NETWORK TECHNOLOGIES INC
1275 Danner Dr Tel:330-562-7070
Aurora, OH 44202 Fax:330-562-1999
www.networktechinc.com

E-MICRO-TRH(P) Hardening Procedure

The procedure below can be used for hardening E-MICRO-TRH(P) settings. It is recommended to upgrade the E-MICRO-TRH(P) to the latest firmware (version 3.32 or newer) before using these settings.

Severity	Description Details:
HIGH	Change the IP address from the Default IP to a customer preferred network setting. Administration -> Network. Change the IP Address setting to either use a preferred static IP or use an appropriate DHCP server to assign the gateway, IP address and DNS addresses. Provide an appropriate DNS server that is trusted and secure. If you prefer to use your device in an air gap setup, you can disconnect the Ethernet and set the IP and gateway to non-working addresses.
MED	Use Secure Email option with encryption. Administration -> Email Server When using SMTP settings in Network-> Email Server Settings, we recommend using SMTP Encryption of TLS or STARTTLS with the appropriate port # for your SMTP Server. We also recommend using Authentication in the SMTP server to limit spam. If you are not using a custom SMTP server and plan to use Microsoft 365 or Gmail, encryption is already handled by the E-MICRO-TRH(P) as appropriate.
MED	Use encrypted SNMP protocols Administration -> SNMP If SNMP is not being used on E-MICRO-TRH(P), it is recommended setting the SNMP Agent Type to “Disabled”. If you are using SNMP, we recommend using “SNMP v3 only” which provides encryption support. While SNMPv2 provides basic authentication, this would be recommended only if SNMPv3 is not compatible in your application. Also, if you do not plan on controlling the E-MICRO-TRH(P) over SNMP and using SNMP just to poll the values, we recommend setting SNMP Write to “Disable”
HIGH	Disable Telnet and HTTP Administration -> Network Settings We strongly recommend disabling Telnet as this is not secure. We also recommend using the Web Server Type in mode “HTTPS” for regular use. HTTP use is recommended only for device setup and during active management. **Please be aware that the E-MICRO-TRH(P) only supports limited features in the HTTPS web server.**
MED	Modbus Setting Administration -> Network Settings We recommend disabling the Modbus setting if you are not using this. **Please be aware that Modbus TCP does not support encryption and we recommend using other forms of encrypted communication over Modbus when appropriate.**
LOW	Set NTP Server Administration -> Time Settings It is recommended setting the appropriate Time Zone and set a NTP server so that any logs will have accurate Timestamps for analysis.

Severity	Description Details:
LOW	Download Configuration Backup Administration -> System -> Configuration File It is recommended keeping a backup of your configuration file in case your E-MICRO-TRH(P) device gets corrupted or is rendered inaccessible for any reason and you have to restore defaults to gain access. If you have this backup, you can upload it and need not repeat the configuration steps.
MED	User Account Privileges Administration -> Users -> Edit <x> User Settings -> Account Settings We recommend that you enable the least required privileges for all users. Privileges for any user can be assigned as Read Only, Operator or Admin.
MED	User SNMP Settings Administration -> Users -> Edit <x> User Settings -> Contact Settings We recommend enabling the desired Authentication Protocol and Privacy Protocol for SNMPv3 settings on this user.
HIGH	X509 Certificate Administration -> System -> Certificates It is recommended that you upload the appropriate certificate with key along with CA certificate for encryption and identification when using HTTPS and other encryption forms. We recommend using a strong key length when generating certificates and keys. For details on certificate generation, please refer to E-MICRO-TRH(P) manual.
HIGH	Firmware Update Administration -> Firmware It is recommended to sign up for the NTI newsletter for Firmware updates and always update the firmware to the latest version, especially when there are security updates. **Please be aware that firmware updates are to be performed in HTTP mode only.**
MED	IP Camera Access Administration -> IP Cameras It is recommend adding IP Cameras that require and use authentication. It is also recommended setting the HTTPS URL on these IP Cameras.