Asure ID® iCLASS SE CP1000 Desktop Encoder

User Guide

PLT-01067, B.0
February 2024

Copyright

Trademarks

Contacts

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

What's new

Date	Description	Revision
February 2024	Minor updates.	B.0

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

Section 01

Overview

1.1 Introduction

The Asure ID iCLASS SE Encoder is a smart card provisioning product that consolidates most of the existing HID Global encoding products including the CP400 iCLASS Programmer, CP600 DESFire Encoder, iCL-ELITE programmer, and 1050 ProxProgrammer.

The following features are included:

- Encode HID Access Control Application with Standard, Elite, and Custom Security on to iCLASS® and MIFARE® Classic credentials
- Encode HID Secure Identity Objects (SIO) with Elite Security on iCLASS, MIFARE Classic, MIFARE DESFire EV1®, and Seos®
- Encode HID Access Control Application on to HID Prox cards and fobs
- Encode Custom Data Objects on iCLASS, MIFARE Classic, MIFARE DESFire EV1, and Seos
- Roll keys on existing card populations from a revoked key set to a new active key set
- Migrate existing iCLASS and MIFARE Classic Standard Security (applications) card populations to SE Security
- Configure encoders for various Security models and Custom Data model interpreters

Other features and use cases:

- Create and manage custom media and application keys
- Export and Import custom keys
- Import keys from HID
- Manage all credential and reader transactions through work orders scripted from instruction sets
- In-line personalization of credentials

Note: From this point, the *iCLASS SE CP1000 Encoder* is now referred to as the *iCLASS SE Encoder*.

1.2 Main concepts

To get the most out of the iCLASS SE Encoder, there are several concepts that should be understood.

1.2.1 Key management

iCLASS SE Encoder is an HID Global product that provides solution to encode user credentials and reader configuration data. To provide a high level of security, the encoder device uses a smart card chip (an ISO 7816 compliant device) to perform the key management as well run the encoding applications. This component of the encoder device is called Secure Access Module (SAM).

A typical encoding operation requires knowledge of default/transport keys of the credential, your credential or reader configuration data and the new keys to be used to protect the credential. The keys that are involved in encoding operation could be ones that are managed by HID Global or ones created by the customer and provisioned in SAM.

To do secure key management, we use cryptographic algorithms and practices that have been validated by our industry to provide security solutions for our customers. The rest of the document describes different types of keys and their management.

1.2.2 Administration keys

To load, update, and delete configuration data and keys used during encoding operations Simple Network Management Protocol (SNMP) version 3 messages are used. SNMP is an Internet-standard protocol for managing devices on IP networks and defined by RFC 3411-RFC 3418. Though the protocol is intended for IP devices HID makes use of it over other transport and application protocols such as ISO 7816-3 (APDU) for PC/SC readers.

A typical SNMP message is encrypted and signed using 16-byte keys and also contains metadata about the cryptographic mechanism used to protect the message. The message defines its actions using verbs, such as GET, SET etc. The keys that are used for encryption are called SNMP encryption and SNMP privacy keys and the keys used for signing are called the SNMP signing and SNMP authentication keys.

A device or a software application implementing the SNMP standard is called an SNMP endpoint or engine and is identified using one or more engineId/username pairs.

The encoder SAM is an SNMP endpoint that has two identities: the HID Admin and the OEM Admin. Each identity is recognized using an engineId and username pair as described in the SNMP standard. Each identity includes two associated keys: SNMP encryption and signing.

The purpose of HID Admin identity is to manage the keys and configuration data that originate from HID. The OEM Admin identity can be used to create custom keys and perform operations that do not require high levels of security.

When a customer receives an encoder, it has OEM Admin SNMP keys that are set to default/public values. When the host application is started for the first time, it prompts you to change the keys to be managed. The host application then stores the changed OEM Admin keys in the local database and the keys are encrypted using your password of the application.

1.2.3 Media keys

The keys that are used to authenticate a credential to perform read/write operations are called media keys. For example, the debit and credit keys for a page in iCLASS credentials are the media keys. In the case of MIFARE Classic, the Key A and Key B of a sector are the media keys and for DESFire EV1 the application keys as well as the PICC master key are examples of media keys.

The lengths of these types of keys as well as the cryptographic algorithms, such as authentication algorithm, that makes use of these keys are dependent upon the credential/media technology.

A typical encoding operation uses the default/known media key to first authenticate to the blank credential, create the application, write the credential, and change the value of the key to the one specified by you. It is important to make a note that the new value can be a diversified key to reduce the surface area of attack. In other words, all the credentials/media have different values for the media keys. For the newer and more secure credentials (for example: Secure Objects) we make use of NIST 108 key diversification algorithm whereas the older/legacy credentials make use of proprietary key diversification algorithms invented by HID Global and/or chip vendors such as NXP.

For all the credential/media, the keys could fall in one of these categories:

- **HID Managed Standard Media Keys**: These keys are managed securely by HID and are intended for general customer base.
- **HID Managed Elite Media Keys**: These keys are managed securely by HID and are specific to customers who participate in the Elite program. For example an Elite customer identified using an ICE0000 have a different set of media keys than the one identified using ICE0133.
- **Customer Generated and Managed Keys**: These keys are either generated using the encoder solution and/or entered by the customer. The keys reside in the encoder SAM, and can be exported in encrypted form to be archived. Once created, knowledge of the plain text key is the responsibility of the administrator. Custom Keys are not archived by HID.

All the HID managed keys are delivered in the form of static SNMP messages targeted to the encoder, for which they were requested. Typically, the customer reads the engineId of the encoder device using the host application and orders from HID Global the appropriate key set (for example: standard, ICEXXX etc.). The keys are delivered in the form of a file that contains the static messages, and the host application provides necessary user interface to load them in the encoder SAM.

Custom keys can be exported from the encoder device. The export format is again an SNMP message that is protected using OEM Admin keys.

1.2.4 Secure object keys

The newer and more secure credentials used by HID Global readers are based on the Secure Object (SO) technology. While it is outside the scope of this document to describe SO technology in detail, in simple words, a SO is a structured credential that is based on industry standards to support extensibility of credential structure and use industry validated and approved security algorithms and mechanisms. The most important aspect of a SO is that it provides an additional security for the credential and therefore we do not only rely on the security mechanisms of the chip/media silicon vendor.

Very much like an SNMP message a SO also has a notion of encryption and signature. To reduce the size of a secure object credential we make use of an Authenticated Encryption with Associated Data (AEAD) algorithm called EAX' (read as EAX prime). In simple words, EAX' one key can be used to perform both encryption and signing of the SO credential. This key is called the SO encryption key.

> **Note:** It is called an encryption key but it also performs signature verification.

The SO encryption key could be managed by HID as a standard key and/or an Elite key, which is similar to the management of Media keys described earlier. We also provide the support to create a customer managed SO encryption key, however a SO credential that is protected using such a key is not managed via HID and also has an additional signature using HID Global's license key.

Additional information about secure objects can be requested from HID Global.

1.2.5 Secure channel key

The messages that are exchanged between a host application and the encoder device are transferred over a mandatory secure channel. The secure channel helps to protect the confidentiality and authenticity of the messages between the host application and the encoder device.

The encoder comes with a default value for the secure channel key, and very much like the OEM Admin keys, the host application prompts you to provide a new value for the secure channel key. This secure channel key is stored on a per user basis.

The secure channel mechanism is based on a slightly modified Global platform SCP secure channel protocol. You can request more information about the secure channel from HID Global.

1.2.6 Credential credit management

All transactions with credentials are enabled by credential credits. These are discrete tokens that are consumed with each transaction until none remain or until additional credits are ordered and applied to the encoder.

The term Credential Credit, refers to the tokens purchased from HID that enable all credential write transactions. The iCLASS SE Encoder is enabled until the authorized credits have been exhausted, then you must request additional credits from HID Global.

The management of credits can be understood as a type of counter. When a customer orders "X" credits, the counter is increased by "X" and the encoder is enabled until the counter is decremented to 0, or until more credits are ordered.

The following attributes, are the building blocks to define a transaction which is enabled by a Credential Credit Token.

Technology	Application	Security	Media
iCLASS	HID	Standard	Genuine HID
MIFARE Classic	SIO	Elite	Third Party
MIFARE DESFire EV1	Custom	Custom	Third Party
Prox	HID	Standard	Genuine HID
Seos	SIO	Elite	Genuine HID

For example: To encode iCLASS with HID Access Control application and Standard keys, this transaction would require a different credential credit token than the same transaction using Elite keys.

Things to know about credential credits:

- Each credit token type is managed by its respective credit counter.
- Credit top up messages are delivered in a secure SNMP message that is targeted for a specific device by diversifying the keys with the device Engine ID.
- Credit top up messages can be loaded only once.
- A cap (10,000 credits) is placed on the number of credits that can be ordered at a time. This is to limit the monetary value that can be loaded into a single encoder device which can be lost or destroyed.

1.2.7 Formats

The iCLASS SE Encoder includes a format interpreter capable of parsing all open and custom formats developed and maintained by HID Global.

Format fields are presented to you in the desktop UI for the purpose of assigning data to each field.

Formats must be ordered from Customer Service. Most formats are custom to a specific OEM or end user, and are not freely distributed.

The H10301 (SIA Wiegand 26-bit) is the default format delivered with the desktop application.

1.2.8 Plugin architecture

The iCLASS SE Encoder includes a plugin architecture which makes it highly configurable with minimal maintenance and few releases. There are two types of plugins:

- Technology
- Configuration

Technology plugins are a packaged bundle that includes an applet which is loaded to the encoder device and a UI plugin for the desktop application that is customized for the associated applet.

- Applets are small C# applications designed to run on the .NET framework that is native to the encoder device. These applets manage the interface to the credential and provide an API to the desktop application. Applets can be tailored for a specific use case.
- The UI plugin manages the interface to the encoder device and provides you with inputs and information specific to the applet loaded on the device. For example, each technology applet comes with a unique set of wizard pages gathering user input for work order creation.

Configuration plugins expose a UI for gathering inputs and creating reader configuration cards. Reader configuration plugins are released as groups that organize parameters.

Things to know about plugins:

- Each applet is digitally signed by a key managed by HID Global and known by all encoder devices (global key). This identifies the applet as Genuine HID. Only Genuine HID plugins are recognized by the encoder device.
- Initially, one applet/plugin is created for each of the four supported technologies (iCLASS, MIFARE Classic, MIFARE DESFire EV1, HID Prox, and Seos).
- Custom plugins can be created on a Custom Product Opportunity (CPO) basis.

1.2.9 Work orders

All credential encoding activity is managed through Work Orders. Each Work Order includes a set of Work Instructions to be executed on every credential presented to the encoder.

- Work orders execute a work flow that you design
- Work Orders are technology independent
- Work Orders can be limited in scope or open-ended

1.2.10 Work instructions

Each Work Instruction represents one step of an overall work flow that is executed on every credential presented to the encoder.

- Work Instructions are analogous to scripts
- Work Instructions are technology specific
- Work Instructions are wholly independent operations

1.2.11 Custom applications

Custom Applications can be written to credentials. The iCLASS SE Encoder supports two types of custom applications; Custom Media and Data Mapper.

1.2.12 Custom media applications

- Manage keys for custom media applications.
- Read and Write custom data to and from custom media applications.

Examples: custom vending applications or HF migration media (not the Config cards).

1.2.13 Data Mapper applications (HF migration)

- Reader accesses custom credential application data autonomously and reports data on communications ports.
- Reader is configured with necessary authentication and encryption keys to access the raw credential data.
- Reader is configured with instructions for manipulating the raw data into a format that can be managed by the host or access control system.

Section 02

Encoder application navigation

2.1 Introduction

The iCLASS SE Encoder Desktop application has the following structure:

Application Modules, each with a subset of tabs.

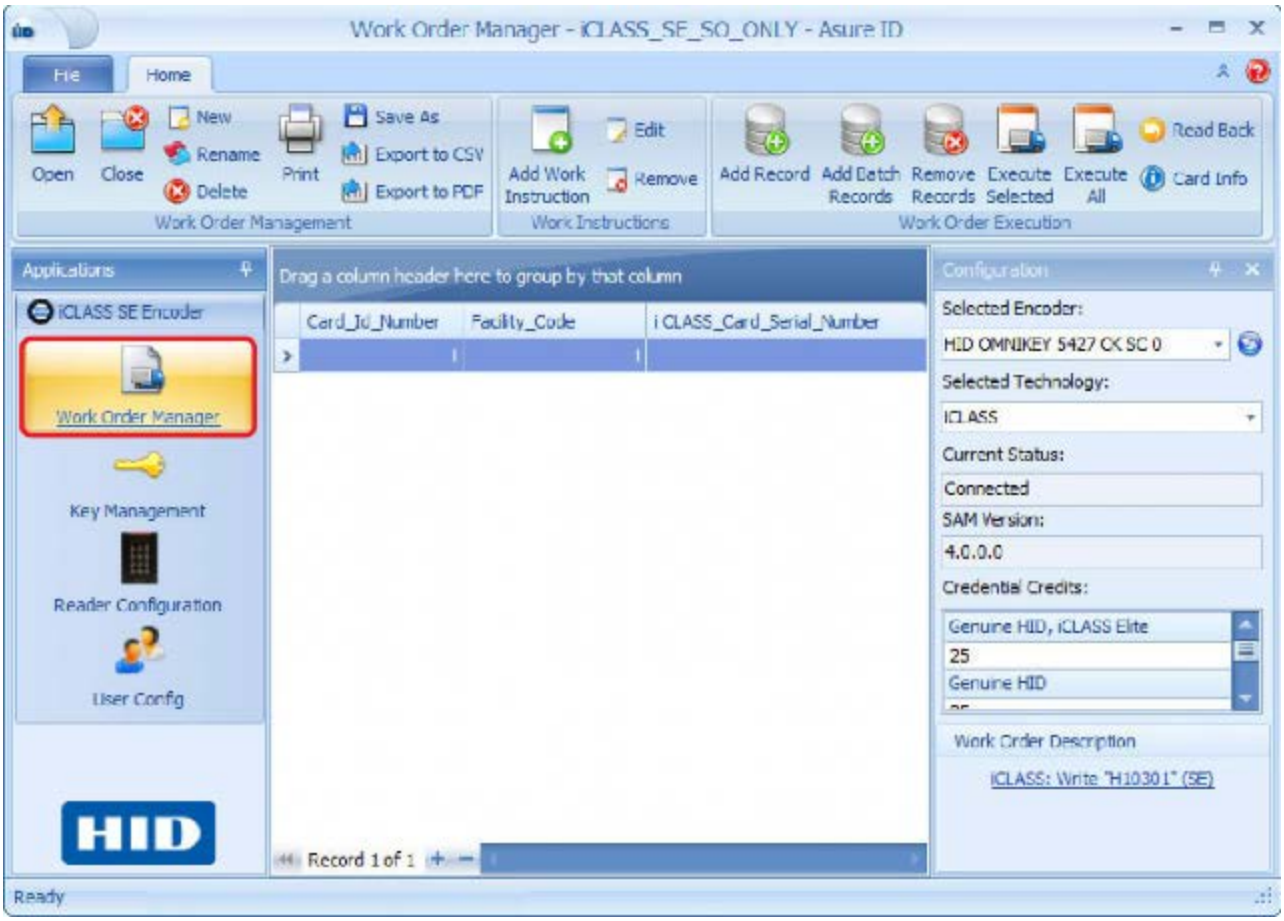
- Work Order Manager (File tab, Home tab)
- Key Management (File tab, Home tab)
- Reader Configuration (File tab, Home tab)
- User Config (File tab, Home tab & View tab)

With the selection of an application module the window displays the specific module toolbar, information and configuration panes, etc. The following is an overview of these windows.

2.2 Work Order Manager module

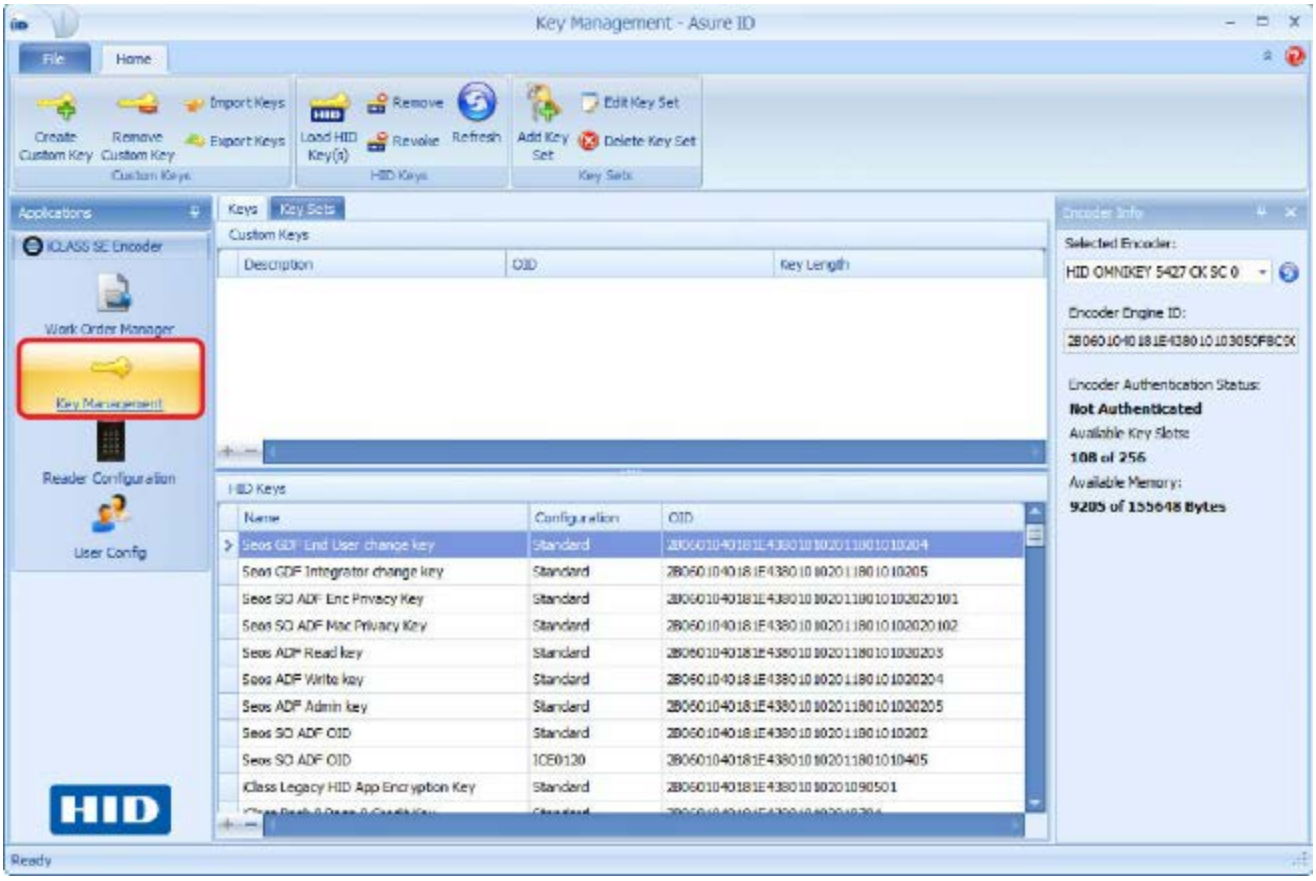
The Work Order Manager module allows you to define and save an encoding profile for a credential deployment. Each Work Order defines the number of data fields encoded, as well as the data type and field size. These data fields are concatenated into a single data stream and encoded into an application, and are defined by the selected format.

A Work Order is comprised of one or many Work Instructions. A Work Instructions is a single command issued during work order execution. The single work instruction can either read or write to a specific memory location.



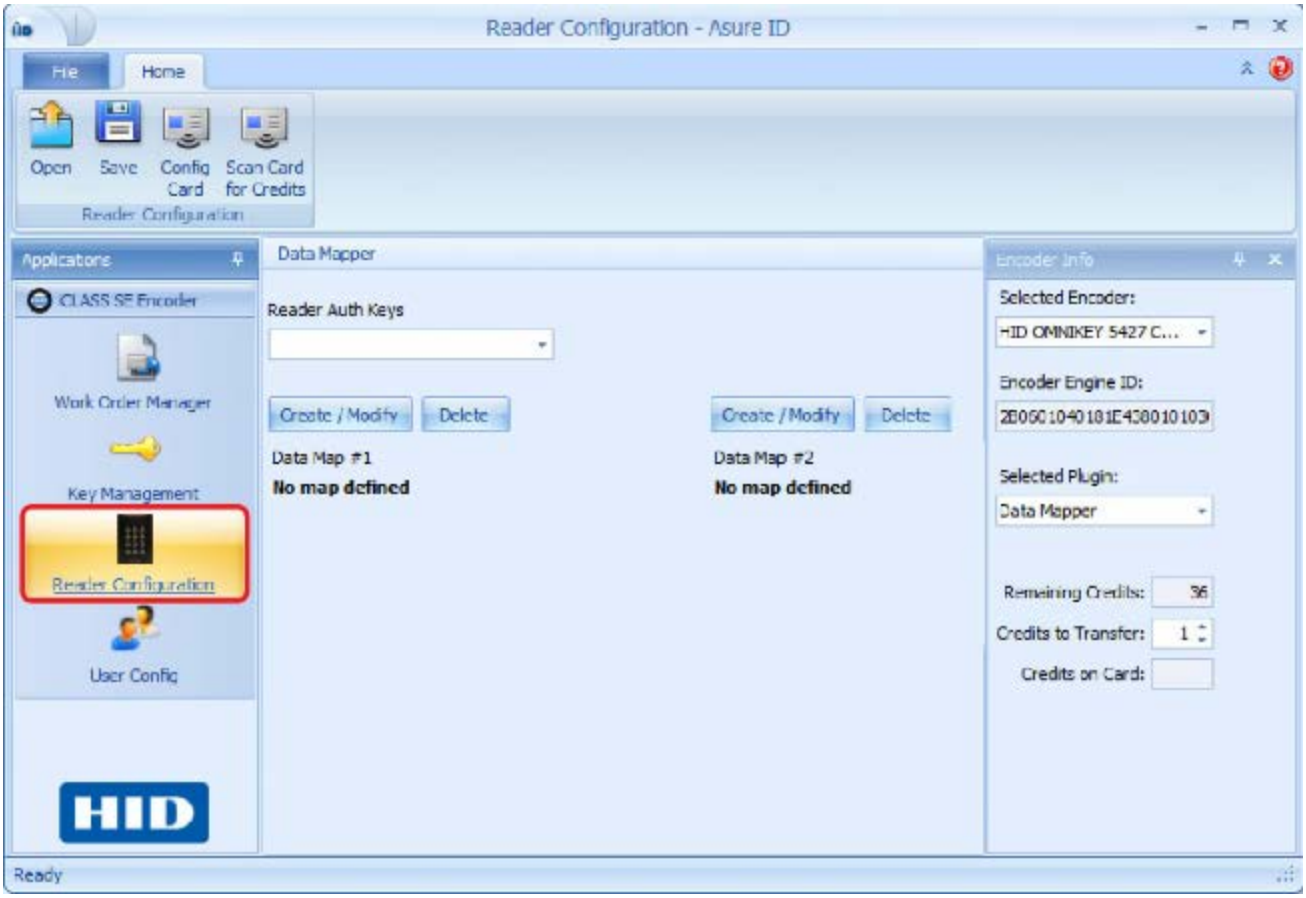
2.3 Key Management module

The Key Management module of the CP1000 Desktop Encoder allows you to view and manage the HID and Custom Keys.



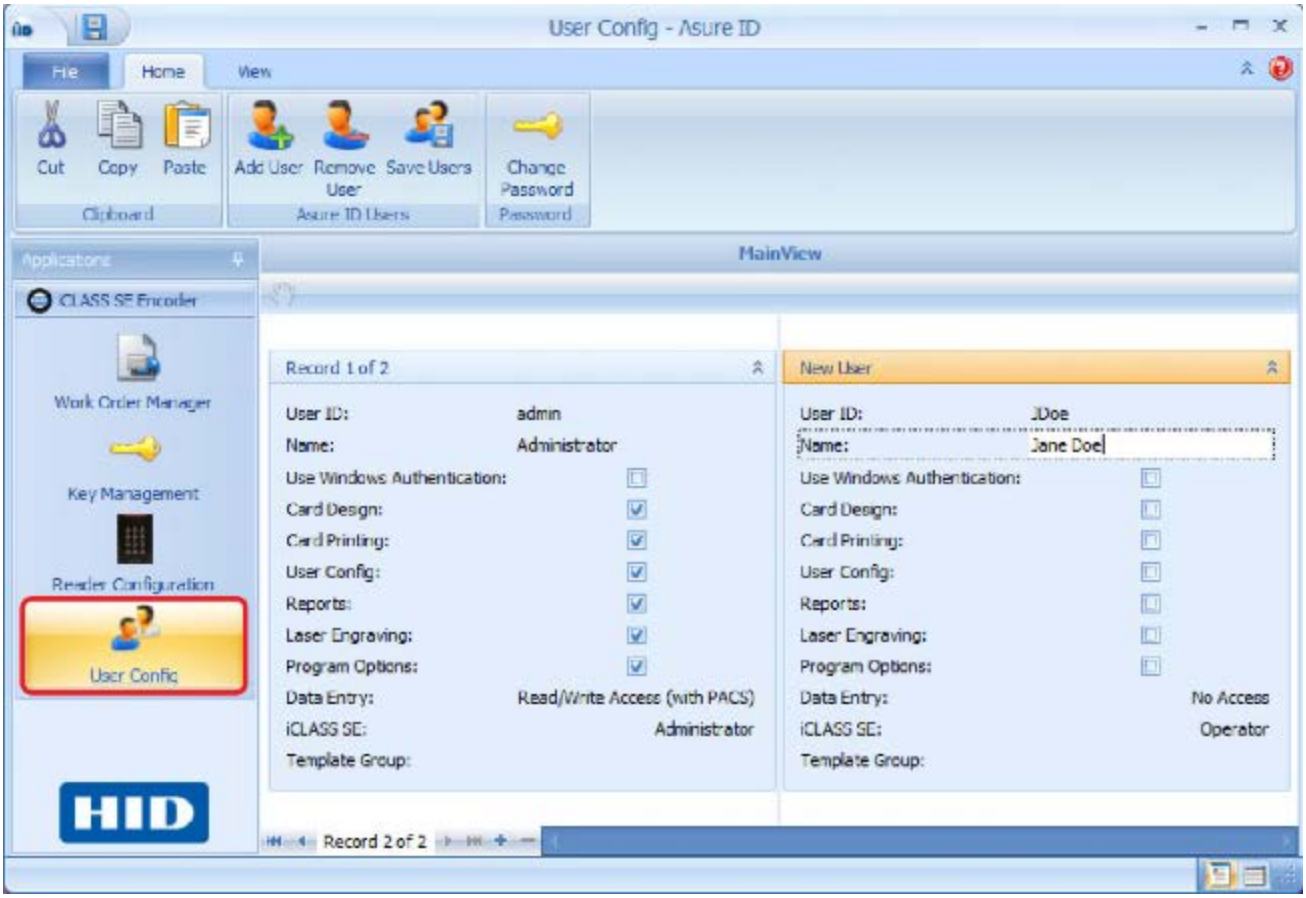
2.4 Reader Configuration module

The Reader Configuration window is used to create the Reader Data configuration cards (for both keys and reader limited settings) The application allows you to change the keys or behavior of a Reader.



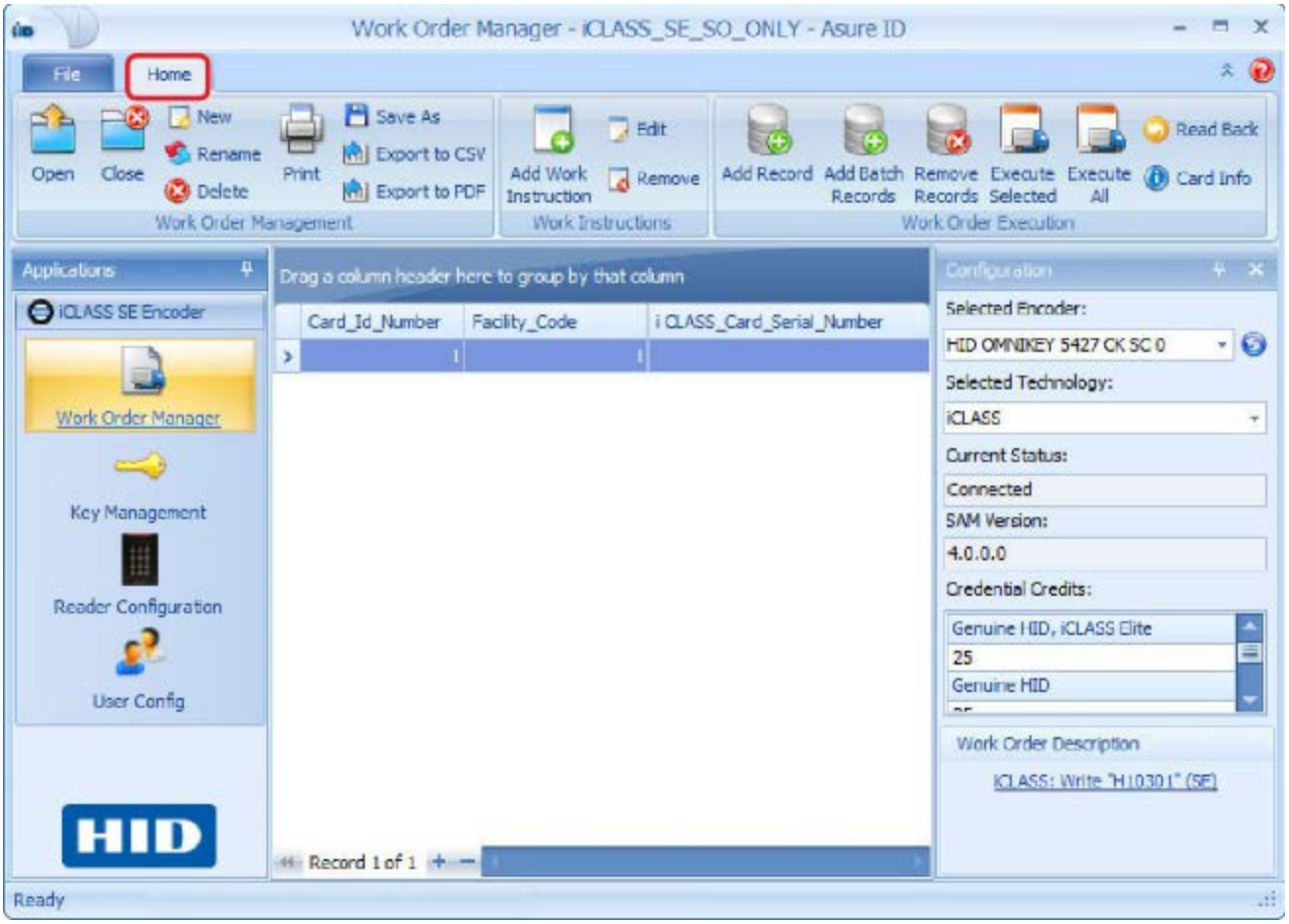
2.5 User Config module

The User Config module allows the administrator to create users for Asure ID and to set the functions each user can access in the application. The Administrator can Add User, Remove User, Save Users and Change Passwords.



