dormakaba

Community

Enhanced Key Security

PK3776 2.4.0-0 - 05/2025
Original document

EN

dormakaba Canada, Inc.
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M3
T: +1 514 735 5410

www.dormakaba.com

Table of contents

1 About this document

1.1 Validity

This document describes the product:

Product designation:	Community
Version:	Community 2.2.x and earlier to Community 2.4.x and later

1.2 Target audience

This document is for Community installation technicians, administrators, and site configurators who are enabling enhanced security mode.

1.3 Purpose and objective

The purpose of this document is to provide the requirements and step-by-step instructions for enabling and configuring enhanced security mode. This document also provides instructions for sites that chose not to enable enhanced key security.

1.4 Additional documents

Community User Guide PK3706

Community Installation Guide PK3695

Community Release Notes PK3696

Enhanced Key Security Reference Sheet (appended to end of this document)

2 Introduction

As a leader in the access control industry, dormakaba recognizes the continuously evolving nature of security technology. We strive to make ongoing improvements in our products, and we *strongly encourage* our customers to take advantage of the security features that our products offer.

dormakaba introduces enhanced key security for Community® Access Management Software. Now, in addition to the security features provided by the key manufacturer, an additional layer of advanced encryption technology is applied to data on RFID keys.

For new installations and upgrades, enhanced key security is disabled by default. Implementing enhanced key security requires manual configuration.

> For sites that need to delay enabling enhanced key security or sites that choose not to enable enhanced key security, action may still be required. For important details, see Without enhanced key security.

2.1 Requirements

Review and establish the following requirements before enabling enhanced key security:

> If all requirements are not met, contact dormakaba Customer Service.
> USA and Canada: 1-800-999-6213 / +1 514-340-9025, Email: lodgingsupport@dormakaba.com

- RFID keys—New, blank MIFARE DESFire EV2/EV3, MIFARE Ultralight C and/or MIFARE Plus keys are required.
- dormakaba RFID Encoder II—Encoders must be part 75720. Identify the part number on the underside of the encoder. At least one compliant encoder must be configured before enabling enhanced security mode. The firmware for all existing part 75720 encoders must be updated to meet minimum firmware requirements before enabling enhanced security mode. For details, refer to the *Community Release Note*s.

  > If using existing encoders that were shipped before September 2022, contact dormakaba Support to make sure that the applet firmware on the encoder is current.

- Lock firmware—All lock profiles support enhanced security mode; however, all locks must meet minimum firmware requirements. For details, refer to the *Community Release Note*s.
- Maintenance Units—Type M-Unit Saflok HH6 NFC is required and must meet the minimum firmware requirement. For details, refer to the *Community Release Note*s. Maintenance Unit authentication must also be enabled, and M-Unit login credentials must be configured.
- New activation key—Contact dormakaba Support to obtain a new activation key. The new key is 64 characters.
- Internet access—The Community server must have access to the internet to configure enhanced security mode.

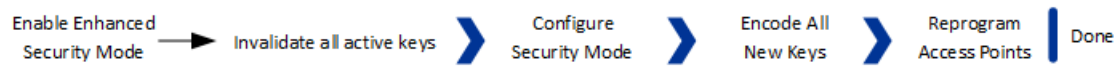
2.2 Limitations

The following known limitations apply to enhanced security mode:

- Toggle mode is not currently supported in locks when enhanced security mode is enabled.
- Locks and elevator controllers as listed in the release notes.

2.3 Process overview

Implementing enhanced key security starts with preparation. The following figure shows the recommended process.



The following sections provide an overview of each step in the process.

2.3.1 Establishing requirements

Establishing requirements involves acquiring and configuring the hardware that supports advanced encryption technology. As listed in the requirements section, only specific RFID key types are supported, all encoders must be part 75720, M-Unit Unit Saflok HH6 NFC is required, M-Unit authentication must be enabled, and M-Unit login must be configured. Finally, all devices must meet minimum firmware requirements as listed in the product release notes.

2.3.2 Enabling and configuring enhanced security mode

Enhanced Security Mode is the system setting that enables and configures enhanced key security. To minimize operational downtime, dormakaba recommends making all new keys before reprogramming locks.

After enhanced security mode is configured, Community generates a security password for the M-Unit. The password is required when reprogramming access points.

After enhanced security mode is configured, the default RFID key type is MIFARE DESFire EV2/EV3. To modify key types, go to *System Settings > Advanced Settings > RFID key types*.

2.3.3 Encoding all new keys

The first new keys to make are Failsafe keys. Updating the backup keys to units and suites prepares the site for emergencies.

After Failsafe keys are made, make all new resident, staff and vendor keys. The following limitations apply:

- BLE keys cannot be remade until after the locks are reprogrammed.
- Certain remote lock management features will not work between the time enhanced security mode is enabled and when the lock is reprogrammed.

2.3.4 Reprogramming access points

Access points are reprogrammed to accept enhanced security keys. The M-Unit security password is required to program the access points.

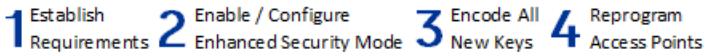
2.4 Getting started

Refer to the following chapter:

Enabling enhanced key security

3 Enable enhanced key security

The following figure shows the steps involved to enable enhanced key security.



3.1 Establish requirements

This section lists the requirements that must be met before enabling and configuring enhanced security mode.

3.1.1 Verify RFID key types

- Verify that the RFID key types used at the site to make resident, staff/vendor and system keys are MIFARE DESFire EV2/EV3, MIFARE Ultralight C and/or MIFARE Plus. If not, acquire the supported key types. When making a decision about which key types to use, factor the maximum number of variable access points that can be encoded:
  - MIFARE DESFire EV2/EV3—94 (recommended)
  - MIFARE Plus (4k)—542
  - MIFARE Plus (1k)—94
  - MIFARE Ultralight C—6 (Due to the lower number of variable access points supported for MIFARE Ultralight C keys, dormakaba does not recommend migration to MIFARE Ultralight C from other higher capacity key types.)

3.1.2 Verify RFID encoder part number

Enhanced security mode requires encoder part 75720. No other encoders are supported. At least one encoder must be configured before enabling security mode. The part number can be found on the underside of the encoder.

3.1.3 Update RFID encoder firmware

Firmware updates can be performed directly in Community for encoder type dormakaba RFID Encoder II.

Before performing the following steps, obtain the firmware file from dormakaba Support.

1. In Community, go to Device Management. (If online communication is enabled, click Encoders.)
2. Click Upload Reference Firmware.
3. Navigate to and select the firmware file (*.enc2), then click Open.

4. Click OK. The firmware version populates in the Reference firmware version field. When the reference version and current version do not match, a warning symbol ( ) displays adjacent to the Current firmware version field.
5. Select the encoder that requires a firmware update.
6. Click Update Firmware.
7. Click OK to acknowledge the update may take several minutes. Expect the LED indicators on the encoder to flash. When the update is complete, the encoder restarts.
8. After the restart, unplug then replug the encoder.

3.1.4 Verify lock firmware

Verify that each lock meets minimum firmware requirements for enhanced security mode. For details, refer to the *Community Release Notes* (PK3696).

