HID® Linq™ Key Manager

User Guide

PLT-08195, Rev. A.0
December 2025

Copyright

Trademarks

Contacts

For technical support, please visit: **https://support.hidglobal.com**.

What's new

Date	Description	Revision
December 2025	Initial release.	A.0

A complete list of revisions is available in **Revision history**.

Section 01

Introduction

1.1 Document purpose

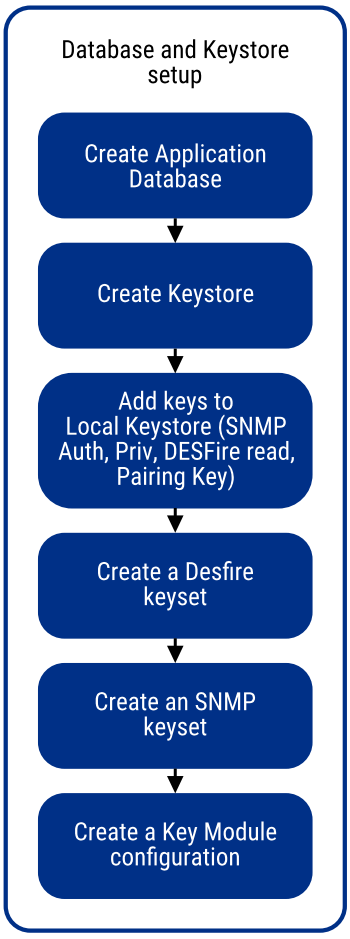
This document provides information on how to install and use HID® Linq™ Key Manager to manage custom keys stored in a local keystore, for use with the HID M1 Key Module.

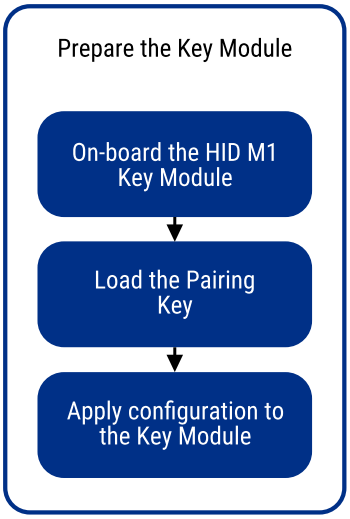
1.2 Intended audience

This document is intended for System Administrators and Device Administrators to install, configure and manage custom credential keysets with the HID Linq Key Manager command-line tool for Windows 11.

1.3 Overview

HID Linq Key Manager allows you to setup and manage databases and keystores and prepare your Key Module for use with the HID M1 system. A Key Module Pairing Key can be loaded to cryptographically bind the Key Module and Main Node.





1.4 System requirements

- Windows 11 64-bit Enterprise Edition 21H22 or newer
- 8 GB RAM
- 20 GB available disk space
- USB port (type A or type C)
- USB cable with a male USB-C connector for Key Module connection.

1.5 Understanding Command Syntax

HID Linq Key Manager commands are structured to specify the main program, the primary action (command), a secondary action (sub-command), and then options/parameters.

General Command Structure

```
LinqKeyManager.exe <command> [sub-command] [options]
```

- **LinqKeyManager.exe** - the executable filename.
- **<command>** - the main category of action to be performed (for example, `keystore`). Replace `<command>` with a command from the **Command reference**.
- **[sub-command]** - a specific action related to the main command (for example, `create-local` for the keystore command). Sub-commands are optional.
- **[options]** - this modifies the command behavior.
  - Options are typically prefixed with `--` for full names or `-` for short names (for example, `-- name` or `-n`).
  - Options values follow the option name (for example, `--name MyKeystore`).

