Step-by-step guide to update AK-SM800A software & Danux

This document provides guidance for updating AK-SM800A units, including upgrade procedures, key software changes, cybersecurity features, and recommended network configuration practices.

Terminology

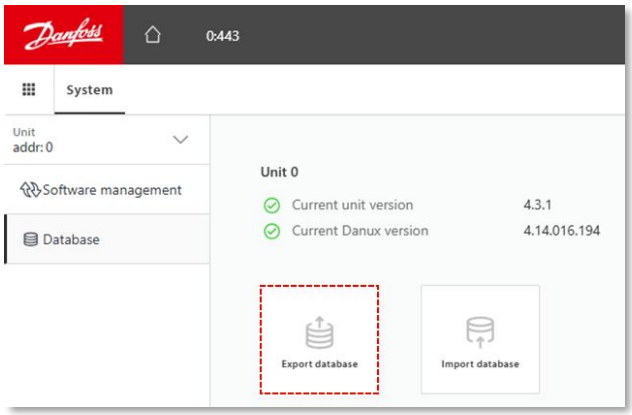


- **Software Package:** The software package contains the Danfoss application software and the EDF package. Updating the software package will install any missing EDF files and overwrite existing official EDFs. EDFs generated through X-Gate, Alsmart, or for MCX controllers are not affected. File extension: .spk
- **Danux:** Danux is the Linux-based operating system used by the AK-SM 800A. File extension: .lpk
- **Store View Web (SvW)** is the latest web-based user interface used to configure the AK-SM 800A and access system data.
- **Store View Browser 5 (SvB5)** is the legacy user interface used to configure the AK-SM 800A and access system data.

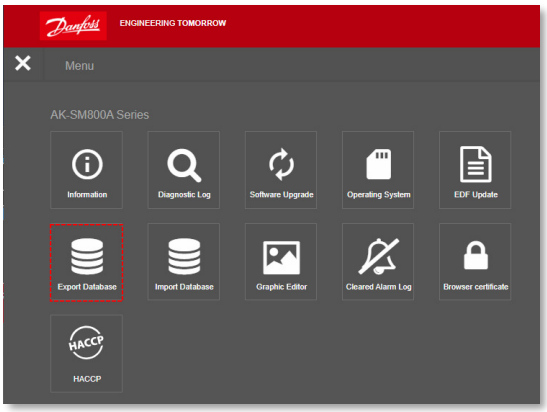
1. Prepare for the Update

The update process does not cause data loss. Nonetheless, it is recommended to download a backup of the unit (Export Database) before proceeding with the update. This procedure is also recommended to be done periodically.

SvW



SvB5



1.1 Pre-Upgrade Checklist

- Record the current Software Package and Danux versions.
- Export the database and any required reports.
- Verify user credentials. Software Package 5.4.0 and later enforce complex password requirements (Must read Section 4.3 before upgrade).
- Backup the history logs. They must be cleared before upgrading to 4.3.1, so export anything that needs to be retained first.
- Ensure on-site access is available in case remote connectivity is lost.
- Download all required .spk and .lpk files.

- Schedule a maintenance window and allow sufficient time for the upgrade.
- Identify any monitoring system connected to the unit (see Section 4.1).

2. Remote Update via SvW or SvB5

Important: Failure to follow the recommended step-by-step upgrade path may result in loss of remote connectivity (SvW and SvB5 access). If this occurs, an on-site update will be required.

Upgrade Rule

- Danux must be upgraded one supported version at a time.
- Software Package upgrades are limited by the installed Danux version.
- Within each upgrade stage, update Danux before the Software Package.

The following procedure illustrates the recommended remote upgrade path from Software Package 3.0.12 to 5.4.0.
If the unit is running a version earlier than 3.0.12, first install Software Package 3.0.12. No Danux update is required.
If the unit is already running Software Package 3.0.12 or later, begin at the next applicable upgrade step as highlighted below. Note for each step, update Danux first, then update the Software Package.

