ESM Remote Access:

A secure way to monitor your emergency lighting over the internet

WHITE PAPER

EXECUTIVE SUMMARY

ETAP Safety Manager (ESM) features web-based monitoring and management of your emergency lighting installation. Employees can access this web-interface from their local pc from within your corporate network or - with ESM Remote Access - from anywhere on the world.

Allowing users to access ESM from outside your corporate network requires a “pass-through” in the firewall of your network. Such a “pass-through” needs to be well-designed so none can access your network unauthorized.

ESM builds multiple security levels to secure the integrity of your network. These security levels ensure that only authorised users can access the ESM interface, that such connection cannot be forced in any way and that none of this communication is accessible for others. This white paper is a technical description on these security levels.

ETAP
EXCELLENT LIGHTING, SAVING ENERGY

www.etaplighting.com

INTRODUCTION

ETAP Safety Manager (ESM)

ESM is a management system that assists you with the monitoring, configuration and maintenance of your emergency lighting through a web-interface.

ESM visualises your emergency lighting system in a user friendly application. It will automatically log all test result and maintenance into a log book (in line with the EN50172) and it allows low-cost precautionary maintenance through visualisation of lamp burning hours and battery duration.

By simplifying monitoring and maintenance ESM gives you extra safety. Furthermore ESM allows you to manage your emergency lighting efficiently so you can save money and time.

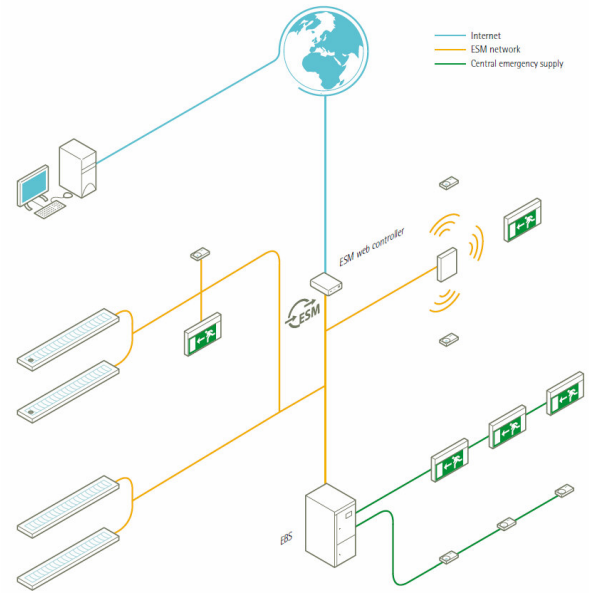
ESM Remote Access

You can connect ESM network to the internet allowing employees and suppliers to access the ESM web interface from outside your corporate network. This feature allows you to make maintenance reports and collect the necessary replacement parts upfront. The complete emergency lighting system can be serviced in a single visit.

To do so, users simply log on to the ESM Central Server (central server) by browsing to www.etapservice.com. (portal.esm.service.etaplighting.com) From this central server they can communicate with the ESM web interface through a secure tunnel.

The key question this white paper gives you an answer to is “Is it safe to connect my ESM to the internet and what measures has ETAP take to avoid unauthorized access?

First we will take a closer look to VPN: the basic mechanism of security: VPN. Then we go more in detail to the communication flow and at last in to the different levels of security.



ESMweb™ Remote Access

VPN: THE CORNERSTONE OF ESM REMOTE ACCESS SECURITY

One of the cornerstones of ESM Remote Access security is VPN: a **V**irtual **P**rivate **N**etwork

- Virtual: not limited to a physical structure, use other networks as a carrier
- Private: outsiders cannot “see” your communication
- Network: you can communicate as if you were on one LAN

VPN is a secure tunnel over the internet. It offers a solution for the risks involved in allowing remote access to servers behind a corporate firewall.

Before the user can access the corporate network, a tunnel has to be established. All communication between the ESM Central server and your ESM web-interface will pass through that tunnel. To establish this tunnel ESMweb™ will send a request, including a certificate, for authentication.

