Network Security Recommendations

UPDATED 10/5/2023

Any device that is connected to the Internet, including network cameras and video recorders, is at risk of potential unauthorised access. To reduce the risk of such events, please review the best practices listed below and implement as many of these suggestions as possible.

Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. Use strong passwords that conform to the follow enhanced security criteria:
    a. Passwords should be at least 8 characters in length but are recommended to be 12 characters or greater.
    b. Passwords should include at least one each of uppercase letters, lowercase letters, numbers, and symbols.
    c. Passwords should not contain the corresponding username.
    d. Passwords should not contain continuous characters such as 1234, abc,etc.
    e. Passwords should not contain repetitive characters such as 1111, aaa, etc.

2. Use the latest approved firmware version for the device. Please contact the authorised seller for any inquiries on current and latest firmware versions.

Optional actions recommended for additional network security:

1. Use strong usernames that conform to the following enhanced security criteria:
    a. Usernames should be at least 5 characters.
    b. Usernames should not match or be contained within a corresponding password.

2. Change passwords often. This can be enforced by the device by setting an Expired Term of Password from the device System Management menu.

3. Perform good user management practices. Create lower-level users with limited group authority as needed rather than sharing an admin account. Regularly audit the user management list to update passwords, delete unused usernames, and adjust group/user authority as needed.

4. Enable auto log-out so the device will automatically log-out after a set period of activity. This can be configured from the device System Management menu.

5. Enable log-in fail event notifications so you can be notified whenever someone attempts to login and fails. This can be configured from the Event System Events menu.

6. Change device port numbers to non-default values. This can be done from the device IP Setup menu.

8. Utilise enhanced, strong usernames and passwords for any connected network services (DDNS, P2P/Cloud, E-mail, etc.).

9. Enable HTTPS for web access. This can be done from the device Network Security menu.

10. Enable DIGEST authentication for HTTP(S) web access.
Note: this can cause issues with PTZ camera control on some monitored sites (e.g., Immix).

11. Enable RTSP encryption to encrypt video feeds transmitted via RTSP. This can be done from the device Network > Security menu.

12. Utilise the IP filter feature to only allow remote access to the device from a known, authorised IP address/range. This can be done from the device Network > Security menu.

13. Disable any unused network protocols such as FTP, SNMP, DDNS, UPnP, PPPoE, etc.

14. Disable audio streaming/recording if not needed.

15. Physically secure devices as much as possible. For example, install video recorders inside network cabinets that can be locked. Employ access control technology to ensure only authorised personnel can gain physical access to the device.

16. Regularly review device logs to confirm if anyone has bypassed existing protocols and has gained unauthorised access. Assess if any additional recommendations can or need to be implemented.

If you suspect your device has been compromised:

1. If possible, immediately remove the network connection from the device to prevent further network compromises.

2. Reboot the device: some botnet and other malware is cleared from the system with a reboot.
3. Check the User Management menu for any unrecognised users/groups. Delete any unrecognised users/groups.

4. Check the Search Event Log for system events indicating log-ins, menu access, and configuration for any unrecognised activity

5. Save the system log from the System Management menu to allow for further analysis

6. Update the recorder to the latest version of firmware to provide the most recent network security features.

7. Factory default the device and input any prompted recovery information during set up in addition to any site specific configuration