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

E-16D/5D/2D Hardening Procedure

The procedure below can be used for hardening E-xD settings. It is recommended to upgrade the E-xD to the latest firmware (version 4.32 or newer) before using these settings.

Below procedure can be used for hardening E-xD settings. It is recommended to use web page on latest firmware for these settings. Serial/SSH menu may not provide all setting options below.

Severity	**Description** **Location Details:**
HIGH	Change IP address from Default IP to customer preferred network settings. In Administration -> Network -> IPV4 Settings/IPv6 Settings. Change the IP Address setting to either use a preferred static IP or use an appropriate DHCP server to assign gateway, IP address and DNS addresses. Provide an appropriate DNS server that is trusted and secure. If you prefer to use your device in air gap setup you can disconnect Ethernet and set the IP and gateway to a non-working gateway. If you have enabled and are using 802.1Q VLAN setup please make sure to use a correct VLAN ID.
MED	Use Secure Email option with encryption. Administration -> Network -> SMTP Settings When using SMTP settings in Network-> SMTP Settings, we recommend using SMTP Encryption of TLS or STARTTLS with appropriate port # for your SMTP Server. We also recommend using Authentication in SMTP server to limit spam. If you are not using custom SMTP server and plan to use Microsoft 365 or Gmail, encryption is already handled by E-xD as appropriate.
MED	Use encrypted SNMP protocols Administration -> Network -> SNMP Settings If SNMP is not being used on E-xD, it is recommended to set SNMP Agent 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.
MED	DDNS with authentication Administration -> Network -> DDNS Settings If you are using DDNS server for remote connections to E-xD, make sure to use authenticated DDNS service only.

MED	MQTT Encryption Administration -> Network -> MQTT Settings If you are planning to use MQTT, we recommend to use Authentication and Encryption. Setting for "Verify TLS certificate" is optional but recommended. To Verify TLS certificate, this certificate must be signed by the same certificate provider as E-xD Root Certificate.
HIGH	Disable Telnet and HTTP Administration -> Network -> Server Settings We strongly recommend disabling Telnet as this is not secure. We recommend disabling HTTP as well once HTTPS is setup properly along with desired HTTPS certificates. Using HTTP for any use makes you vulnerable to man-in-the-middle type of attacks.
MED	Disable SSH Access Administration -> Network -> Server Settings We recommend disabling SSH access if you do not plan on using this actively.
MED	Login Timeouts Administration -> Network -> Server Settings We recommend to set Console and Web Login Timeout and set it anywhere from 5 minutes to 20 minutes according to your usage and monitoring.
MED	Modbus Setting Administration -> Network -> Server Settings We recommend to Disable Modbus setting if you are not using this. **Please note: Modbus TCP does not support encryption and we recommend to use other forms of encrypted communication instead of Modbus when possible.**
HIGH	Enable Network Security Administration -> Network -> Server Settings We strongly recommend to Enable Network Security as this mitigates several kinds of attack vectors like disabling access over HTTP completely, disable autofill of password and ICMP timestamp mitigation.

HIGH	Use Secure Passwords Only Administration -> Network -> Server Settings We strongly recommend that you Enable “Use Secure Passwords Only”. This strictly stores only FIPS 198-1 standard compatible passwords. Any hashes are salted with strong hashing algorithm.
HIGH	Disable 3G/4G/5G Data Administration -> Network -> 3G/4G Data connection We recommend disabling a modem’s data connection if you are not actively using this. This is because the modem connection may leave you open to public network access and opens attack vectors from any public network. If you are using the modem data connection, we recommend to set appropriate username and password and IP Filter Rules.
MED	Disable Legacy Management Software Administration -> Network -> Disable Legacy Management Software We recommend disabling Legacy Management Software and migrate to E-MNG-SH Management Software. Legacy Management software is not actively supported and any bugs and features on this will not be actively fixed.
LOW	Set NTP Server Administration -> System -> Time Settings It is recommended to set appropriate Time Zone and set an NTP server so that any logs will have an accurate Timestamp for analysis.
LOW	Download Configuration Backup Administration -> System -> Configuration Backup It is recommended to keep a backup of your configuration file in case your E-xD device gets corrupted or 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 configuration steps.

LOW	Enable Login Banner Administration -> Enterprise -> Enterprise Settings You can enable Login Banner to display a Banner message with legal notice and implications for unauthorized access.
LOW	Disable SMS Relay Server Administration -> Enterprise -> SMS Relay If you are not planning to use this E-xD to send SMS on behalf of other devices, it is recommended to Disable SMS Relay option. This option is disabled by default.
MED	User Account Privileges Administration -> Users -> Edit <x> User Settings -> Account Settings We recommend that you Enable only those users that are necessary for E-xD device operation. For all users, we recommend to Enable the least required privileges. Order of Privileges for any user starting with the least privilege would be Read Only, Operator and Admin.
MED	User SNMP Settings Administration -> Users -> Edit <x> User Settings -> SNMP Settings We recommend enabling the desired Authentication Protocol and Privacy Protocol for SNMPv3 settings on this user here. We also recommend SNMPv3 Traps as it can be encrypted.
MED	User Authentication Mode Administration -> Security -> User Authentication We recommend using appropriate user authentication mode that supports 2 Factor Authentication within LDAP or Radius.
HIGH	User Password Restrictions Administration -> Security -> User Password Restrictions We recommend enabling all password restrictions and set minimum password length of 10 characters. This restriction applies to local users logging into E-xD directly.

HIGH	X509 Certificate Administration -> Security -> X509 Certificate It is recommended to upload appropriate certificate with key along with CA certificate for encryption and identification when using HTTPS and other encryption forms. We recommend using strong key length when generating certificates and keys. For details on certificate generation, please refer to this manual: https://www.networktechinc.com/pdf/sman154-04.pdf Steps I or II
MED	Enable IP Filtering Administration -> Security -> IP Filtering It is recommended allowing only IP Addresses that are expected to have valid access to this device. All other IP's which do not need inbound access via Modem data, SSH, MQTT, Modbus, HTTP, HTTPS etc. need to be set to DROP with appropriate rule and subnet.
HIGH	Firmware Update Administration -> Firmware It is recommended to sign up for NTI newsletter for Firmware updates and always update the firmware to the latest version, especially when there are security updates.
MED	IP Sensors HTTPS access Monitoring -> IP Sensors It is recommended to add IP Sensors only in HTTPS mode and recommended to keep the firmware of these IP sensors updated.
MED	IP Camera Access Monitoring -> IP Cameras It is recommend using IP Cameras that only require authentication with Digest Access to prevent a man-in-the-middle attack on these cameras. It is also recommended to set https on these IP Cameras.
MED	Remote SSH Commands Events -> Remote SSH Commands It is recommended to only have commands that do not need authentication credentials on command line here. Any commands with credentials will not by encrypted by E-xD and are discouraged.