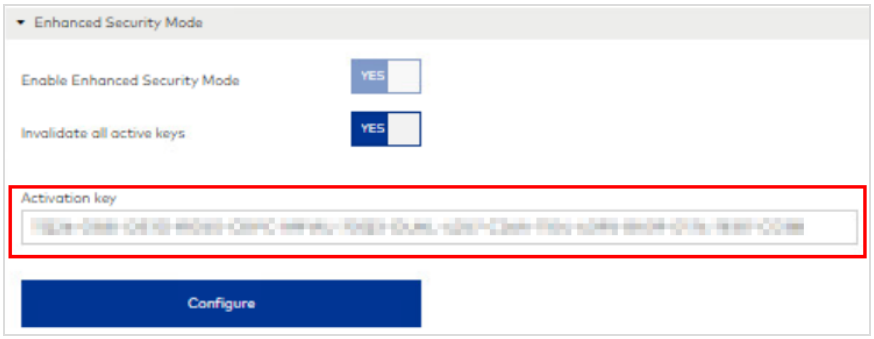
3.1.5 Enable M-Unit authentication and create M-Unit login credentials.

M-Unit Saflok HH6 NFC is required and must meet the minimum firmware version requirement. Moreover, M-Unit authentication is required to program locks. Authentication must be enabled at System Settings > Security > Maintenance Unit. Login credentials are configured for an operator at Staff/Vendor Management > Operator Info> Maintenance Unit Login.

3.1.6 Obtain activation key

The process of configuring enhanced security mode requires a new activation key. dormakaba Support provides the 64-character key upon request.

The key is required to configure enhanced security mode.



After enhanced security mode is configured, the new activation key replaces the previous activation key.

3.1.7 Verify internet access

The Community server must have access to the internet before enabling enhanced security mode.

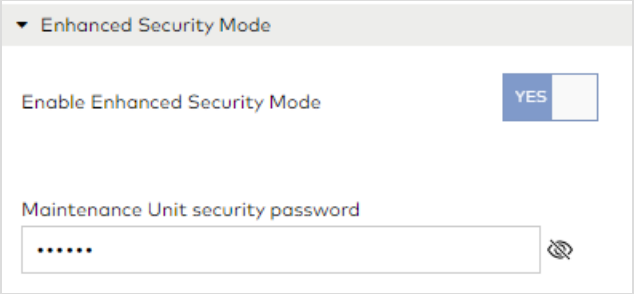
3.2 Enable / configure enhanced security mode

Enhanced security mode cannot be disabled after clicking *Configure* in step 4.

Perform the following steps:

1. Go to *System Settings > Security > Enhanced Security Mode*. and change the Enhanced Security Mode switch to YES. Click YES to proceed.
2. For Invalidate all active keys, select YES.
3. Specify the 64-character activation key provided by dormakaba Support.
4. Click Configure, then click YES to proceed.

   ⇨ Community configures the site. The Maintenance Unit Security Password setting appears. Click to view the password. The password is required when using the M-Unit to program access points. If the password setting does not display, verify that a compliant encoder is configured.



After enhanced security mode is configured, the default RFID key type is MIFARE DESFire EV2/EV3. To deselect either key type, go to *System Settings > Advanced Settings > RFID key types*.

3.3 Encode all new keys

Make keys before reprogramming locks.

3.3.1 Encode Failsafe keys

Failsafe Keys are backups of individual unit keys that are made in advance and maintained in complete sets to be issued in the event of a system or power failure. The recommendation is to create three sets of two keys for each unit and suite door. Using a Failsafe Key invalidates previous resident key access to units, suite common doors and suite units.

To make Failsafe keys:

1. Go to *System Settings > Failsafe Keys*.
2. Specify the default number of Failsafe Keys to create for each access point. Default: 3.
3. Specify the number of days Failsafe Keys remain valid. After first use, the Failsafe Keys expire after the specified number of days. Default: 1.
4. Select the time after which Failsafe Keys are invalid on the final day of the stay. Default: 11am.
5. Click (Save) .

3.3.2 Encode resident, staff, and vendor keys

Make all new keys for active residents, staff, and vendors.

BLE keys cannot be remade until after the locks are reprogrammed.

Certain remote lock management features will not work between the time enhanced security mode is enabled and when the lock is reprogrammed.

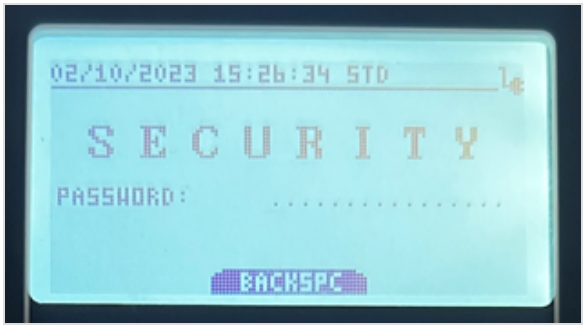
3.4 Reprogram access points

Reprogram access points to accept only enhanced security keys.

1. Go to Programming & Auditing > Programming.
2. Select all access points that require synchronization. Select the access points that you want to synchronize with Community configuration data. You can select access points from different buildings and filter the list to show only access points that require synchronization. The selected access points display in the Summary section organized by building and floor.
3. For Lock out current resident on programming, select NO.
4. Connect the M-Unit to the workstation.
5. In Community, click Transfer. Messages on the workstation and M-Unit display that the transfer is in progress. Wait

until the message on the workstation indicates transfer is complete and that you can unplug the M-Unit. Click OK

6. Disconnect the M-Unit from the workstation. The remaining steps are on the M-Unit.



7. Specify the security password. (In some cases, the M-Unit displays a message prior to the password prompt indicating that the unit is not personalized; simply select OK.)
8. Specify the M-Unit login credentials.
9. On the M-Unit menu, select LOCKS.
10. Use the UP / DOWN arrow keys to highlight 1- Program, then press ENTER. The access point names display in groups of five.
11. Select the access point name for the lock, then press ENTER. Use the PREV, NEXT and SEARCH options to navigate and refine the list of names.
12. Select the type of probe that you are using to connect the M-Unit to the lock.
13. When prompted, insert the probe into the lock. Programming starts immediately. If the lock has already been programmed, the M-Unit issues a message requesting confirmation to overwrite the existing programming.
14. When prompted that programming is complete, click OK.
    ⇨ Locks accept only enhanced security keys.

3.5 Make BLE keys

Make all new BLE keys for active residents, staff, and vendors.

3.6 Process complete

All steps for enabling enhanced key security are complete. Proceed to make new keys.

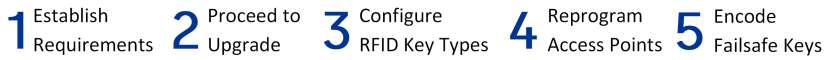
When remote lock management (online communication) is enabled, dormakaba recommends to test online operations.

4 Without enhanced key security

dormakaba strongly recommends taking advantage of the enhanced key security feature introduced with Community 2.4. However, for sites that choose not to enable enhanced security, the following options are available:

- Standard Key Security is recommended for sites that do not enable enhanced security mode. In Community, standard key security is implemented by using the MIFARE DESFire EV2/EV3 (recommended) and/or MIFARE Ultralight C key types exclusively. The security features provided by the manufacturer offer greater security than the legacy option.
- Legacy Key Security is an acceptable temporary choice. In Community, legacy key security is implemented by using the MIFARE Plus and/or MIFARE Classic key types exclusively. Do not use Legacy key security indefinitely.
- Sites that require maximum flexibility may use both standard and legacy RFID key type security.

