



TKH SECURITY FD2026M Cybersecurity Camera Hardening User Guide

[Home](#) » [TKH SECURITY](#) » TKH SECURITY FD2026M Cybersecurity Camera Hardening User Guide 

Contents

- 1 TKH SECURITY FD2026M Cybersecurity Camera Hardening User Guide
- 2 About this guide
- 3 What's in this guide
- 4 We like to hear from you!
- 5 Hardening measures
- 6 Camera
- 7 Factory Default
- 8 Firmware update
- 9 2.1.3 Strong password
- 10 Change password regularly
 - 10.1 Authentication lockout
- 11 User accounts with least privileges
- 12 Time synchronization
- 13 Disable unused protocols
- 14 Change the default ports
- 15 Review Settings
- 16 Audio input
- 17 IP filtering
- 18 Session logout
- 19 SD card encryption (securing local recording)
 - 19.1 Physical Security
 - 19.2 Network
- 20 Network segmentation
- 21 Controlled access to the network
- 22 Set the router firewall
- 23 Port authentication (802.1x)
- 24 Multicast
 - 24.1 Data Security
 - 24.2 SSL/TLS versions
 - 24.3 HTTP authentication
 - 24.4 RTSP authentication
 - 24.5 HTTPS
 - 24.6 Encrypted streaming (RTP/RTSP/HTTPS, SRTP)
- 25 Data Retention Policy
 - 25.1 Monitoring and Logging
 - 25.2 Logging
 - 25.3 Tamper Detection
 - 25.4 Check the log file regularly
 - 25.5 Network Traffic
 - 25.6 Use secure syslog with TLS
 - 25.7 Security matrix
 - 25.8 Incident Response Plan
 - 25.9 Decommissioning and Disposal
 - 25.10 Read More About This Manual & Download PDF:
- 26 Documents / Resources
 - 26.1 References

TKH SECURITY FD2026M Cybersecurity Camera Hardening User Guide



About this guide

What's in this guide

This guide outlines essential steps to harden the cybersecurity of TKH Security cameras. Implementing these measures will help protect your surveillance system from unauthorized access, data breaches, and other cyber threats.

By following the following steps, you can significantly improve the security of your TKH Security cameras, reducing the risk of unauthorized access and ensuring the integrity and confidentiality of your surveillance data. Regularly review and update your cybersecurity measures to keep pace with evolving threats.

We like to hear from you!

Customer satisfaction is our first priority. We welcome and value your opinion about our products and services. Should you detect errors or inaccuracies in this manual, we would be grateful if you would inform us. We invite you to offer your suggestions and comments, Your feedback helps us to further improve our documentation.

Hardening measures

Camera

Factory Default

Before installing make sure that the camera is in its factory default state. If in doubt, force the camera to its factory defaults again.

Firmware update

Update the camera firmware to the latest version available from TKH Security. Regularly check for updates to ensure the device is protected against the latest vulnerabilities.

2.1.3 Strong password

The administrator password should be unique and as strong as possible (minimum of 8 characters with a mix of letters, numbers, and symbols).

It is recommended to avoid subsequent series such as 1234, 555, or abcd, or the use of existing words.

Generally, the best random passwords are generated by using a password generator tool.

Change password regularly

Change your passwords regularly. The best practice is to change the passwords every 90 days.

Authentication logout

Enable the account logout policies after a defined number of failed login attempts to protect against brute-force attacks.

User accounts with least privileges

Assign user roles with the principle of least privileges. Limit administrative access to only those who need it. VMS clients, support engineers or operators may access the camera as “Operator” or “Viewer”. Be aware that some VMS clients require “administrator” access.

As a general guideline, following principle roles exist (not limited to):

- Administrator: full control of all camera features and functions
- Supervisors: full control except for user management and restoring factory defaults
- Operators: access to view cameras, control PTZ
- Viewers: access to view cameras

Time synchronization

Use a single time provisioning source, and configure the camera to synchronize against this single time source regularly.

Disable unused protocols

Turn off unnecessary network protocols such as Telnet and FTP to reduce the attack surface. Only keep those protocols enabled that are used, and document these.

Do not use SNMPv1, SNMPv2, TLSv1.0, TLSv1.1, UPnP, Telnet, FTP, Basic authentication, Bonjour, DDNS.

Whenever these protocols are used during installation, make sure that these are disabled upon completion of the work.

Change the default ports

It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.

Review Settings

Regularly review and adjust camera settings to enhance security.

Audio input

Disable the audio feature of the camera if this is not used.

IP filtering

Use black and white list to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.

Session logout

Inactive users will be logged out after a set period.

SD card encryption (securing local recording)

If the camera supports encryption of the recordings then it is highly recommended to use/enable this function.

Physical Security

Ensure cameras are physically secured to prevent tampering or unauthorized access. This includes using tamper-resistant mounts and enclosures.

Network

Network segmentation

Place security cameras on a dedicated VLAN separate from the main network. This minimizes the risk of cross-network infections or attacks.

Controlled access to the network

Use a Virtual Private Network (VPN) for remote access to the camera system. Do not expose to the public network or the Internet.