1.5.1 Syntax placeholders

The syntax placeholders in angled brackets (for example, **<your_keystore_name>**, **<password>**, **<file_path>**) throughout the document represent the data that you must provide. Replace the brackets and placeholder in the syntax string. For example:

`LinqKeyManager.exe keystore create-local --name` **<your_keystore_name>** `--password` **<your_password>**

Becomes:

`LinqKeyManager.exe keystore create-local --name` **MyDeviceKeys** `--password` **Secure123!**

1.6 Syntax conventions

1.6.1 Quoting paths

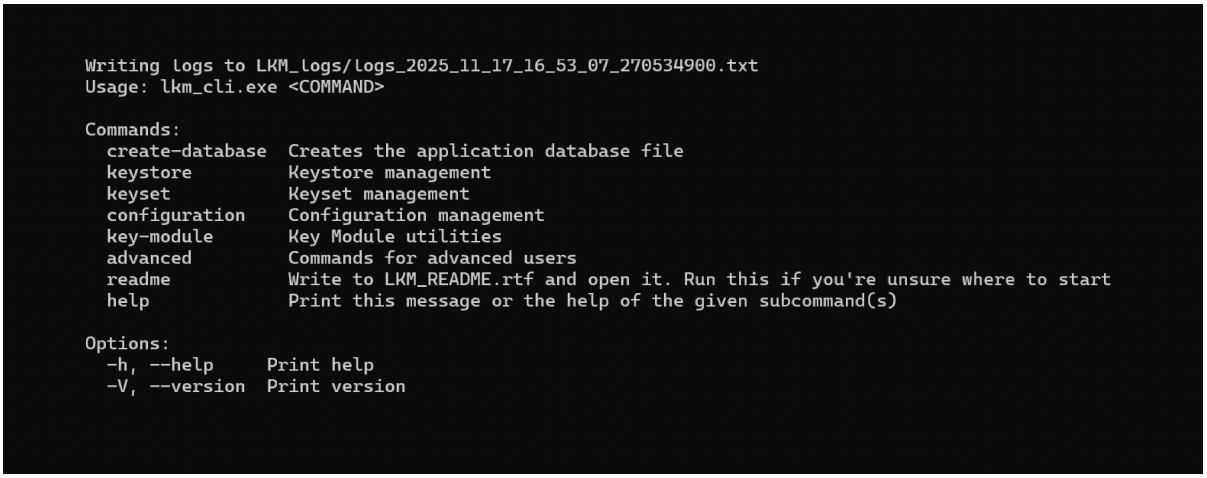
Enclose file paths or names with spaces in quotation marks. For example:

- **"C:\My Tools\LinqKeyManager"**
- `LinqKeyManager.exe configuration create --name "My DESFire Config"`

> **Note:** It is recommended to use an underscore (_) instead of a space. This avoids the need to enclose file paths in quotation marks.

1.6.2 Execute a command

1. Open the Command Prompt window.
2. Type `LinqKeyManager.exe` followed by the required command, sub command, and options if applicable.
3. Press **Enter**.



1.6.3 Command history

Press the **Up** and **Down** arrows on your keyboard to cycle through previously entered commands and press **Enter** to execute the required command.

1.6.4 Interactive mode (-i)

HID Linq Key Manager gives guidance and provides input for the required prompts when the **-i** command is used at the end of a string. This is helpful for complex commands or if you are unsure of the required parameters.

Section 02

Download and install HID Linq Key Manager

2.1 Download and install HID Linq Key Manager

1. Download **LinqKeyManager.exe** from the **HID Developer Portal**.
2. Create a new folder on your computer specifically for this tool.

   > **Note:** Avoid using spaces in the folder path to simplify command-line navigation. For example, **C:\Users\YourUserName\Desktop\LinqKeyManager**

3. Move the downloaded **LinqKeyManager.exe** file to the new folder.

2.2 Update HID Linq Key Manager

New versions of HID Linq Key Manager are uploaded to the **HID Developer Portal**.

1. Download the newest **LinqKeyManager.exe** file.
2. Replace the old version in the **C:\Users\YourUserName\Desktop\LinqKeyManager** folder.

   > **Note:** Always check the new version release notes for specific update instructions or database compatibility information.

Section 03

Create Main Node Pairing Key file

3.1 Main Node Pairing Key

The Main Node Pairing Key is a symmetric cryptographic key that securely binds the Key Module to a specified Main Node at a hardware-level. This ensures that the Key Module cannot be re-used with another Main Node outside of your organizations control.