For sites that choose to upgrade the RFID key type for increased security, use the following process:



4.1 Establish requirements

This section applies to sites that plan to upgrade the RFID key type for increased security.

4.1.1 RFID key types

- Acquire the keys for the RFID key types to be configured after upgrade.

The key types selected in System Settings determine the type of keys that locks accept. For example, when MIFARE Ultralight C is the only selected key type in System Settings, locks are programmed to accept only MIFARE Ultralight C keys. The exception is when MIFARE Classic is selected in System Settings. Due to the legacy security level of MIFARE Classic, locks are programmed to accept all supported key types.

The following table lists RFID key type options in Community2.4.

Enhanced Key Security	Standard Key Security	Legacy Key Security
MIFARE DESFire EV2/EV3	MIFARE DESFire EV2/EV3 (recommended, available after fresh install/upgrade)	MIFARE Plus
MIFARE Plus	MIFARE Ultralight C	MIFARE Classic (available after upgrade if previously selected before upgrade; not available for fresh installs)
MIFARE Ultralight C		

When making a decision about which key types to use, factor the maximum number of variable access points that can be encoded:

- MIFARE DESFire EV2/EV3—94 (recommended)
- MIFARE Plus (4k)—542
- MIFARE Plus (1k)—94
- MIFARE Ultralight C—6, Due to the lower number of variable access points supported for MIFARE Ultralight C keys, dormakaba does not recommend migration to MIFARE Ultralight C from other higher capacity key types.

4.1.2 (conditional) Verify RFID encoder part number

- If using the DESFire EV2/EV3 key type, verify or acquire the dormakaba RFID encoder II (part 75720).

The DESFire EV2/EV3 RFID key type requires encoder part 75720. No other encoders are supported for this key type. The part number can be found on the underside of the encoder.

4.1.3 (conditional) Update RFID encoder firmware

- If using the DESFire EV2/EV3 key type, acquire the firmware update file for the required encoder (part 75720), then update the encoder firmware.

The encoder (part 75720) requires a firmware update before encoding DESFire EV2/EV3 keys. Firmware updates can be performed directly in Community for encoder type dormakaba RFID Encoder II.

Before performing the following steps, obtain the firmware file from dormakaba Support.

1. In Community, go to Device Management. (If online communication is enabled, click Encoders.)
2. Click Upload Reference Firmware.
3. Navigate to and select the firmware file (*.enc2), then click Open.
4. Click OK. The firmware version populates in the Reference firmware version field. When the reference version and current version do not match, a warning symbol ( ) displays adjacent to the Current firmware version field.
5. Select the encoder that requires a firmware update.
6. Click Update Firmware.
7. Click OK to acknowledge the update may take several minutes. Expect the LED indicators on the encoder to flash. When the update is complete, the encoder restarts.
8. After the restart, unplug then replug the encoder.

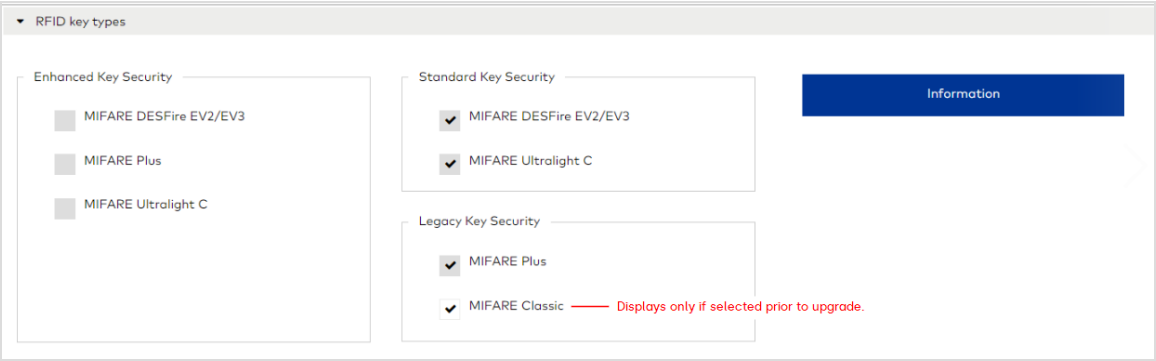
4.2 Upgrade software

Proceed to upgrade to Community 2.4. dormakaba recommends to read the product release notes before upgrading.

4.3 Configure RFID key types

Configure RFID key type settings.

1. Go to *System Settings > Advanced Settings > RFID key types*.



2. Select the desired RFID key type.
3. Click (Save) .

The MIFARE DESFire EV2/EV3 key type cannot be deselected.

4.4 Reprogram access points

Reprogram access points to accept only those key types selected.

1. Go to Programming & Auditing > Programming.
2. Select all access points that require synchronization. Select the access points that you want to synchronize with Community configuration data. You can select access points from different buildings and filter the list to show only access points that require synchronization. The selected access points display in the Summary section organized by building and floor.
3. For Lock out current resident on programming, select NO.
4. Connect the M-Unit to the workstation.
5. In Community, click Transfer. Messages on the workstation and M-Unit display that the transfer is in progress. Wait until the message on the workstation indicates transfer is complete and that you can unplug the M-Unit. Click OK.
6. Disconnect the M-Unit from the workstation. The remaining steps are on the M-Unit.
7. If M-Unit authentication is enabled, specify the M-Unit login credentials.
8. On the M-Unit menu, select LOCKS.
9. Use the UP / DOWN arrow keys to highlight 1- Program, then press ENTER. The access point names display in groups of five.
10. Select the access point name for the lock, then press ENTER. Use the PREV, NEXT and SEARCH options to navigate and refine the list of names.
11. Select the type of probe that you are using to connect the M-Unit to the lock.
12. When prompted, insert the probe into the lock. Programming starts immediately. If the lock has already been programmed, the M-Unit issues a message requesting confirmation to overwrite the existing programming.
13. When prompted that programming is complete, click OK.
    ⇨ Locks accept only the selected key types.

4.5 Encode Failsafe keys

This section is a prerequisite for sites that use MIFARE Classic keys and sites that want to upgrade the key type from MIFARE Plus to MIFARE DESFire EV2/EV3 and/or MIFARE Ultralight C.

Failsafe Keys are backups of individual unit keys that are made in advance and maintained in complete sets to be issued in the event of a system or power failure. The recommendation is to create three sets of two keys for each unit and suite door. Using a Failsafe Key invalidates previous resident key access to units, suite common doors and suite units.

To make Failsafe keys:

1. Go to *System Settings > Failsafe Keys*.
2. Specify the default number of Failsafe Keys to create for each access point. Default: 3.
3. Specify the number of days Failsafe Keys remain valid. After first use, the Failsafe Keys expire after the specified number of days. Default: 1.
4. Select the time after which Failsafe Keys are invalid on the final day of the stay. Default: 11am.
5. Click (Save).

5 Change summary

This chapter lists changes related to enabling enhanced key security.

5.1 RFID keys

- MIFARE Classic keys are not supported with fresh installs or when enhanced key security is enabled.
- Keys encoded before enabling enhanced key security cannot be reused.
- The default RFID key type after enhanced security mode is enabled is MIFARE DESFire EV2/EV3 (Enhanced Key Security).
- After enabling enhanced security mode, high-security keys are site-specific. Keys encoded at one site cannot be read or reused at a different site.
- Keys encoded after enabling enhanced key security cannot be erased; however, they can be reused at the same property to encode a different credential.