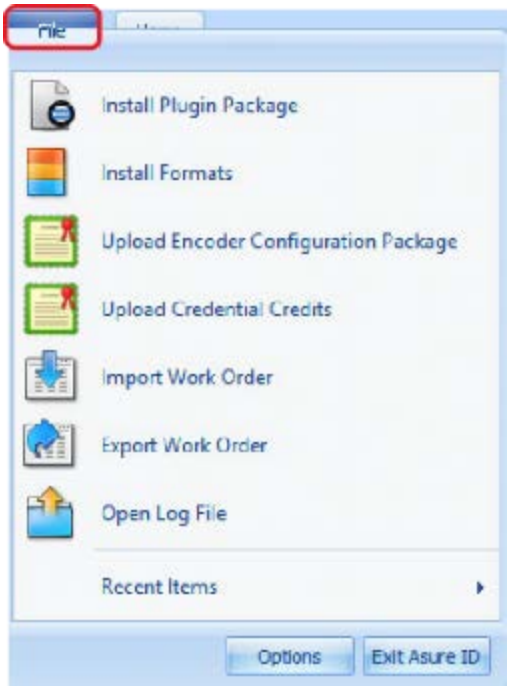
2.6 Home tab

The **Home** tab allows configuration and implementation of the iCLASS SE Desktop Encoder. See the **Work Order Manager**, **Key Management**, **Reader configuration**, and **User Config module** sections for information on each of these **Home** tabs.



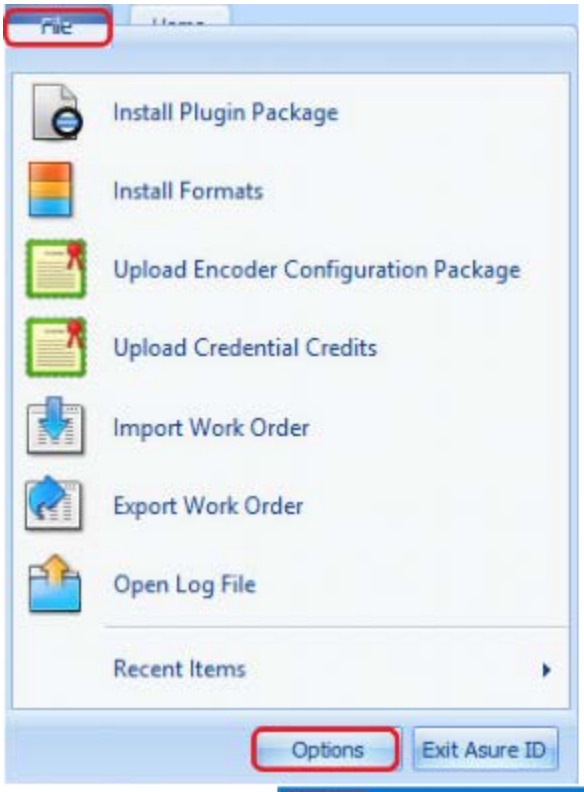
2.7 File tab

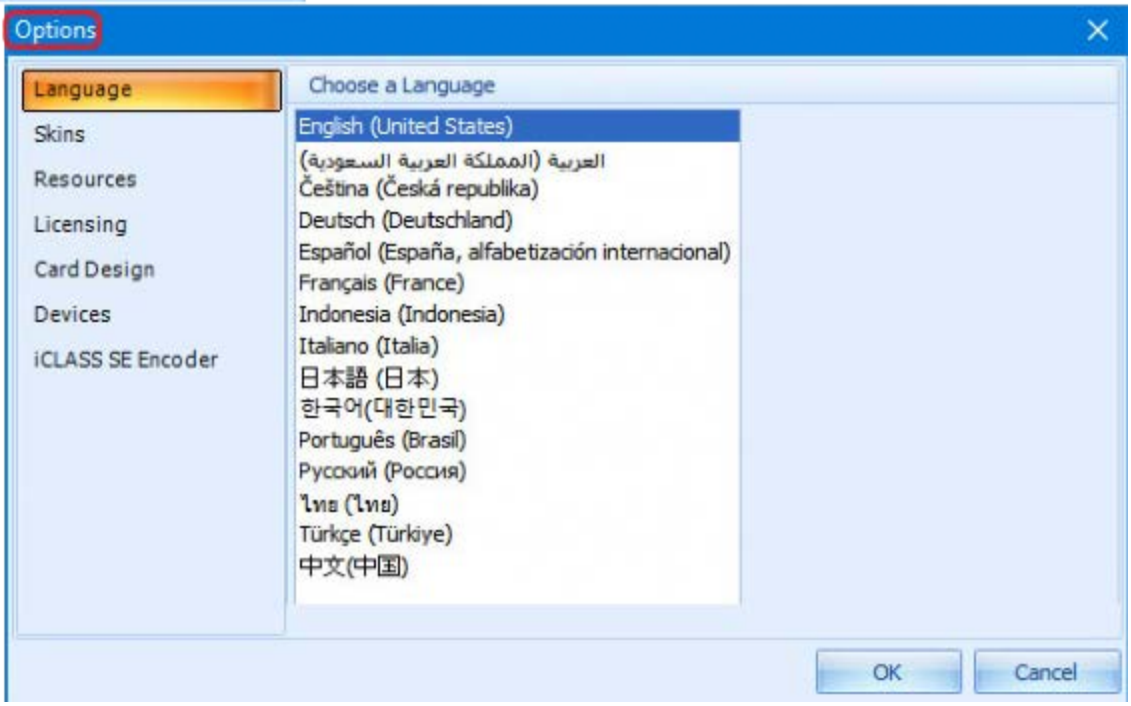
The **File** tab contains specific options depending on which Application Module is selected. See the **Work Order Manager**, **Key Management**, **Reader configuration**, and **User Config module** sections for information on each of these **File** tabs.



2.8 Options window

The **Options** window is available on every **File** tab, and allows you to manage the iCLASS SE Encoder Formats, Plugins, Database, Options and User Options.





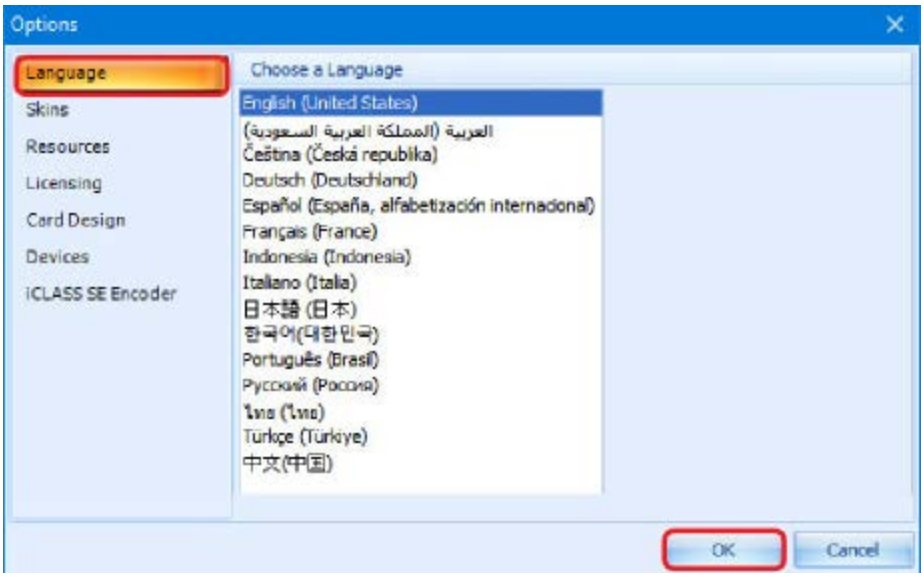
2.9 Language options

Asure ID allows you to set the default language of the application. Available languages are:

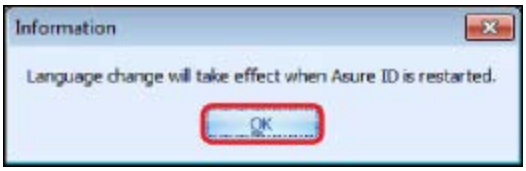
- English
- Indonesian
- Spanish
- Arabic
- Italian
- Thai
- Chinese
- Japanese
- Turkish
- Czech
- Korean
- French
- Portuguese
- German
- Russian

To set the default language of the application:

1. From the **Language** option, select a language from the list.
2. Click **OK**.



3. An **Information** window is displayed with a message that the language change occurs after Asure ID is restarted. Click **OK**.



4. Restart the application.

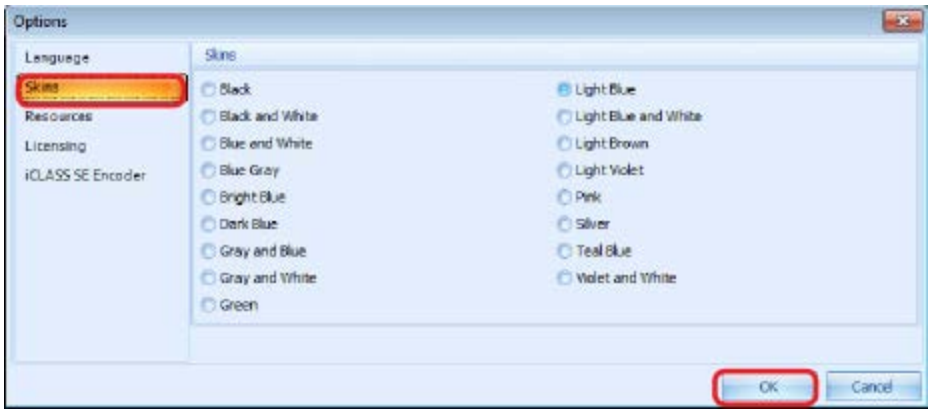
2.10 Skins options

Asure ID allows you to customize the look of the Asure ID application by selecting a predefined skin.

1. From the **Skins** options, select a Skin from the list.

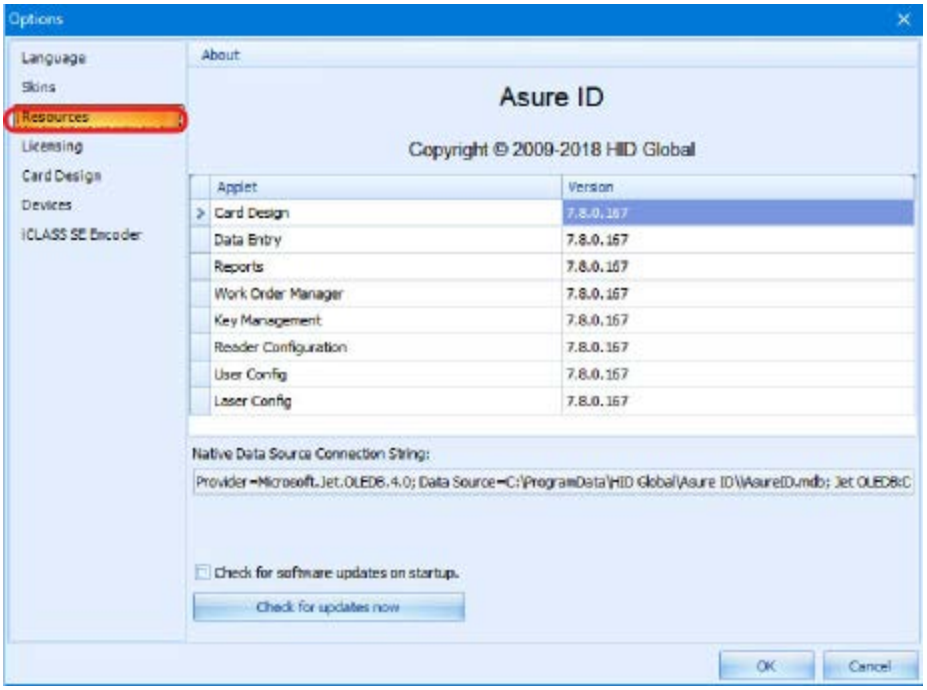
   > **Note:** The change is immediately visible.

2. Click **OK**.



2.11 Resources options

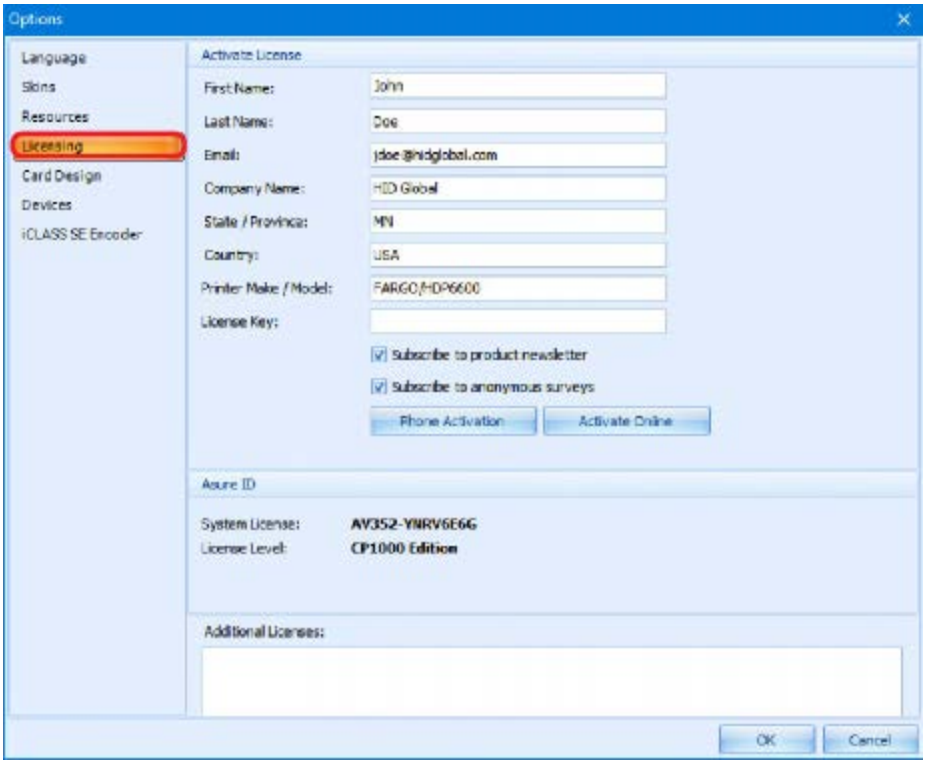
Asure ID allows you to access resource information for the application.



Field	Description
About	Displays the current applets loaded and their version.
Native Data Source Connection String	This is the connection string used to connect to the native Data Source. It contains location and connection information.
Check for software updates	This option directs the software to check for updates when launched.
Check for updates now	This button checks for software updates immediately. • If changes are required, follow the instructions on the installation wizard. • If changes are not required, a message indicating that the software is up to date is displayed.

2.12 Licensing options

Asure ID allows you to view, modify and activate the licensing information of the Asure ID application. To activate the License Key, enter the information listed below and click an activation button.



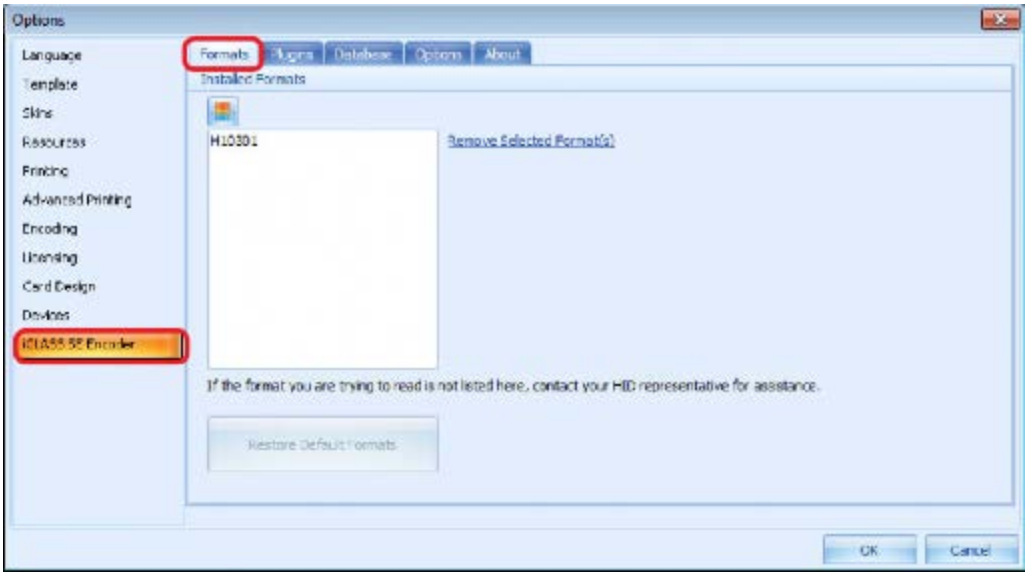
Field	Description
Activate License	
First Name	Enter the first name as it appears in the HID license.
Last Name	Enter the Last Name as it appears in the HID license
Email	Enter a valid email address that can obtain messages about licenses and accounts.
Company Name	Enter the Company Name.
Field	Description
State/Province	Enter the State or Province where the Company is located.
Country	Enter the name of the Country where the Company is location.
Printer Make/Model	Enter the printer (or Encoder) make and model.
License Key	Enter the License Key for Asure ID received from HID Global.
Subscribe to product newsletter	Select the check box to subscribe to Asure ID product newsletters.
Subscribe to anonymous surveys	Select the check box to subscribe to surveys.
Phone Activation	This option displays an Activate Offline window that provides HID Global contact information to activate the software. This window displays an Offline Request Key that you submit to the HID Global contact. An Offline Response Key is given to you to enter and Submit in the window.
Activate Online	This option requires an Internet connection and completely activates the license on this device.

Field	Description
Asure ID	
System License	Displays the License Key activated for your information listed above.
License Level	Displays the license level for the activated license key.
Additional Licenses	Additional license keys can be viewable if HID Global support has directed you to install additional license keys.

2.13 iCLASS SE Encoder options

This option allows you to modify iCLASS SE Encoder options on the Asure ID application.

Note: This option has multiple tabs for configuration. See the following sections for details.



2.13.1 iCLASS SE Encoder Formats tab

The iCLASS SE Encoder includes a format interpreter capable of interpreting all open and custom formats developed and maintained by HID Global. Formats must be ordered from Customer Service, as formats are custom to a specific OEM or end user, and not freely distributed.

The **Formats** tab (see graphic above) lists the formats Installed on an Encoder. The default format, delivered with Asure ID is H10301. Contact a HID Global representative for assistance if additional formats are required.

Field	Description
Installed Formats	
	Select the Install Format icon, to select and install an .EFI format file that was ordered and provided by HID Global.
Remove Selected Format(s)	This option removes the selected Format from the list of available formats.
Restore Default Formats	This option allows you to restore a default Format that may have been removed from the list.

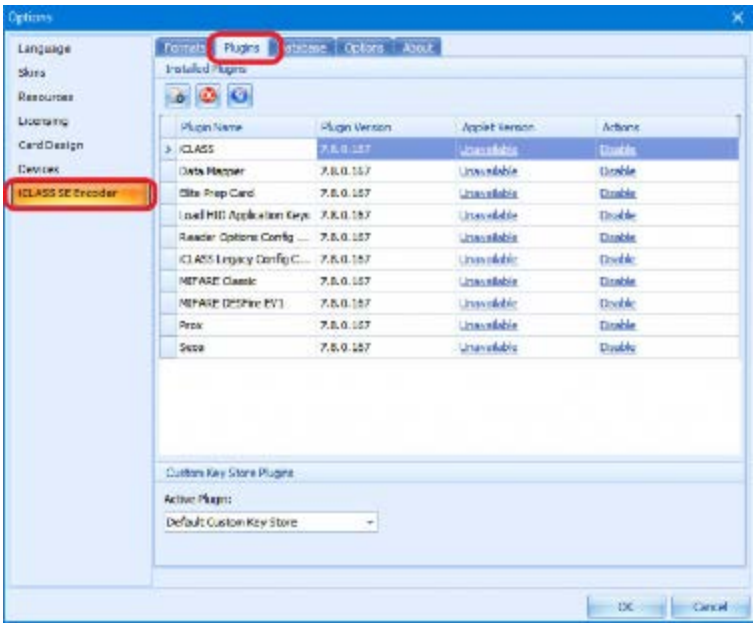
2.13.2 iCLASS SE Encoder Plugins tab

Each plugin used by the iCLASS SE Encoder is digitally signed by a key managed by HID and known by all encoders. Only Genuine HID plugins are recognized by the encoder. Initially, one plugin is created for each supported card type (iCLASS, MIFARE Classic, MIFARE DESFire EVI, Prox and Seos.

Plugins automatically install or refresh when Asure ID is started. Although additional plugins can be installed, you can not delete the plugins installed by default. These plugins can only be Disabled or Enabled.

> **Note:** Disabling unused plugins may increase the overall performance of the Work Order Manager and Reader Configurations within Asure ID.

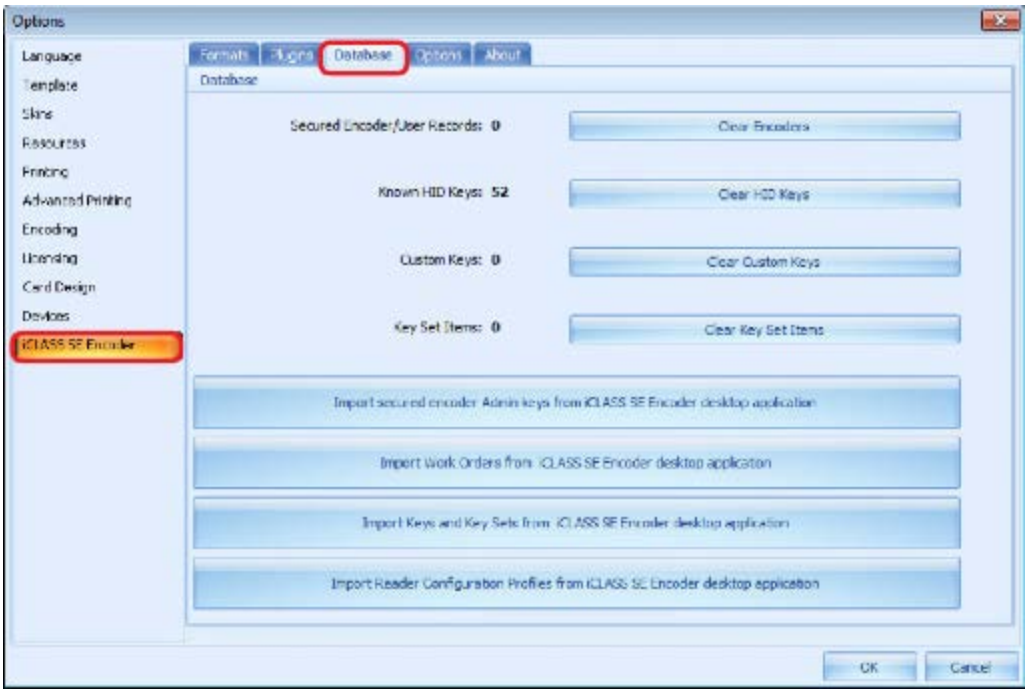
The **Plugins** tab lists the plugins currently installed, the version number, the Applet version, and whether the Applet is enabled or disabled.



Field	Description
In addition to viewing the installed plugins, you can perform the following tasks:	
	Install Plugin. Browses for a plugin from HID Global and installs the file.
	Delete Applet. Clears all applet .dll files from the SAM. These applets are uploaded automatically on an as-needed basis when required for an encoding operation.
	Refresh Plugin View.
Custom Key Store Plugins	Active Plugin: Allows you to develop a module for encrypting custom keys and how custom keys are imported and exported.

2.13.3 iCLASS SE Encoder Database tab

The **Database** tab displays information stored in the Asure ID database for the iCLASS SE Encoder. The Database window allows you to view and manage records and keys.

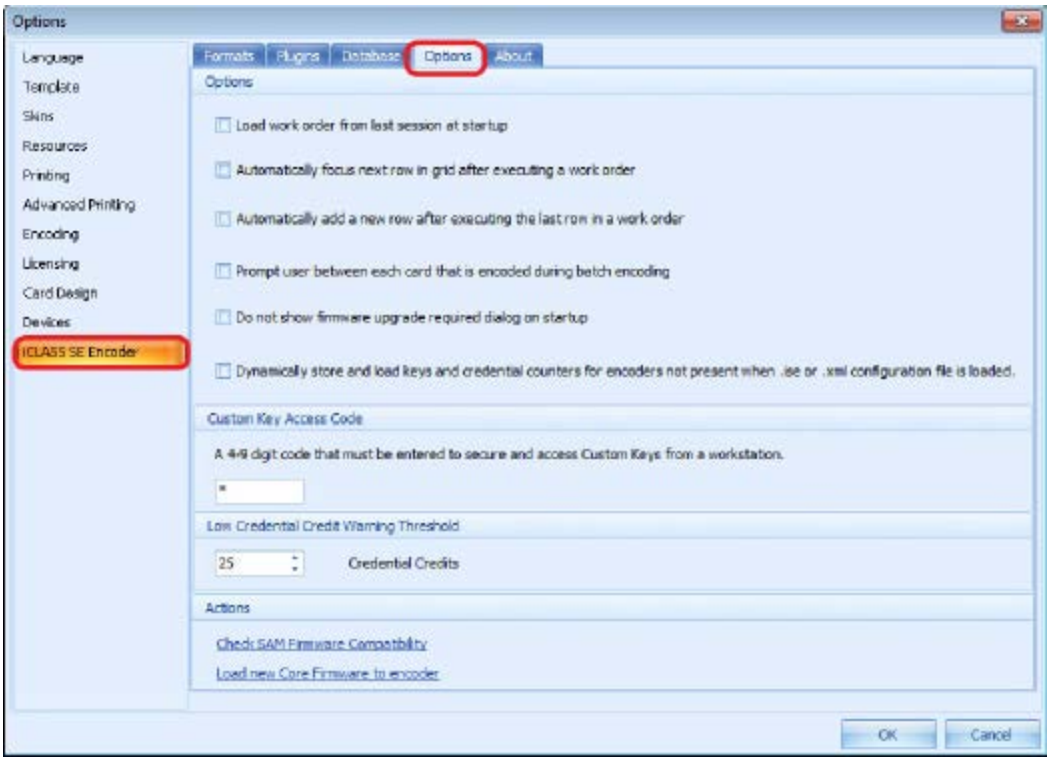


Field	Description
Secure Encoder/User Records	Displays the number of iCLASS SE Encoder/User Records. **Clear Encoders**: Removes all Encoders (and admin keys) from the database. **Important: Admin Keys must be re-entered to retain access to credentials and credits on the encoder.**
Known HID Keys	Displays the number of known HID Keys loaded on the database. **Clear HID Keys**: Deletes all HID Keys from the database. Keys require reloading in Key Management. **Note:** These keys are not deleted from the currently active encoder.
Custom Keys	Lists the number of custom keys that are on the database. **Clear Custom Keys**: Deletes all Customer Keys from the database. **Note:** These keys are not deleted from the currently active encoder.
Key Set Items	Lists the number of Key sets. **Clear Key Set Items**: Deletes all Key Sets.
Import secured encoder Admin keys from iCLASS SE desktop application	The iCLASS SE Encoder is secured on a per user basis with Admin Keys. This option allows these Secure Admin Keys to be imported to allow the specific credential, keys, etc. to be moved from the original iCLASS SE Encoder Desktop application (version 2.3.6.8 or 2.4.0.10) into Asure ID. **Note:** The importer uses the current Asure ID user name and password to decrypt the admin Keys. If the passwords are different, you are prompted to enter the old password from the iCLASS SE Encoder Desktop software.

Field	Description
Import Work Orders from iCLASS SE desktop application	HID Work Orders can be imported from the original iCLASS SE desktop application (version 2.3.6.8 or 2.4.0.10). Asure ID automates the importing of these (non-encrypted) items.
Import Keys and Key Sets from iCLASS SE desktop application	Custom Keys and Key Sets can be imported from the original iCLASS SE desktop application (version 2.3.6.8 or 2.4.0.10).
Import Reader Configuration Profiles from iCLASS SE Encoder desktop application	Import saved profiles created in the original iCLASS SE Encoder desktop application Reader Configuration application.

2.13.4 iCLASS SE Encoder Options tab

The **Options** tab contains basic configuration options, along with the option of checking the SAM Firmware compatibility.

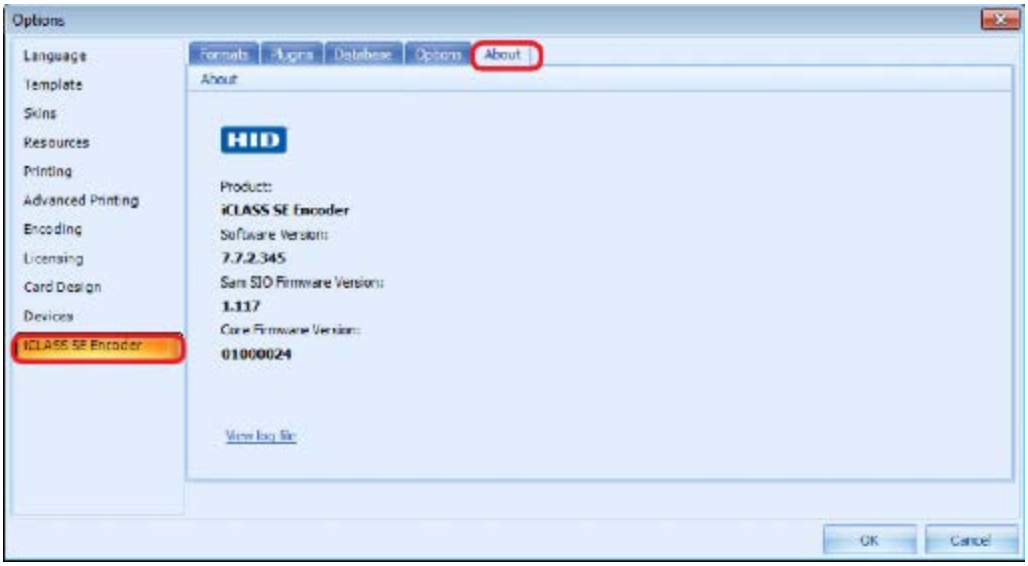


Field	Description
Options	You can set several basic configuration options, select all that are needed: • Load work order from last session at startup • Automatically focus next row in grid after executing a work order • Automatically add a new row after executing the last row in a work order • Prompt user between each credential that is encoded during batch encoding • Do not show firmware upgrade required dialog on startup • Dynamically store and load keys and credential counters for encoders not present when .ise or .xml configuration file is loaded.
Custom Key Access Code	You must enter the 4-9 digit code to securely access the Custom Keys from a workstation. This code should be the same across all workstations where custom keys are automatically synchronized. **Note:** The SNMP encoder Admin keys must also match on all workstations where custom keys are automatically synchronized.
Low Credential Credit Warning Threshold	Sets the minimum threshold for consumed printing/encoding credits. A warning is issued when the threshold is reached after an encoding operation is performed in the Work Order Manager. The default minimum threshold is 25.