Step 1. Upgrade to Software Package 3.0.12 (*only if running an earlier version*)

- Install Software Package 3.0.12 (no Danux update required)

Step 2. Upgrade to Software Package 3.2.6

- Install Danux 4.14.011.193
- Install Software Package 3.2.6

Step 3. Upgrade to Software Package 4.0.14 ***("Important Notes" at Section 4.3 must be read to start migrating to complex passwords)***

- Install Danux 4.14.013.194
- Install Software Package 4.0.14

Step 4. Upgrade to Software Package 4.1.4

- Install Danux 4.14.014.194
- Install Software Package version 4.1.4

Step 5. Upgrade to Software Package 4.3.1 **(*"Important Notes"* at *Section 4.3 must be read before this step*)**

- Install Danux 4.14.016.194
- Install Software Package version 4.3.1

Step 6. Upgrade to Software Package 5.4 **(*"Important Notes"* at *Section 4.3 must be read before this step*)**

- Install Danux 4.14.017.194
- Install Software Package version 5.4.0

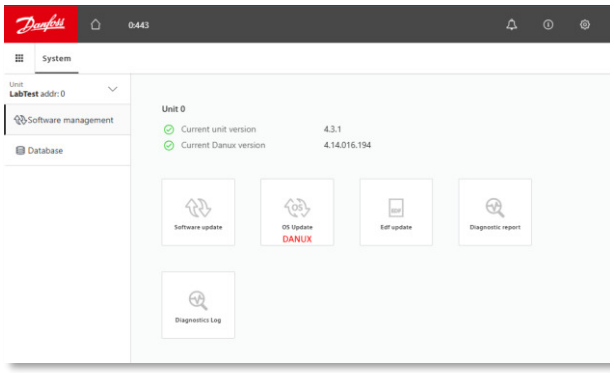
Expected Update Duration

- Danux: ~6 minutes per update; Software Package: ~3 minutes per update.
- Additional time may be required over VPN or slow internet connections.

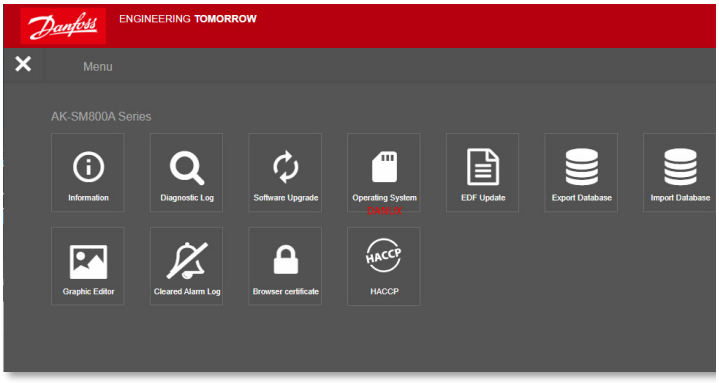
2.1 How to Install Danux and Software Package Updates via SvW and SvB5

Click the **Menu** icon ( ) in the upper-left corner and select either **Operating System** (Danux) or **Software Upgrade**, as shown below.

SvW



SvB5



3. On-Site Update

An on-site update allows the AK-SM800A to be upgraded locally, with the Danux operating system and Software Package installed through the web interface from a laptop on the local network or via Wi-Fi.

This method can also be used to recover access to SvW and SvB5 if connectivity is lost during a remote upgrade.