5.2 Encoders

- Encoders must be part 75720 for enhanced key security.
- At least one encoder (75720) must be configured before enabling enhanced security mode. After enhanced security mode is configured, Community automatically reconfigures all compliant encoders to work in security mode. The encoder type changes to dormakaba RFID Encoder II.
- The firmware for existing 75720 encoders must be updated before enabling enhanced security mode.

5.3 Maintenance Units

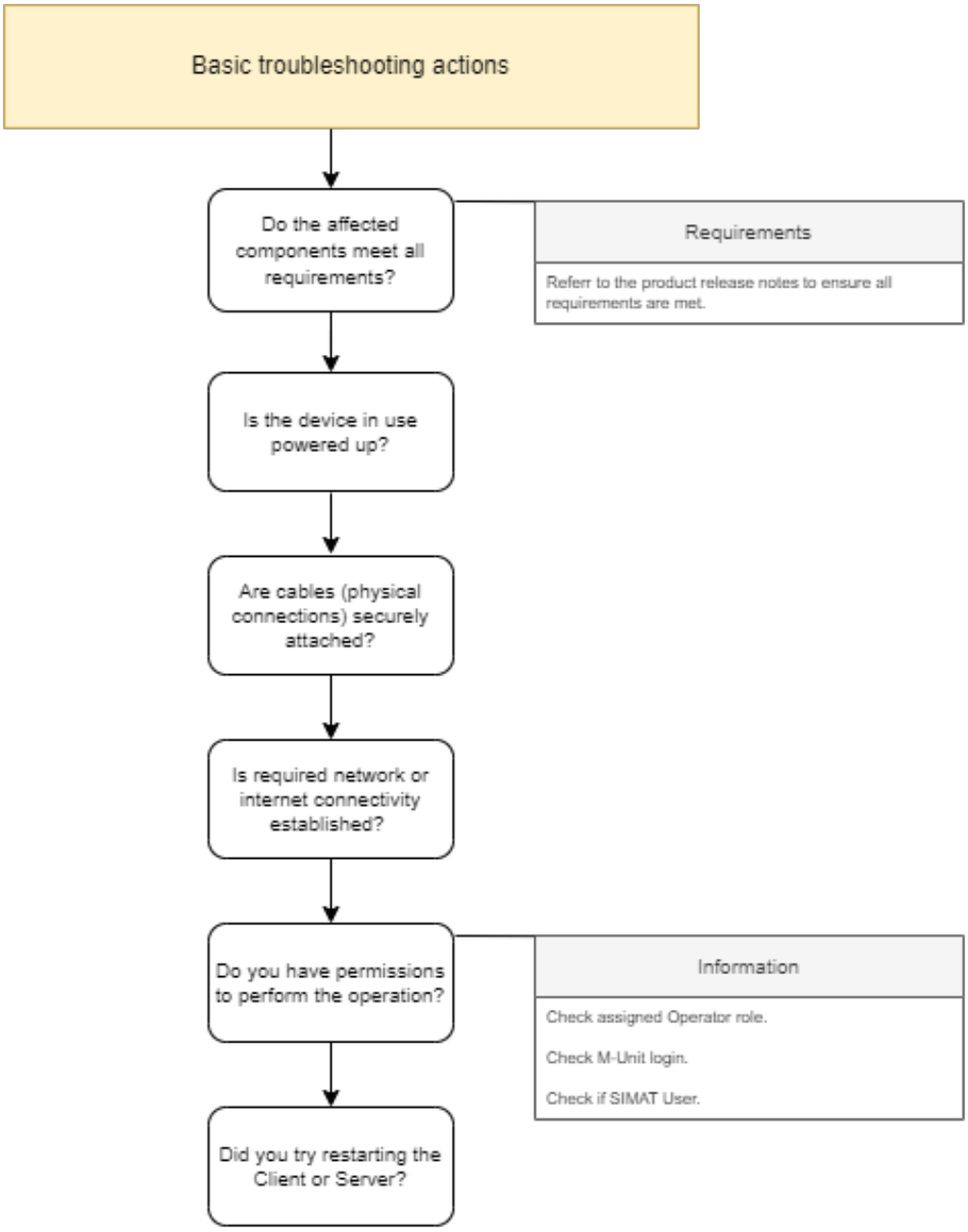
- M-Unit Saflok HH6 NFC is required for enhanced key security.
- The M-Unit security password is required to program access points. The password displays at *System Settings > Security > Enhanced Key Security*.
- When Enhanced Security Mode is enabled, the M-Unit is site-specific. Using the M-Unit at a different site requires a factory reset.

6 Troubleshooting

This chapter provides basic troubleshooting topics for enhanced key security.