To establish a secure pairing between the Key Module and the Main Node:

1. Save the Pairing Key in a **.bin** file in hexadecimal format.
2. Use HID Linq Key Manager to inject the Pairing Key into the Key Module
3. Load the same key **.bin** into the Main Node through its Admin User Interface during the system configuration.
4. Perform the pairing in a secure environment.

> **Note:** Once paired, the devices establish a secure communication channel using Pairing Key derived session keys.

3.2 Create Main Node Pairing Key file

To create a Pairing Key file:

1. Open PowerShell.
2. Copy and paste the following command: `$hex="A1B2C3D4E5F6A7B8C9D0E1F2A3B4C5D6"; [IO.File]::WriteAllBytes("$env:USERPROFILE\Desktop\MainNodePairing.key",($hex -split '(..)'|?{$_}|%{[Convert]::ToByte($_,16)}))`
3. Replace `A1B2C3D4E5F6A7B8C9D0E1F2A3B4C5D6` with your 32-character hex key.
4. Press **Enter**.

> **Note:** Save the file to your desktop for use in **4.2 Onboard the HID M1 Key Module**.

Section 04

Command line actions

4.1 Managing MIFARE DESFire keys and Key Modules

This section covers the typical end-to-end process for creating custom MIFARE DESFire keysets and injecting them into an HID M1 Key Module.

4.1.1 Launch the command line interface

HID Linq Key Manager is a command-line tool that runs through the Windows Command Prompt.

> **Note:** It is not recommended to only double-click the **LinqKeyManager.exe** file in File Explorer. The tool will open but you cannot enter commands.

1. Open the Command Prompt.

   > **Note:** Alternatively, press the **Windows** key + **R** simultaneously to open the **Run** dialog. Type **cmd** and click **OK** to open the Command Prompt.

2. Navigate to the required HID Linq Key Manager Directory using the `cd` command and the **LinqKeyManager.exe** file location.

   > **Note:** For example, `cd C:\Users\YourUserName\Desktop\LinqKeyManager`

3. Type **LinqKeyManager.exe** and press **Enter** to launch HID Linq Key Manager.

4.1.2 Create the application database

The database file stores all keystores, keys, keysets, and Key Module configurations.

> **Note:** This is a one-time operation when setting up HID Linq Key Manager in a new location.

1. Navigate to the Command Prompt.
2. Type `LinqKeyManager.exe create-database`.
3. Press **Enter**.

   > **Note:** A success message is displayed. A Logs folder and Database file are created in the same folder as the **LinqKeyManager.exe**.

4.1.3 Create a local keystore

Keystores are a secure container for cryptographic keys. The following steps create a password protected local keystore managed by HID Linq Key Manager.

1. Navigate to the Command Prompt.
2. Type `LinqKeyManager.exe keystore create-local -i`
3. Press **Enter**.

   Note: Follow the tool prompts to provide the required information.

   - **Keystore name:** type a descriptive name (for example `MyCompany_DESFire_Store`) and press **Enter**.
   - **Password:** type a strong password and press **Enter**.

     Note: No visual feedback such as dots or asterisks are displayed when typing the password.
   - **Confirm password:** re-enter the password and press **Enter**.

   Note: A **Keystore `MyCompany_DESFire_Store` created successfully** message is displayed.

4.1.4 Add keys to the local keystore

Prerequisites

You must have at least the following for a typical MIFARE DESFire setup for the HID M1 Key Module.

- MIFARE DESFire Read key (or Application Master Key dependent on the setup)
- SNMP Authentication Key
- SNMP Privacy Key
- Main Node Pairing Key

To add a key to your local keystore:

1. Navigate to the Command Prompt.
2. Type `LinqKeyManager.exe keystore add-local-key -i`.
3. Press **Enter**.

   Note: Follow the tool prompts to provide the required information.

   - **Keystore:** select the required keystore using the arrow keys (for example `MyCompany_DESFire_Store`) and press **Enter**.
   - **Key name:** type the required key name (for example `DESFire_Read_Key`, `SNMP_Auth`, `SNMP _Priv`, `Pairing_Key`) and press **Enter**.