Once the ESMweb™ has been authenticated, the tunnel will be established. All the data that passes through the tunnel is encrypted and therefore not vulnerable to modification or eavesdropping by hackers.

Direct communication that is not passing through the tunnel will still be blocked by the corporate firewall.

OpenVPN and Firewall pass-through

ESMweb™ implements OpenVPN for its remote access communication. OpenVPN is a full-featured open source VPN solution. Starting with the fundamental premise that complexity is the enemy of security, OpenVPN combines security with ease-of-use

OpenVPN's lightweight design sheds many of the complexities that characterize other VPN implementations. OpenVPN is not a web application proxy and does not operate through a web browser.

Most VPN solutions are IPsec (Internet Protocol security) which require firewalls with special VPN support. OpenVPN is SSL-VPN based and can be used in such a way that no special requirements are imposed on the corporate firewall.

In the implementation of OpenVPN in ESMweb™ most corporate firewalls will even allow the establishing of the VPN tunnel without any modification to the existing firewall rules.

A SECURE COMMUNICATION FLOW

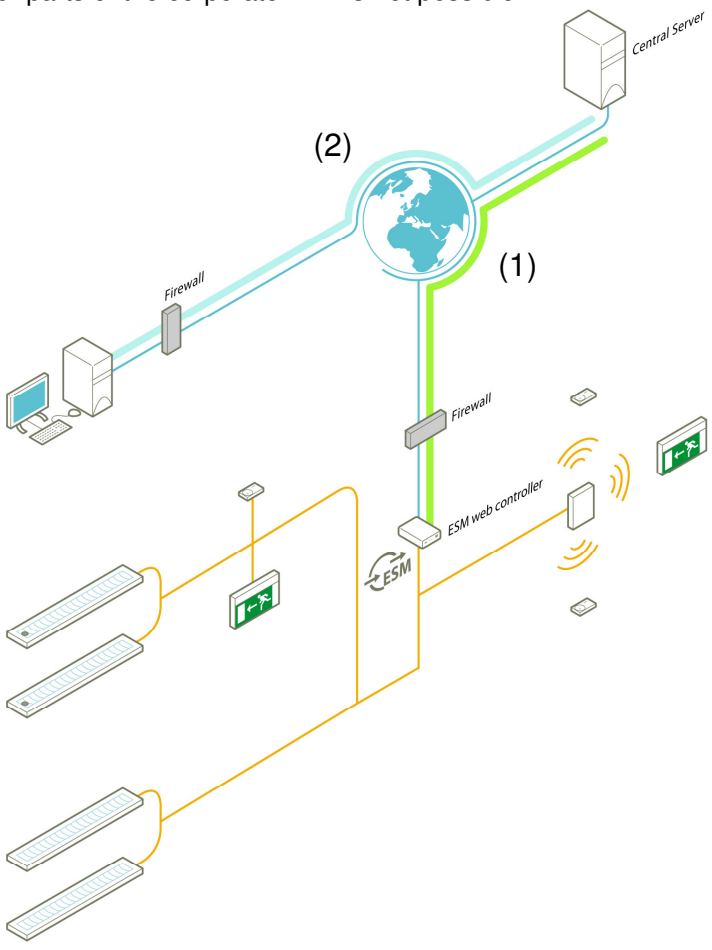
When the ESM web controller boots with VPN activated, the controller will establish a connection to the central server. After successful authentication of the controller by the central server a VPN tunnel (1) will be established between the controller and the central server.

An SSL (Secure Sockets Layer) session is established with bidirectional authentication. If this authentication succeeds, then different keys are exchanged to enhance security even further.

Once the VPN tunnel has been established the ESM web controller synchronizes data (local account information, etc.) through the VPN tunnel. This synchronization will be repeated at regular intervals. If the tunnel should disappear, the ESM web controller will automatically try to reestablish the VPN tunnel.

The user communicates with the ESM Central Server through a TLS(Transport Layer Security) connection (2). This means HTTPS (HyperText Transfer Protocol Secure) using TLS certificates. The central server will use the VPN tunnel to relay http traffic between the user and the controller. Relaying is only allowed after authentication on the central server and is limited in time.