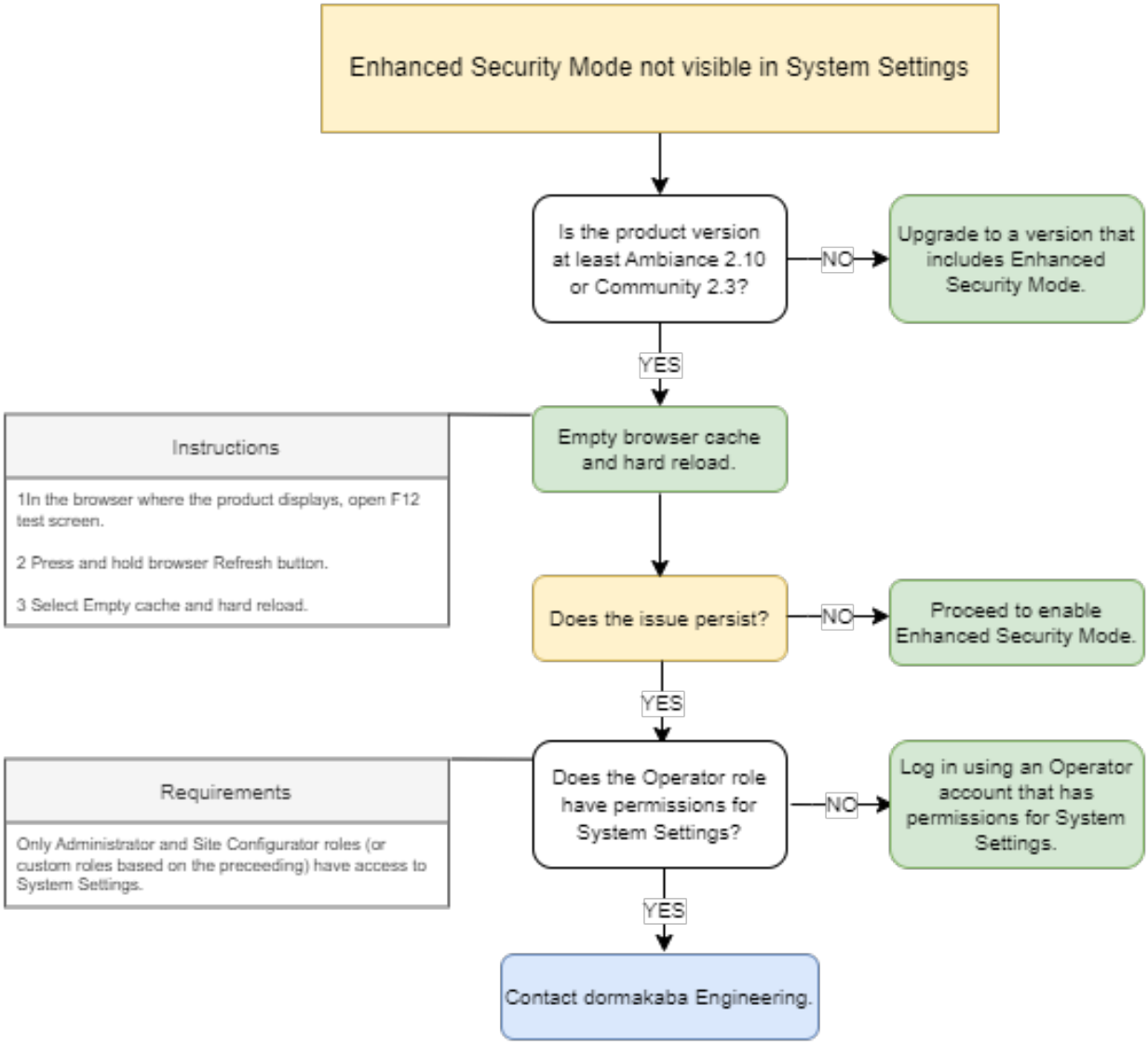
6.1 Basic troubleshooting actions

Start troubleshooting an issue with basic actions.



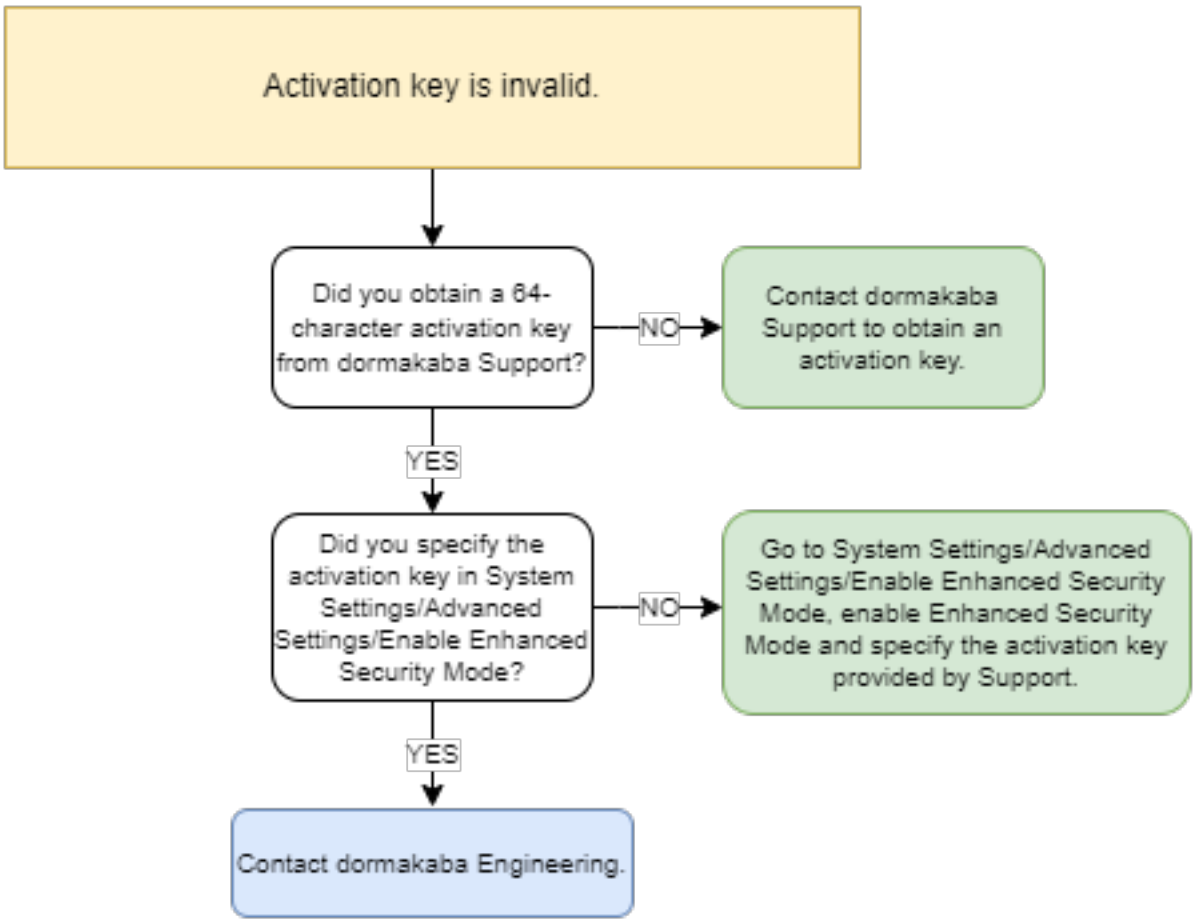
6.2 Enhanced Security Mode not visible in System Settings

Use the following workflow to troubleshoot the issue.