     Note: You must create a **.bin** file containing the value of the key in hexadecimal format for the Pairing key. See **3.1 Main Node Pairing Key** for more information.
   - **Key value:** type the 32 character hexadecimal string and press **Enter**.
   - **Wrap key?:** type **yes** or **no** and press **Enter**.

     Note: Most standard MIFARE DESFire keys used directly do not require a **Wrap key**.
   - **Keystore password:** Type the password for the required keystore and press **Enter**.
4. Repeat the above steps for each individual key required for the same keystore.

   Note: A success message is displayed if the key is added successfully.

4.1.5 Create a MIFARE DESFire keyset

Keysets group one or more keys from the keystore for a specific purpose.

1. Navigate to the Command Prompt.
2. Type **LinqKeyManager.exe keyset create-desfire -i**.
3. Press **Enter**.

   > **Note:** Follow the tool prompts to provide the required information.

   - **Keyset name:** type a descriptive name (for example `DESFire_Keyset`) and press **Enter**.
   - **Keystore:** Select the required keystore and press **Enter**.
   - **Key:** Select the required key and press **Enter**.
   - **Configure a RandomUID key?:** type **yes** or **no** and press **Enter**.

     > **Note:** This is typically **no** for standard applications.
4. Repeat the above steps for each key required for the same keyset.

   > **Note:** A success message is displayed if the key is added successfully.

4.1.6 Create an SNMP keyset

SNMP keys are cryptographic credentials that are used to authenticate and secure communication with the Key Module. You must provide these to ensure full ownership and control over device access and key management.

Prerequisites

You must have at least the following for a typical SNMP keyset.

- SNMP Authentication Key
- SNMP Privacy Key

1. Navigate to the Command Prompt.
2. Type **LinqKeyManager.exe keyset create-snmp -i**.
3. Press **Enter**.

   > **Note:** Follow the tool prompts to provide the required information.

   - **Keyset name:** type a descriptive name (for example `SNMP_Keyset`) and press **Enter**.
   - **SNMP Authentication Key:**
     - Select the required keystore and press **Enter**.
     - Select the required SNMP Authentication key and press **Enter**.
   - **SNMP Privacy Key:**
     - Select the required keystore and press **Enter**.
     - Select the required SNMP Privacy key and press **Enter**.
4. Repeat the above steps for each key required for the same keyset.

   > **Note:** A success message is displayed if the key is added successfully.

4.1.7 Create a Key Module configuration

Key Module configurations define how the MIFARE DESFire application on the card is accessed, including application IDs, key numbers, diversification, and data formatting.

1. Navigate to the Command Prompt.
2. Type `LinqKeyManager.exe configuration create --name <your_config_name>`.
3. Press **Enter**.

> **Note:** Follow the tool prompts to provide the required information.

- **Configure with ANSSI CSPN mode:** type **yes** or **no** and press **Enter**.
- **DESFire Application ID (AID):** type the required 1 to 3 byte hex value and press **Enter**.
- **File Number:** type the required MIFARE DESFire file ID.
- **Card Data Length:** enter the required length of data to be read.
- **DESFire Keyset:** select the required MIFARE DESFire keyset.
- **Application Key number:** enter the required MIFARE DESFire application key number.
- **Diversification settings for the application key:**
  - Select the required diversification algorithm (for example, **None**, **AES128_NXP**).
  - Enter the system ID (if diversification is used).
  - Select the required diversification input (for example, **UID**, **Random**)
  - **Configure proximity check?:** select **yes** or **no**.
  - **Enforce a communication mode?:** select **yes** or **no**.
- **Output format configuration:**
  - Enter the required start bit offset.
  - Enter the required bit length.
  - Select the required endianness (for example, BigEndian, LittleEndian).
  - **Configure conversion type?:** select **yes** or **no**.

> **Note:** A success message is displayed if the configuration is created successfully.

4.1.8 Remove a configuration from Key Module

> **Note:** The following steps are optional and can be used to change a Key Module configuration.

Key Modules can only store one configuration at a time. The existing configuration can be removed to apply a different configuration to the Key Module.