Field	Description
Actions	**Check SAM Firmware Compatibility**: Allows you to check and upgrade the SAM firmware version. When the desktop application is launched, it checks for the current SDK version of the encoder device. If the SDK detected on the encoder is too old, the desktop application boot loads the version of the SDK that is built into the assembly file to ensure compatibility. A message is displayed if the firmware is up to date. **Note:** If the detected version is too new, you are directed to the HID support site to download the latest version of the software. It cannot downgrade an encoder. **Load new Core Firmware to encoder**: Allows you to upgrade the core firmware (.fw file) on an iCLASS SE Encoder.

2.13.5 iCLASS SE Encoder About tab

The **About** tab is displayed with the current application information.



Section 03

Setup and configuration

3.1 Introduction

The following setup and configuration instructions are for the iCLASS SE Encoder Desktop application.

3.2 System requirements

Type	Microsoft Windows 10 (32-bit and 64-bit) Microsoft Windows 8.1 (32-bit and 64-bit) Microsoft Windows 8 (32-bit and 64-bit) Microsoft Windows 7 (32-bit and 64-bit)
Computer/Processor	1 GHz or higher Pentium-compatible CPU USB Ports
Memory	64-bit systems: 2 GB RAM 32-bit systems: 1 GB RAM or higher
Hard Disk	1 GB free space
Display	VGA or higher resolution monitor
Software Environment	Latest Operating System service pack
User Permissions	Local machine administrative rights for iCLASS installation and secure database administration Internet access for license activation or phone for phone activation

3.3 Administrative privileges

You must have Administrator privileges to complete the Installation and Startup procedures. To verify you are an Administrator on your computer:

1. Go to **Control Panel** > **User Accounts** > **Manage User Accounts**.
2. Under Users for the computer, locate your User Name and verify the associated Group column displays **Administrators**.

3.4 Getting started

3.4.1 Administrative privileges

You must have Administrator privileges to complete the Installation and Startup procedures. To verify you are an Administrator on the system:

1. Go to **Control Panel** > **User Accounts** > **Manage User Accounts**.
2. Under **Users for this computer**, locate your **User Name** and verify the associated Group column displays Administrators.

3.4.2 Initial setup

1. Plug in the CP1000 Desktop Encoder to a USB port on your PC.
2. Plug in the HID USB Flash Drive to a 2nd USB port on your PC.
3. From the USB flash drive, install the **Asure_ID_Setup** application file located in the **Install** folder. Follow the Installation Wizard to install the application. If prompted, allow the application to make changes to the computer.
4. Launch the Asure ID application and perform the configuration tasks.

Note:
Log on credentials: Username: **admin** Password: **admin**.

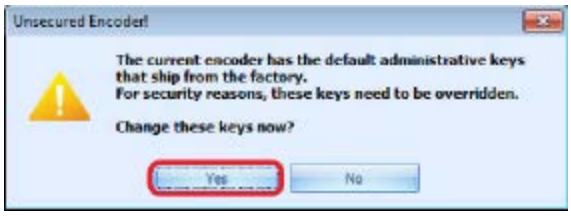
A Windows error may appear indicating that not all of the all drivers were installed correctly. This is expected as the encoder has a chip that appears as a smart card and if **Smart Card PnP** is enabled, Windows tries to locate a driver for this chip which cannot be located.

3.5 Initial configuration

3.5.1 Change default administrative keys

It is important to change the default Administrative Keys during initial setup for security reasons.

1. During the initial installation, the **Unsecured Encoder!** window is displayed, click **Yes** to change the keys.



2. The **Provide New Admin Keys for Encoder** window is displayed. This window gives three different options for changing the default Admin Keys:
   - **Manual Entry** – this option allows you to move information from a previous encoder, or enter customer created keys. Manually enter your Admin Keys in the **Auth Key**, **Privacy Key**, and **Secure Channel Key** fields and click **OK** to confirm.

     > **Note:** Admin Keys must contain 32 characters.

   - **Randomly Generated Keys** – this option generates random keys. Click **Generate Random Keys** to have the software randomly generate keys. Click **OK** to confirm.

- **Passphrase Generated Keys** – this option allows you to enter a memorable passphrase (minimum of five characters). The software then generates keys based on the passphrase. Enter your passphrase in the **Passphrase** field and click **Generate Keys From Passphrase**. Click **OK** to confirm.

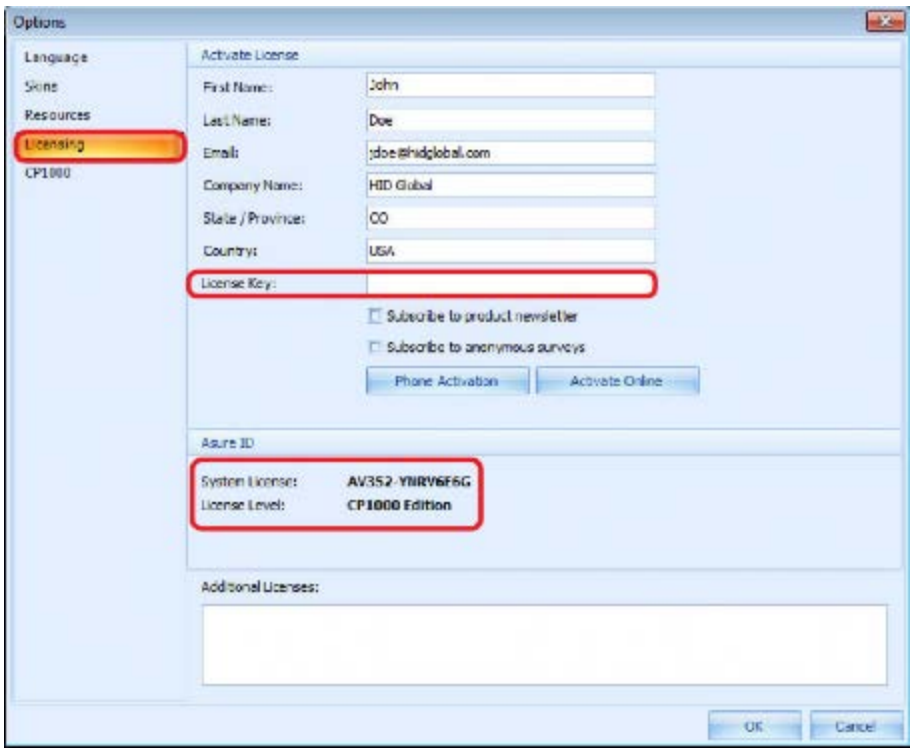
3. A message is displayed prompting you to make a backup copy of your new Admin Keys. Click **Yes** to copy the new Admin Keys to the clipboard.

> **Important: Safely store the value of the admin keys for future reference as HID is unable to recover these keys if lost. If the admin keys are lost, the encoder needs to be sent to HID to be reset.**

3.5.2 Enter the Asure ID CP1000 Edition license key

The Asure ID CP1000 Edition License Key is **AV352-YNRV6E6G**. The Admin password should be modified from the default values for security reasons.

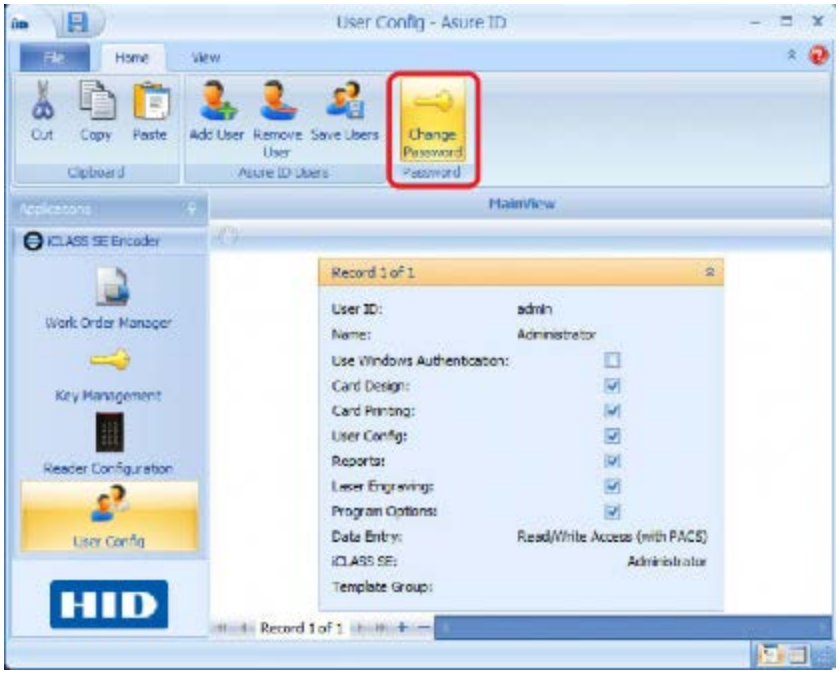
1. Select **Work Order Manager** > **File** tab > **Options**.
2. Select the **Licensing** option.
3. Enter the License Key **AV352-YNRV6E6G** and click your activation option.
4. When the License Key is activated, the CP1000 Edition is displayed as shown.



3.5.3 Change default Admin password

The Admin password should be modified from the default values for security reasons.

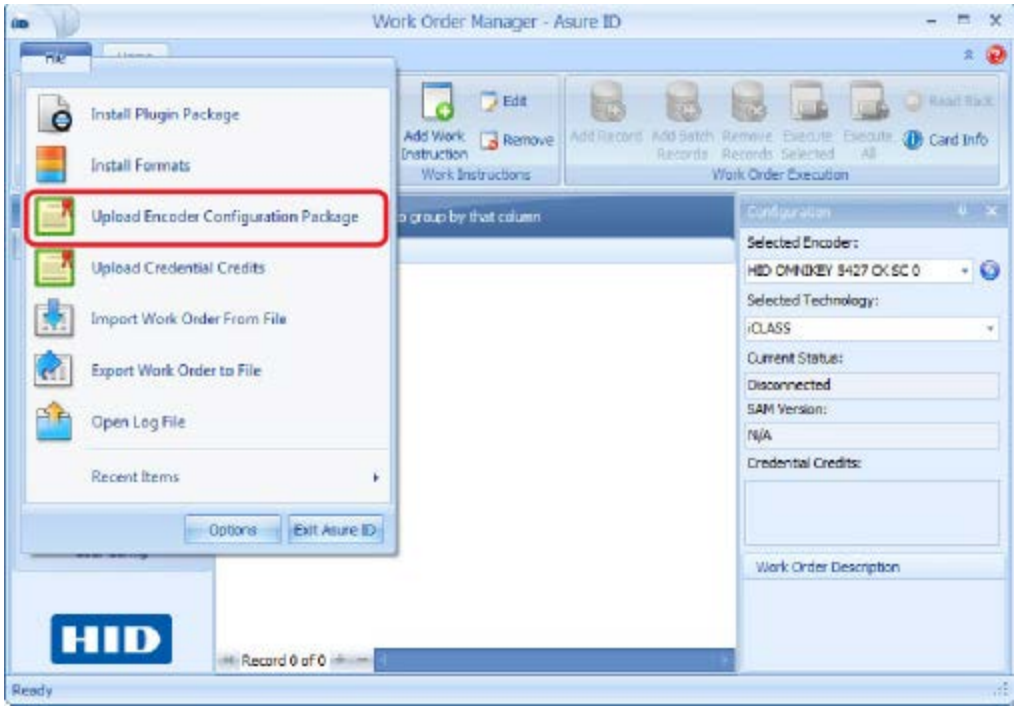
1. Select **User Config** > **Home** tab > **Change Password**.
2. Enter new and confirm password. Click **OK**.



3.5.4 Upload encoder configuration package

The following steps load the required files (on the USB flash drive) on the CP1000 Desktop Encoder.

1. Go to **Work Order Manager** > **File** tab > **Upload Encoder Configuration Package**.
2. Locate the **Credits and Keys** folder, on the USB Flash drive. Load the .ise file included on the USB Flash drive.



3.6 Change default Admin password

The Admin password must be modified from the default values immediately (Username: **admin**, Password: **admin**). For security reasons, this access should not be left on the application.

> **Important: When creating, a new Admin user, or changing an Admin password, it is important that this password is saved in a secure location. At this time there is no password reset feature in place.**

See **9.8 Change password** for detailed information on modifying the default Admin password.

3.7 Add system users

See **9.5 Add a user** for detailed information on User Management and adding users.

> **Important: When creating a new Admin user, or changing an Admin password, it is important that this password is saved in a secure location. At this time there is no password reset feature in place.**

Section 04

Initial configuration (startup)

4.1 Introduction

This User Guide is specific to the iCLASS SE CP 1000 Desktop Encoder. The following sections cover the initial configuration of the iCLASS SE Desktop Encoder.

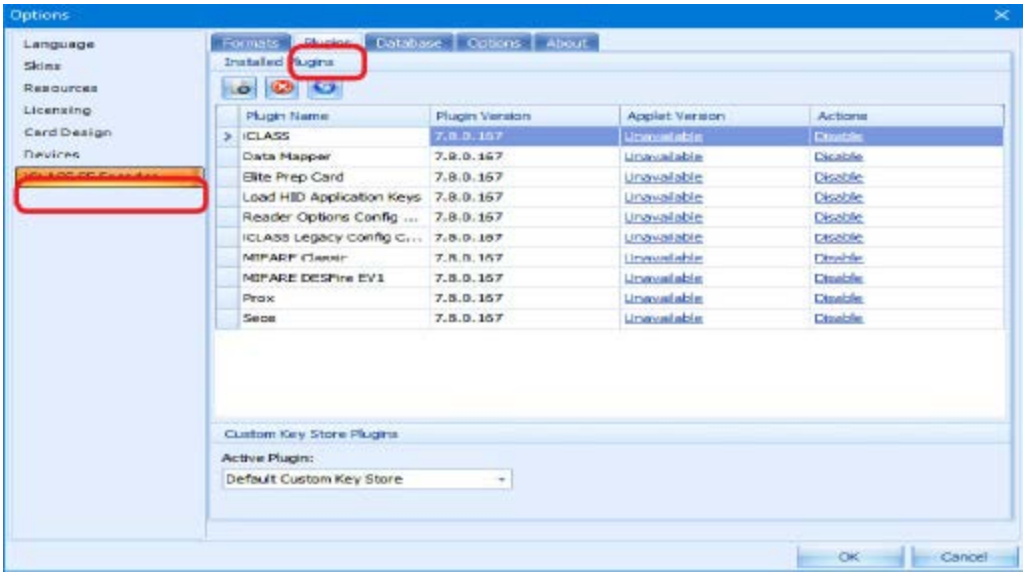
4.2 Plugin package

A plugin package configures both the iCLASS SE desktop software and the encoder for the type of technology being used (for example iCLASS). This installation package contains all the counters, configuration, format and key files necessary to execute work orders for various technologies.

Plugins initially provided include:

- iCLASS
- MIFARE Classic
- Data Mapper
- MIFARE DESFire EV1
- Elite Prep Card
- Prox
- Load HID Application Keys
- Seos
- iCLASS Legacy Config Card

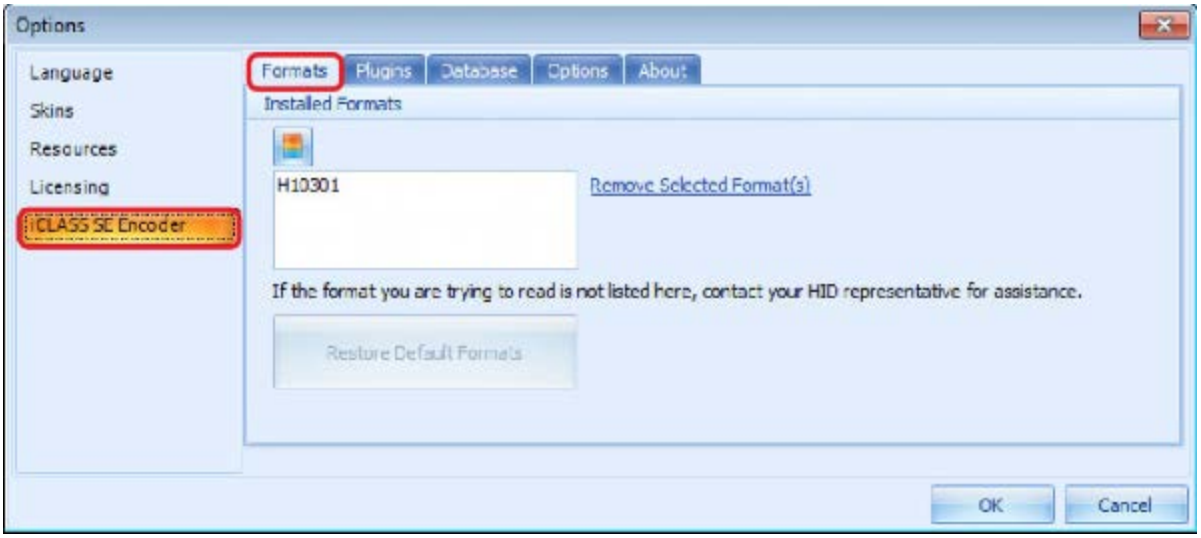
During initial installation, all required plugins are installed. By default, the iCLASS SE Encoder Kit ships with standard keys and a small number of credits to get started. See **2.13.2 iCLASS SE Encoder Plugins tab** for more information on plugins.



4.3 Formats

HID programs thousands of formats used in the security business. Every format has a name and a number. A format describes how a credential is to be constructed and deciphered (for example: the number of data fields, size, legal value ranges, and how they are constructed when written to a card).

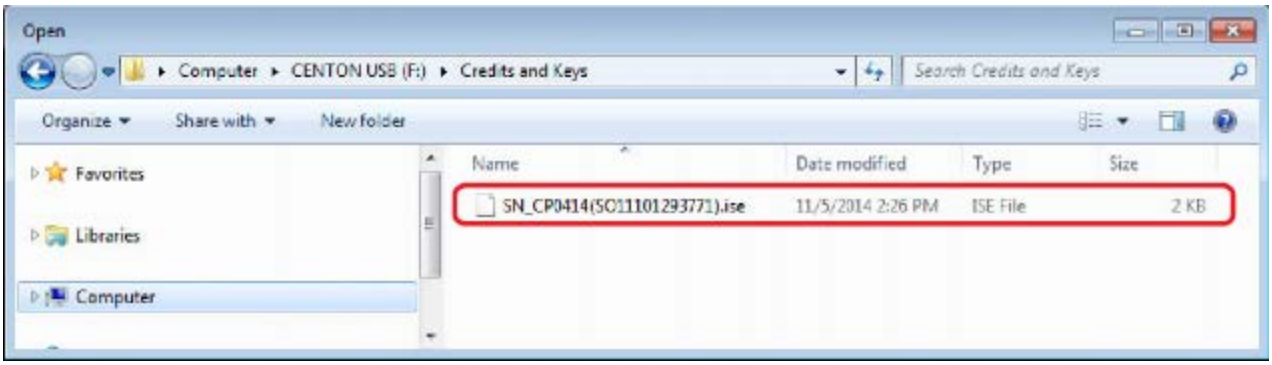
The application is provided with a default format of H10301. If an additional/different format is required, contact an HID Global representative for assistance. To install a format file, follow the steps listed in **2.13.1 iCLASS SE Encoder Formats tab**.



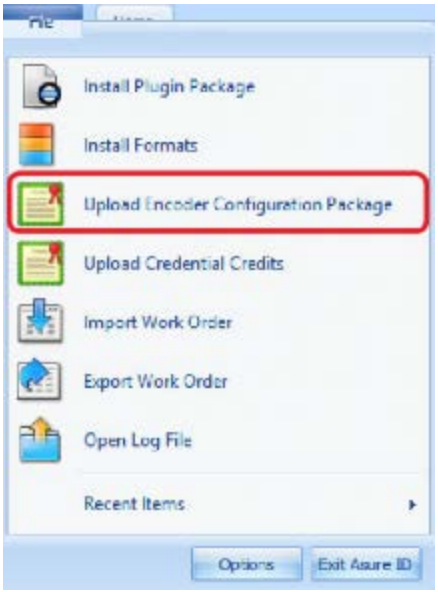
4.4 Upload encoder configuration package

The Credential Credits and Keys are delivered on the USB Flash drive in the **Credits and Keys** folder. However, when additional credits are required they are ordered from HID Global.

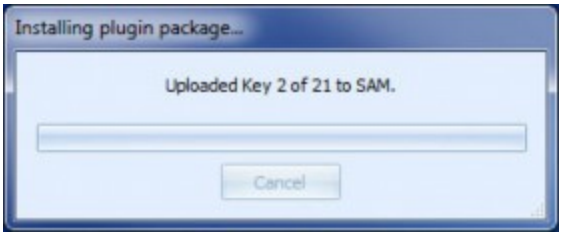
> **Note:** Credential Credits and/or Keys can be received as a single .ise from HID Global. See **7.8 Load HID keys** for information on loading these files.



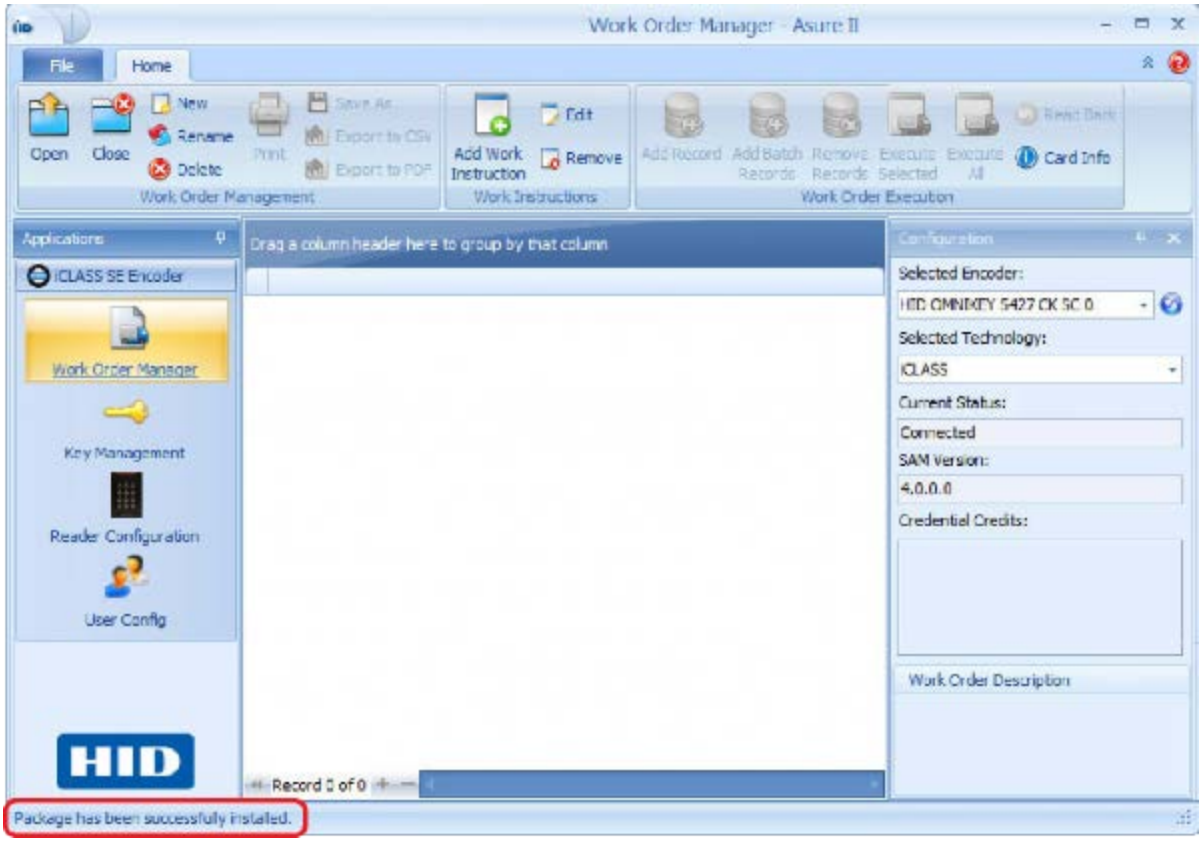
1. Select **Work Order Manager** > **File** tab > **Upload Encoder Configuration Package**.



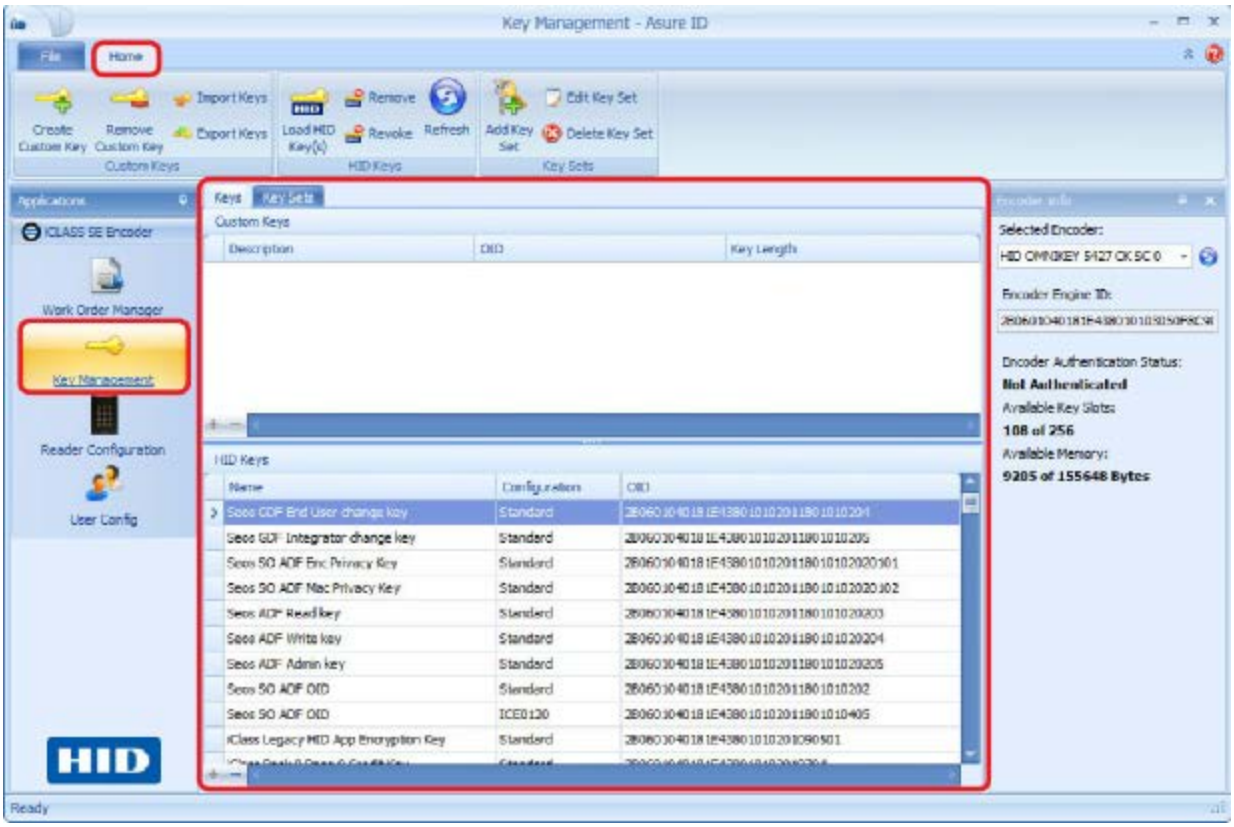
2. Browse to the **iCLASS SE Encoder File** (.ise file) provided by HID Global.
3. Double-click the file to be loaded or select the file and click **Open**.
4. The software updates the keys and key sets. A progress bar is displayed as the keys and credits are loaded.



5. When successfully loaded, the message **Package has been successfully installed** appears at the bottom of the window.