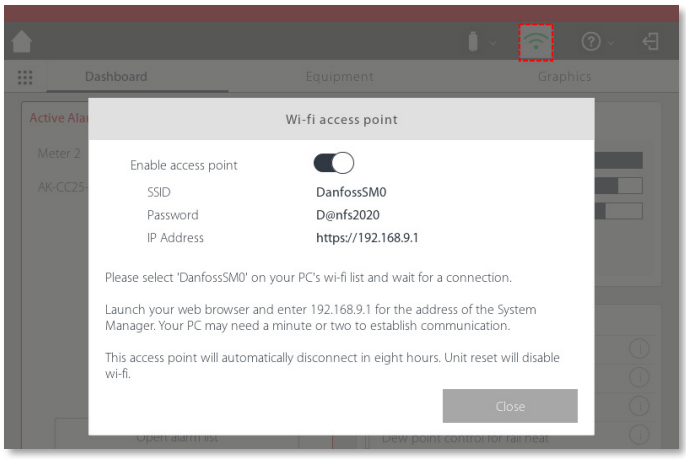
Before traveling to site, ensure the following:

- A laptop with Wi-Fi or access to the local network connected to the System Manager.
- Valid credentials for the System Manager.
- The required .lpk and .spk files downloaded in advance if internet access may not be available on-site.

3.1 Connect to the System Manager

Connect to the System Manager using either **SvW** or **SvB5**.

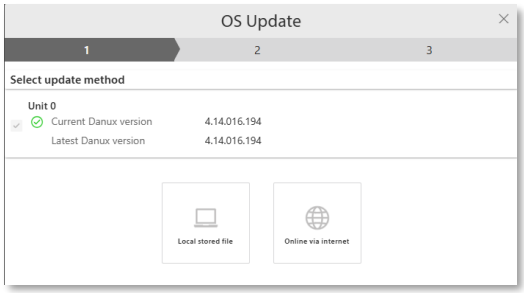
If network access is unavailable, enable the System Manager's built-in Wi-Fi hotspot and connect directly using a laptop, as shown below. (It is optional in case Ethernet ports are not available).



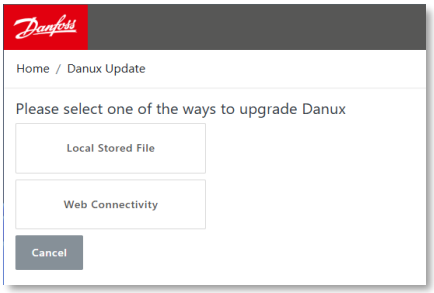
3.2 Update the Danux version

Use the "*Local stored file*" option and apply the Danux update via the web interface.

SvW



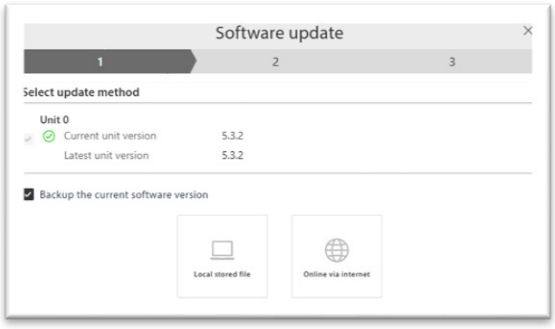
SvB5



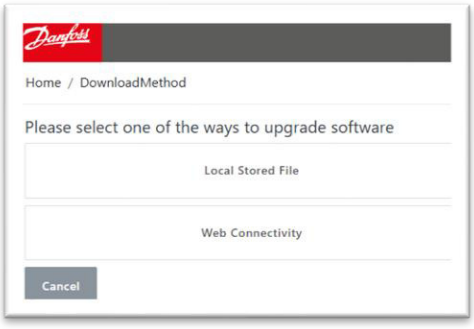
3.3 Update the Software Package

Use the "*Local stored file*" option and apply the respective Software Package update via the web interface.

