Merit LILIN Application Note

LILIN Network Product Hardening Guide

Document Number：A00141
Date：2018/3/29
Dept: Technical Support, Taipei

LILIN product hardening guide provides security guidence for responsibly installing LILIN network products including LILIN Navigator, LILIN NVRs/DVRs, and LILIN IP cameras for home, enterprise, and government users.

Products: LILIN NVR, IP camera, and LILINViewer App

Home	Update to the latest firmware for IP cameras and NVRs
	Update to the latest WiFi AP / Router 's firmware
	Do not use the DMZ feature of either Wi-Fi AP's or Routers for NVRs or camera's connected to the internet
	Change the default admin password
	Use a strong password
	Create a viewer's account for remote viewing and recording
	Disable IP Cam's Bypass logon (default off)
	Set Date/Time using NTP sync
	Disable audio when not in use
	Use LILIN Viewer app with P2P connection for NVR remote viewing

Products: LILIN NAV Corporate, Enterprise, NAV Client

Enterprise	Ensure Windows updates and Windows Defender updates are applied upon release
	Use Digest authentication
	Enable RTSP authentication (default)
	Disable unused services
	Enable IP filter function
	Enable HTTPs Encryption
	Use LILIN DDNS with HTTPs Encryption service

Government	Disable IPScan Bypass logon
	Disable IP camera's ONVIF search function
	Use SNMP v3 to monitoring
	Set network detection loss on IP Cam to save video to SD card

	Enable 802.1x for network access control
	Use Virtual Private Network and Virtual Local Area Network

Detail Description

Update the latest IP camera/NVR firmware
At regular intervals visit LILIN web site for the latest product firmware.

Update the latest WIFI AP / Router's firmware
Update the firmware for WiFi station or router to avoid security flaws.

Do not enable the DMZ mode in WiFi AP or Router for NVRs or cameras to internet
DMZ (Demilitarized Zone) feature of WiFi access points or routers might expose IP devices to Internet, thus, please disable DMZ feature.

Change the Admin account and default password
Change the default user account and password. For LILIN NVRs or IP cameras, these products have only one user account for remote access. Please change the default user account and password.

Use strong username and passwords
Use at least 8 digits including one upper letter, one lower, and one digit for username and password for IP products. Change username and password regularly.

Create a viewer's account just for remote viewing
Create a viewer's account just for Smart Phone remote viewing access. Do not use single admin account for IP products.

Disable IP camera's Bypass Logon
Do not use Bypass Logon for private use. Bypass Logon should only be used for publicly accessible cameras.

Set Date/Time using NTP sync
Constantly check timer of IP products for log system. Some of the authentication encrypting algorithm is based on timer.

Disable audio when not in use
For privacy purpose, do not turn audio on for recording.

Use LILIN Viewer app with P2P connection for remote viewing
For using LILIN Viewer Smart Phone access, use LILIN proprietary P2P protocol for remote video access.

Keep the Windows update and Windows Defender in the latest updates
For using LILIN NAV products, constantly manual run Windows Update and Windows Defender updates to avoid cyber attack. Turn off the auto update for Windows Update and Windows Defender to avoid Windows reboot itself meaning loss of recording whist the system is offline.

Using Digest authentication
Use Digest authentication rather than traditional base64 encode for accessing IP cameras or NVRs.

Enable RTSP authentication
RTSP is the video and audio streaming protocol. Use RTSP authentication for a video client for accessing LILIN IP cameras.

Disable unused services
Disable the following network services UPNP (default OFF), Bonjour (default OFF), SDDP (default ON, SNMP (default OFF), ONVIF Search (default ON). For enterprise NAV recorder usage, turn off SDDP to avoid network storm.

Enable IP filter function
Enable IP filter feature to enable an allowed access list for a NVR, a WiFi AP, and a router.

Enable HTTPs Encryption
Enable HTTPs for remote video access for IP cameras and NVRs. HTTPs encryption can avoid unauthorized access by a third party.

Use LILIN DDNS with HTTPs encryption service
If a public IP address is not available, PPPoE is applied. Use the LILIN DDNS service for LILIN IP products. LILIN provide free HTTPs based DDNS service. This keeps connection security and avoid data piracy issues. Sensitive user information and database are encrypted. Data redundancy of LILIN DDNS is also considered at AWS New York.

Disable IPScan Bypass logon
IPScan is a LAN device scanning application which is easy-to-use for changing IP addresses. Disable IPScan Bypass logon (default ON) of IP cameras and NVRs, this can avoid IP addresses chaning by the access of an unauthorized person.

Disable IP Camera's ONVIF search function
Disable IP camera's ONVIF search function, this can avoid IP addresses of ONVIF IP cameras being changed by the access of an unauthorized person.

Using SNMP v3 to monitor
If SNMP is needed for monitoring network devices, use SNMP v3 to protect sensitive information of the network devices.

Set network loss detection and record to SD card
Enable record to SD card when network loss or connection loss of IP cameras. LILIN NAV recorder is able to sync SD card recording back to NAV recorder for failover purpose.

Enable IEEE 802.1x network access control
Enable IEEE 802.1x network authentication feature. IEEE 802.1x is able to provide extra security protection accessed in between the VMS and the switch.

Use Virtual Private Network and Virtual Local Area Network
For highly secured access, use Virtual Private Network (VPN) for accessing network devices, NVRs, or IP cameras via Internet to become a Virtual Local Area Network.

Contact
Contact lilin.zendesk.com if you have further questions.