Installer guide: to support Installers and their supermarket customers following the cyber incident in Europe

Purpose of this guide:

Danfoss is taking a proactive approach to help Installers assist their customers using the following controllers: AK-SM800A, AK-SM800, AK-SM720, AK-SC255, or AK-SC355.
It explains the actions installers should take to identify the installed system, remove unsafe internet exposure, recover, verify affected configurations, update supported equipment, and restore remote access securely.

Installer checklist for customer sites

1

Identify the installed product
Confirm the exact controller model and software version at each site before giving product-specific advice and determining the recommended next steps.

2

Protect the site immediately
Remove public-internet exposure from affected units and from any unit reachable through a public IP address.
Ensure the default username and password have been changed.

3

Recover and verify
If the site was affected, restore the complete configuration from a trusted backup and validate the restored settings against the approved site configuration before returning the system to normal operation.

4

Update supported systems
For AK-SM800A, install latest available software and enable Strict Mode (Step-by-step guide & SW download). End-of-life systems, do not receive further updates. Danfoss therefore recommends to migrate to supported products.

5

Restore remote access safely
Re-establish remote access only through a secure VPN or another protected network. Do not expose the controller directly to the public internet.

6

Document and escalate
Record the product, software version, actions completed, and any remaining issue. Contact Danfoss Technical Support when further help is required.

Product-based guidance

Installed system	What the installer should do	Lifecycle direction
AK-SM800A	Update to the latest available software. Enable Strict Mode. Apply the network-protection actions in this guide.	Current generation product.
AK-SM800 / AK-SM720	Apply network protection and remove public-internet exposure. There is no product-specific firmware action stated in this guide.	End-of-life.
AK-SC255 / AK-SC355		Recommend migration to AK-SM800A.

Detailed instructions for installers

A. Identify the site configuration

- Confirm the installed controller model: AK-SC255/355, AK-SM720/800, or AK-SM800A.
- For AK-SM800A, confirm the installed software version before planning the update.
- Confirm whether the controller is directly exposed to the public internet or accessed through a protected network or VPN.
- Confirm that a usable configuration backup is available.

B. Apply the immediate containment actions

- Remove internet exposure from affected units.
- Remove public-IP exposure from all supervisory units, whether or not an incident has been confirmed.
- Keep remote access disabled until a secure VPN or protected network is in place.
- Ensure factory user and password is changed.

C. Restore and verify after an incident

- Restore the complete system configuration from a trusted backup.
- Verify the complete configuration before returning the site to normal remote operation.
- If the configuration cannot be verified, contact Danfoss Technical Support.

D. Update AK-SM800A

- Install the latest software available for the AK-SM800A series.
- Follow the Danfoss step-by-step update guide.
- Enable Strict Mode after completing the update.

Installer resources: AK-SM800A step-by-step guide | AK-SM800A software download page

E. Re-establish remote access

- Do not reconnect a controller directly to the public internet.
- Use a secure VPN or another protected network.
- Ensure appropriate firewall protection is in place.

Cybersecurity best practice for all connected systems

- Change passwords regularly. Do not share or publish credentials.
- Change standard management ports, or restrict access to allow-listed sources only.
- Segment the control network, for example by using VLANs, and isolate it from corporate and guest networks.
- Allow remote access only through a secure VPN or another protected network.
- A firewall alone is not considered sufficient protection.
- Back up system configurations securely and verify that backups can be restored.
- Review the lifecycle status of installed products and plan migration from end-of-life systems to supported solutions.
- For further guidance, consult relevant industry standards such as ISO/IEC 27002.

Frequently asked questions

Which products are relevant to this support guide?

AK-SC255/355, AK-SM720/800, and AK-SM800A supervisory systems.

Which systems require a firmware update?

The product-specific firmware action in this guide applies to **AK-SM800A** series: update it to the latest available software and enable Strict Mode.

Can the systems continue to operate?

Yes, when operated in accordance with Danfoss cybersecurity recommendations, including the latest software for AK-SM800A, protected remote access, and standard cybersecurity best practices.

What is the recommendation for end-of-life products?

Apply the network-protection measures and recommend migration from AK-SC255/355 and AK-SM720/800 to the AK-SM800A series so the customer can receive continuous cybersecurity updates.

What if I cannot complete or verify the recovery?

Keep unsafe remote access disabled and contact Danfoss Technical Support.

Danfoss Technical Support

Europe	Outside European support hours
Email: support.foodretail@danfoss.fr Languages: English and French Or contact your regular regional technical support team. Hours: 08:00-17:00 CET	Email: sm-security@danfoss.com Or contact your regular regional technical support team. Hours: 14:00-23:00 CET