1. Navigate to the Command Prompt.
2. Type `LinqKeyManager.exe key-module remove-configuration -i`.

   > **Note:**
   > Alternatively, if the name of both configuration and Key Module are known, type:
   > `LinqKeyManager.exe key-module remove-configuration --keymodule-name <module_name> --configuration-name <config_name_to_remove> [--slot <slot_number>]`
   > Replace the placeholders as necessary.

3. Press **Enter**.

   > **Note:** Follow the tool prompts to provide the required information.

   - Select the Key Module by name or serial port
   - Select the required configuration to remove
   - Enter the keystore password

   > **Note:** A success message is displayed if the configuration is removed successfully.

4.2 Onboard the HID M1 Key Module

Onboarding registers the physical Key Module with the HID Linq Key Manager application database and prepares it to receive configurations.

1. Connect the HID M1 Key Module to the USB port of the required computer.
2. Navigate to the Command Prompt.
3. Type `LinqKeyManager.exe key-module onboard -i`.
4. Press **Enter**.

   > **Note:** Follow the tool prompts to provide the required information.

   - Select the required serial port from the COM ports list and press **Enter**.

     > **Note:** A success message is displayed if any Secure Access Modules (SAM) are found.

   - Type **yes** and press **Enter** to continue.
   - Type the required Key Module name (for example, Key_Module01) and press **Enter**.
   - Select the required SNMP keyset and press **Enter**.
   - Enter the required password for the keystore containing the required SNMP keys and press **Enter**.

     > **Note:** A success message is displayed if the Key Module is on-boarded successfully.

5. Type `LinqKeyManager.exe advanced configure-pairing-key` and press **Enter**.

   > **Note:** This step wipes all keys from the Key Module. This must always be done before applying the configuration.

6. Type `LinqKeyManager.exe key-module apply-configuration --name <NAME>` and press **Enter** to apply the configuration to the Key Module.
7. Connect the Key Module to the Main Node.

Section 05

Command reference

5.1 General help

This section provides a reference to the available commands for HID Linq Key Manager.

Navigate to the Command Prompt and type `LinqKeyManager.exe help` and press **Enter** for a list of all available main commands.

For help on a specific command navigate to the command prompt and type:

`LinqKeyManager.exe <command_name> --help`.

> **Note:** Replace the `<command_name>` placeholder with the required command. For example `LinqKeyManager.exe` **`keystore`** `--help` will display **keystore** information.

create-database

This command creates the application database files. This must be run during initial setup.

Syntax

```
LinqKeyManager.exe create-database
```

Options

None

Example

```
C:\Users\YourUserName\Desktop\LinqKeyManager> LinqKeyManager.exe create-database
```

- Database created - **C:\Users\YourUserName\Desktop\LinqKeyManager\LinqKeyManager.SST**
- Logs folder - **C:\Users\YourUserName\Desktop\LinqKeyManager\Logs**

configure-pairing-key

This command allows you to add a Pairing Key that is required to complete the HID M1 system set up.

Syntax

```
LinqKeyManager.exe advanced configure-pairing-key
```

> **Note:** The tool will prompt you through the key adding process.

Options

None

Example

```
C:\Users\YourUserName\Desktop\LinqKeyManager> LinqKeyManager.exe advanced configure-pairing-key
```

5.2 keystore list

This command lists all keystores currently defined in the application database.

Syntax

```
LinqKeyManager.exe keystore list
```

Example output

Available keystores:

- `MyCompany_DESFire_Store (local)`
- `NXP_SAM_AV3_Store (NXP)`

keystore create-local

This command creates a local keystore. The keys are encrypted and user password protected.

Syntax (interactive)

```
LinqKeyManager.exe keystore create-local -i
```

Syntax (Command Arguments)

```
LinqKeyManager.exe keystore create-local --name <keystore_name> --password <password>
```

Parameters

- `-i`: (optional) use interactive mode to be prompted for name and password.
- `--name <keystore_name>`: required if not using `-i`. Replace the place holder with the required keystore name.
- `--password <password>`: required if not using `-i`. Replace the place holder with the required password.

> **Note:** No visual feedback such as dots or asterisks are displayed when typing the password.

keystore create-nxp

The NXP keystore stores keys on an NXP SAM AV3 chip. The keys reference metadata on an NXP SAM. The NXP keystore does not store key material.

