# Secure and Seamless Remote Device Management

## HOW SECURITY IS ENSURED WITH SECOMEA SOLUTIONS

The connection is based on TLS, and protected against man-in-the-middle attacks by letting every Secomea M2M server (GateManager) have a unique TLS certificate/key, to which the Secomea gateway, the SiteManager, binds (aka ToFu "Trust-on-first-use).

If you want to remove the binding between a SiteManager and GateManager, you will have to explicitly reconfigure the M2M server (GateManager) settings in the SiteManager. Since a man-in-the-middle cannot do that by just intercepting the connection, the attacker cannot direct the SiteManager connection to another GateManager - even if the attacker had one.

ProtectEM

Secomea obtained security certification by the esteemed German security organization ProtectEM GmbH that works in close cooperation with the Deggendorf Institute of Technology. ProtectEM performs security audits of the entire Secomea remote access solution continuously. The auditing processess were undergone according to NIST-SP800-115 & ISECOM OSSTMM and passed succesfully every year since 2014.

## INDUSTRIAL SPECIFICATIONS

The SiteManager not only complies to standards for safety and interference, it is also both security and Industry 4.0 certified end-to-end according to: NIST SP800-115 & SECOM OSSTMM, ISA 99 / IEC 62443 & BSI and Industry 4.0 (RAMI4.0) ref. IEC/PAS 62443-3

## LEARN MORE

If you would like to learn more details about our technology or the security certification process visit www.secomea.com/security or contact us at info@secomea.com

## WHY SECOMEA?

### FIREWALL FRIENDLY
The Secomea solution is Firewall friendly. Only outbound connection required for the SiteManager. (either port 80 or 443 or 11444).

### AES 256bit
AES 256bit encrypted tunnel based on TLS

### 3rd PARTY CERTIFICATION
Cyber security due dilligence: The entire Secomea solution is security audited by 3rd party company (ProtectEm) Audit based on NIST SP800, ISECOM OSSTMM, BSI, ISA99 and IEC62443.

### TWO-FACTOR AUTHENTICATION
Password combined with personal security certificates, and optionally extended with SMS code validation.

### USER MANAGEMENT
Full control of who can access the SiteManager gateway – even access time frames can be specified at your preference.

### AUDIT & REPORTING
All access activity is logged for auditing and to provide full transparency of user activity.

### NOTIFICATIONS
Get notified upon login and/or events.

### DEVICE MANAGEMENT
Control who gets access to your devices: Full control of which device can be accessed by whom, all the way down to IP address or port level.

### NETWORK CONNECTIVITY
Ethernet/WIFI or 3G/4G for total network separation.

### PHYSICAL CONTROL
IO ports to physically control remote access.

secomea
secomea.com