AK-System Manager cybersecurity: Mandatory requirements and recommended best practices

Cybersecurity - mandatory requirements

Danfoss considers the following aspects mandatory when planning to connect your System Manager to digital networks. Failure to implement the mandatory requirements below exposes your System Manager and connected applications to malicious attacks and is outside Danfoss' recommended operating posture.

AK-SC355 (end of life in 2016, end of service in 2021. Replaced with the AK-SM 800)
- Do not connect a System Manager directly to public internet or any untrusted open networks
- Protect remote access with a secure VPN terminated behind a stateful firewall using a deny-by-default policy
- Ensure factory User and password is changed

AK-SM 800 (end of life in 2021, end of service in 2023. Replaced with the AK-SM 800A)
- Do not connect a System Manager directly to public internet or any untrusted open networks
- Protect remote access with a secure VPN terminated behind a stateful firewall using a deny-by-default policy
- Ensure factory User and password is changed

AK-SM 800A (actively sold and supported globally)
- Do not connect a System Manager directly to the public internet or any untrusted open networks
- Protect remote access with a secure VPN terminated behind a stateful firewall using a deny-by-default policy
- Ensure System Manager is running latest software version to maximize cyber security functionality
- Ensure the System Manager security level is set to **Strict mode** (Configuration>Security-Strict)

Cybersecurity - best practices

Follow these best practices in addition to the mandatory requirements

- Change passwords on a regular basis and do not share or publish
- Change standard management ports or restrict access to allowed sources only
- Segment the control network (e.g., VLANs); isolate from corporate and guest networks
- Back up configurations securely
- Consult available industry standards (i.e. ISO/IEC 27002:2013) for further reference and guidance