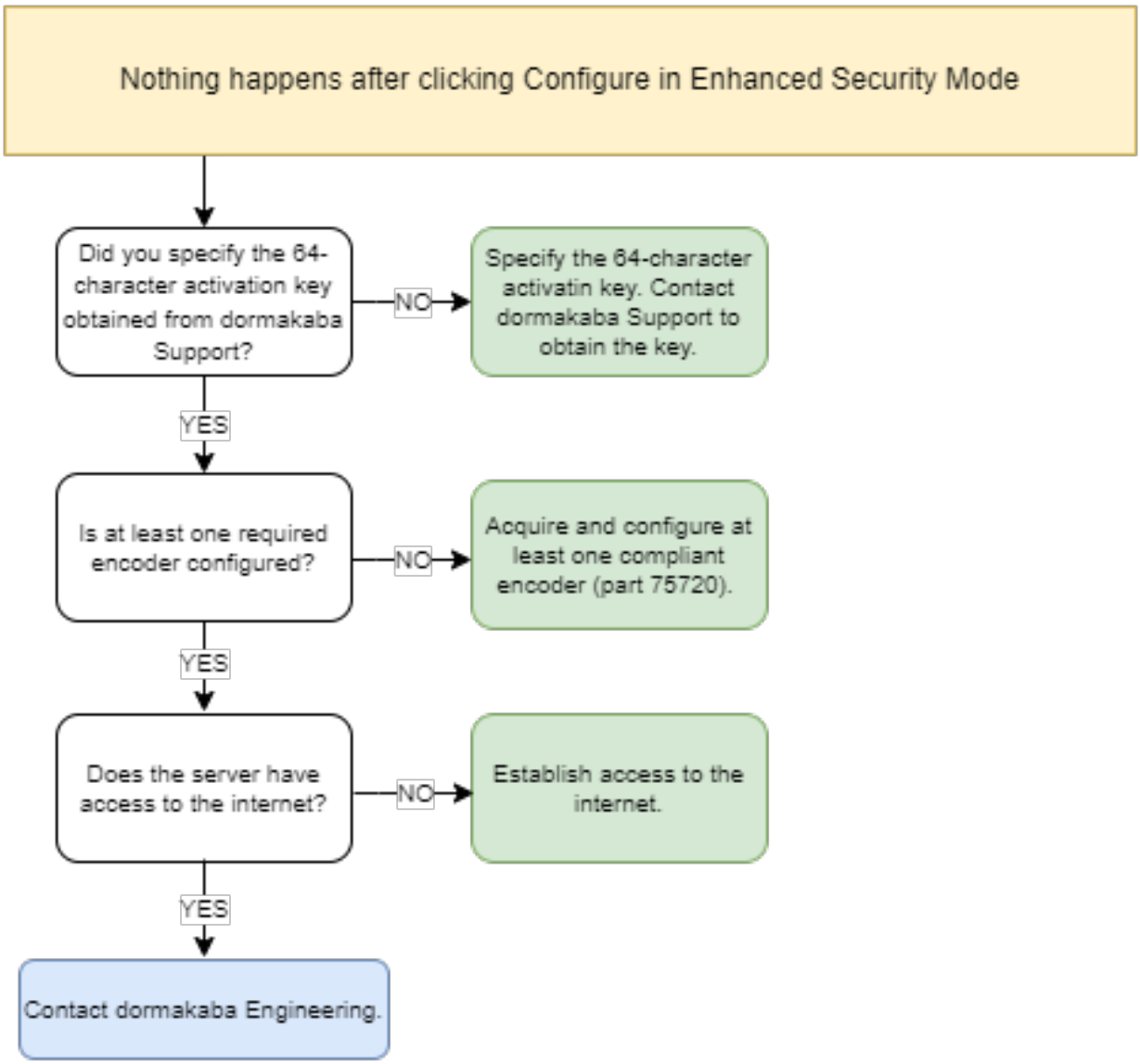
6.3 Activation key is invalid

Use the following workflow to troubleshoot the issue.



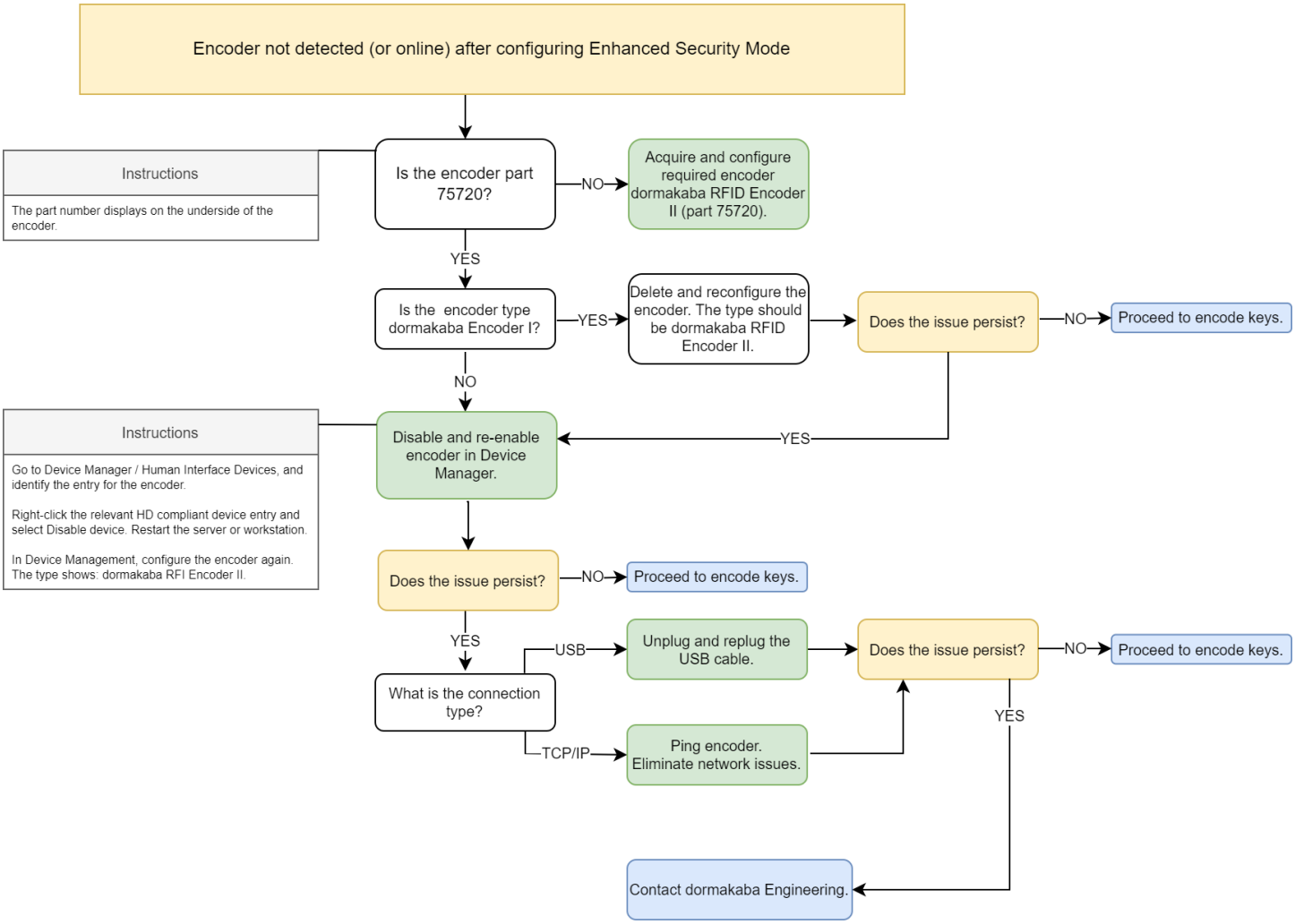
6.4 Nothing happens when clicking Configure in Enhanced Security Mode

Use the following workflow to troubleshoot the issue.



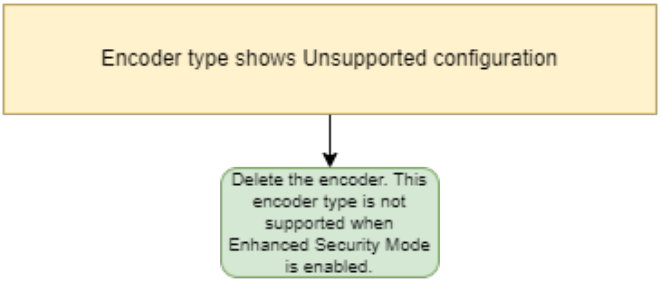
6.5 Encoder not detected/online after configuring Enhanced Security Mode

Use the following workflow to troubleshoot the issue.