The NXP keystore requires an authentication key to perform operations. When a SAM key is pushed, it is dumped in the computer memory first.

There are two ways to create a local keystore:

Syntax interactive (recommended)

```
LinqKeyManager.exe keystore create-nxp -i
```

Syntax (Command Argument)

```
LinqKeyManager.exe keystore create-nxp --name <keystore_name> [--pcsc-reader <reader_name>]
```

Parameters

- `-i`: (optional) use interactive mode. The tool scans for PCSC readers and prompts for selection.
- `--name <keystore_name>`: replace the place holder with the required NXP keystore name.
- `--PCSC-reader <reader_name>`: (optional when using `-i`). replace the placeholder with the required PCSC reader connected to the SAM.

keystore create-pkcs

This command creates a reference to a PKCS#11 Hardware Security Module (HSM) or token, treating it as a keystore.

Syntax interactive (recommended)

```
LinqKeyManager.exe keystore create-pkcs -i
```

> **Note:** Other parameters such as `--module-path`, `--slot-id`, and `--pin`, are required when not using the interactive syntax. Type `create-pkcs --help` and press **Enter** for more information.

keystore delete

This command deletes a keystore from the application database. This command does not delete keys from external HSMs (NXP, PKCS#11).

Syntax (interactive)

```
LinqKeyManager.exe keystore delete -i
```

Syntax (Command Arguments)

```
LinqKeyManager.exe keystore delete --name <keystore_name> --password <password_if_local>
```

Parameters

- `--name <keystore_name>`: The name of the keystore to be deleted.
- `--password <password_if_local>`: required for confirmation to delete the keystore.

keystore list-keys

This command lists all the keys in the specified keystore.

Syntax

```
LinqKeyManager.exe keystore list-keys --keystore-name <keystore_name>
```

keystore add-local-key

This command adds a new AES128 key (provided in clear text) to an existing local keystore.

Syntax (interactive)

```
LinqKeyManager.exe keystore add-local-key -i
```

Syntax (Command arguments)

```
LinqKeyManager.exe keystore add-local-key --keystore-name <keystore_name> --key-name <new_key_
name> --key-value <32_hex_char_key> --password <keystore_password>
```

Parameters

- `--keystore-name <keystore_name>`: name of the required local keystore.
- `--key-name <new_key_name>`: the required name of the new key.
- `--key-value <32_hex_char_key>`: the 32-character hexadecimal key value (for example **AABBCCDDEEFF00112233445566778899**).
- `--password <keystore_password>`: the required password for the target keystore.

keystore add-wrapped-local-key

This command adds a key already wrapped (encrypted) by another key to a local keystore. Only AES128 is currently supported.

> **Note:** This is an advanced operation. Type `keystore add-wrapped-local-key --help` in to the Command Prompt and press **Enter** for specific wrapping key ID and format parameters.

keystore add-nxp-key

This command adds a reference to an existing key on an NXP SAM (configured as a keystore).

Syntax (interactive)

```
LinqKeyManager.exe keystore add-nxp-key -i
```

Syntax (Command Argument)

```
LinqKeyManager.exe keystore add-nxp-key --keystore-name <nxp_keystore_name> --key-name <new_key_reference_name> --key-number <SAM_key_slot_num> --key-version <SAM_key_version_num>
```

Parameters

- `--keystore-name <nxp_keystore_name>`: the name of the NXP keystore.
- `--key-name <new_key_reference_name>`: the name for the required key within HID Linq Key Manager.
- `--key-number <SAM_key_slot_num>`: the key slot number of the NXP SAM.
- `--key-version <SAM_key_version_num>`: the key version number of the NXP SAM.

keystore get-key

This command retrieves and displays the value of a key from a keystore in clear text.

Syntax

```
LinqKeyManager.exe keystore get-key
```

> **Note:** The tool will prompt for keystore, key name, and password.

5.3 Keyset

the keyset manages a group of one or more keys from a keystore, intended for a specific use, for example a MIFARE DESFire application or SNMP.

keyset list

This command displays all available keysets.

Syntax

```
LinqKeyManager.exe keyset list
```

keyset create-seos

This command creates a new Seos® keyset.