Because the ESM web controller acts as the endpoint for the VPN connection, access to other parts of the corporate LAN is not possible.



DIFFERENT SECURITY LEVELS

Level 1: Separation

The ESM web controller's remote access is designed to work from behind a corporate firewall. As a result, your ESM web controller will be protected by the firewall in the same way your corporate computers are protected.

In order to achieve the highest possible security level, the ESM web controller should always be protected by such a firewall.

Level 2: Encryption

All information exchange between the remote user, the central server and the ESM web controller is encrypted. This prevents outside modification of the data as well as eavesdropping (or listening-in).

Between the remote user and the ESM Central Server this encryption is achieved by using a TLS connection over https (2); similar to online banking. The connection between the ESM web controller and the central server on the other hand is effectively an OpenVPN connection (1), which is similar to what is frequently used for teleworking. And, because the encryption uses so-called private-keys, it is impossible for other computers to decrypt the data or to pose as either party.

Level 3: Connection flow

The connection must always be initiated from the ESM web controller to the central server. This means that it is not possible to force a connection from the remote user to the ESM web controller directly, nor will the ESM Central Server attempt to contact the ESM web controller on its own initiative. This also implies that when the remote access feature is turned off in the ESM web controller, no attempts to connect to it from the ESM Central Server can be made. This feature can only be switched on by a local user. This connection flow is further enforced by the firewall which in general will not allow direct access from the outside.

Level 4: Central Authentication

Both the remote user and the ESM web controller must authenticate before gaining access to the ESM Central Server. This is an additional line of defence against unwanted intruders. Any attempt by a remote user to gain unauthorized access to a web controller of your company will be stopped at the central server, and thus before entering the secure tunnel to the ESM web controller.

Level 5: Local Authentication

After the user has been authenticated to the central server, he/she still has to log in to the ESM web controller, just like any local user would. This keeps the fine-grained control of who is allowed to do what on the local ESM web controller.

CONCLUSION

ESM offers the advantage of Remote Access while it safeguards the integrity of your network.

The ESM web controller is **separated** from direct access by the firewall of your network. Access is only possible through a secure **VPN tunnel**, all communication in this tunnel is **encrypted**. The ESM web controller is the endpoint for the VPN connection, access to other parts of the corporate LAN is not possible.

To access the ESM web controller via Remote Access, you have to log in to the **ESM Central Server**. The **central authentication** on the ESM Central Server prevents unauthorized access to the ESM web controller in your network.

On the ESM web controller a **local authentication** is needed to enter the web-interface.

The **connection flow** prevents a forced connection to the ESM web controller: the secure tunnel can only be established from the ESM web controller itself.

With these measures ESM tackles the risk of unauthorized access to your network on every level.

EXPLANATORY LIST OF TERMS

Emergency lighting

Emergency lighting is the lighting that comes on when the supply to the normal lighting fails. It allows people to safely evacuate the building without panic.

ESM web controller

Central hardware device in an ESM network. The ESM web controller is connected to your corporate network. This way the ESM user-interface can be accessed from any PC within that network.

Remote Access

Function of ESM that allows users to access the ESM web controller from outside the corporate network over a secure internet connection.

ESM Central Server

Website you log in to to use Remote Access. From this website you can log in to your ESM installation from anywhere in the world.

Local user

User which accesses the ESM web controller via the corporate network.

Remote user

User which accesses the ESM web controller via Remote Access.

SSL (Secure Sockets Layer) & TLS (Transport Layer Security)

Cryptographic protocols that provides communication security over the Internet. TLS and SSL encrypts internet connections and makes use of authentication keys for message integrity.

LAN (Local Area Network)

Network for exchanging data between computers and other electronic devices. The LAN a company is referred to as 'corporate network'.

ETAP
EXCELLENT LIGHTING, SAVING ENERGY

ETAP NV
Antwerpsesteenweg 130 • 2390 Malle • Tel. +32 (0)3 310 02 11 • Fax +32 (0)3 311 61 42
e-mail: info.be@etaplighting.com • www.etaplighting.com