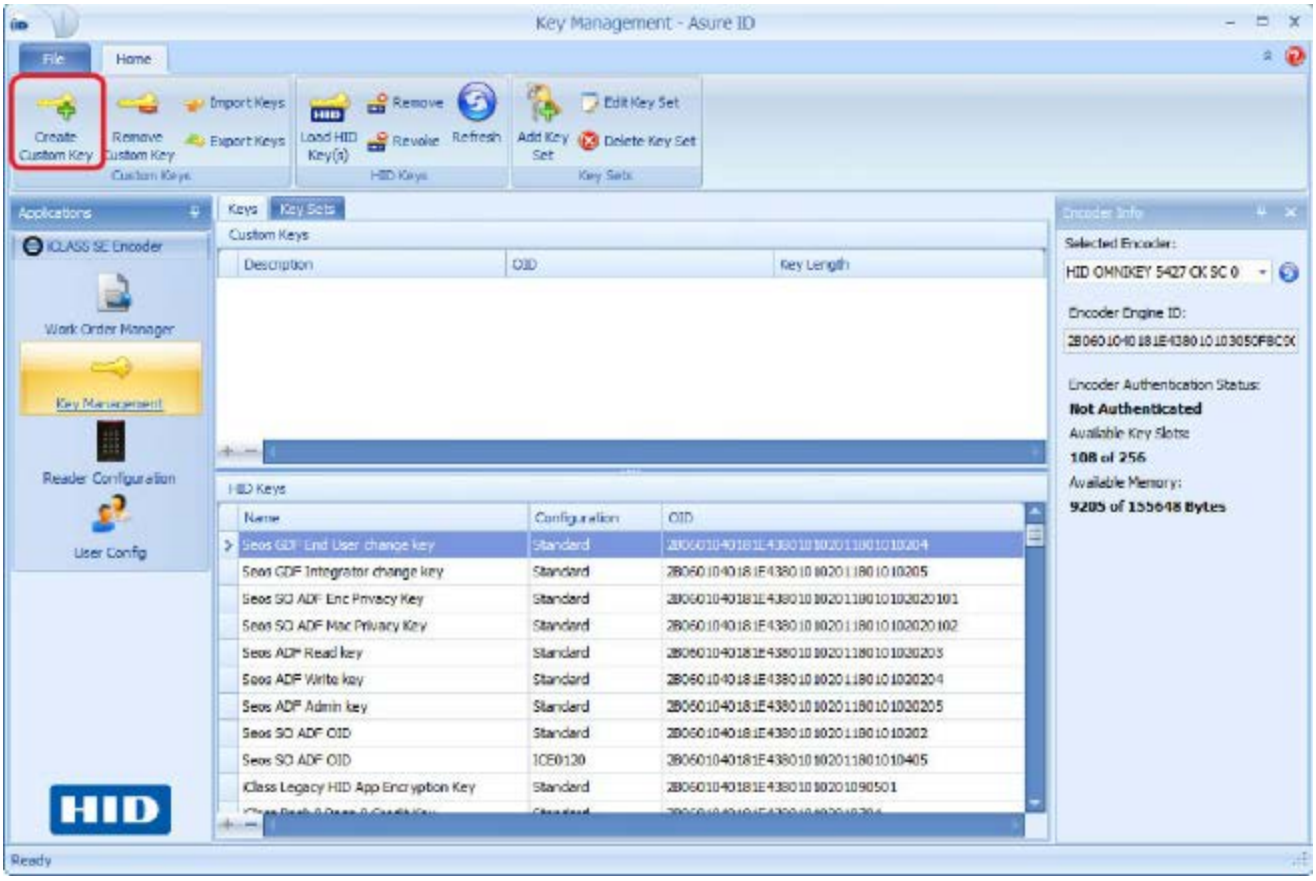


After the upload is complete, the installed package contents are displayed on the **Key Management** > **Keys** tab pane.


Key Management - Asure ID
File
Home
Import Keys
Export Keys
Create Custom Key
Remove Custom Key
Custom Keys
Load HID Key(s)
Remove
Revoke
Refresh
HID Keys
Add Key Set
Edit Key Set
Delete Key Set
Key Sets
Applications
iCLASS SE Encoder
Work Order Manager
Key Management
Reader Configuration
User Config
Keys
Key Sets
Custom Keys
Description
OID
Key Length
HID Keys
Name
Configuration
OID
Seos GDF End User change key
Standard
Seos GDF Integrator change key
Standard
Seos SO ADF Enc Privacy Key
Standard
Seos SO ADF Mac Privacy Key
Standard
Seos ADF Read key
Standard
Seos ADF Write key
Standard
Seos ADF Admin key
Standard
Seos SO ADF OID
Standard
Seos SO ADF OID
ICE0120
iClass Legacy HID App Encryption Key
Standard
Selected Encoder:
HID OMNIKEY 5427 CK SC 0
Encoder Engine ID:
Encoder Authentication Status:
Not Authenticated
Available Key Slots:
108 of 256
Available Memory:
9205 of 155648 Bytes
Ready

4.5 Custom keys

The initial package provided to the customer includes a limited number of credentials to get you started. Custom Keys are created from the Key Management application.



For information on Creating Custom Keys, see **7.2.1 Key Management toolbar**.

Section 05

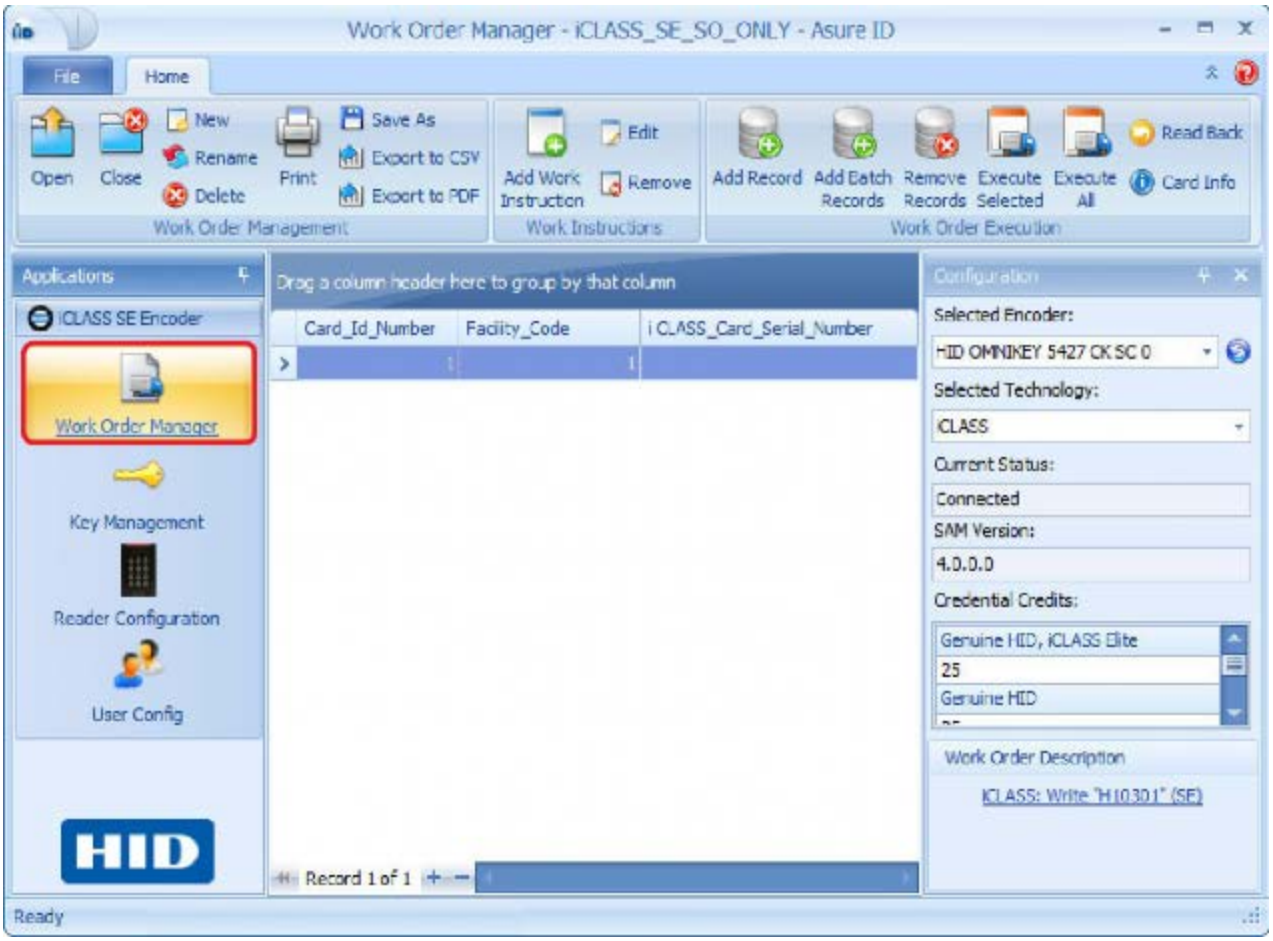
Work Order Manager

5.1 Introduction

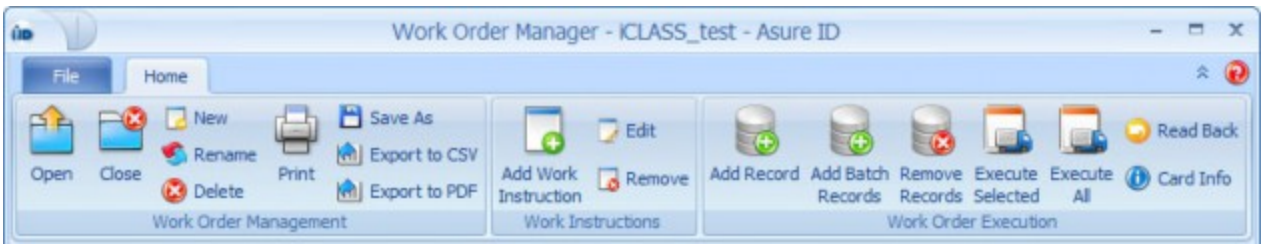
The Work Order Manager module allows you to create, manage and execute Work Orders.

5.2 Work Order Manager Home tab

The Work Order Manager Home window contains the following areas.



5.2.1 Work Order Manager toolbar



Toolbar Function	Description
Open	Opens an existing Work Order. See 5.4 Open a work order.
Close	Closes the current Work Order. See 5.5 Close a work order.

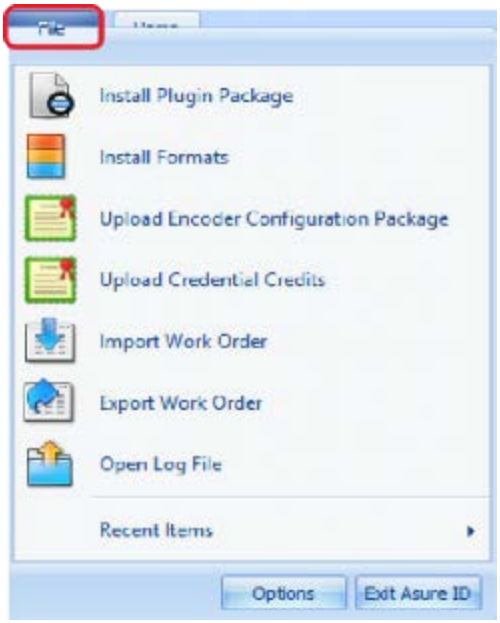
Toolbar Function	Description
New	Closes any currently open Work Order and opens the Work Instruction Wizard to create a Work Order. See 5.6 Create a work order.
Rename	Renames an existing Work Order. The Manage Work Orders window appears. Select the correct work order and click Rename Work Order. See 5.7 Rename a work order.
Delete	Deletes an existing Work Order. See 5.8 Delete a work order.
Print	Prints the open Work Order. See 5.9 Print a work order.
Save As	Saves the open Work Order with a new name. See 5.10 File save as a work order.
Export to CSV	Exports the work order to a comma separated file. See 5.11 Export work order data to a CSV file.
Export to PDF	Exports the work order to a Adobe PDF file. See 5.12 Export work order data to a PDF file.
Add Work Instruction	Opens the Work Instruction Wizard to walk you through the creation of a Work Instruction. See 5.13 Add a work instruction to a work order.
Edit	Modifies an open Work Order as needed. See 5.14 Edit a work instruction.
Remove	Removes an open Work Order. See 5.15 Remove a work instruction.
Add Record	Adds a single record to the Work Order database. Each record added is a credential to be encoded with the Work Order. See 5.12 Export work order data to a PDF file. See 5.16.1 Add a credential record.
Add Batch Records	Adds a batch of records to be encoded with the Work Order database. See 5.16.2 Adding a batch of credential records.
Remove Records	Deletes one ore more Work Order records at a time. Shift + Click to select all records or Ctrl + Click to select individual records for removal. See 5.16.3 Removing records.
Execute Selected	Executes selected Work Order record. This allows you to select a record, and encode the work instructions. As each card is completed, the display for the credential record is grayed out and the serial number of the card is displayed in the column. With each encoding, the associated Credential Credits decreases by one. See 5.16.4 Execute a work order on selected credential records. **Note:** If there are not enough encoding credits for the process, a message is displayed. You need to contact HID Global and order more encoding credits.
Execute All	Executes all records in a Work Order. The system selects all records and encode. The process continues until all the credential records have been encoded. See 5.16.5 Execute a work order on all credential records.
Read Back	Reads back the card currently on the encoder and attempts to read a card and locate its corresponding record in the data of the current Work Order. An error message is displayed if the card information does not match that in the Work Order. See 5.16.1 Add a credential record. See 5.16.6 Read back.
Card Info	Reads the UID and memory configuration of the presented card. Place a card on the iCLASS SE Encoder, select the card technology type, then select this option. Note: Not all cards display the same information. In general the information is: • CSN - Card Serial Number • Card Type (for example, SO Only)

5.2.2 Work Order Manager Configuration pane

Field	Description
Selected Encoder	All available encoders are listed in the drop-down list. Click the **Refresh** to refresh the type of encoder.
Selected Technology	Displays all card technologies loaded on the encoder.
Current Status	Displays the status of the encoder.
SAM Version	Displays the current SAM firmware version.
Credential Credits	Displays all the credits loaded on the encoder.
Work Order Description	Displays each work instruction on the open Work Order.

5.3 Work Order Manager File tab

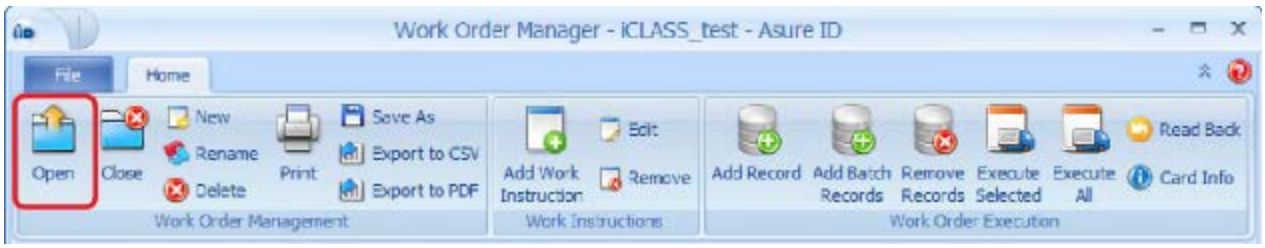
The **Work Order Manager File** tab contains specific options for this module.



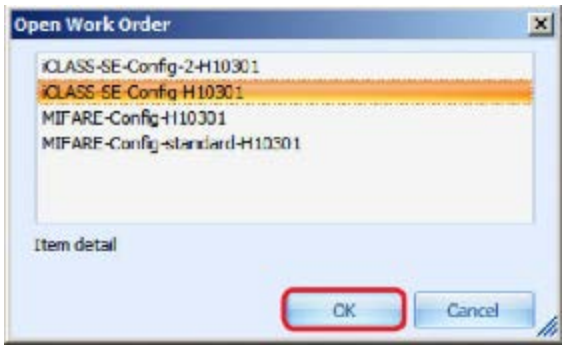
Option Function	Description
Install Plugin Package	A bundle of files that installs all the necessary plug-ins for the encoder.
Install Formats	Imports an encrypted file determining how a PACS credential is formatted. See 1.2.7 Formats.
Upload Encoder Configuration Package	Uploads credential credits and HID Keys on to the encoder. See 4.4 Upload encoder configuration package.
Upload Credential Credits	Allows the upload of Credential Credits (.xml and .ise) provided by HID Global.
Import Work Order	Allows you to upload a Work Order Export file (.xml) to Asure ID CP1000 Edition application. Can also import key sets and formats from .isx packages.
Export Work Order	Allows you to save a Work Order for backup and to upload the file at a later time.
Open Log File	Allows you to view the log file of events for the Asure ID CP1000 Edition application.
Recent Items	Displays the Recent Work Orders, for quick reference. Work Orders can quickly be opened by double-clicking a Work Order on the list
Options	See 2.8 Options window for detailed information.
Exit Asure ID	Logs the current user out and exits the application.

5.4 Open a work order

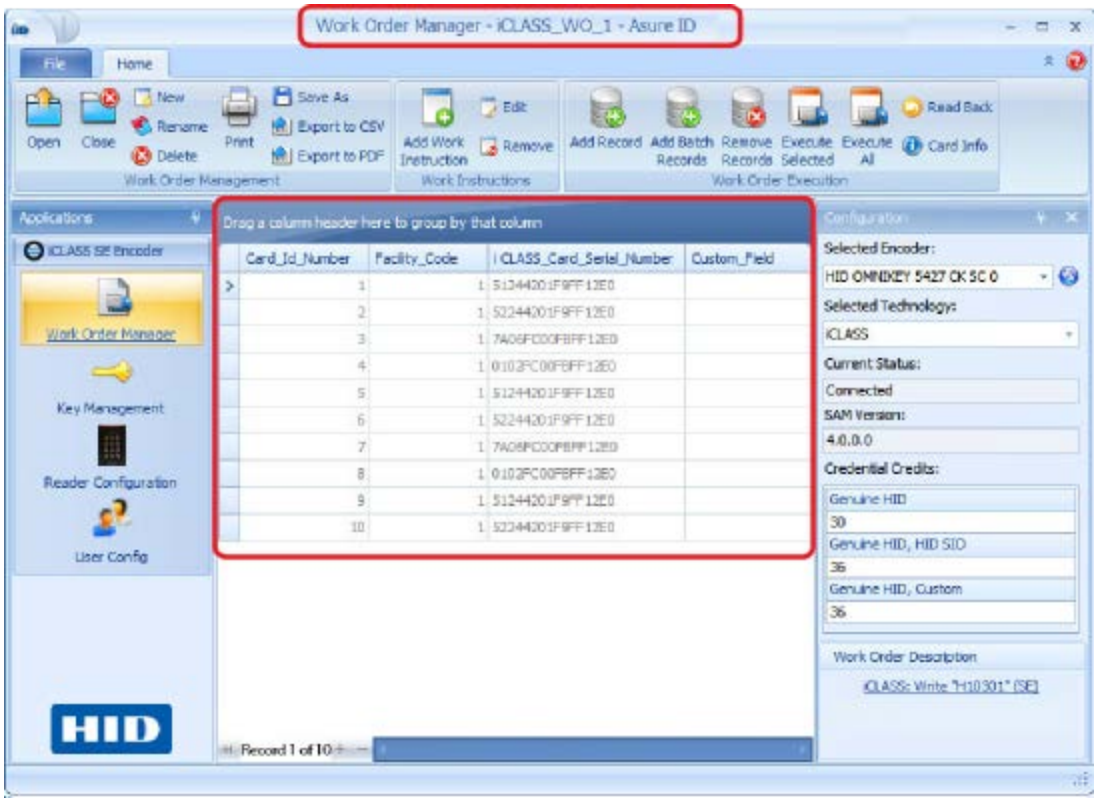
1. To Open an existing Work Order, select **Work Order Manager**.
2. Select **Open** from the toolbar.



3. Select a Work Order from the list, and click **OK**.

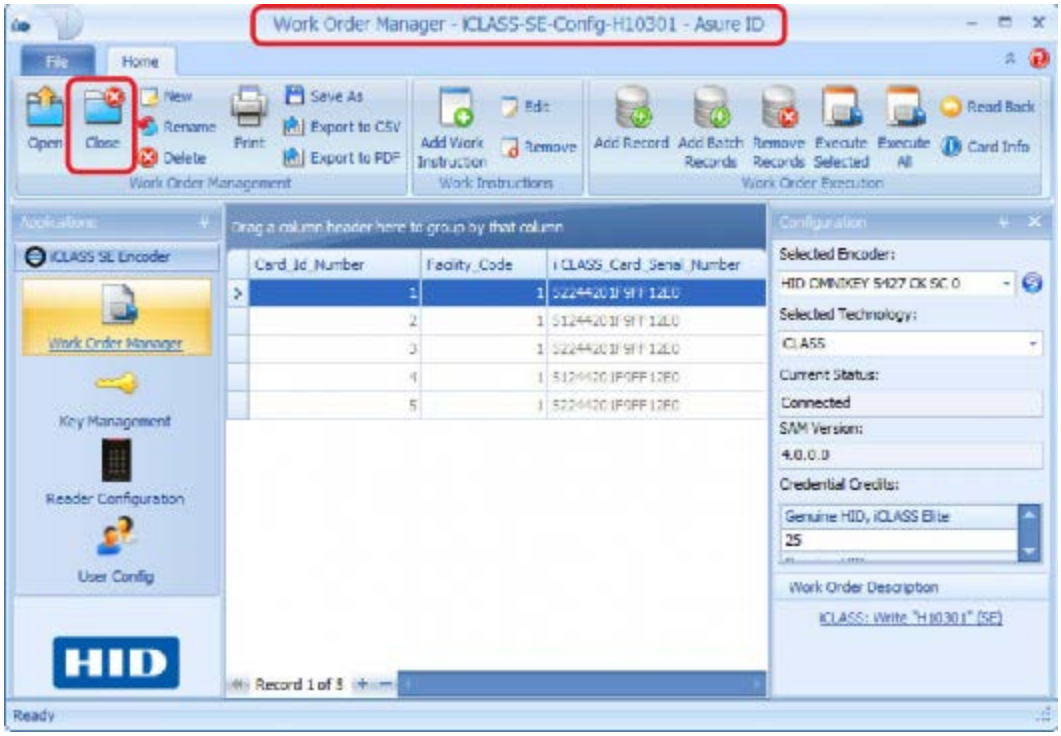


4. The Work Order information populates the Work Order Manager window.

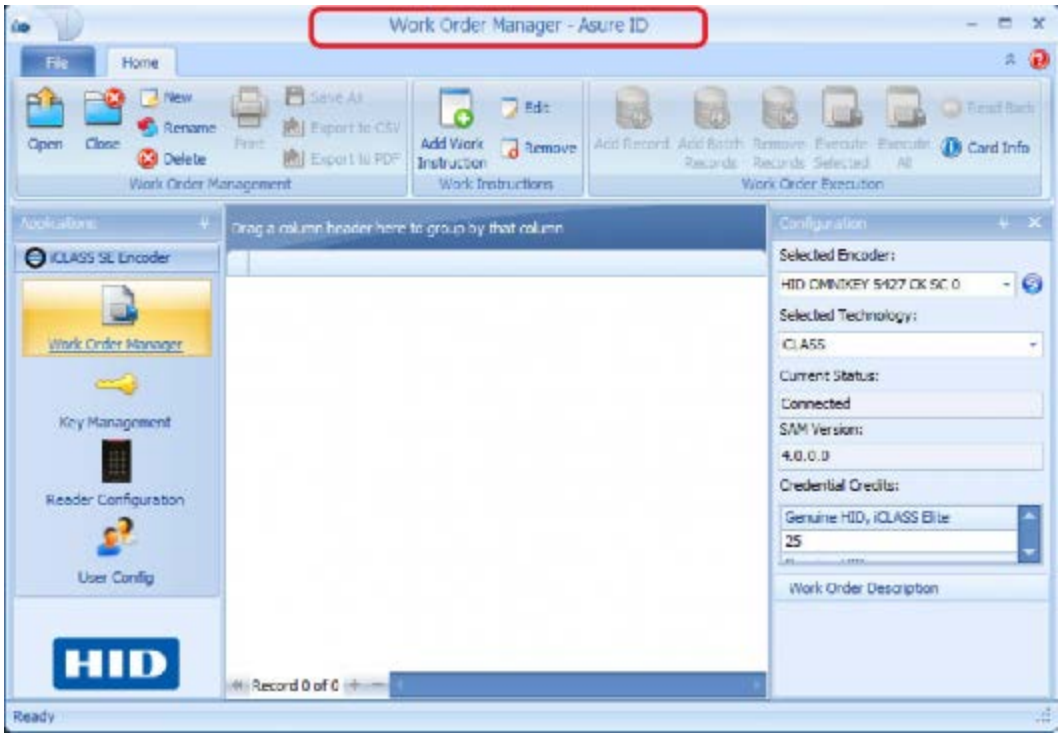


5.5 Close a work order

1. When a Work Order is Open, select **Close** from the toolbar. See **5.4 Open a work order**.



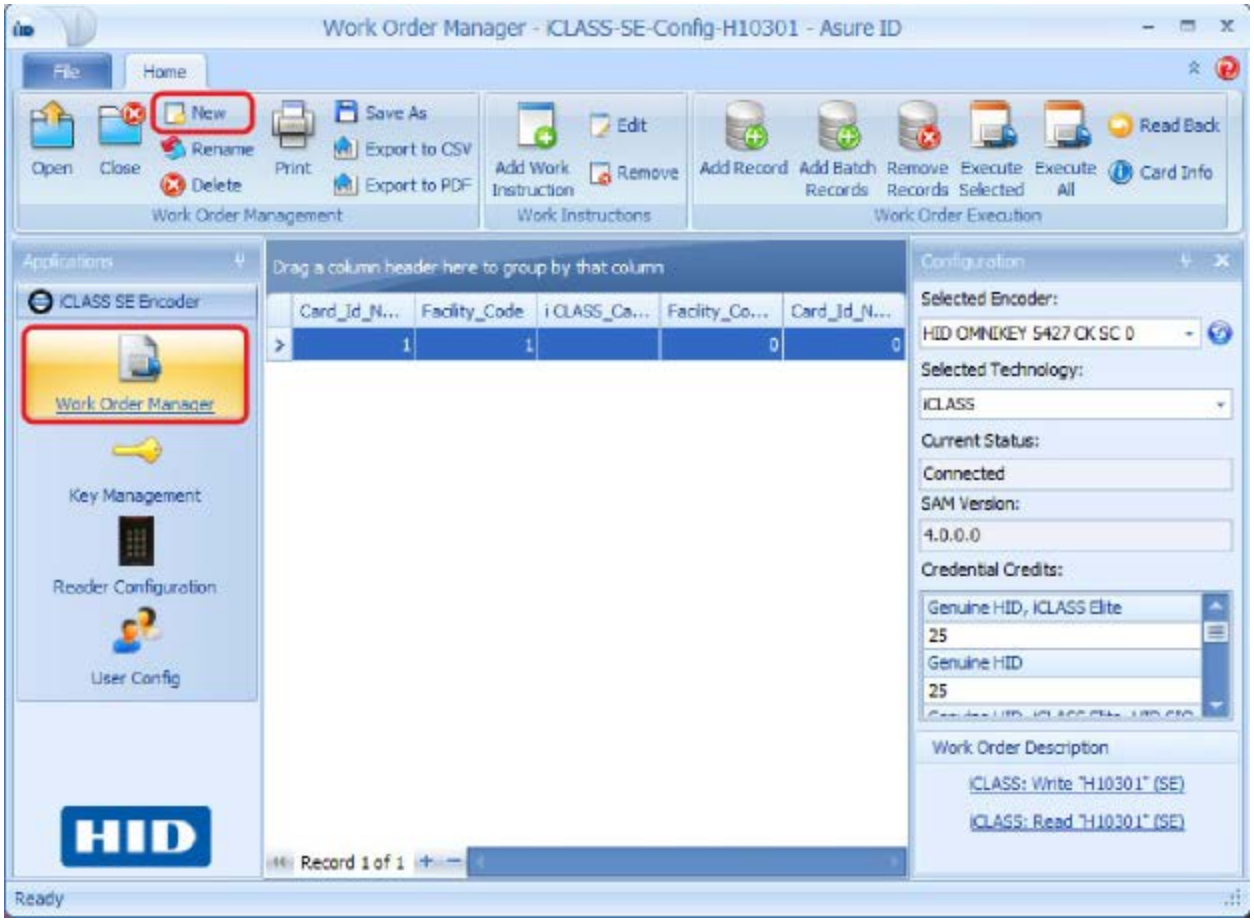
2. The Work Order is closed.



5.6 Create a work order

A Work Order is comprised of one or many Work Instructions. A Work Instruction is a single command issued during Work Order execution. The single Work Instruction can either read or write to a specific memory location.

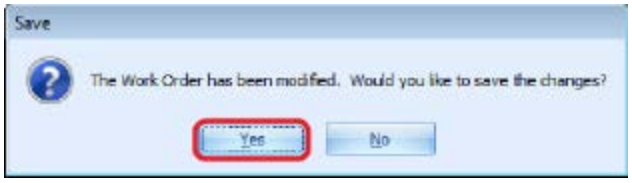
1. Select **Work Order Manager** module. Select **New** from the toolbar.



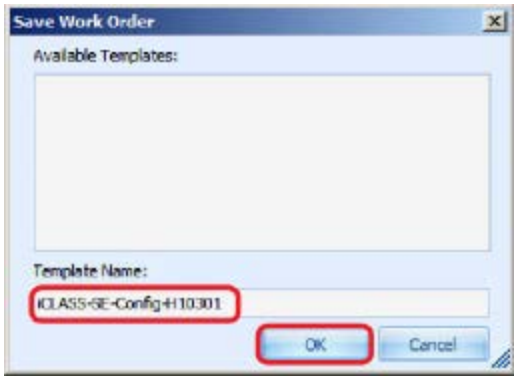
2. Select the required technology, and click **OK**.

3. See **Work instruction wizard** for details on each technology wizard. When you have completed the wizard, return to the following step.

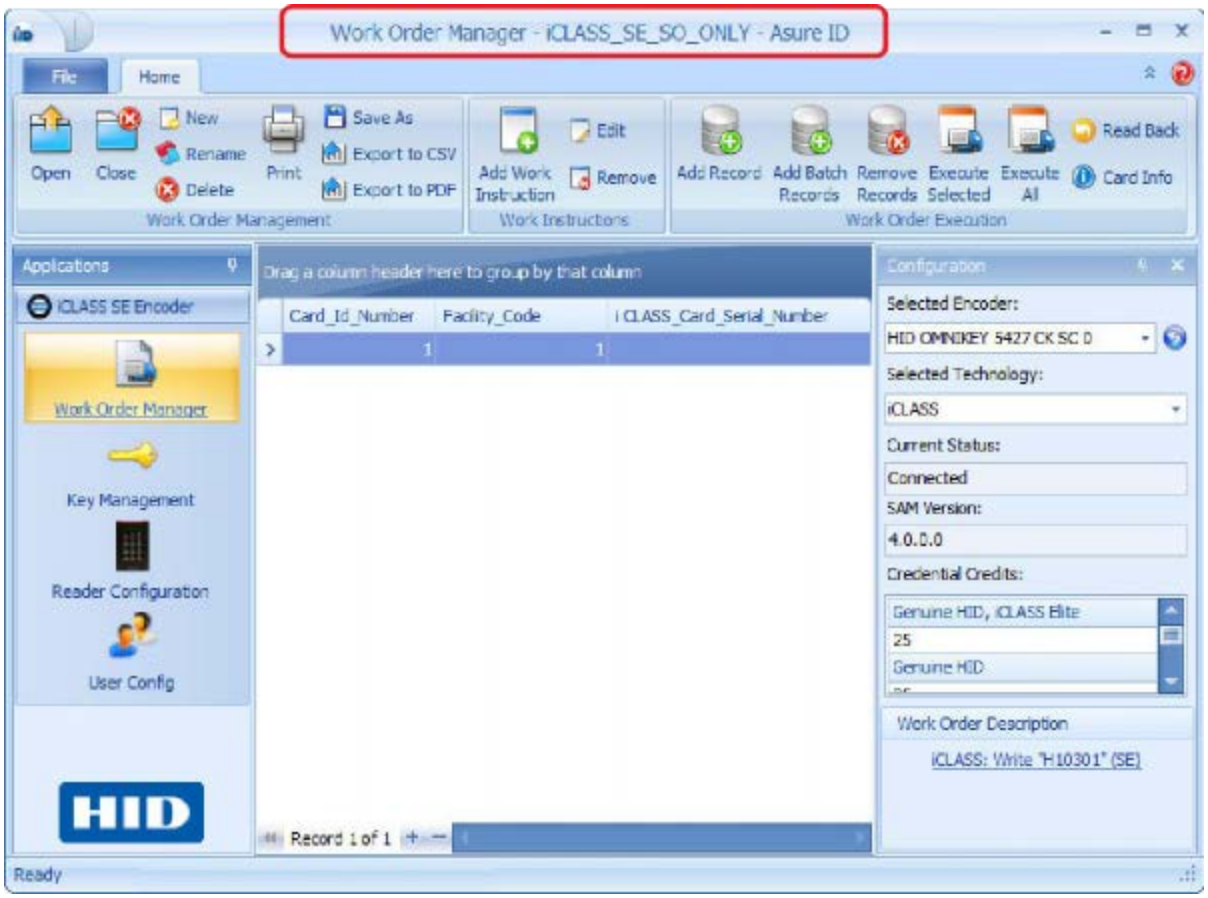
4. Select **Yes** to save the Work Order.



