Introducing FieldSafe

FieldSafe is a security feature set added to every FieldServer gateway. The FieldSafe feature set ensures device security in a world where cyberattacks are increasing in frequency and threats are becoming more sophisticated every day.

In today's cyber landscape, it is no longer good enough for customers to erect a virtual fence around their on-premise network. Not only are end-users accessing equipment data from several different networks and devices, but the number of internet access points within buildings is increasing. A new approach to security must be considered – one that encourages precautions implemented at every access point.

The FieldServer team has done this by securing the local hardware and our SMC Cloud application with some of the latest technologies that are currently available on the IoT marketplace. In addition, we have successfully passed the latest in 3rd party penetration testing for both our FieldServer gateways and the SMC Cloud.

FieldSafe provides device security with a multi-layer approach

HTTPS

Our "gateway-internet browser" and "gateway to SMC Cloud" connections are secured with HTTPS, which uses TLS/SSL.

AWS Partnership

We've also strategically partnered with Amazon Web Services so our SMC Cloud customers can benefit from the many security features Amazon provides.

Compliant with IoT Legislation

FieldSafe ensures all FieldServer devices are compliant with California State Bill 327 and its national counterparts.

Login Variability

With three robust security levels and user profiles to choose from, FieldSafe provides security measures that grow with your business requirements.

Trusted

Don't take our word for it, our FieldServer gateways and SMC Cloud have passed rigorous 3rd party security penetration testing.

Secure Internet Connectivity

Our "gateway-internet browser" and "gateway to SMC Cloud" connections are secured with HTTPS, which uses TLS/SSL.

AWS Partnership

Our SMC Cloud service was built on Amazon Web Services and uses many of its security features to provide SMC Cloud customers some of the best that industry has to offer, including:

- TLS 1.3
- X25519
- AES_256_GCMSOC3
- FISMA, DIACAP and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- IPS 140-2
- MTCS Level 3

Compliant with IoT Legislation

FieldSafe ensures all FieldServer devices are compliant with California State Bill 327 and its national counterparts.

California – SB-327 **is one of the most recent and strictest IoT safety standards in the world**. It requires that industrial devices connected to the Internet provide protection for user credentials.

The FieldServer has a unique password for each device. User credentials are protected as verified by penetration test assessments. Although California is the first state requiring these standards, we anticipate many more states to be following in their footsteps.

Additionally, many sites' IT departments now require security-based inspections of devices that are connected to their internal network.

Login Variability

Additionally, we have varied levels of security and user access to best suite your business needs.

Three Security Levels:

- HTTP – low level security
- HTTPS supplied certificate – Secure
- HTTPS self-signed certificate – Very secure

Three User Levels:

- Admin – Change all settings
- Operator – Only change settings to configure a device
- Viewer – View settings

Trusted

Don't take our word for it, our FieldServer gateways and SMC Cloud have passed rigorous 3rd party security penetration testing.

Penetration Testing: FieldServer Gateways

Securicon is a 3rd party that conducts network vulnerability assessments. Through multiple rounds of testing and analysis, Securicon assessed that the FieldServer hardware meets the needs of current security standards.

The certificate is available on the company web site and the full report is available on request.

Penetration Testing: SMC Cloud

Breachlock is a 3rd party that is powered by certified hackers and artificial intelligence to ISO 27001 standard. Through the use of manual as well as automated vulnerability discovery methods that are aligned with industry best practices, Breachlock deemed that SMC Cloud meets current security standards. In addition, the SMC Cloud is tested monthly to ensure no new vulnerabilities are exposed.

The certificate is available on the company web site and the full report is available on request.

Enterprises and organizations across industries and verticals choose IoT solutions from FieldServer by MSA Safety for their automation and integration projects. With more than 200,000 units deployed worldwide, you'll find FieldServer gateways embedded in some of the largest building and industrial automation projects in the world.

MSA Safety
1991 Tarob Court, Milpitas, California 95035 USA
O. +1 408 262-6611 TF. +1 800 72 SIERRA (74377) E. SMC-insidesales@msasafety.com
www.sierramonitor.com