ENGINEERING
TOMORROW

Application Guide

AK-SM 800A Series
Security Guidance and Session Control

ADAP-KOOL® Refrigeration Control System

1. Why be concerned about security?

Product Security and the secure installation of your AK-SM 800A is very important for several reasons:

Data Protection: Security measures such as HTTPS and strong passwords help protect sensitive data from unauthorized access and ensure that communication between the device and other systems is secure.

Prevention of Unauthorized Access: Security features like strong passwords and session control help prevent unauthorized users from accessing the device, protecting it from tampering and misuse.

Network Security: Wireless Wi-Fi WPA2 ensures that only authorized devices can connect to the network, reducing the risk of unauthorized access and potential security breaches.

Business Continuity: Ensuring the security of your embedded controller can help prevent disruptions to your business operations caused by security breaches or data loss.

Compliance Requirements: Many industries have strict security and privacy regulations that require companies to implement certain security measures. Ensuring the AK-SM 800A meets these requirements can help you avoid fines and legal issues.

2. AK-SM 800A built-in security functionality

Your AK-SM800A offers several built-in security features. Enabling and enforcing these features will strengthen the overall security posture of your application. The following overview of System Manager functions assumes latest software installation.

Remote encrypted communications

- Session Control (configurable)
- HTTPS Web browser support Port 443 (configurable)
- HTTPS XML (token based)
- Encrypted emails (Using TLS 1.2)

System Passwords / User Access

- All passwords stored in encrypted format
- User authentication required for unit access
- Passwords comply with min 8 characters (1 capital, 1 special character, 1 numeral)
- User accounts and passwords not stored in system application database
- Password reset via authenticated unit check and issue of temporary code
- Danfoss does not have access nor can view passwords

Wireless access point

- WPA2 encryption
- Default state off, enabled only via authorized users for 8 hours
- Isolated from WAN / Host network
- Password protected SSID associated with unit host #, password

General

- System software and OS stored and distributed via Danfoss approved software server
- Access to USB application functions (USB flash drive) based on user authentication level/permission
- Factory set Linux OS firewall enabled - all non-required ports are closed on external Ethernet as well as between wireless access point and internal ethernet ports
- All software publications are subject to Danfoss Penetration testing
- FTP not supported

3. Recommended best practice / product

- Ensure your AK-SM 800A units have the latest software from Danfoss
- If using a 'host network', all units must have same software and users / passwords
- Never connect your AK-SM 800A on an open public network
- The System Manager 800A series has been designed to reside behind appropriately configured firewalls and secure LAN. Do not install on any public or non-secure network
- Use Strong passwords
- Enable strict Session control (includes HTTPS)

4. Session Control: Technical implementation

With AK-SM 800A software package 4.0 and above, an updated security posture is introduced. In compliance with IT best practice and mandatory[1)] standards, Danfoss will default to a strong security[2)] 'posture' on the System Manager AK-SM 800A.

With AK-SM 800A software package 4.0 and above, Danfoss is promoting a stronger security 'posture' with the inclusion of session control and the default setting of **Strict**. Sesson control in the 800A is an authentication rules engine/module and is intended to improve the overall security posture of your system. Session control offers different configuration settings (Backward compatibility, Permissive and Strict). Depending on how these settings are configured, the remote interface will need to comply accordingly.

- Session control pertains to Northbound connection security (remote UI and XML)
- AK-SM 800A Session control consists of 3 levels [Backward Compatibility, Permissive, Strict]
- Upon installation of Release 4.0 session control is immediately defaulted to strict (can be manually changed to backward compatibility mode)
- Strict setting requires session tokens for XML1.0 and HTTPS for SvB5 and SvW
- After upgrade of software package 4.0, user is informed via local screen and remote UI (SvB5/SvW) and has opportunity to select backward compatible mode (requires manual selection).

Table: AK-SM 800A session control options

Session Control setting	Description
Backward Compatible	Not recommended but when selected, http is available, and no session tokens needed
Permissive (used as a transition to strict level)	Set this level to view any error responses so that adjustments can be made in preparation for strict mode. Permissive is allowing both the old authentication and the new authentication scheme at the same time.
Strict (defaulted immediately after s/w package R4.0.x install)	Require HTTPS connection XML requests cannot contain usernames and passwords. Must provide session token in the AKSM-auth header. HTTPS becomes mandatory and authentication moves from plain-text to session-based authentication. Strict mode will sanitize all strings in the Northbound connection of XML, rejecting any commands that conflict with the sanitization

<u>If Strict mode remains configured, and 3rd Party XML messaging is being used, ensure the XML messaging is updated for Strict mode (below)</u>

Strict (highest security level)

- XML requests cannot contain usernames and passwords, but must provide the session token in the AKSM-auth header. If an issue is discovered in the request, it gets rejected
- Required changes from 3rd party perspective
  - username and password must be removed from the XML request payload
  - session token must be placed in a CORS header called AKSM-auth

1) Example include but not limited to, Nis2 (Network Information Security), CRA (cyber resilience act), IEC 62443-4-1

2) Strong security posture = **HTTPS** + Session control **Strict**

5. Session Control: benefits

Danfoss recommends Strict mode for Session Control, in doing so please consider the following benefits:

Enhanced Security:
Session Control improves the overall security posture of your system by enforcing authentication rules. It requires HTTPS connection, encrypting all data in transit, and ensures that XML requests do not contain usernames and passwords, enhancing the security of your communication.

Compliance:
By defaulting to Strict mode, Session Control helps your system comply with internationally recognized regulations such as the NIS2 and CRA Directives, as well as the IEC 62443-4-1 Standard. This ensures that your system meets the highest security standards and regulatory requirements.

Flexibility:
Session Control offers different configuration settings, allowing you to choose the level of security that best suits your needs. Whether you need a backward-compatible mode for certain legacy systems or a strict mode for maximum security, Session Control provides the flexibility to adapt to your requirements.

Centralized Management:
Session Control can be managed centrally through the System Manager Configuration>Security menu, making it easy to configure and maintain security settings across your system. This centralized management ensures consistency and simplifies security administration.

Future-Proofing:
By enabling Strict Session Control, you are adopting security best practices and standards that are continuously updated and improved. This future-proofs your system against emerging security threats and ensures that your system remains secure and compliant in the long run.

In conclusion, Session Control offers a range of benefits, including enhanced security, compliance with regulations, flexibility, centralized management, and future-proofing. By implementing Session Control, you can ensure that your system is secure, compliant, and well-equipped to handle evolving security challenges.

DISCLAIMER: Professional Use Only

This product is not subject to the UK PSTI regulation, as it is for supply to and use only by professionals with the necessary expertise and qualifications. Any misuse or improper handling may result in unintended consequences. By purchasing or using this product, you acknowledge and accept the professional-use-only nature of its application. Danfoss does not assume any liability for damages, injuries, or adverse consequences ("damage") resulting from the incorrect or improper use of the product and you agree to indemnify Danfoss for any such damage resulting from your incorrect or improper use of the product.

Danfoss A/S
Climate Solutions • danfoss.com • +45 7488 2222