5. Enter a descriptive name for the Work Order, and click **OK**.

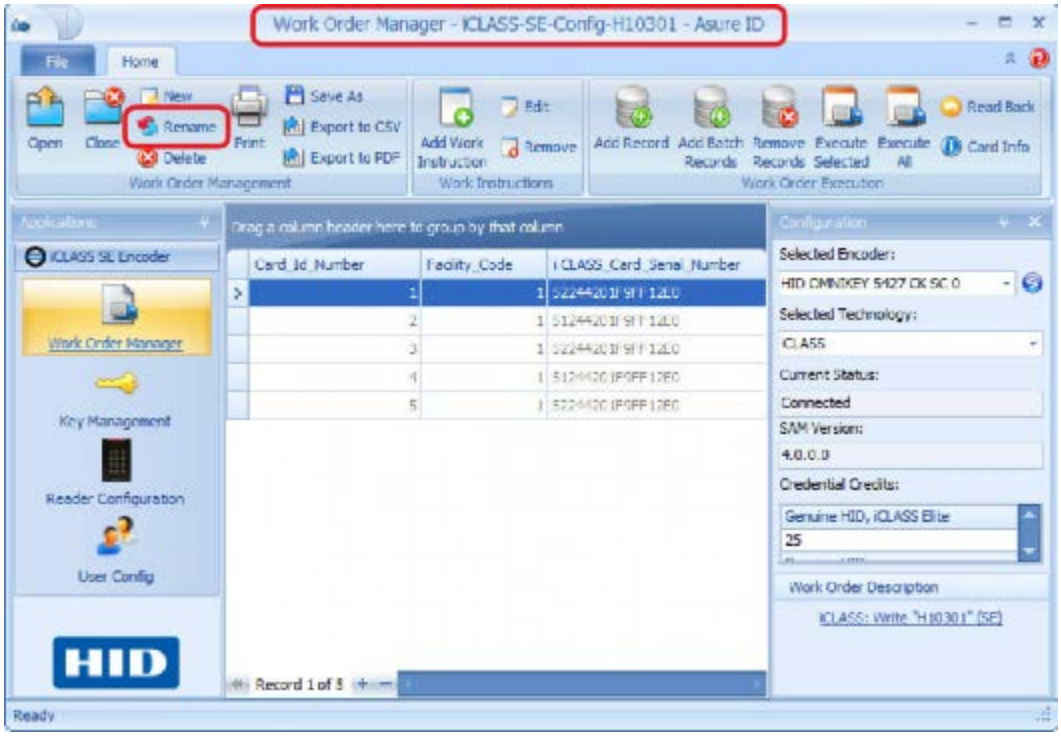


6. The Work Order information is now displayed on the **Work Order Manager** window, with the Work Order name displayed across the top of the window.

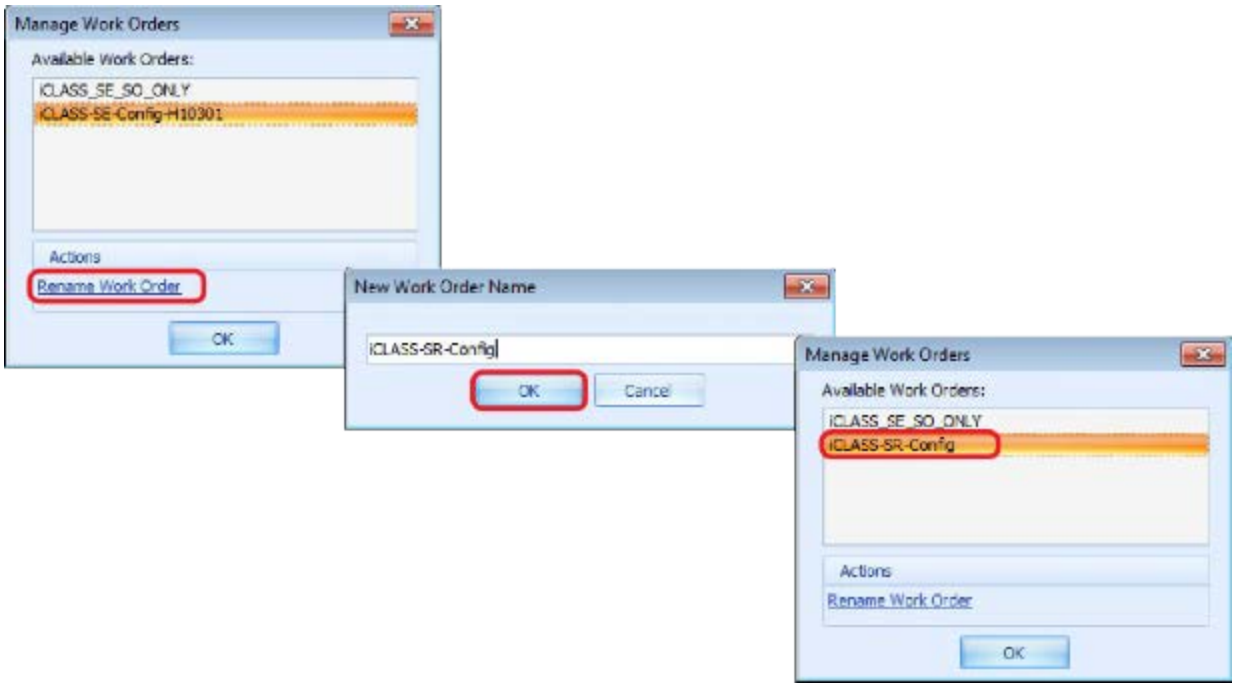


5.7 Rename a work order

1. While in the **Work Order Manager** module, select **Rename** from the toolbar.

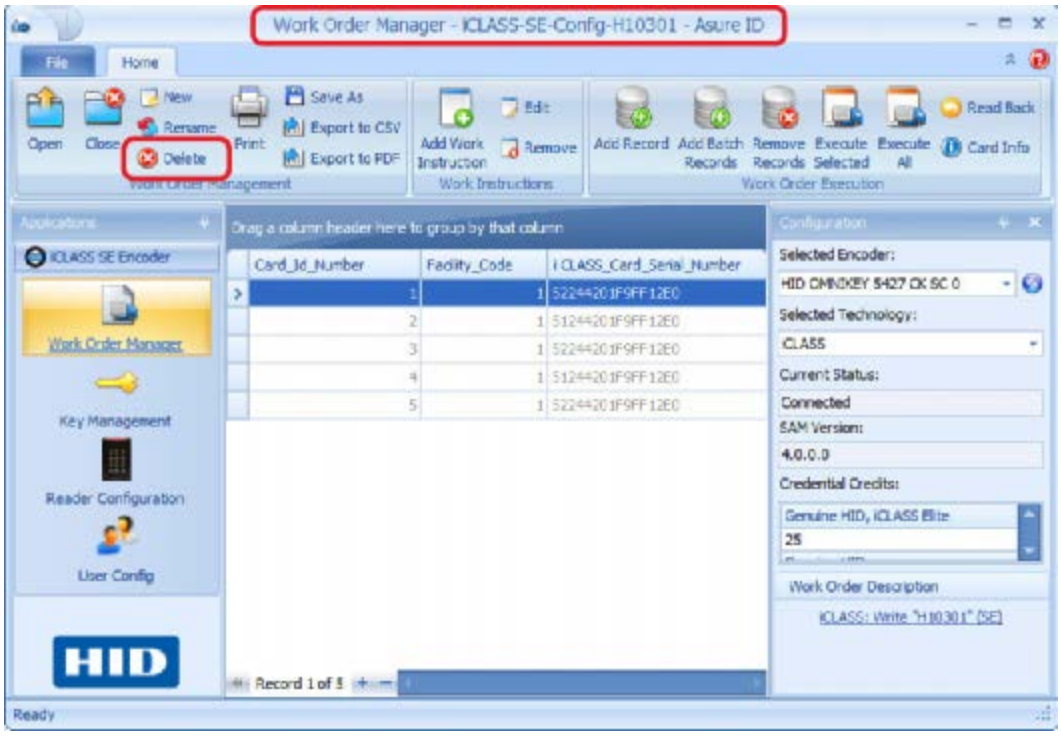


2. Select a Work Order from the Manage Work Order window, and click **Rename Work Order**.
3. Enter a new name of the Work Order on the **New Work Order Name** window, and click **OK**.
4. The Work Order name is updated on the list. Click **OK**.

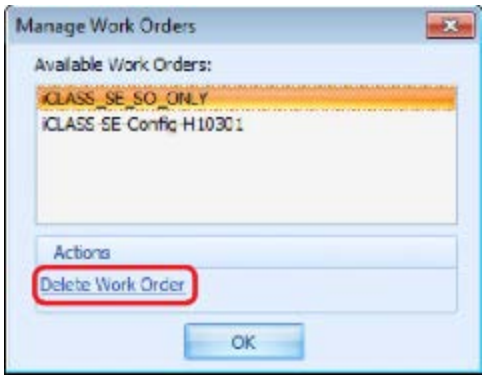


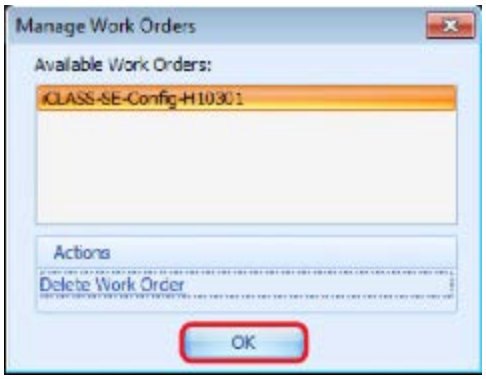
5.8 Delete a work order

1. While in the **Work Order Manager** module, select **Delete** from the toolbar.



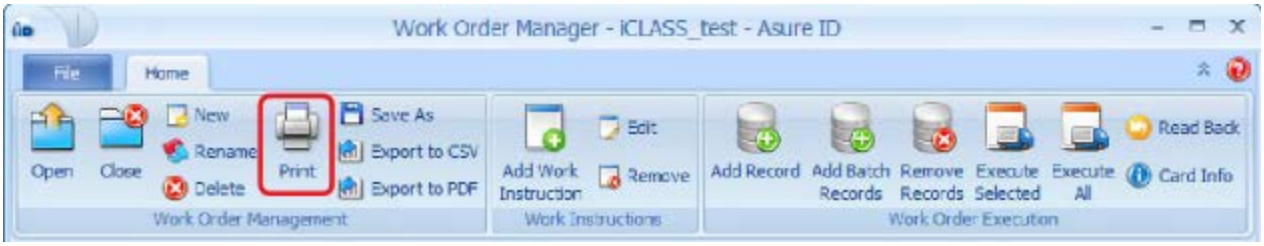
2. Select a Work Order from the Manage Work Order window, and click **Delete Work Order**.
3. The file is removed from the list.
4. Click **OK**.





5.9 Print a work order

Work Orders can be simply printed to a local printer.



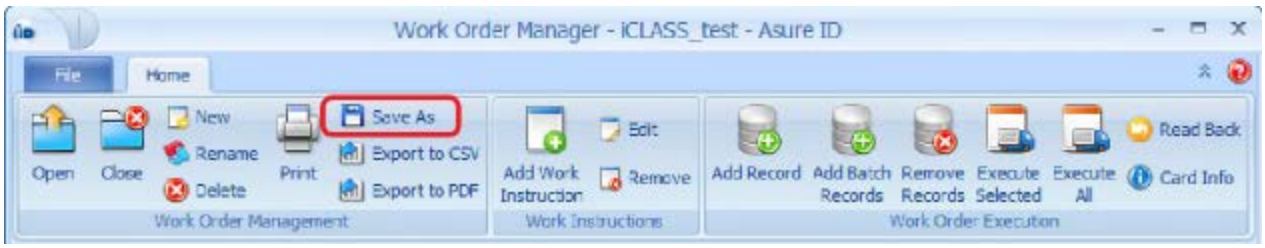
1. Open the **Work Order Manager** module.
2. Open a Work Order. See **5.4 Open a work order**.
3. Click **Print** from the toolbar.
4. Select your normal printer options from the Print manager.
5. Click **Print**.

5.10 File save as a work order

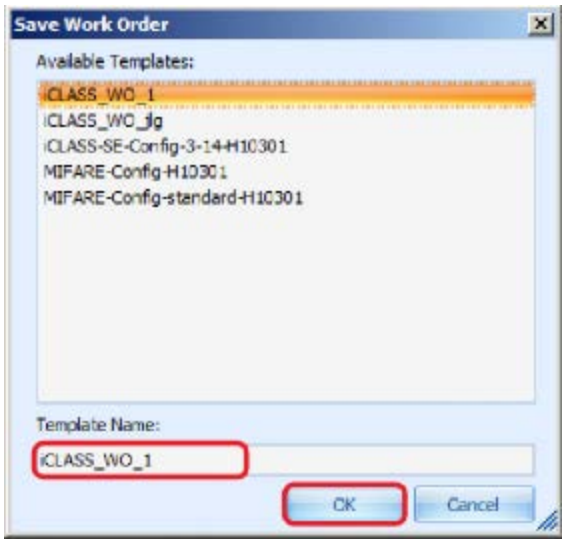
This process makes a copy of the Work Instruction to a new Work Order, where it can then be modified, as needed.

> **Note:** The database is cleared for the new Work Order.

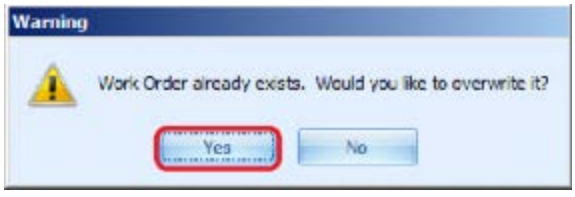
1. Open the **Work Order Manager** module.
2. Open a Work Order. See **5.4 Open a work order**.
3. Click **Save As** from the toolbar.



4. Enter a new Template Name for the **Work Order**, and click **OK**.



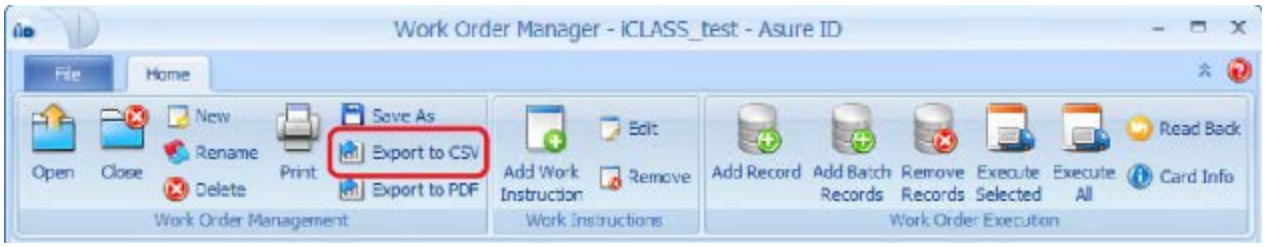
5. The new Work Order is saved and opened with the new name ready to edit, if needed.
6. If the Work Order with this Template Name already exists, a **Warning** window appears. To continue, click **Yes** to overwrite the current Work Order.



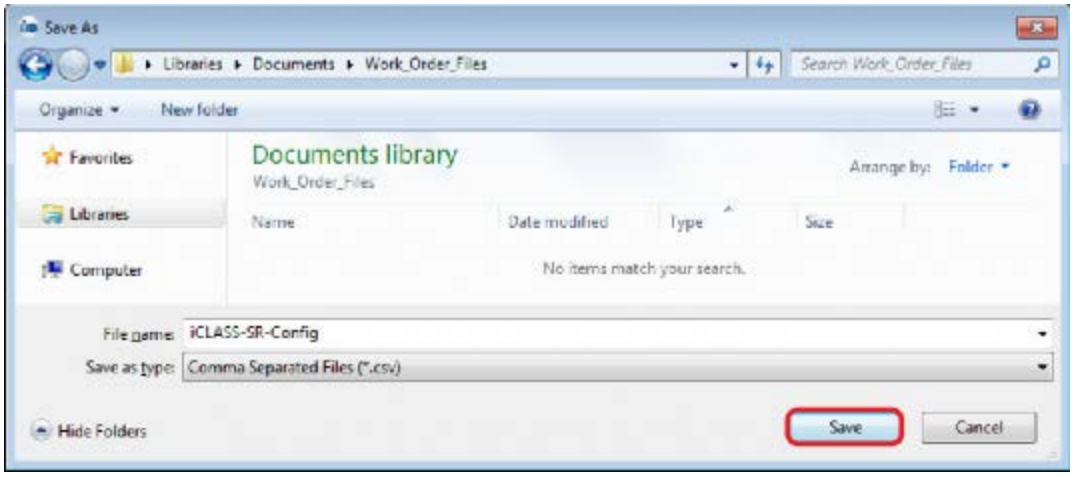
5.11 Export work order data to a CSV file

Work Order Data can be exported to a Comma Separated Values file (CSV) file.

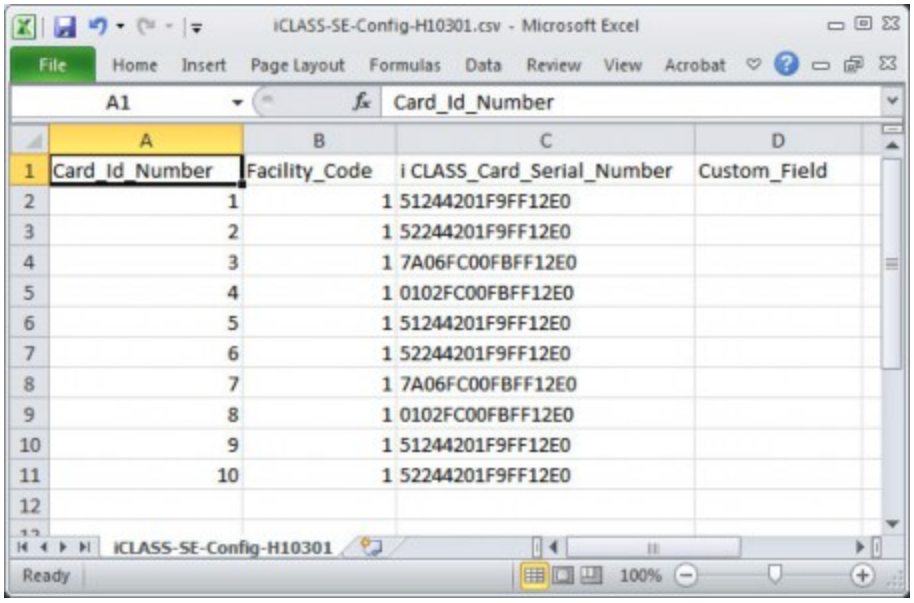
1. On the **Work Order Manager** toolbar click **Export to CSV**.



2. Browse to a location to save the file, and click **Save**.



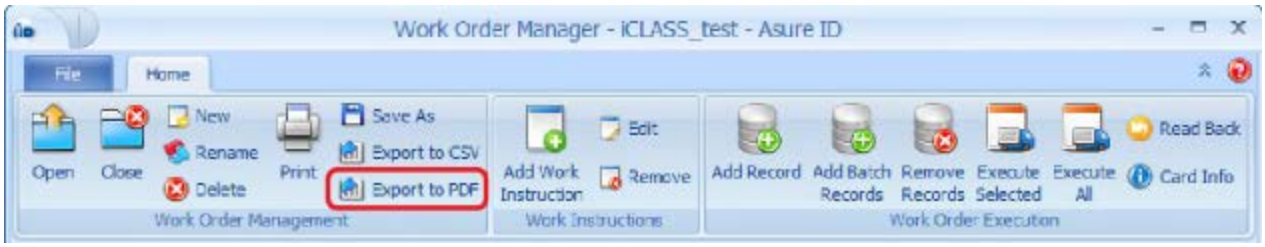
3. Below is an example of the CSV file.



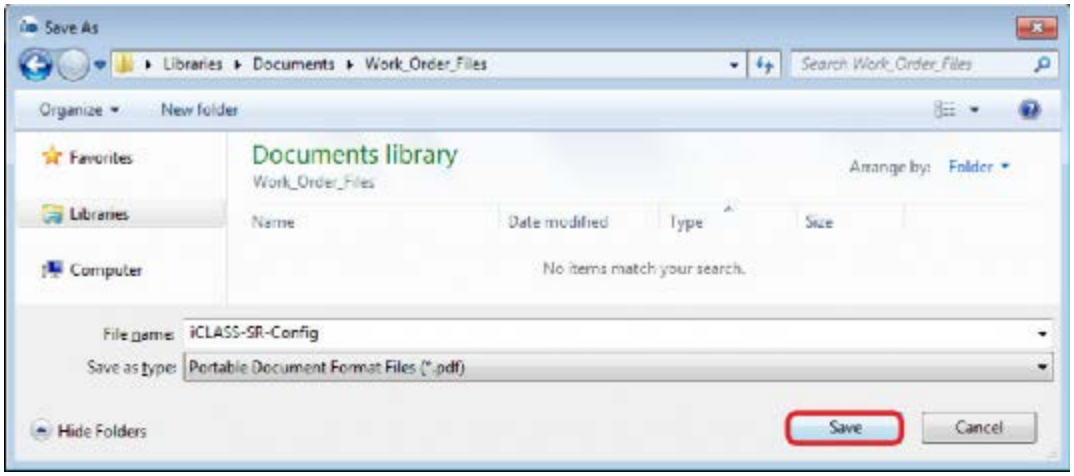
5.12 Export work order data to a PDF file

Work Order data can be exported to a portable document format (PDF) file.

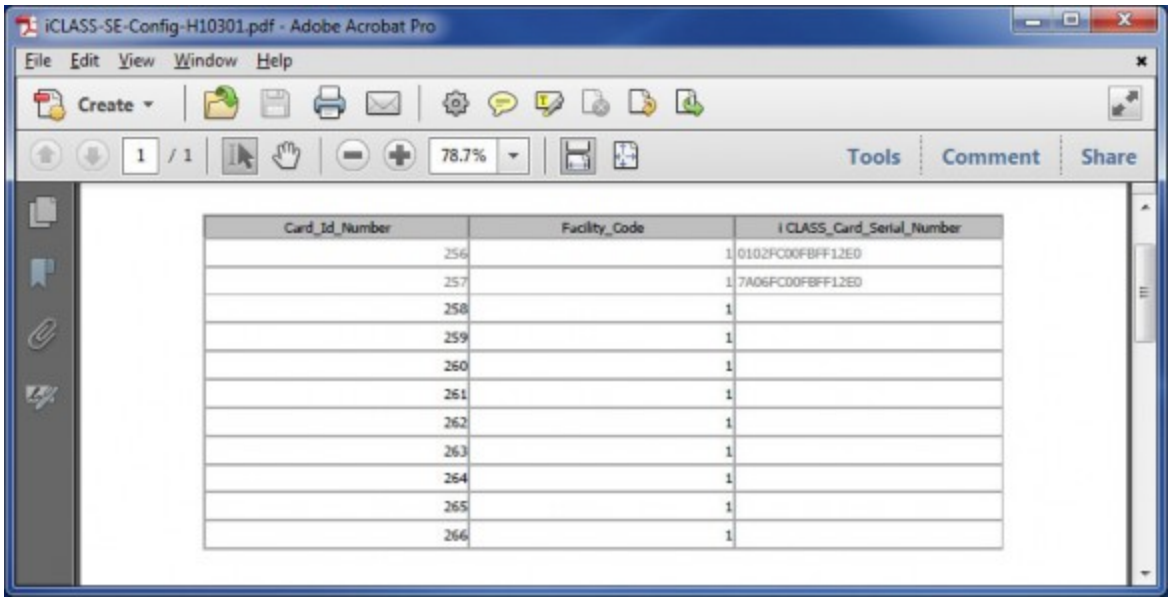
1. **Work Order Manager module** click **Export to PDF**.



2. Browse to a location to save the file, and click **Save**.



3. Below is an example of the PDF file:

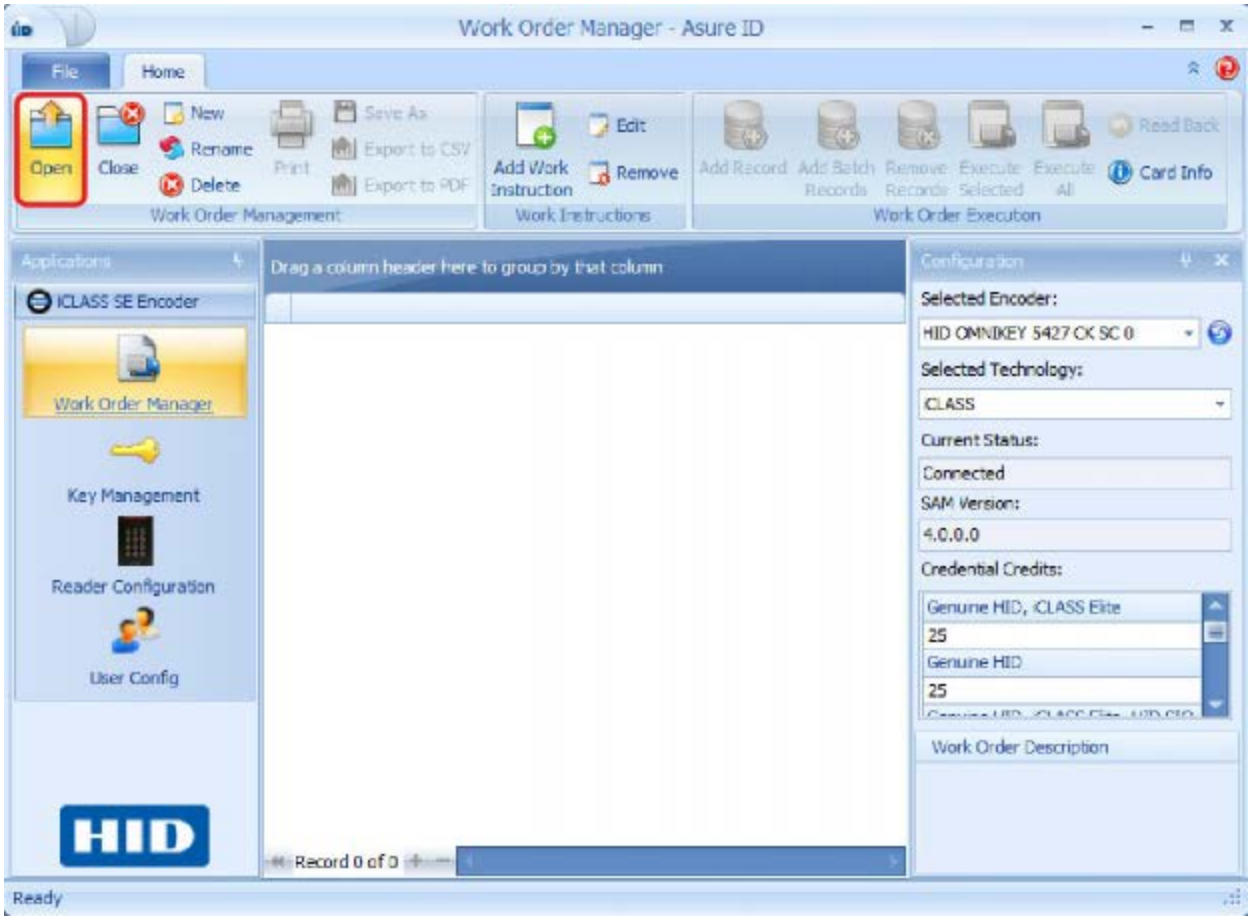


5.13 Add a work instruction to a work order

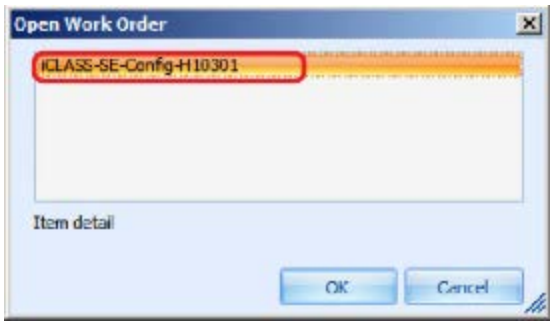
A Work Instruction is a single routine issued during Work Order execution. The single Work Instruction can either read or write to a specific memory location.

> **Note:** This example is of a Custom Configuration.