SvW



SvB5



3.4 Verify Successful Upgrade

Once the System Manager has restarted, reconnect using SvW or SvB5 and verify:

- Access to the web interface
- Software Package and Danux version
- Normal system operation

Additional Information

4. Operational Impacts of Cybersecurity Enhancements

4.1 Software Package 4.3.1 - Strict Mode Enabled by Default

Beginning with **Software Package 4.3.1**, Strict Mode is enabled by default.
Strict Mode requires all communications to use **HTTPS** and replaces password-based authentication with temporary session tokens. This prevents user credentials from being transmitted across the network, improving overall system security.
Impact: Third-party XML integrations may stop functioning after the upgrade unless they are updated to support token-based authentication. User credentials are no longer accepted within XML payloads; instead, a valid session token must be provided in the **AKSM-auth** header. Moreover, once the communication port is changed to 443 by default, remote access can be affected.

4.2 Software Package 5.4.0 - Enhanced Password Policy

The **AK-SM 800A** enforces password complexity requirements beginning with **Software Package 5.4.0**.
Impact: Existing simple passwords are no longer supported and must be updated during or immediately after the upgrade.
Passwords must contain:

- A minimum of **8 characters**
- At least **one uppercase letter**
- At least **one number**
- At least **one special character**

Note: The following characters are not accepted for the passwords:
" & ' ( ) + , - . / : ; < = > ? [ ] \ ^ _ ` { } | ~ and spaces

As a security best practice, account and password expiration policies can also be configured to require users to periodically renew their credentials.

4.3. Important Notes during the upgrade procedures

Software Package 4.0.14 (Step 3)
After upgrading to 4.0.14: Enable complex password for users login via "*Configuration -> System -> Users*". Assign a complex password for each user before going through the next steps.

Software Package 4.3.1 (Step 5)
Before upgrading to 4.3.1: Back up the history logs, then clear them via "*Configuration > History > Clear History Logs*". Sufficient free memory is required for the 4.3.1 package to install, and the upgrade may fail if the history logs are not cleared first.

Software Package 5.4.0 (Step 6)
Before upgrading to 5.4.0: Ensure you have enabled complex password for users login via "*Configuration -> System -> Users*" and have assigned a complex password for each user before upgrading to R5.x to ensure a migration for the next step without any issue.
After upgrading to 5.4.0 After upgrading to Software Package 5.4.0 or later, leave the unit powered on for at least two hours. The system optimizes the history logs during this period, and the unit should not be powered off or restarted until the operation has completed.

5. Recommended Network Security Practices

The AK-SM800A should not be directly reachable from the public internet. This recommendation applies to all software versions, including those with **Strict Mode** enabled. While security features help protect the system, they do not eliminate the risks associated with internet exposure.

5.1 What Constitutes Internet Exposure

A system is considered internet-exposed if any of the following conditions apply:

- It has a public IP address, including a public IP assigned through a cellular SIM.
- Ports are forwarded from the site router or modem to the unit.
- The unit is configured as a DMZ host.
- UPnP is enabled, allowing ports to be opened automatically.
- A Dynamic DNS (DDNS) service points to the site.

Note: DDNS does not create internet exposure by itself, but it makes an exposed system easier to locate.

5.2 Recommended Network Configuration

To minimize cybersecurity risks:

- Place the unit behind a firewall that blocks inbound traffic by default.
- Provide remote access through a VPN only.
- Install the unit on a dedicated network segment, isolated from corporate, guest, and point-of-sale networks.
- Replace factory credentials and use individual user accounts instead of shared logins.
- Keep the Software Package up to date and maintain **Strict Mode** enabled.

5.3 Cellular Connectivity

Cellular connectivity is acceptable provided the unit remains inaccessible from the public internet.
Recommended practices:

- Use SIM plans that provide private or NATed IP addressing.
- Configure VPN tunnels initiated from the site network rather than allowing inbound connections.
- Disable port forwarding, DMZ configuration, and UPnP on the cellular router or modem.

5.4 Site Verification Checklist

Before leaving the site, verify that:

- The WAN address is not publicly routable.
- No port forwarding, DMZ, or UPnP rules are configured.
- Remote access is available only through a VPN.
- Factory default credentials have been changed.

Visit our Danfoss AK-SM800A product page here: [AK-SM 800A Series | Danfoss]