Syntax

```
LinqKeyManager.exe keyset create-seos
```

Parameters

- `--name <name>`: the new keyset name.
- `--read-key <keystore-name> <key-name`: select the required read key from the keystore.
- `--privacy-mac-key <keystore-name> <key-name>`: select the required privacy mac key from the keystore.
- `--privacy-enc-key <keystore-name> <key-name>`: select the required privacy encryption key from the keystore.

keyset create-desfire

This command creates a new MIFARE DESFire keyset.

Syntax

```
LinqKeyManager.exe keyset create-desfire
```

> **Note:** The tool will prompt for keyset name, keystore, the MIFARE DESFire key(s) from the required keystore, and RandomUID configuration.

Parameters

- `--name <name>`: the name of the new keyset.
- `--read-key <keystore-name> <key-name>`: select the required read key from the keystore.

keyset create-snmp

This command creates a new SNMP keyset using an authentication key and a privacy key from a keystore.

Syntax (interactive)

```
LinqKeyManager.exe keyset create-snmp -i
```

> **Note:** The tool will prompt for keyset name and the required authentication key and privacy key from the required keystore(s).

keyset create-snmp-with-key-id

This command creates an SNMP keyset using the keystore name and key ID. This is useful for keys that cannot be referenced by name. This command does not typically have an interactive mode.

Syntax

```
LinqKeyManager.exe keyset create-snmp-with-key-id --name <keyset_name> --authentication-key <keystore_id> <key_id> --privacy_key <keystore_id> <key_id>
```

> **Note:** Type `--help` for the exact key identifier parameter names.

keyset get

This command retrieves and displays the details of a specific keyset.

Syntax

```
LinqKeyManager.exe keyset get --name <keyset_name>
```

keyset delete

This command deletes a specific keyset.

Syntax

```
LinqKeyManager.exe keyset delete --name <keyset_name>
```

5.4 Configuration

The following commands allow you to manage the MIFARE DESFire configurations that can be applied to Key Modules.

configuration create

This command allows you to create a new MIFARE DESFire configuration.

Syntax

```
LinqKeyManager.exe configuration create --name <config_name>
```

> **Note:** This is an advanced operation. Type `--help` in to the Command Prompt and press **Enter** for the specific parameters that define MIFARE DESFire application access, diversification, and data formatting.

configuration list

This command lists all of the saved configurations.

Syntax

```
LinqKeyManager.exe configuration list
```

configuration show

This command display the details of a specific saved configuration.

Syntax

```
LinqKeyManager.exe configuration show --name <configuration_name>
```

configuration delete

This command deletes the required saved configuration from the application database.

Syntax

```
LinqKeyManager.exe configuration delete --name <configuration_name>
```

5.5 key-module

The following commands allow you to manage Key Modules

key-module onboard

This command onboards the Key Module, registers it with the application database, and associates it with an SNMP keyset.

Syntax (interactive)

```
LinqKeyManager.exe key-module onboard -i
```

> **Note:** The tool will prompt for serial port, Key Module name, SNMP keyset, and the keystore password.

key-module apply-configuration

This command applies a previously created MIFARE DESFire configuration to an on-boarded Key Module.

Syntax

```
LinqKeyManager.exe key-module apply-configuration --name <configuration_name>
```

> **Note:** The tool will prompt for the keystore password, Key Module selection (by name or serial port), and target customer key slot number.

key-module remove-configuration

This command removes the specified MIFARE DESFire configuration from a Key Module slot to allow the application of a new configuration to the same slot.

Syntax

```
LinqKeyManager.exe key-module remove-configuration --configuration-name <config_name>
```

key-module compare-report

This command compares configurations for consistency across SAMs within a single Key Module.

Syntax

```
LinqKeyManager.exe key-module compare-report --serialport-path <serial_port_path>
```

> **Note:** The tool will prompt you to select a Key Module.

key-module list

This command lists all Key Modules on-boarded in the application database.

Syntax

```
LinqKeyManager.exe key-module list
```

key-module identify

This command scans for available serial (COM) ports and attempts to identify the connected Key Modules.