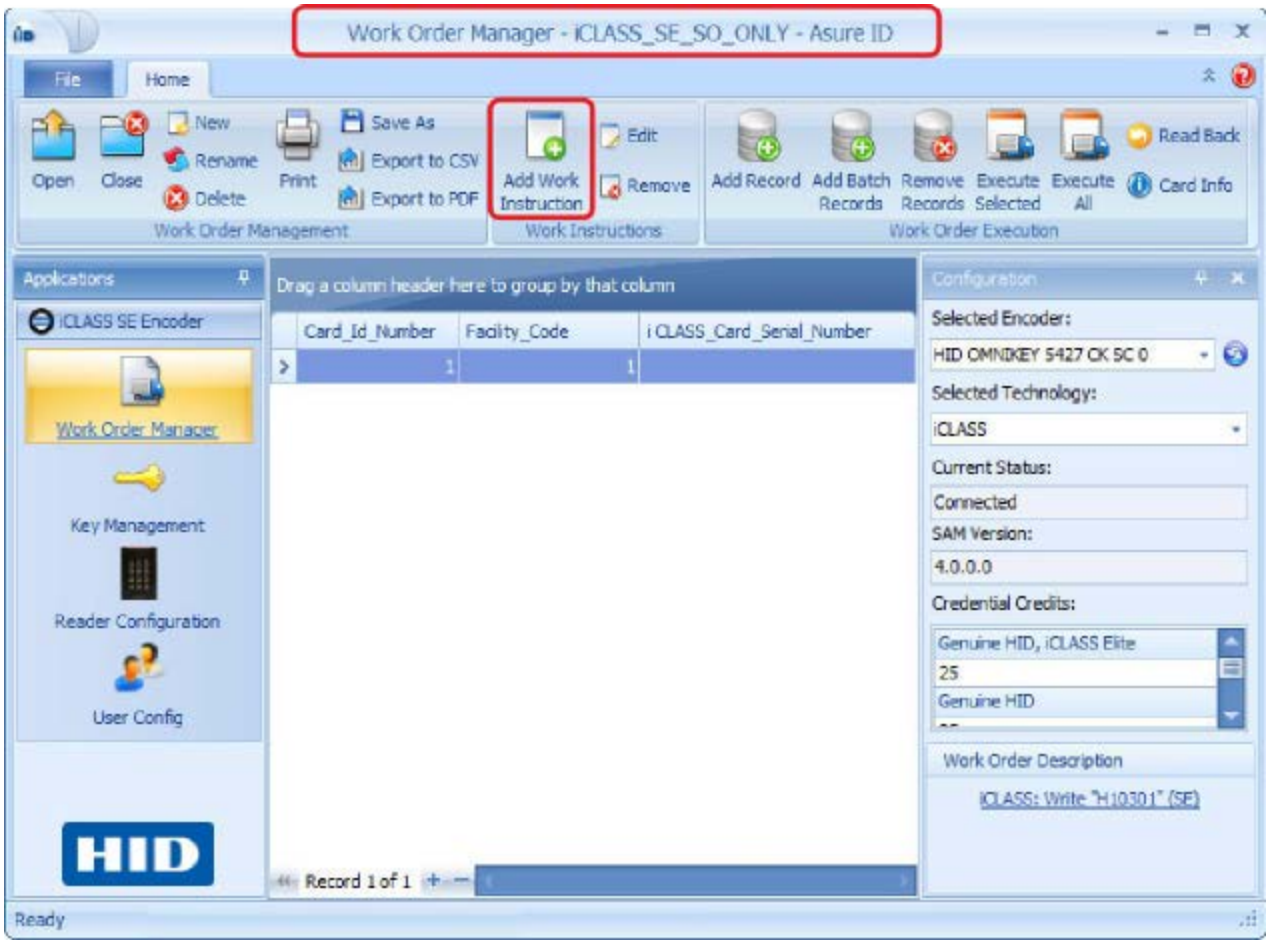
1. Open a Work Order.



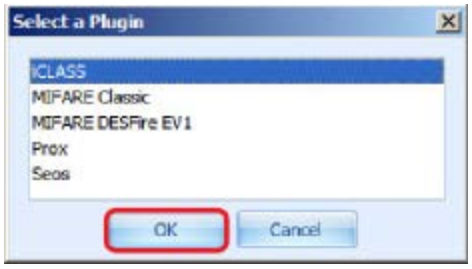
2. Double-click a Work Order from the list to open.



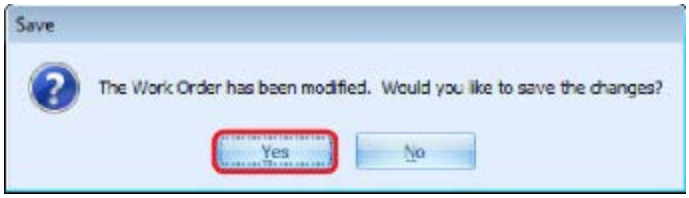
3. The Work Order information is displayed on the Work Order Manager window. Select **Add Work Instruction**.



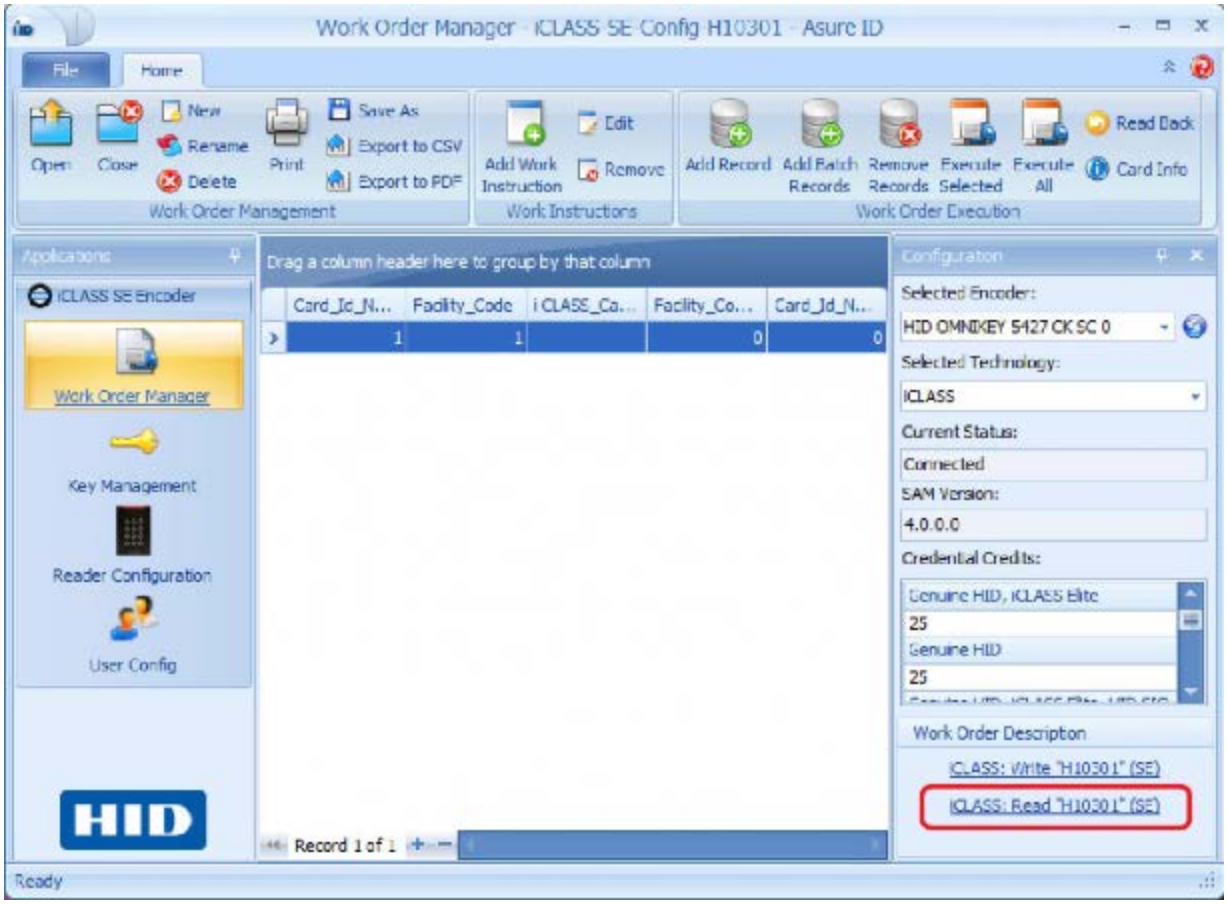
4. Select the technology type from the list and click **OK**.



5. See **Work instruction wizard** for details on each technology wizard. When you have completed the wizard, return to the following step.
6. Select **Yes** to save the Work Order.



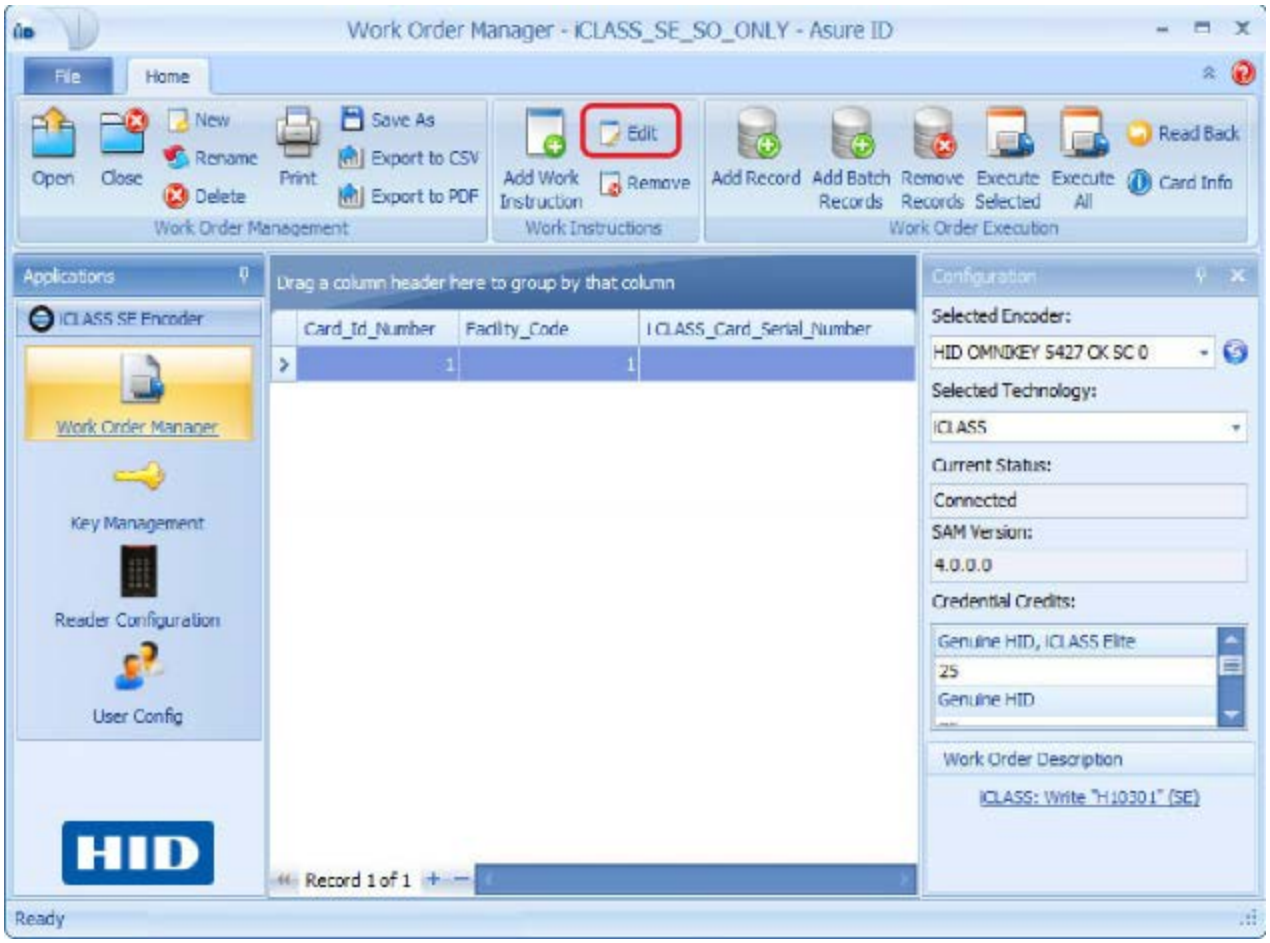
7. The new Work Instruction is now listed on the Work Order Description.



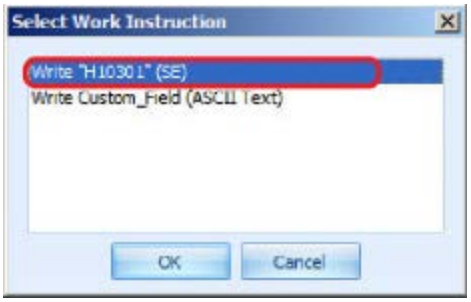
5.14 Edit a work instruction

The following describes the simple process of editing an existing Work Instruction.

1. Open a Work Order.
2. Click **Edit** in the Work Instructions section of the toolbar.



3. Double-click a Work Instruction from the list to edit.

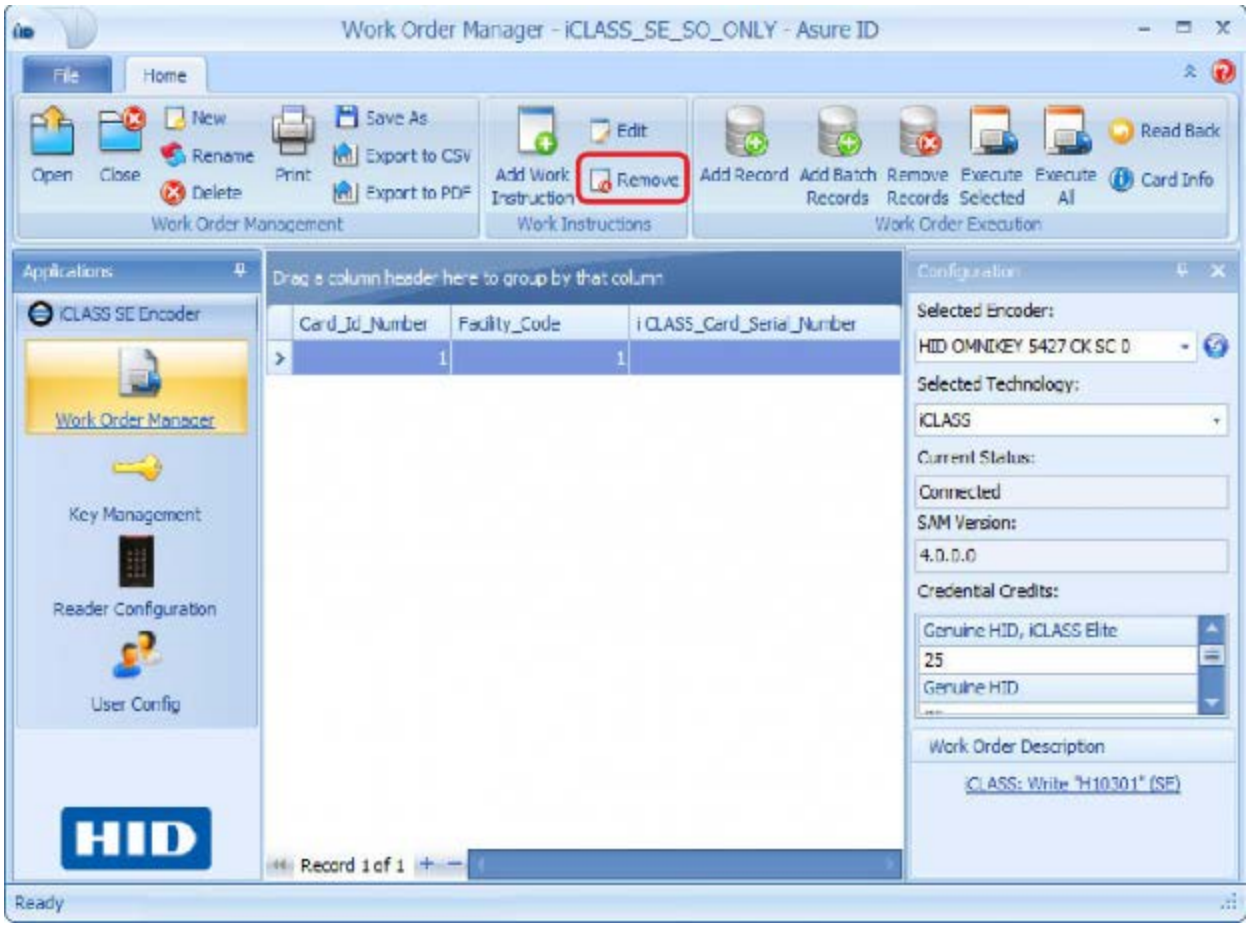


4. The Work Order Instruction wizard is opened. See **Work instruction wizard** for details on each technology wizard.
5. When complete, the Work Instruction selected is modified.

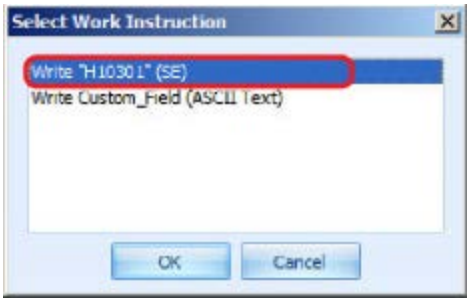
5.15 Remove a work instruction

The following describes the simple process of removing an existing Work Instruction.

1. Open a Work Order.
2. The Work Instruction is now displayed on the Work Order Manager page.
3. Click **Remove** in the Work Instructions section of the toolbar.



4. Double-click the Work Instruction from the list to remove.



5. When complete, the Work Instruction is removed.

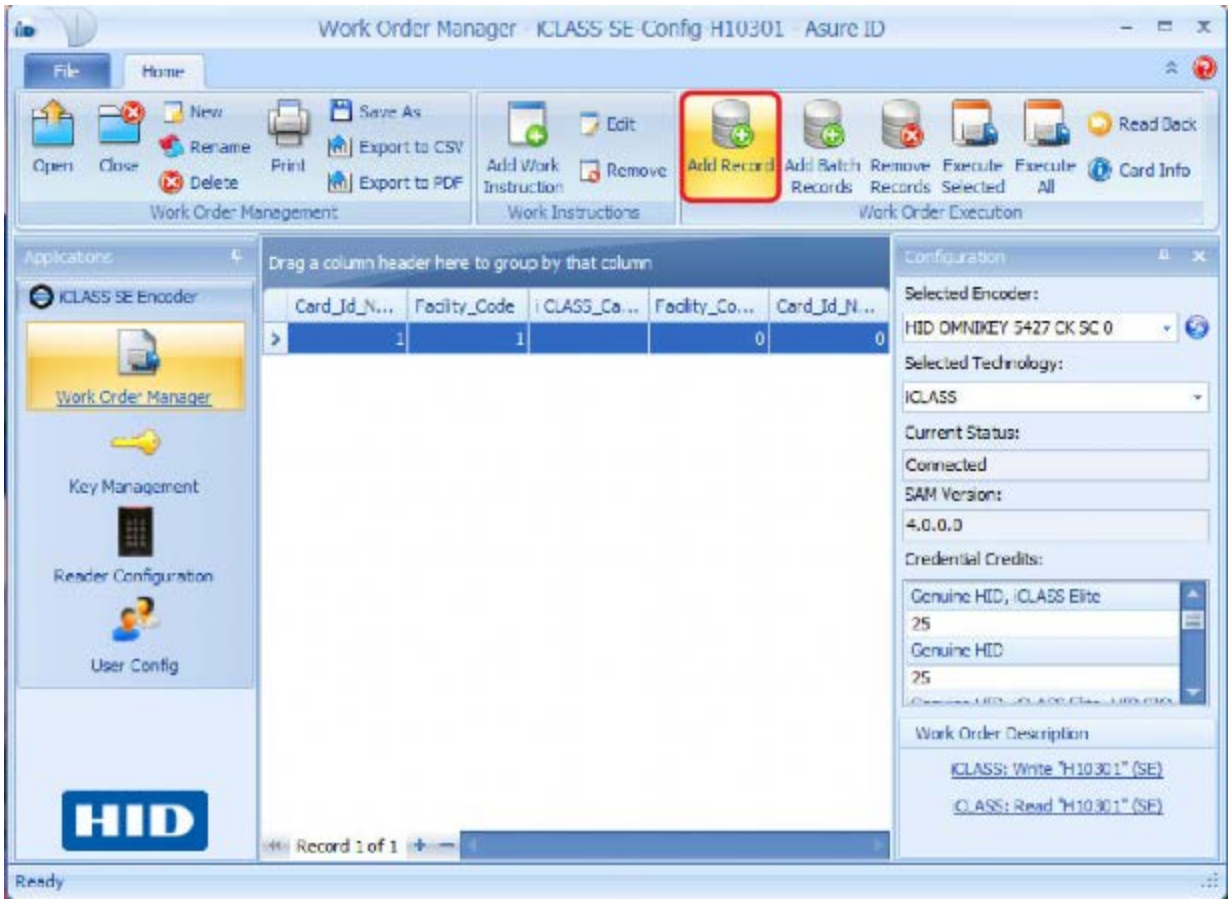
5.16 Work order execution

After the Work Instruction and Work Orders are created, you execute a work order. This section gives an overview of the process to write SIO credentials to an iCLASS card, but is applicable to other Use Cases.

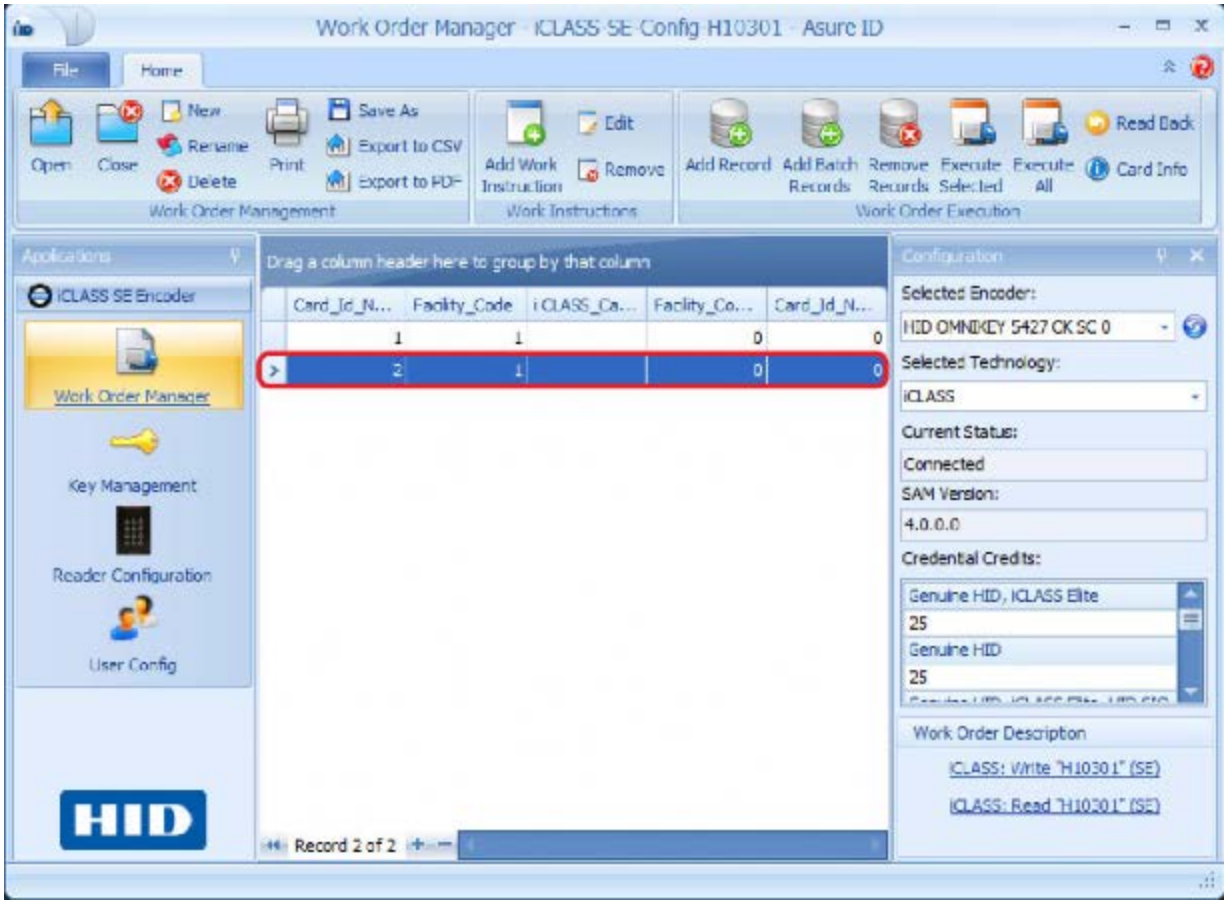
5.16.1 Add a credential record

This section covers how to add a single credential record.

1. Open a Work Order.
2. From **Work Order Manager** click **Add Record**.



3. A single credential record is added.

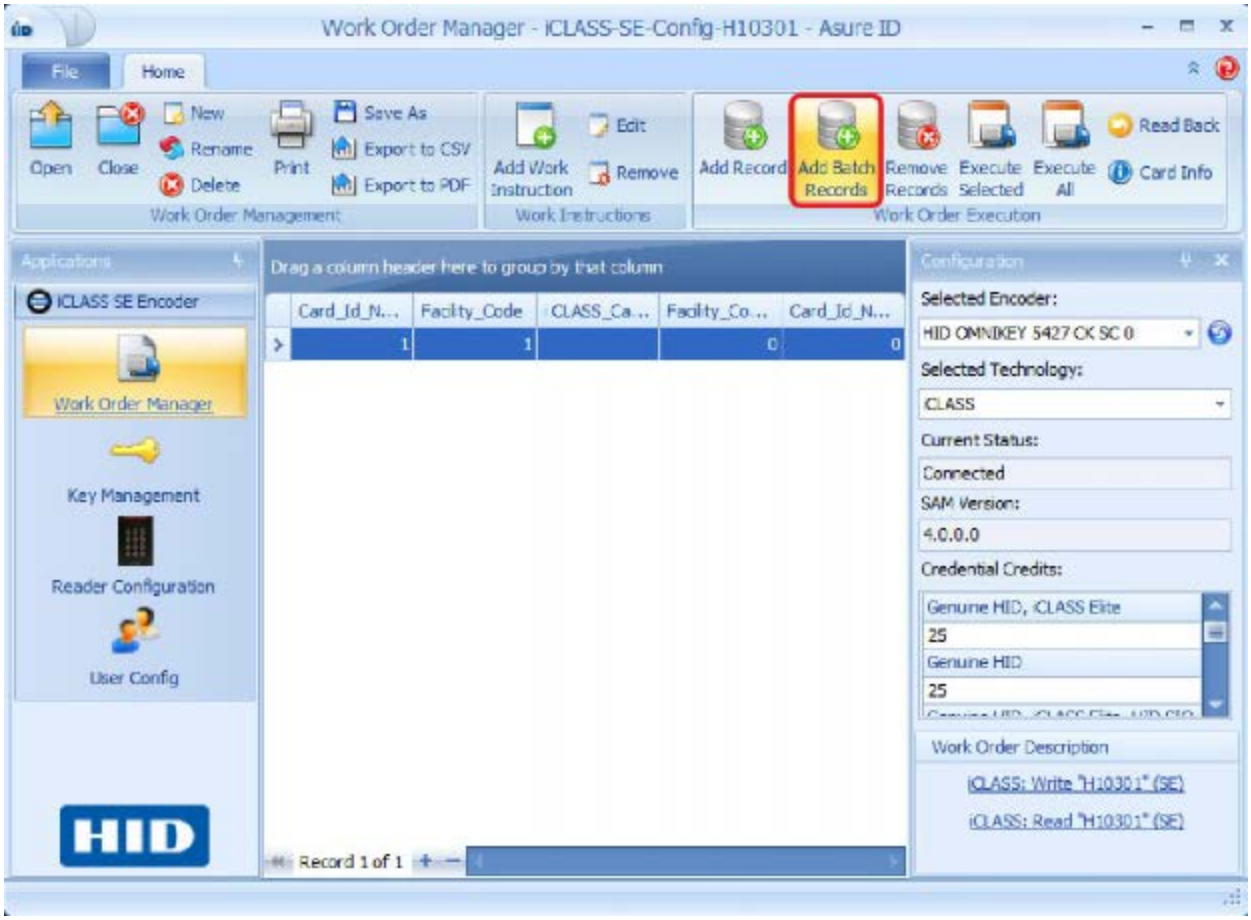


5.16.2 Adding a batch of credential records

This section covers how to add a batch of credential records.

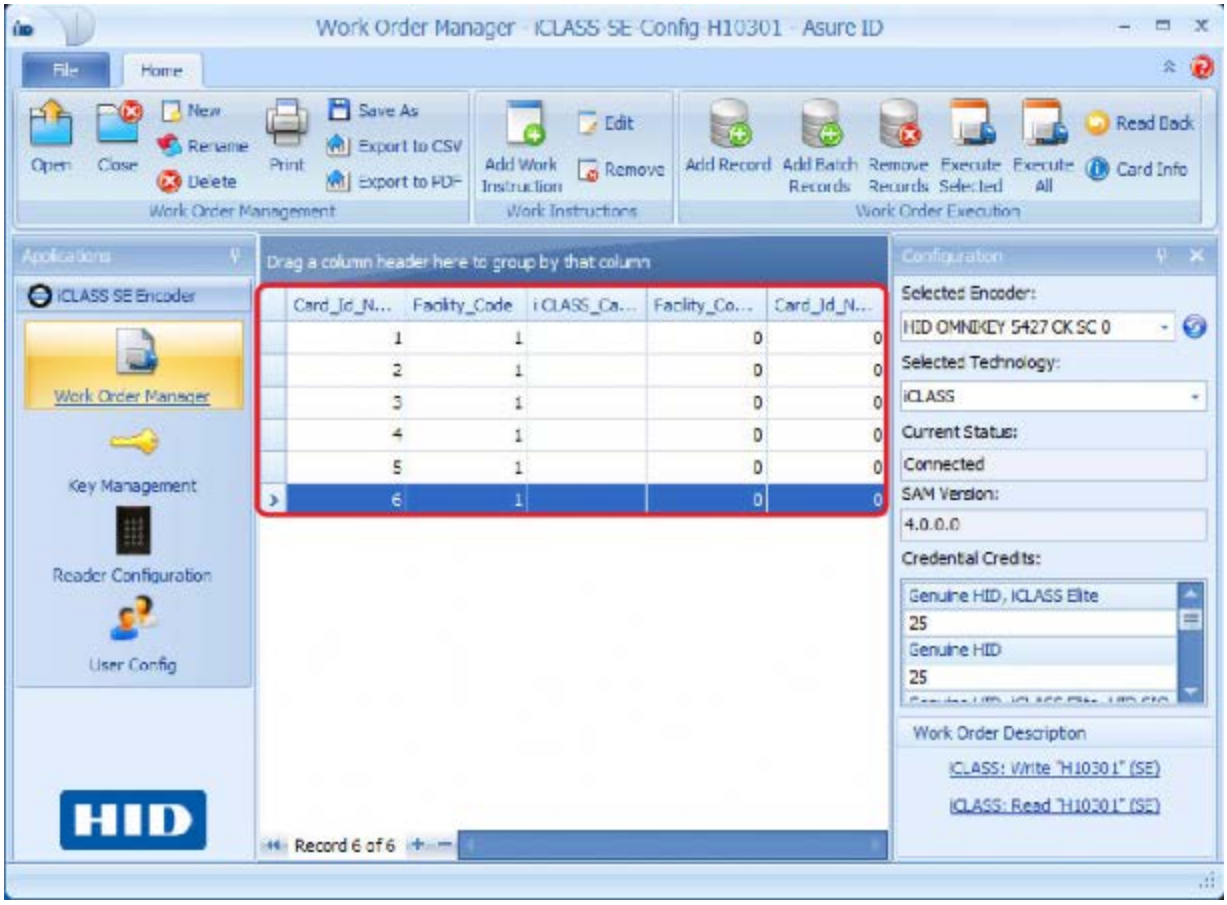
Note: A single credential record or a batch of credential records can be added by following these steps.