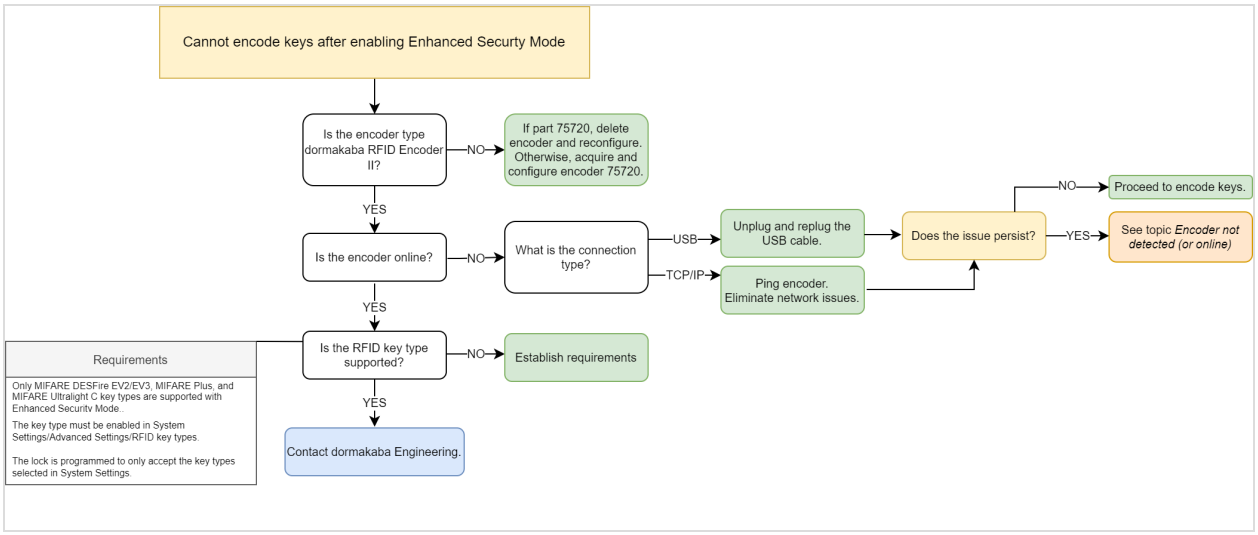
6.6 Encoder type shows Unsupported configuration

Use the following workflow to troubleshoot the issue.



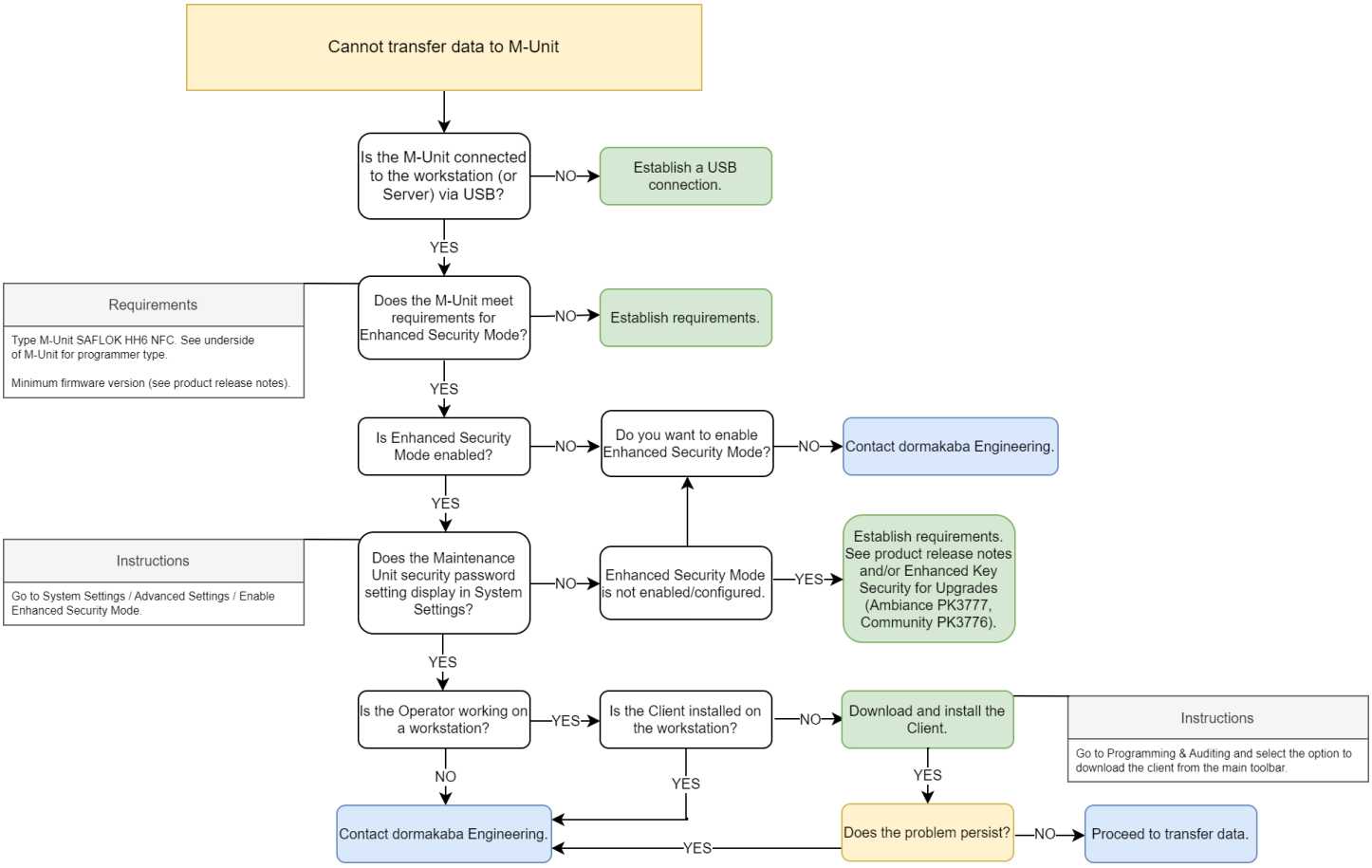
6.7 Cannot encode keys after enabling Enhanced Security Mode

Use the following workflow to troubleshoot the issue.



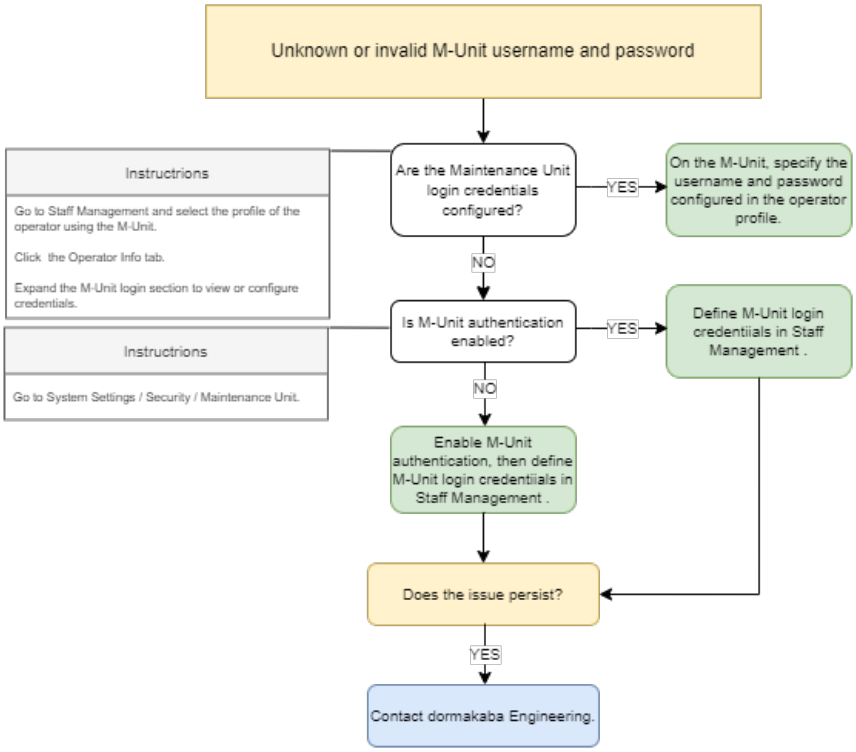
6.8 Cannot transfer data to M-Unit

Use the following workflow to troubleshoot the issue.