Syntax

```
LinqKeyManager.exe key-module identify
```

key-module unboard

This command removes a specified Key Module registration from the application database.

> **Note:** This command does not perform any operation on the physical Key Module for example deleting keys, or configurations from the device.

Syntax

```
LinqKeyManager.exe key-module unboard --name <onboarded_module_name>
```

5.6 Advanced

The `advanced` commands are intended for advanced users, diagnostics, or specific low-level operations.

> **Important: It is recommended you only use the following commands if you understand their impact.**

- `advanced configure-pairing-key`: allows you to add a pairing key. The pairing key is required to complete the M1 system set up.
- `advanced configure-wrapping-key`: allows provisioning wrapped keys to the SAM
- `advanced static-roll-snmp`: roll SNMP keys for a single SAM
- `advanced write-oid`: writes an arbitrary value to a specific OID on a SAM. This command requires the OID, value, and the required SAM.
- `advanced read-oid`: reads the value of a specific OID from a SAM.
- `advanced enum-oid`: lists the available OIDs of a specific SAM on a Key Module.
- `advanced get-sam-mode`: retrieves the operating mode of a Key Module (not individual SAMs).
- `advanced reset-sam`: instructs the Key Module to reset the SAM.
- `advanced get-samatr`: retrieves Answer to Reset (ATR) from a SAM.
- `advanced checksum-sam`: compute a checksum of configuration present on a SAM for consistent configuration across multiple SAMs.
- `advanced get-kcv`: retrieves the Key Check Value (KCV) for a key of a specific OID on a SAM.

Section 06

Troubleshooting

6.1 Troubleshooting

Issue	Action
Command Not Found (LinqKeyManager.exe is not recognized)	• Use the `cd` command to verify you are in the correct directory and Command Prompt that the LinqKeyManager.exe file is located. • Verify that the .exe file is named LinqKeyManager.exe.
Cannot Connect to Key Module/Key Module Not Detected	• Check the USB-C cable connection at the computer and the Key Module. • Make sure the Key Module has power (indicated by an LED). • Try to identify the Key Module using the `LinqKeyManager.exe key-module identify` command. • Check if the Key Module is recognized as a serial device (COM port) using Windows Device Manager.
Access Denied/Permission Errors (when creating database or logs)	• You must have write permission in the folder containing the LinqKeyManager.exe. • Right click the Command Prompt icon and click Run as administrator.
Incorrect Password Errors	• Passwords are case sensitive. • No visual feedback such as dots or asterisks are displayed when typing the password.
File Not Found or Keystore Not Found errors	• Check the names of keystores, keysets, and configurations are correct. • Make sure the application database file (LinqKeyManager.SST) and the .exe file are in the same directory.
Invalid key format	Make sure MIFARE DESFire keys are provided in 32-character hexadecimal strings.
Key Module pairing failed	Use strong keys when entering SNMP keys.

6.2 Check log files

HID Linq Key Manager creates a **Logs** folder in the same directory as the LinqKeyManager.exe file.

When contacting HID Technical Support, you will need access to the log files. These can be found by navigating to the **Logs** folder.

Appendix **A**

Security best practices

A.1 Keystore passwords

- Use strong, unique passwords.
- Do not share your password.
- Store passwords securely.

> **Note:** It is recommended to use a trusted password manager.

A.2 Key management

- Manage raw MIFARE DESFire key values with extreme care before they are imported into HID Linq Key Manager. Store them securely and limit their exposure.
- Understand the implications of key diversification if used.

A.3 Database backup

If the application database file is lost, you will lose access to your defined keys (for local keystores) and configurations. Regularly back up the application database file to a secure location.

A.4 Physical security

- Secure the computer running HID Linq Key Manager, especially if it holds sensitive key information.
- Physically secure the HID M1 Key Modules before and after they are provisioned.

A.5 Air-gapped systems

HID Linq Key Manager supports air-gapped computers. It is recommended to use the tool on a dedicated offline computer to minimize exposure risk.

Revision history

Date	Description	Revision
December 2025	Initial release.	A.0

hidglobal.com

For technical support, please visit: https://support.hidglobal.com

PLT-08195, Rev. A.0

Part of ASSA ABLOY