DHCP client and will take all these requirements automatically.

11. **What is the Logbook tab used for?**
    The Logbook allows you to see and generate a report of the connections that have been made between a Service Technician and a Machine. You can specify the time range, the Technician, the Machine or any combination. This is useful for tracking time spent resolving a customer issue for billing purpose, to verify a technician's activity, etc.

12. **Can more than one Technician use the Secure Cloud at the same time?**
    Yes, multiple Technicians can collaborate on the same Machine and multiple Technicians can be connected to different machines at the same time. The only scenario that isn't supported is a single Technician connected to multiple machines at once.

13. **Can more than one Machine be accessed on the Secure Cloud at the same time?**
    Yes, all of your machines may be actively tunneled in at the same time, and more than one machine can be accessed (as long as by different technicians, see #12) at the same time.

14. **Do I have to pay for extra Machine or Technician configurations?**
    No, the mSC is a FREE service, you can have as many technicians and machines on your account as you would like. And unlike some other cloud-based services, there is no limit to how many technicians can be logged in or actively working at one time.

15. **Is there a tiered service or upcharge for premium features or speed?**
    No, the mSC is a FREE service. We provide top-notch speed and excellent service to all of our customers without and sort of extra charge, "platinum" or "pro" service. We also don't throttle or restrict bandwidth to users or accounts, so all of your connections are bound only by their own Internet connection speed.