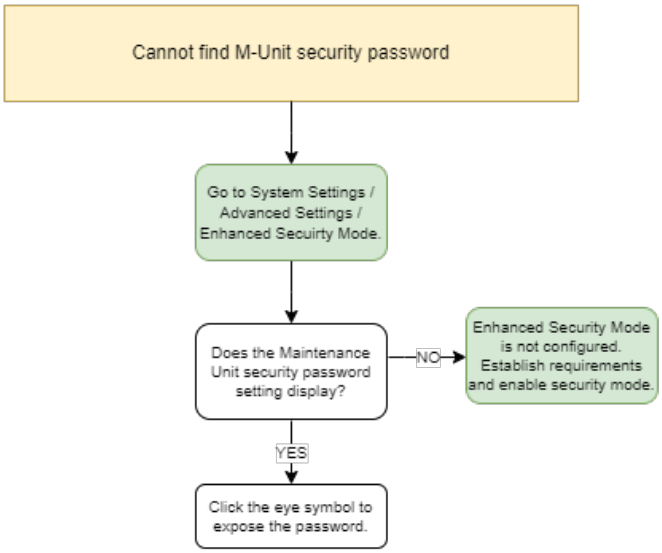
6.9 Unknown or invalid M-Unit username/password

Use the following workflow to troubleshoot the issue.



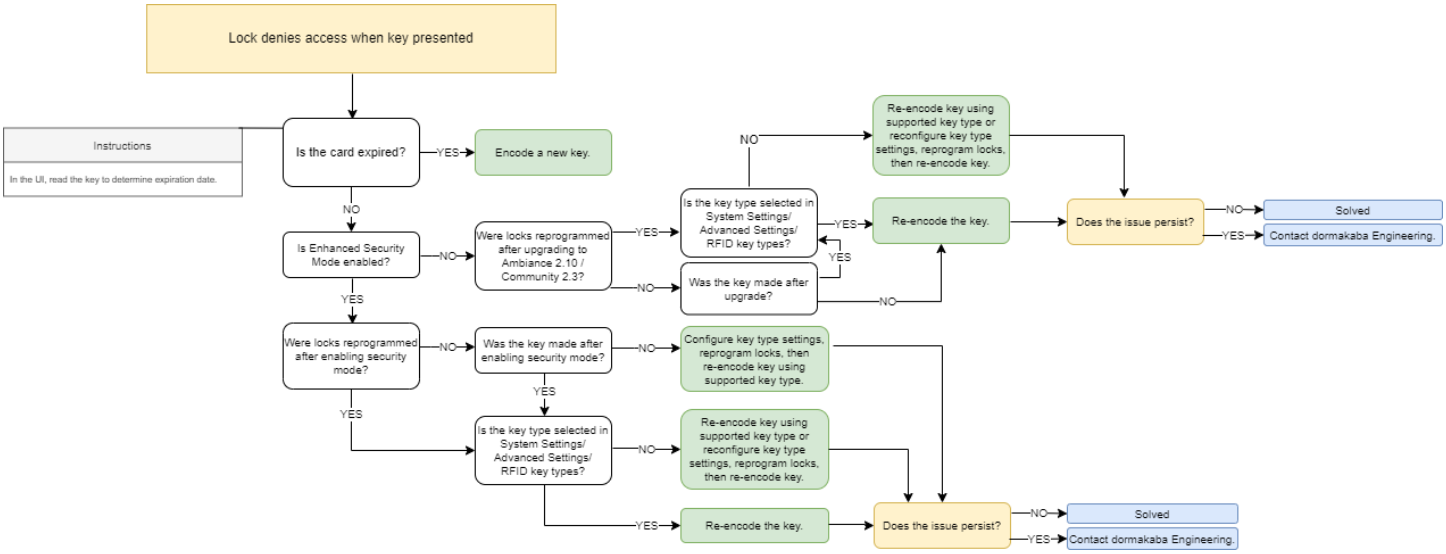
6.10 Cannot find M-Unit security password

Use the following workflow to troubleshoot the issue.



6.11 Lock denies access when key presented

Use the following workflow to troubleshoot the issue.



PK3776-EN 2.4.0-0 - 05/2025

www.dormakaba.com

dormakaba Canada
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M3
Canada
T: +1 877 468-3555

www.dormakaba.com

Enhanced Key Security Reference Sheet

Welcome

dormakaba® introduces enhanced key security for Community® Access Management Software. Now, in addition to the security features provided by the key manufacturer, an additional layer of advanced encryption technology is applied to data on RFID keys. For new installations and upgrades, enhanced key security is disabled by default. Implementing enhanced key security requires manual configuration.

IMPORTANT: Enhanced security mode cannot be disabled once configured.

Requirements

RFID keys. New, blank MIFARE DESFire® EV2/EV3, MIFARE Ultralight C® and/or MIFARE Plus® keys are required.

Encoders. 1) Encoders must be dormakaba RFID Encoder II (part 75720). Identify the part number on the underside of the encoder. 2) At least one compliant encoder must be configured before enabling enhanced security mode. 3) The firmware on all existing 75720 encoders must be updated before enabling enhanced security mode. (If using existing encoders that were shipped before September 2022, contact dormakaba Support to make sure that the applet firmware on the encoder is current.)

Lock firmware. All lock profiles support enhanced security mode; however, all locks must meet minimum firmware requirements.
For details, refer to the *Community Release Notes* (PK3696).

Maintenance Units. M-Unit Saflok HH6 NFC is required. M-Unit authentication must be enabled, and M-Unit login must be configured.

New activation key. Contact dormakaba Support to obtain a new activation key. The new key is 64 characters.

Internet access. The server must have access to the internet to configure enhanced security mode.

Process

1. Establish requirements.
2. Go to System Settings > Security > Enhanced Security Mode.
   a. Change the Enhanced Security Mode switch to YES.
   b. For Invalidate Active Keys, click YES.
   c. Specify the 64-character activation key.
   d. Click Configure. M-Unit security password is generated.
3. Go to System Keys and encode Failsafe keys.
4. Go to Staff/Vendor Management and make all new RFID keys for active staff and vendors.
5. Go to Resident Management and make all new RFID keys for active residents.
6. Reprogram access points. Use the M-Unit security password. After reprogramming, locks accept high-security keys.
7. Go to Staff/Vendor Management and Resident Management and make all new BLE keys for active staff, vendors, and residents, respectively.

Ready to resume regular business operations with high-security keys for residents and staff/vendors

Change Summary

RFID Keys

- MIFARE Classic keys are not supported with fresh installations or enhanced security mode.
- Keys encoded before enabling enhanced security mode cannot be reused.
- The default RFID key type after enhanced security mode is enabled is MIFARE DESFire EV2/EV3.
- After enabling enhanced security mode, high-security keys are site-specific. Keys encoded at one site cannot be read or reused at a different site.
- Keys encoded after enabling enhanced key security cannot be erased; however, they can be reused at the same property to encode a different credential.

Encoders

- Encoders must be part 75720. At least one encoder (75720) must be configured before enabling enhanced security mode.
- The firmware on all existing 75720 encoders must be updated before enabling enhanced security mode.

Maintenance Units

- M-Unit Saflok HH6 NFC is required with minimum firmware version.
- The M-Unit security password is required to program access points. The password displays at System Settings > Security > Enhanced Security Mode.