Set the router firewall

It is recommended to set the firewall of your router.

Note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).

Port authentication (802.1x)

Make use of network access control using IEEE 802.1x with at least EAP-TLS (MD5 is listed as an vulnerability). Use the safely stored private key that is generated by the camera itself to request a CA client certificate.

Multicast

Avoid the use of multicast in an open accessible network. It is very easy to eavesdrop on multicast streams.

Data Security

SSL/TLS versions

TLS versions 1.0 and 1.1 are not to be used. They accept simple encryption schemes that are hacked. The current TLS version is TLSv1.3.

HTTP authentication

Select digest authentication for HTTP. It encrypts the passwords over the network. Basic authentication is considered unsafe, as it transmits the password in plain text over the network.

RTSP authentication

Using Digest Authentication with RTSP makes the video stream only accessible when you have the proper credentials. Digest Authentication should be chosen over the unsafe Basic Authentication.

HTTPS

Enable HTTPS for accessing the camera's web interface to ensure that data transmitted between the camera and the user is encrypted.

Encrypted streaming (RTP/RTSP/HTTPS, SRTP)

In HTTPS mode HTTP tunnelling of RTP/RTSP encrypts the stream over the secure socket. Only the receiving VMS is able to decrypt the video content. If the camera supports the SRTP protocol, then this protocol is preferred over the RTP protocol.

Data Retention Policy

Establish a data retention policy to regularly delete or archive old footage in a secure manner.

Monitoring and Logging

Logging

Logging is by default enabled on the camera to monitor access and configuration changes. The log files are stored securely on the device.

Tamper Detection

The camera are fitted with a Tamper Detection System to monitor the quality and integrity of the image.

Check the log file regularly

Regularly inspect the log files to stay informed of reported irregularities.

Network Traffic

Analyse network traffic to detect potential anomalies related to the cameras.

Use secure syslog with TLS

The best practise for logging is the use of remote syslog over a secure channel (TLS). If the camera is not supporting secure syslog, use local logging with the minimum options.

Make sure that the logging server is adequately secured to allow authorized access only.

Security matrix

Feature	Default setting	Medium security level	High security level
Factory Default	Manual check	Okay	Manual check
Initial login wizard	HTTP or HTTPS	HTTPS	HTTPS
Password policy	8 char, upper/lower case, digit	8 char, upper/lower case, digit, no dictionary	Up to 16 char, upper/lower case, special char, digit, no dictionary
Firmware Updates	Manual check	Manual check	Manual check
Signed Firmware	Default*	Default*	Default*
User management	Admin	Admin	Operator/Viewer
Lockout Mechanism	Enabled	Disabled	Enabled
Session Timeout	Enabled	Enabled	Enabled
HTTP/HTTPS	HTTP	HTTPS	HTTPS
IEEE802.1x	Disabled	EAP-MD5/TLS	EAP-MD5/TLS
TLS version	TLSv1.3	TLSv1.3	TLSv1.3
HTTP Authentication	Digest	Digest	Digest
RTSP Authentication	Disabled	Digest	Digest
Certificate (HTTPS)	Self signed cert	Self signed cert	CA
Certificate (802.1x)	CA/Enterprise	CA/Enterprise	CA/Enterprise

Streaming	UDP, unicast	TCP (RTP/RTSP)	Tunneled over HTTPS (RTP/RTSP/HTTPS), SRTP if supported
Multicast	Disabled	Enabled or Disabled	Disabled
Telnet	Disabled	Disabled	Disabled
SSH	Disabled	Disabled	Disabled
FTP	Disabled	Disabled	Disabled
NAS	Disabled	Disabled	Disabled
SNMP	Disabled	SNMPv3	Disabled
ONVIF	Enabled	Enabled	ONVIF via HTTPS

MX	Enabled **	Disabled	Disabled
UPnP	Disabled	Disabled	Disabled
NTP	Disabled	Enabled	Enabled
Syslog	Disabled	Enabled or Disabled	Disabled or Enabled over TLS (if supported)

* Signed firmware available for the 840-series, XCU-series, and TPU-series

**MX proprietary protocol is supported by the 840-series, XCU-series, and TPU-series

Incident Response Plan

TKH Security has a dedicated Incident Response plan.


For more information please visit: <https://tkhsecurity.com/vulnerability-disclosure/>

Decommissioning and Disposal

Before decommissioning any camera, ensure that all data is securely wiped to prevent unauthorized access to sensitive information. Follow proper procedures for the secure disposal of camera hardware, including the destruction of storage devices.

Read More About This Manual & Download PDF:

Documents / Resources

	<p>TKH SECURITY FD2026M Cybersecurity Camera Hardening [pdf] User Guide FD2026M Cybersecurity Camera Hardening, FD2026M, Cybersecurity Camera Hardening, Camera Hardening, Hardening</p>
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

References

- [**> TKH Security - Home**](#)
- [**> TKH Security - Home – TKH Security**](#)
- [**> TKH Security - Vulnerability Disclosure**](#)
- [**User Manual**](#)

Manuals+, Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.