1. Important Notice for a PCs using a software firewall

MiCOM S1 Studio and our current ranges of Protection relays were designed to be used inside a site's logical security perimeter. Schneider Electric recommends a secure perimeter including such security measures as industrial firewalls. When using MiCOM S1 Studio remotely from outside of the site, it is advised to use a secured VPN and/or Jump host.
The software firewall and/or anti-virus configuration could potentially interfere with MiCOM S1 Studio.
Our commitment to move towards secure communication means that future versions of MiCOM S1 studio and device firmware will support secured communication over TLS both internally and remotely from the site, with easily configurable firewall rules.

1.1. Description

MiCOM S1 Studio uses a fixed port to establish communications with devices, after communication is established, the RPC protocol is used. The RPC Protocol dynamically assigns a port within a fixed range of TCP ports. To ensure proper work of all MiCOM S1 Studio functions related ports need to be opened for MiCOM S1 Studio.

1.2. Applications that can use Ethernet and may need Rules added to firewall.

Beside MiCOM S1 Studio some tools in MiCOM S1 Studio that can connect with device over Ethernet may need separate Rules added in firewall policy, as per the following list:

- Data Model Manager (DMM);
- PSL Editor (Px40);
- Courier Monitor;
- IED Configurator;
- AE2R;
- GOOSE Editor.

1.3. Opening ports in firewall tool (general instruction)

To open ports for application:

- Open Rules window;
- Add new Rule;
- Select application executive file;
- Select TCP protocol;
- Select source IP as Any;
- Select source port as Any;
- Select destination IP as Any;
- Select destination port as Any;
- Allow communication;
- Save Rule;
- Repeat instructions for UDP protocol.