1. Open a Work Order.
2. From **Work Order Manager** click **Add Batch Records**.



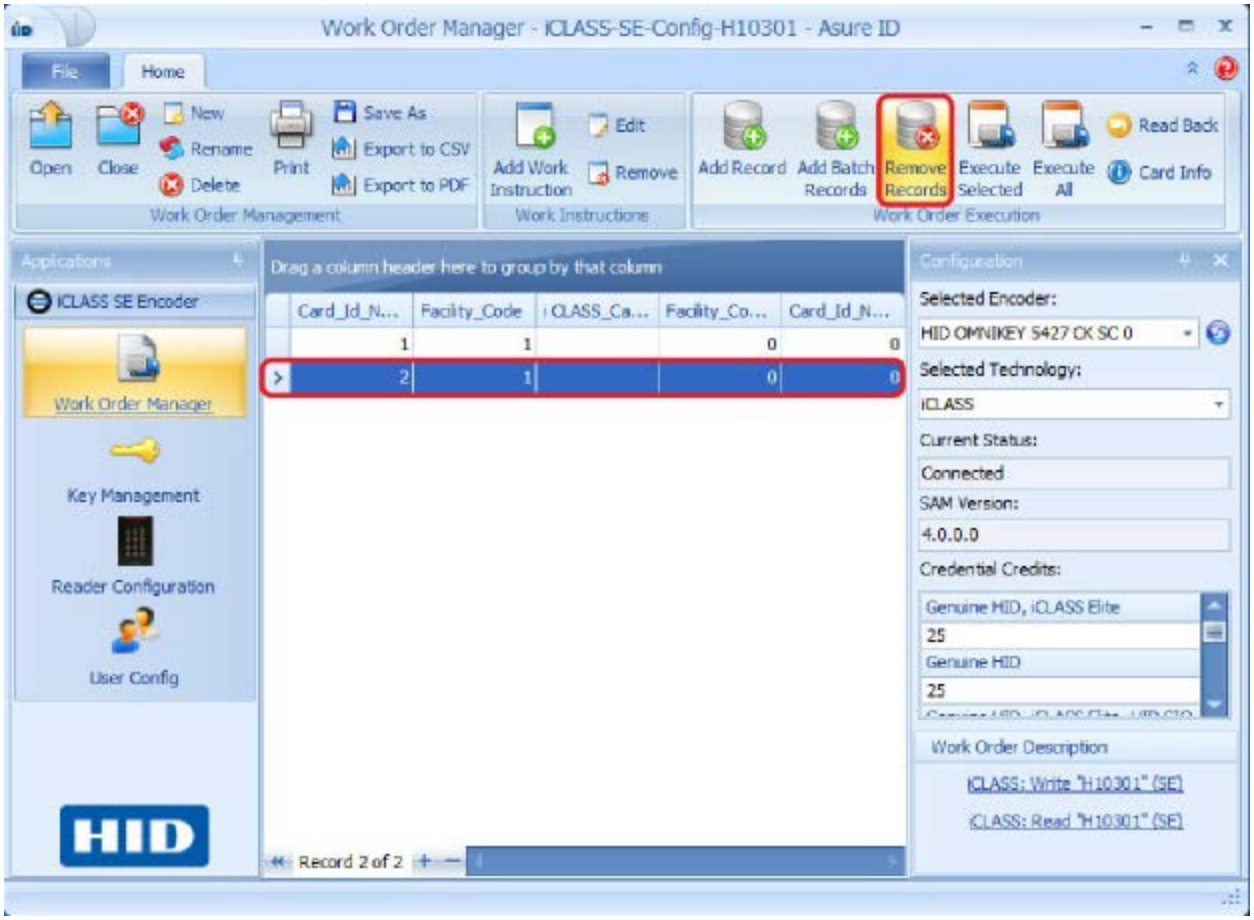
3. Enter the number of credential records to add. Click **OK**.

4. The credential records are added to the list.

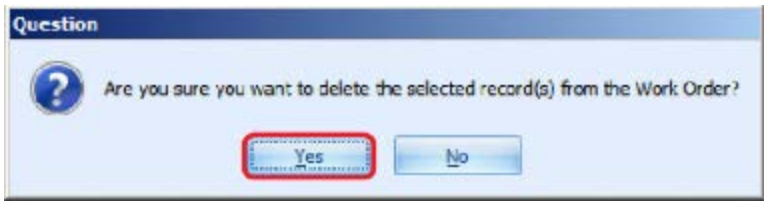


5.16.3 Removing records

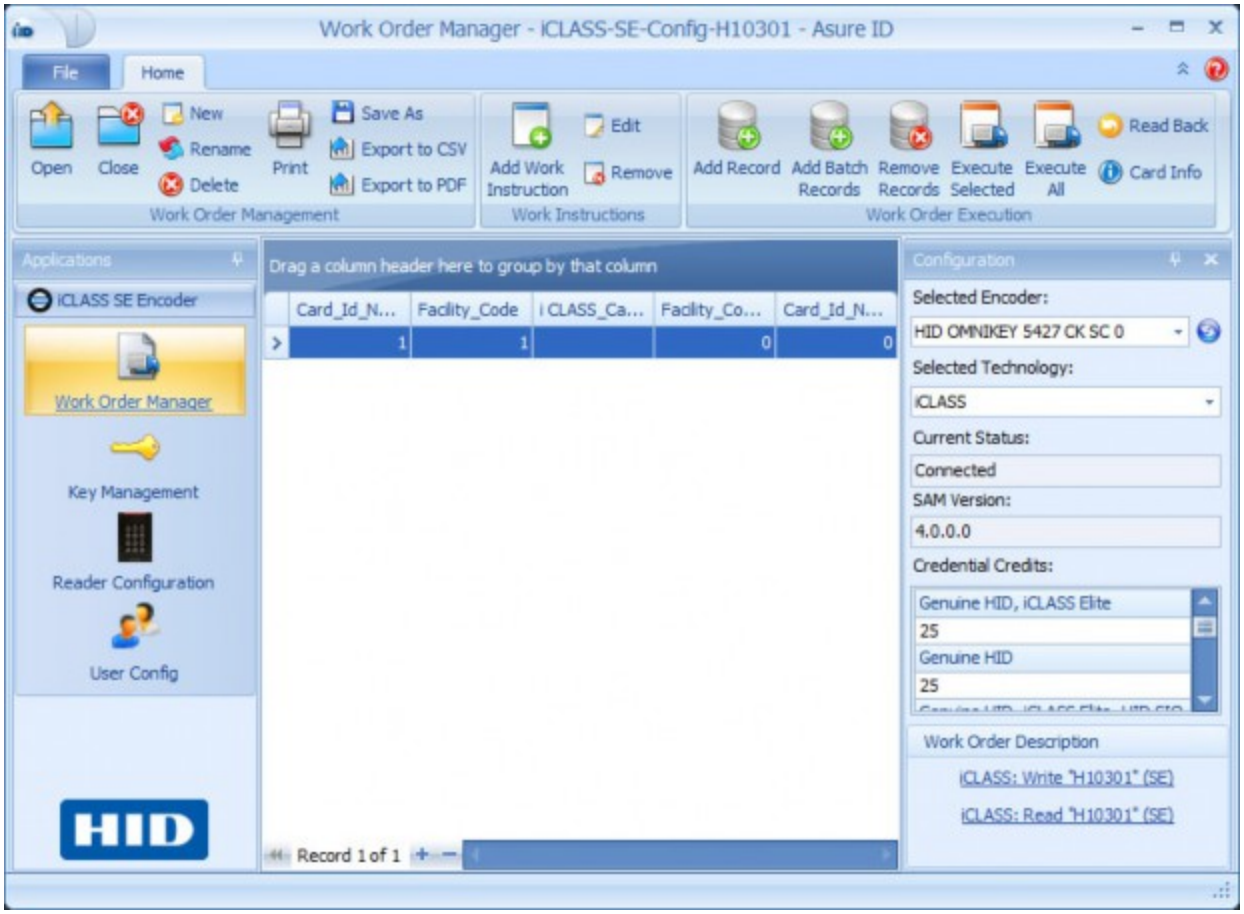
1. Open a Work Order.
2. Select one record, or a range of records.
3. Click **Remove Records**.



4. Click **Yes** to verify the deletion.



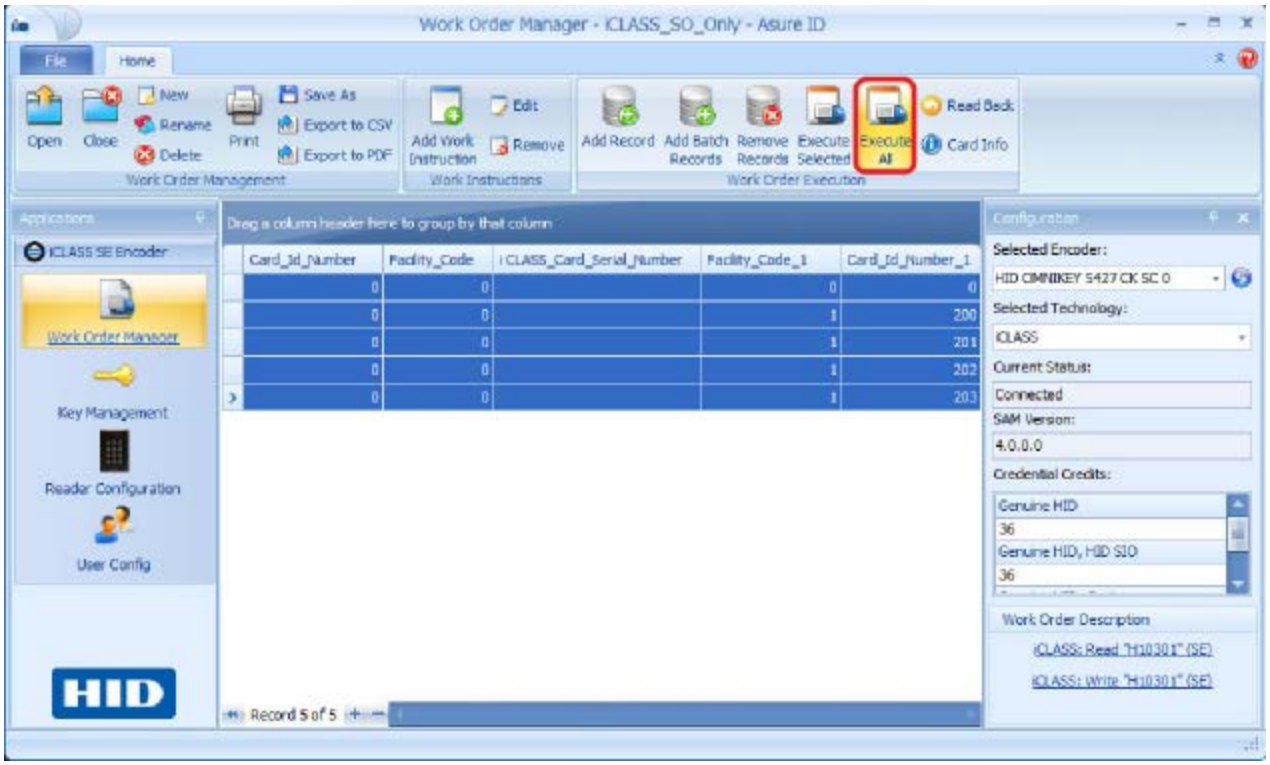
5. The credential records are removed.



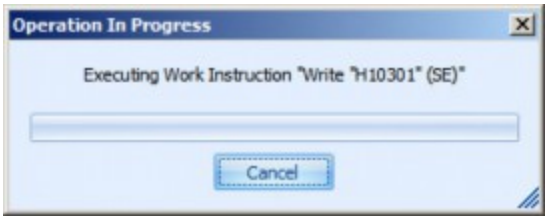
5.16.4 Execute a work order on selected credential records

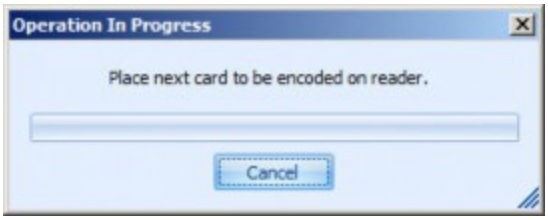
This section covers how to execute a Work Order on a credential record.

1. Open a Work Order.
2. Place the correct card type on the CP1000 Desktop Encoder.
3. Select the records to encode (Ctrl+Click or Shift+Click) to select a range of records.
4. From **Work Order Manager** click **Execute Selected**.



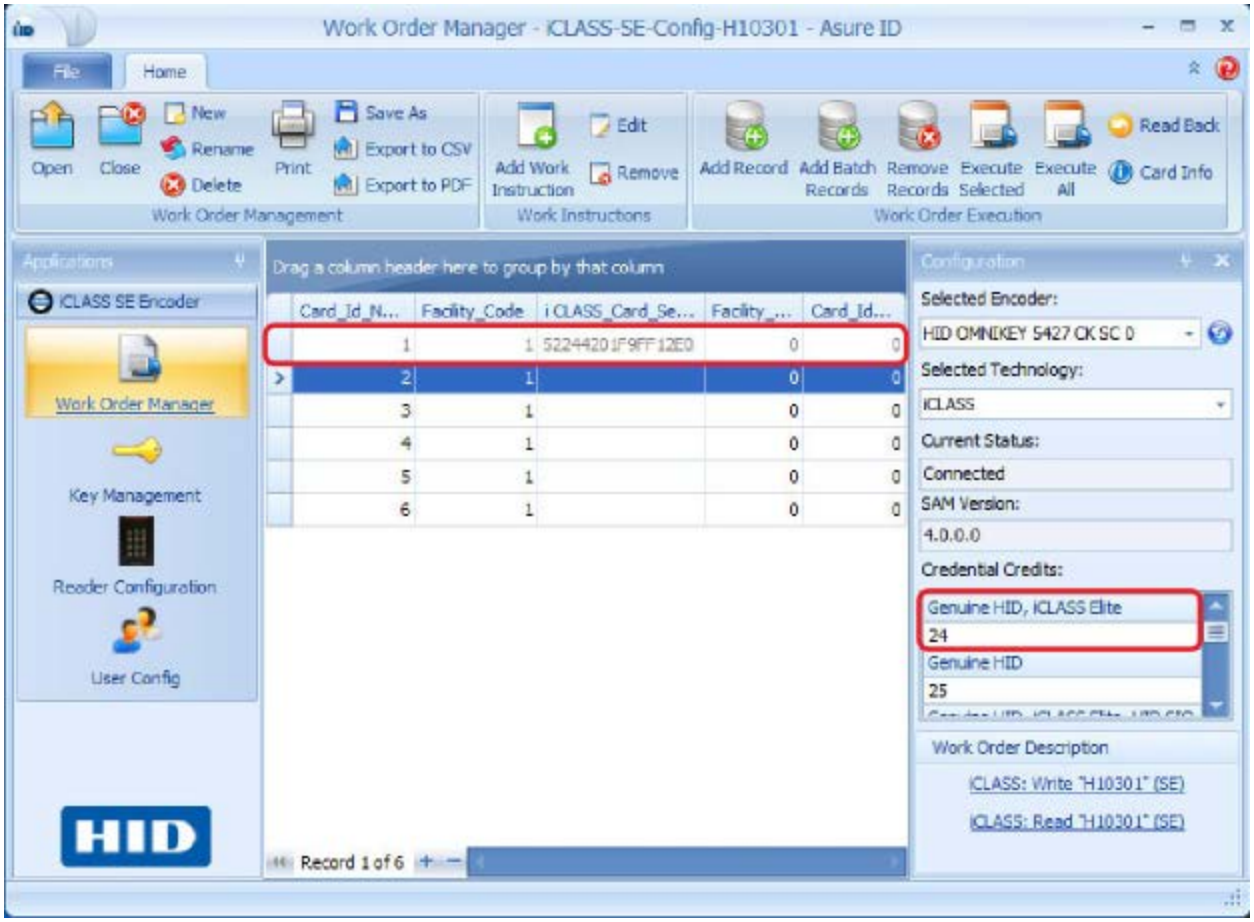
5. A progress window is displayed.
6. When the first card is complete, and if more than one credential was selected, a notice is displayed, asking to place the next card on the encoder.





7. If prompted to do so, place the next card to be encoded on the reader.

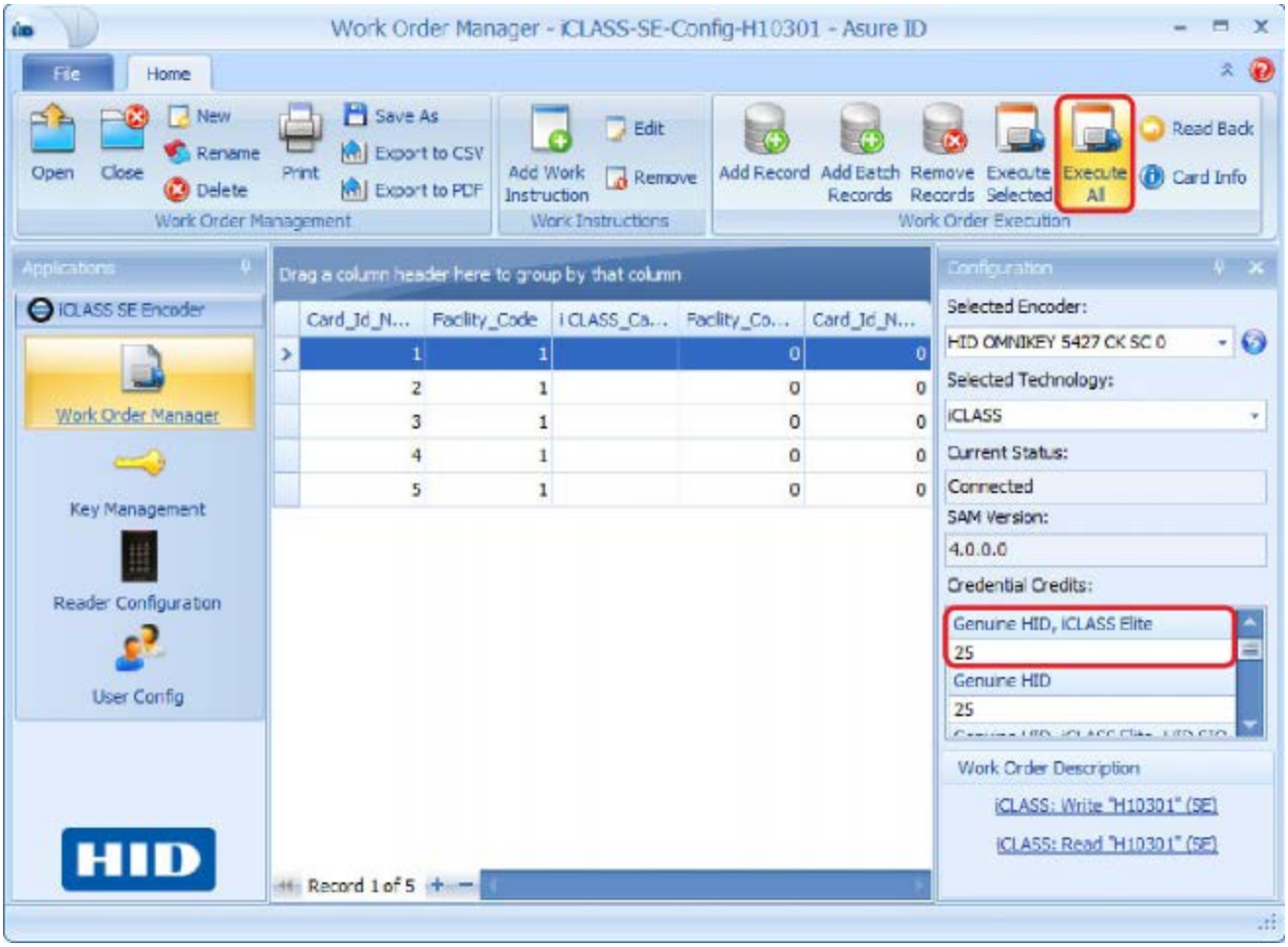
8. If encoding multiple cards, as each card is complete, the display for the credential record is grayed out and the serial number of the card is read into the column. Note that the associated Credential Credits decrements by 1 with each execution. Counter is updated only after all selected records have been encoded if encoding multiple records.



Note: If there are not enough encoding credits for the process you are executing, a message appears with a similar message as shown below. You need to contact HID Global and order more Encoding Credits.

5.16.5 Execute a work order on all credential records

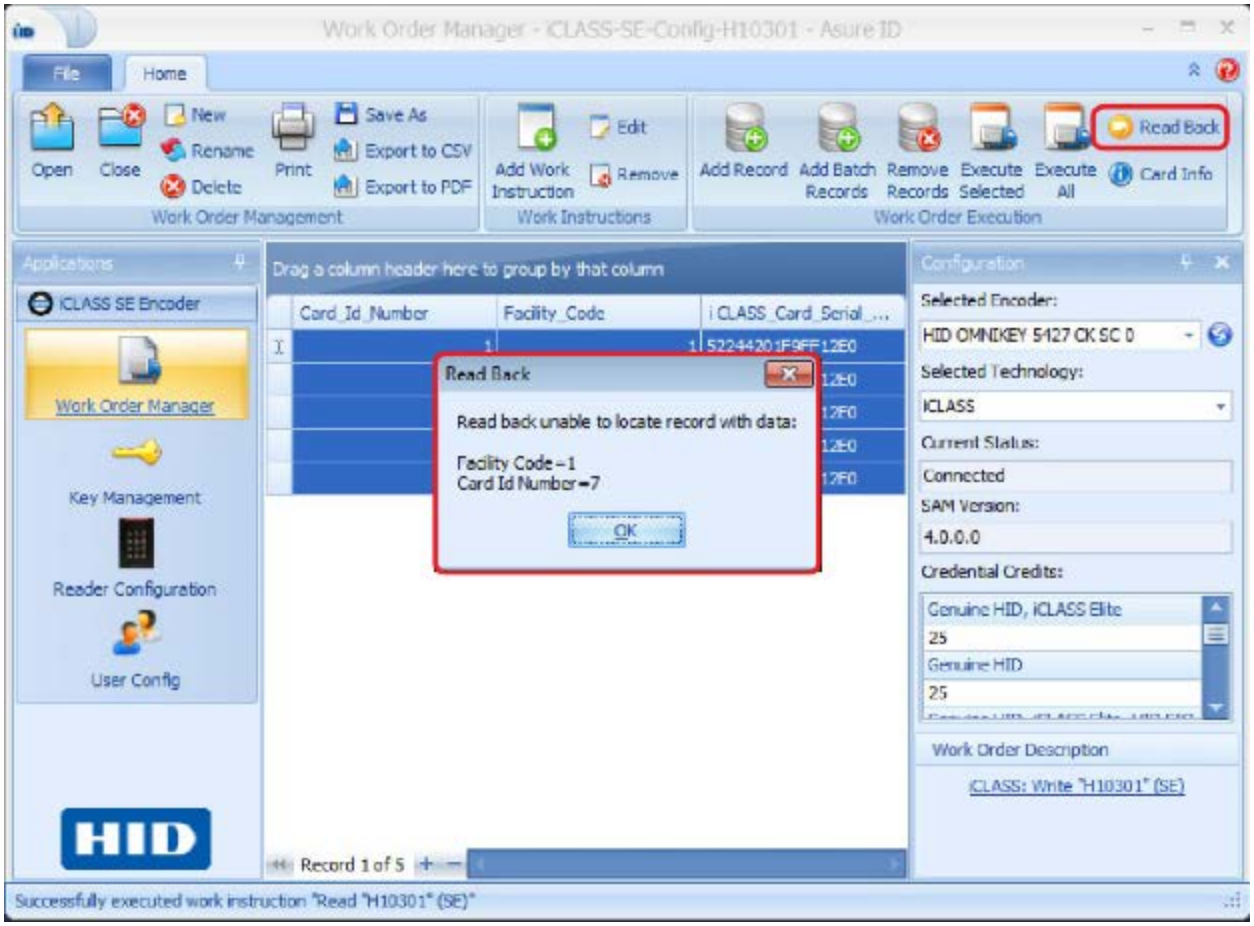
This is the same process, as **5.16.4 Execute a work order on selected credential records** above. However, you do not need to select any credential records, and the process continues until all the credential records have been executed.



5.16.6 Read back

The Read Back functionality attempts to read a card and decipher/locate its corresponding record in the data.

1. To read a card, open a Work Order with the correct technology type and format.
2. Place the card on the reader.
3. From **Work Order Manager** click **Read Back**.
4. If successful, the Credential Record information on the card appears in the Card Info window if a match is found.



Section 06

Work instruction wizard

6.1 Introduction

The Work Instruction Wizard appears any time you:

- Create a New Work Order
- Add a Work Instruction to a Work Order
- Edit a Work Instruction

There are currently five (5) technology types available, with a corresponding Work Instruction wizard.

- iCLASS
- MIFARE Classic
- MIFARE DESFire EV1
- Prox
- Seos

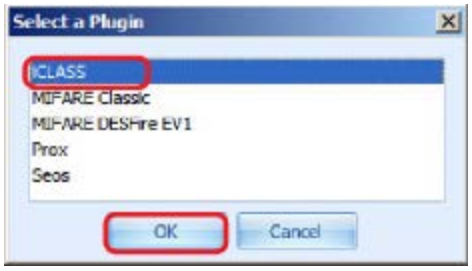
See the following sections for detailed information on each work instruction wizard.

6.2 iCLASS work instructions

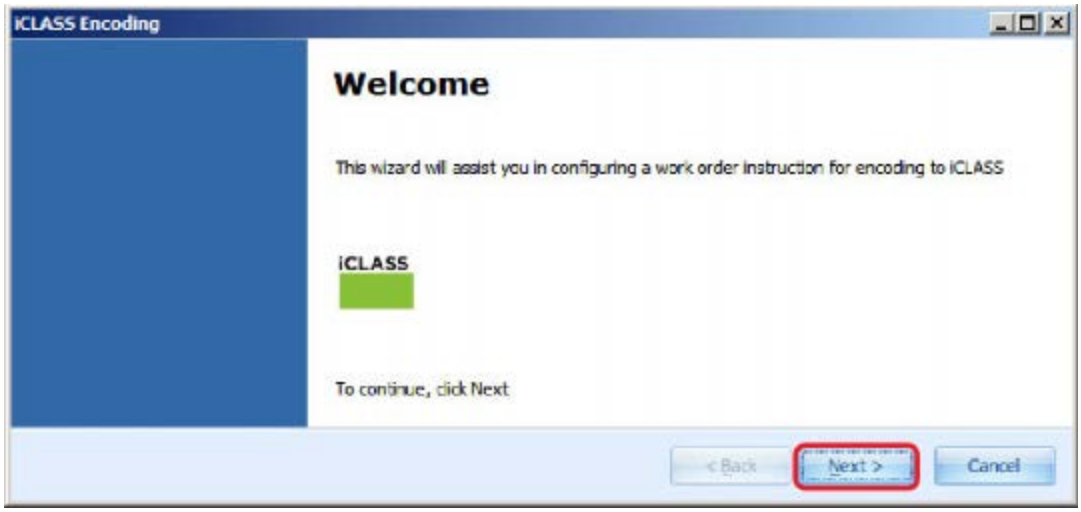
6.2.1 iCLASS: HID access application

This section covers the Work Instruction wizard for iCLASS, with the HID Access Application encoding.

1. Select the **iCLASS** technology type, and click **OK**.



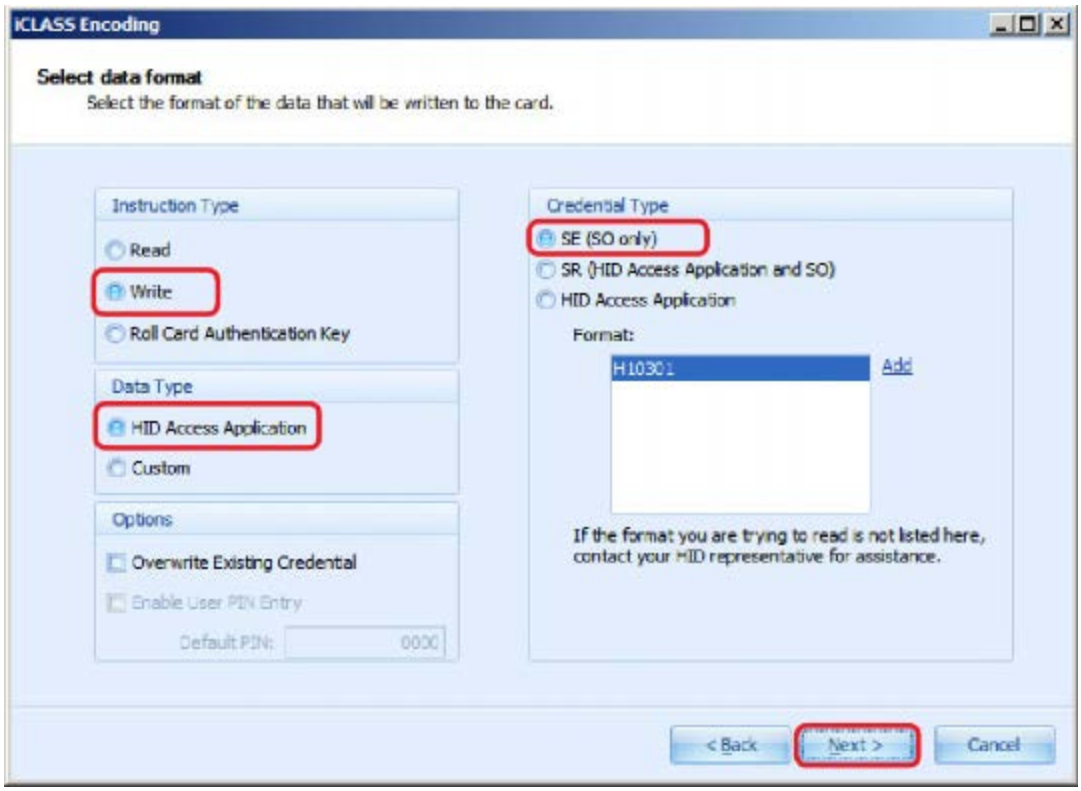
2. The Work Instruction Wizard opens to allows you to configure the Work Instruction for iCLASS. Click **Next**.



3. **Select Data Format:** You can make selections from the following. When complete click **Next**.

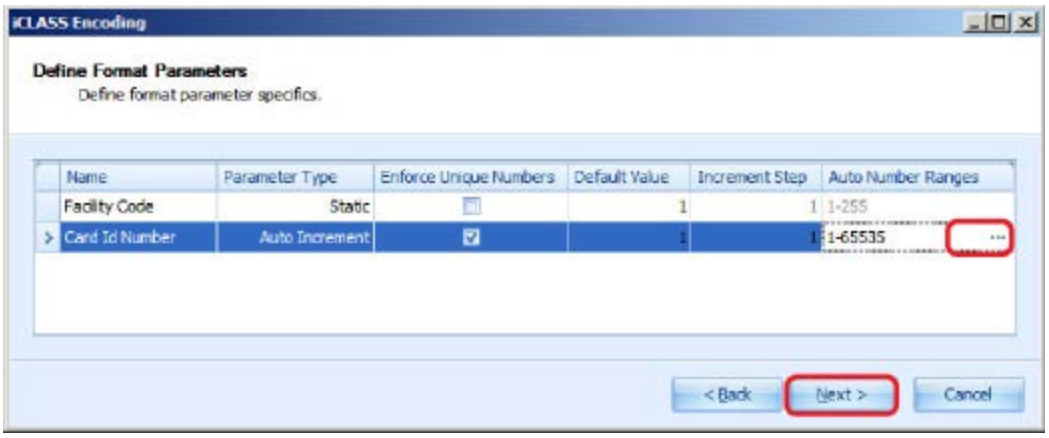
Field	Description
Instruction Type	Read, Write, or Roll Card Authentication Key
Data Type	HID Access Application, or Custom
Options	Overwrite Existing Credential: Allows the iCLASS SE Encoder to write over an application that has already been recorded in the Work Order database. Enable User PIN Entry available with SR (HID Access Application and SO only)
Credential Type	SE (SO only), SR (HID Access Application and SO), or HID Access Application. Format: Select a Format from the list.

Note: For this example a **Write/HID Application/SE (SO only)** configuration is selected.



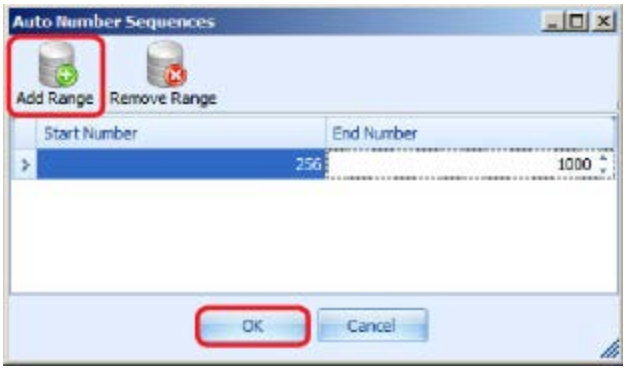
4. **Define Format Parameters:** You select, then customize each parameter defined for the selected format. Select the line to modify. Each parameter is editable with text or from a drop-down menu.

Field	Description
Name	The name is read from the Format file. It is recommended to not change this name unless necessary.
Parameter Type	This can be Auto Increment, Static, or Manual User Entry. **Note:** Type is typically determined by the Format file.
Enforce Unique Numbers	Check this box for a runtime check of the manual value entered to guarantee uniqueness, prior to executing the Work Order.
Default Value	The default Static value is used when auto-creating a new Credential record.
Increment Step	The step value used to increment Auto Number sequences.
Auto Numbers	This field sets the Auto Number Sequences for the Work Instruction. The ranges are set by selecting the ellipses (…) and entering the ranges (see following graphic).



Auto number sequences window

Select **Add Range** and set the range in the editable fields. Click **OK**.



5. Click **Next** to continue with the Wizard.

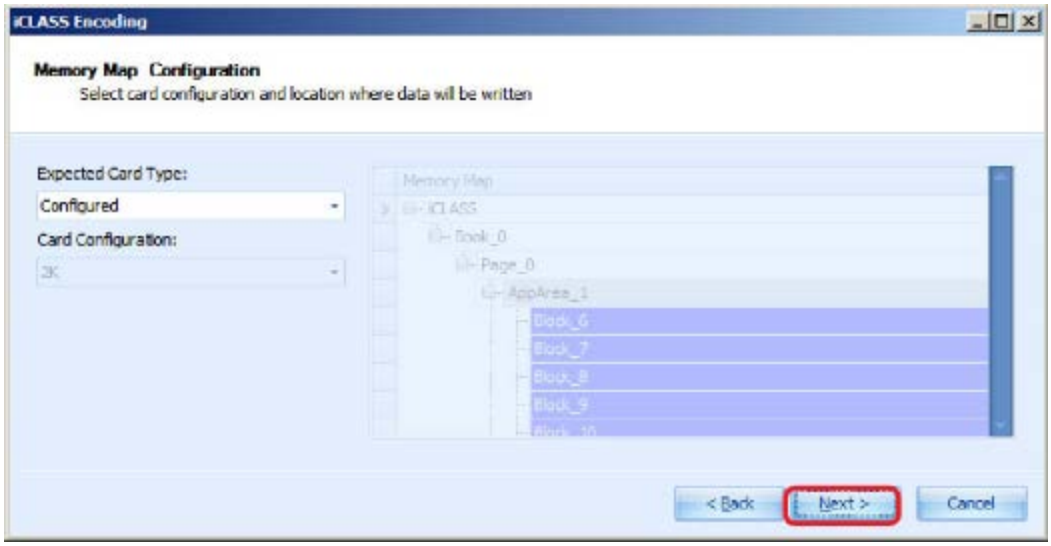
6. **Memory Map Selection:** Select card configuration and location where the data is written. Click **Next**.

Field	Description
Expected Card Type	Configured or Unconfigured. **Note:** If Configured is selected, the Card Configuration field below must be set. Unconfigured cards are not supported on CP1000 encoders.
Card Configuration	Select the memory configuration from the drop-down list. Options are: 2K (default), 16k2, 16k16, 16k2+16k1, 16k16+16k1, 2K (SO Only), 16k2 (SO Only), 16k16 (SO Only), 16k2+16k1 (SO Only), 16k16+16k1 (SO Only).

Note: Memory Map is grayed out with the **Data Type** set to *HID Access Application*, as the HID Access Application is always encoded in the same place. However, if the Data Type is set to **Custom**, the *Memory Map* is active.

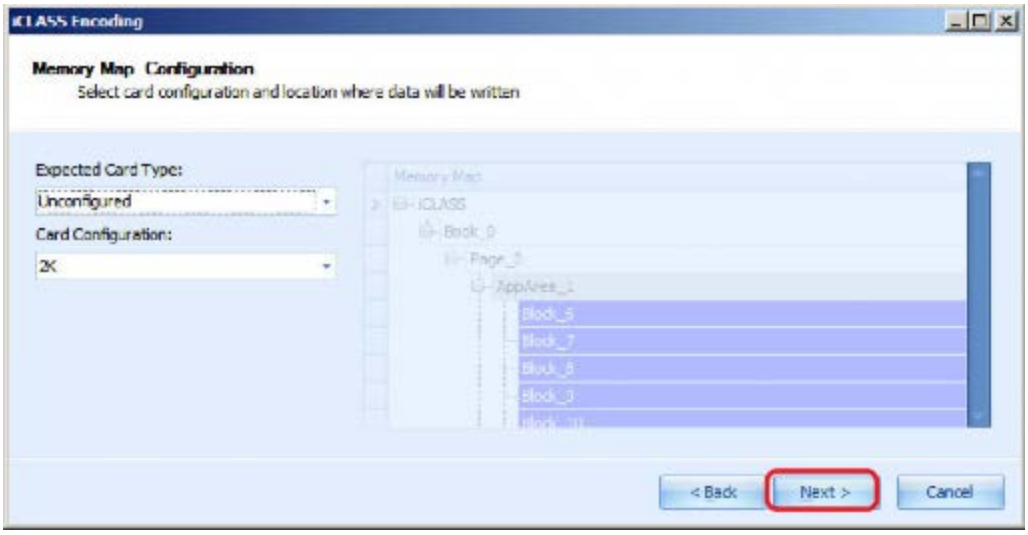
Expected card type: configured

Note: This is the default and recommended setting. All iCLASS cards shipped from the HID factory are configured, unless specifically requested.



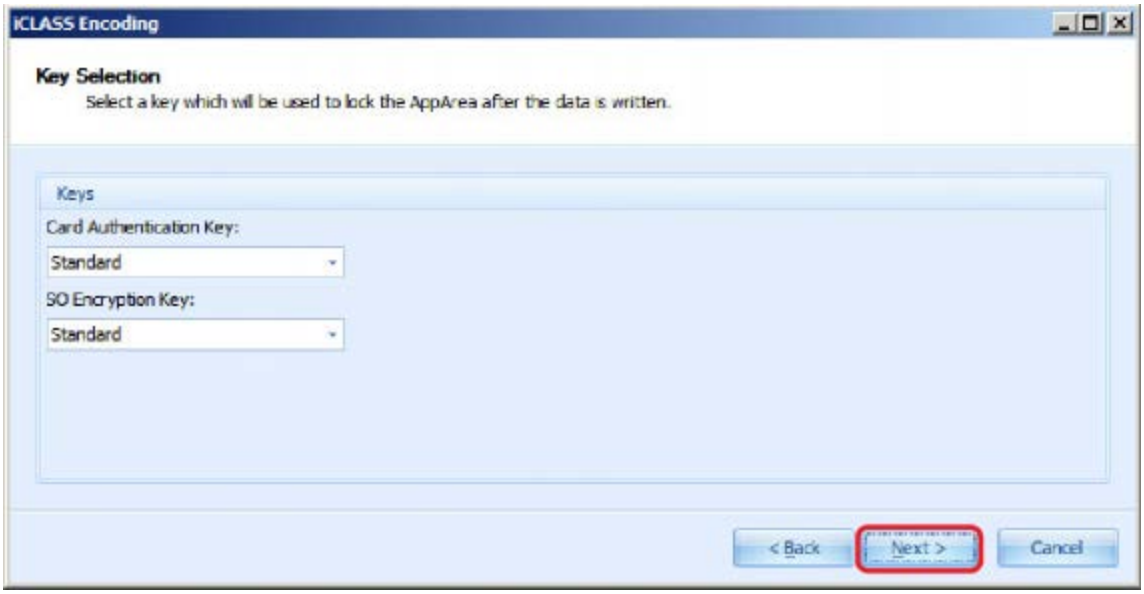
Expected card type: unconfigured

> **Note:** Not available on CP1000 encoders.



7. **Key Selection:** Select a key to lock the AppArea after the data is written, and click **Next**.

Field	Description
Card Authentication Keys	Custom or HID defined Key Sets may be selected.
SO Encryption Key	Custom or HID defined SO Encryption Key Sets may be selected.

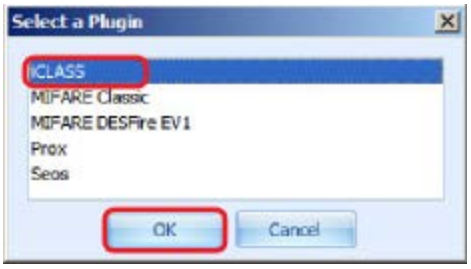


8. You have completed the wizard. Click **Finish**.
9. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.2.2 iCLASS: custom encoding

This section covers the Work Instruction wizard for iCLASS, with Custom Encoding.

1. Select the **iCLASS** technology type, and click **OK**.

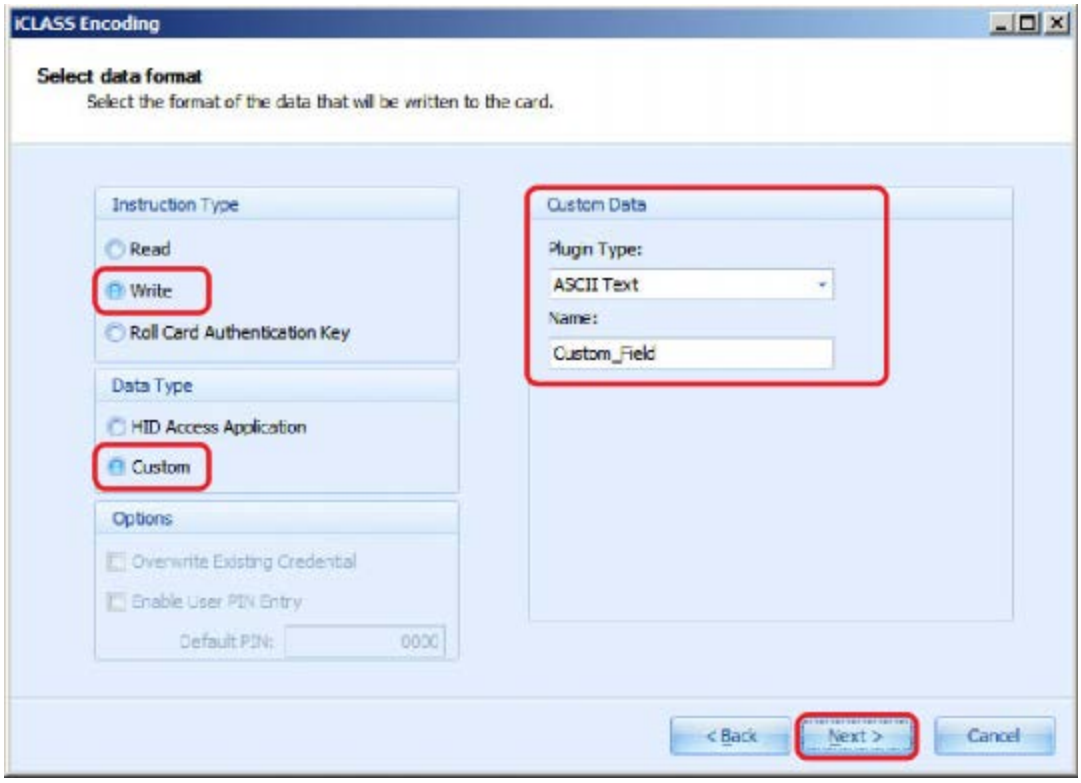


2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for iCLASS. Click **Next**.

3. **Select Data Format:** You can make selections from the following. When complete click **Next**.

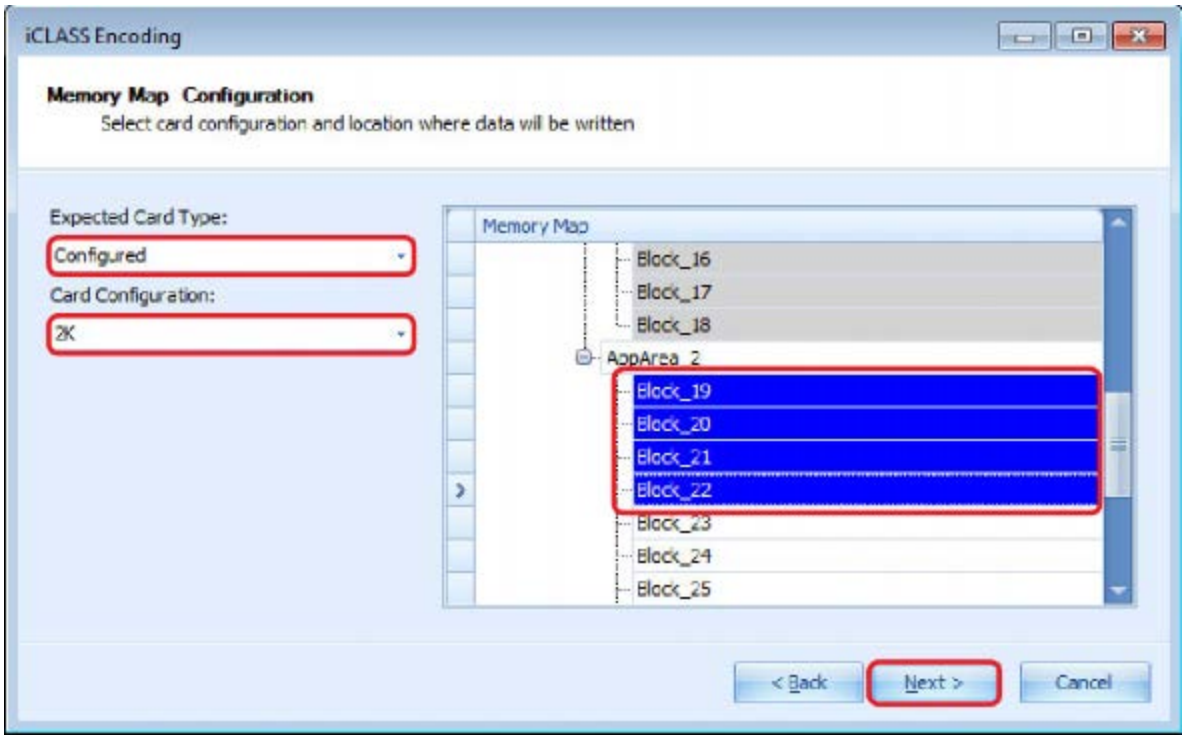
Field	Description
Instruction Type	Read, Write, or Roll Card Authentication Key
Data Type	For this example **Custom** must be selected.
Options	Not available with Custom.
Custom Data	Plugin Type: ASCII Text, Hexadecimal Data, Unicode Text, and Integer. Name: Modify the Name, if needed. **Note:** Name field constitutes column in Work Order data view.

Note: For this example Write/Custom/ASCII Text/Custom_Field configuration is selected.



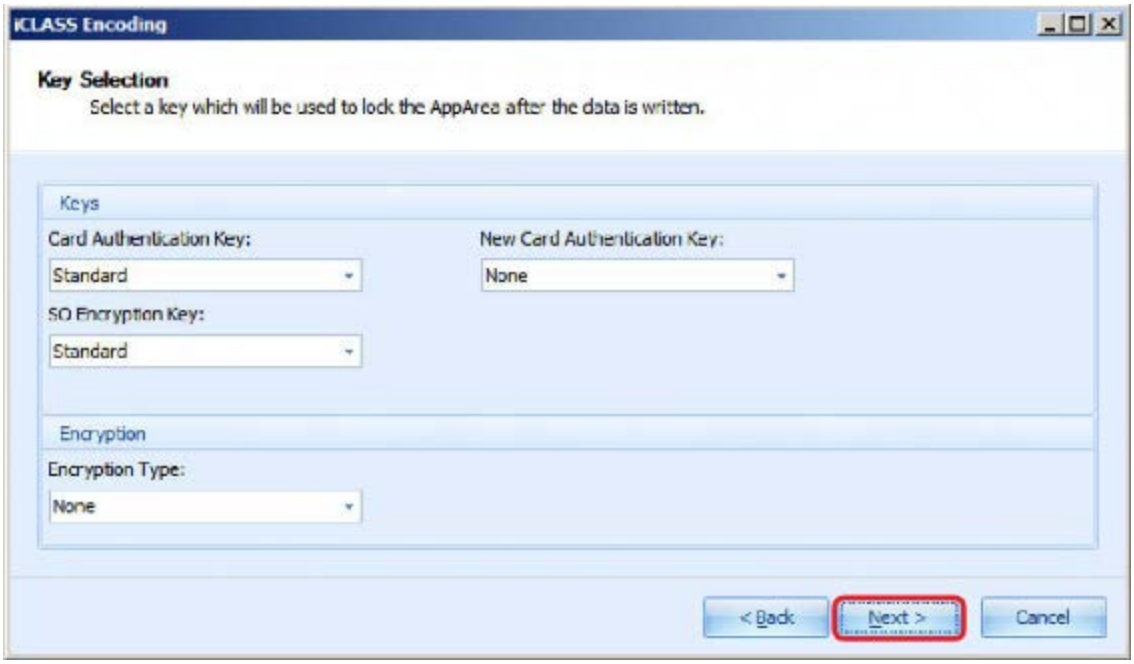
4. **Memory Map Selection:** Select card configuration and location where the data is written. Click **Next**.

Field	Description
Expected Card Type	Configured or Unconfigured. **Note:** Unconfigured cards are not supported on CP1000 encoders.
Card Configuration	Select the memory configuration from the drop-down list. Options are: 2K, 16k2, 16k16, 16k2+16k1, 16k16+16k1, 2K (SO Only), 16k2 (SO Only), 16k16 (SO Only), 16k2+16k1 (SO Only), 16k16+16k1 (SO Only) Default is 2K.
Memory Map	Define (select) the AppArea/Block. **Note:** This field can be scrolled.



5. **Key Selection:** Select a key to lock the AppArea after the data is written, and click **Next**.

Field	Description
Keys	Card Authentication Key: Custom or HID defined Key Sets may be selected. Select the key used to authenticate to the key currently securing the AppArea to encode. SO Encryption Key: Custom or Standard Key Sets may be selected. New Card Authentication Key: None or Custom Key Sets may be selected. Select a new key here only to change the key that is used to secure this AppArea.
Encryption	Encryption Type: None, or 3DES Encryption Key: This field appears with the 3DES selection above. Select the Encryption Keys loaded. This encrypts the data on the card. Data must be decrypted accordingly, when read by 3rd-party applications.



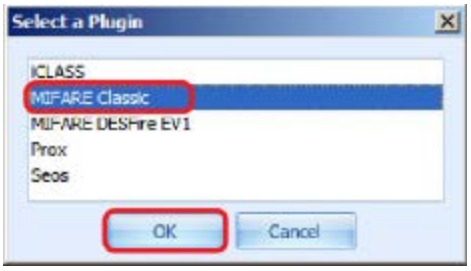
6. You have completed the wizard. Click **Finish**.
7. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.3 MIFARE Classic work instructions

6.3.1 MIFARE Classic: HID access application

This section covers the Work Instruction for MIFARE Classic, with HID Access Application encoding.

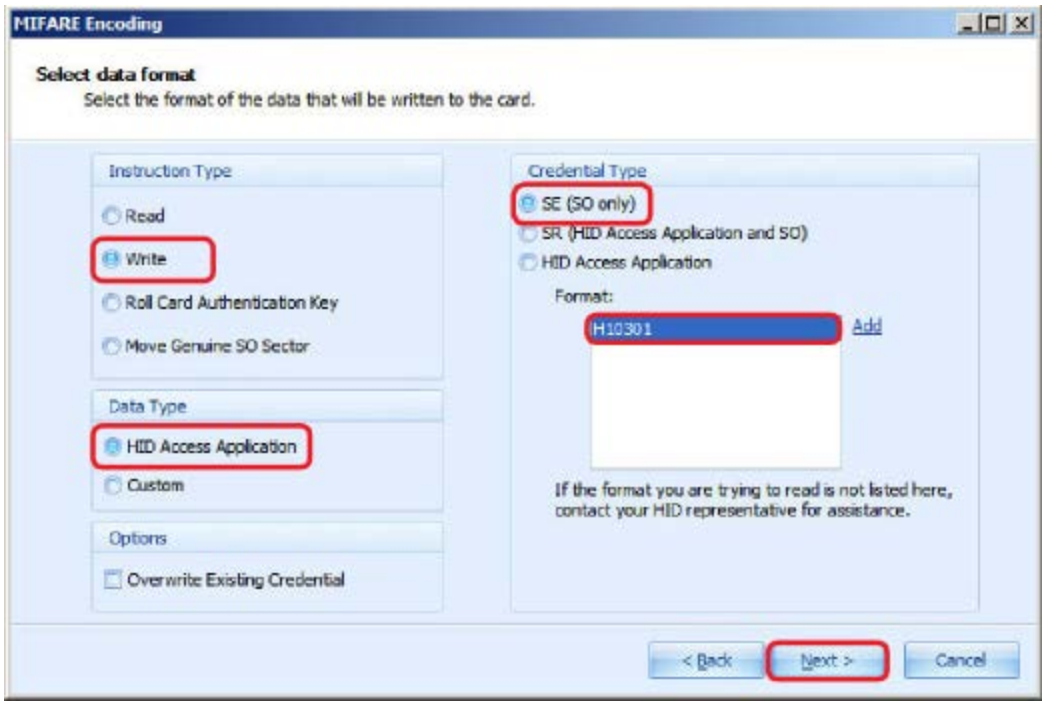
1. Select the **MIFARE Classic** technology type, and click **OK**.



2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for MIFARE Classic. Click **Next**.
3. **Select Data Format:** You can make selections from the following. When complete click **Next**.

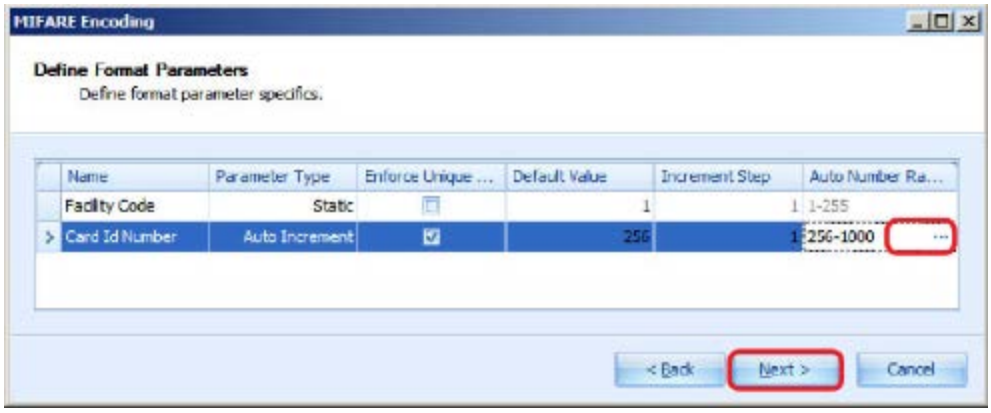
Field	Description
Instruction Type	Read, Write, Roll Card Authentication Key, or Move Genuine SO Sector
Data Type	HID Access Application, or Custom
Options	Overwrite Existing Credential: Allows the iCLASS SE Encoder to write over an application that has already been recorded in the Work Order database.
Credential Type	SE (SO only), SR (HID Access Application and SO), or HID Access Application. Format: Select a Format from the list.

Note: For this example, a Write/HID Application/SE configuration is selected.



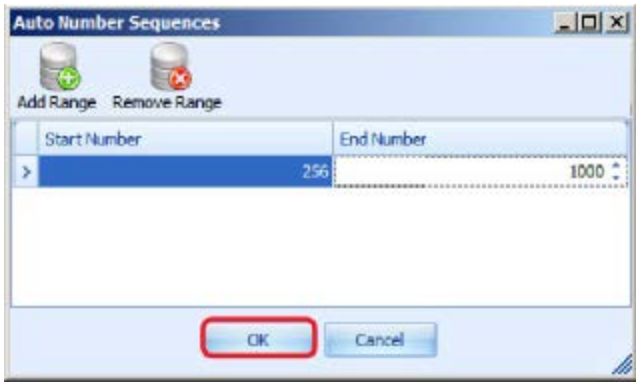
4. **Define Format Parameters:** Select, to define each parameter for the selected format. Select the line to modify, each parameter is editable with text or from a drop-down menu.

Field	Description
Name	The name is read from the Format file. It is recommended to not change this name unless necessary.
Parameter Type	This can be Auto Increment, Static, or Manual User Entry.
Enforce Unique Numbers	Check this box for a runtime check of the manual value entered to guarantee uniqueness, prior to executing the Work Order.
Default Value	The default Static value for Static and Manual parameters.
Increment Step	The step value used to increment Auto Number sequences.
Auto Numbers	This field sets the Auto Number Sequences for the Work Instruction. The ranges are set by selecting the ellipses (…) and entering the ranges. See following graphic.



Auto number sequences window

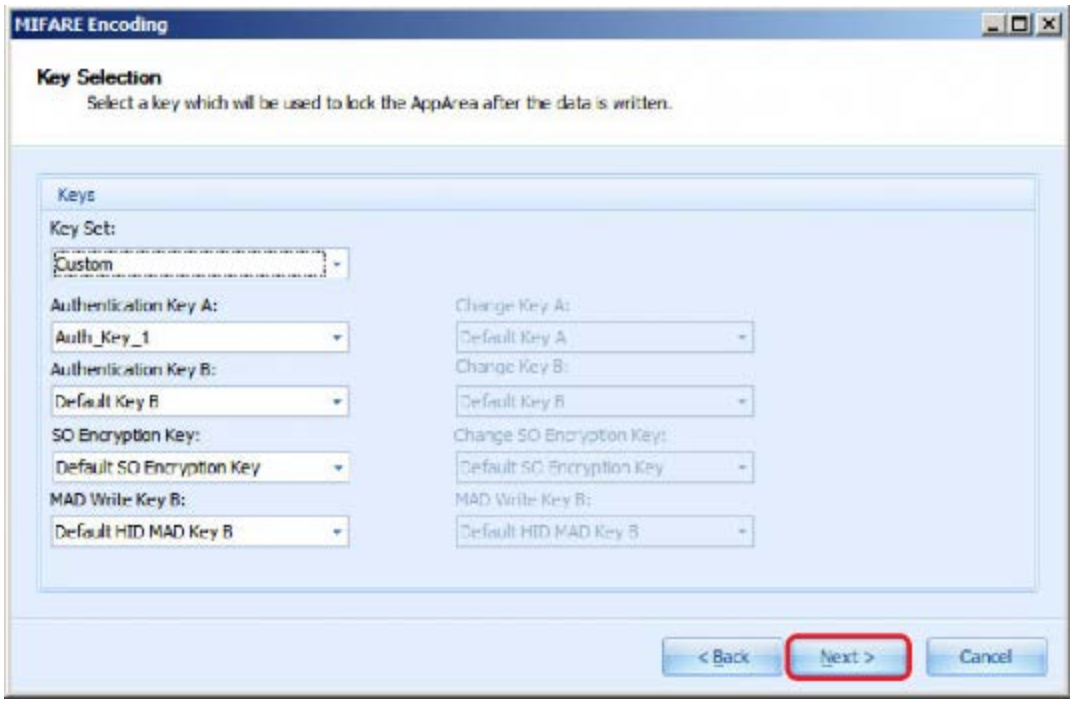
Select **Add Range** and set the range in the editable fields. Click **OK**.



5. Click **Next** to continue with the Wizard.

6. **Key Selection:** Select a key to lock the AppArea after the data is written, and click **Next**.

Field	Description
Keys	Key Set: Standard, Custom or HID defined Key Sets may be selected. Authentication Keys are the keys currently used to protect the Sector. Select Default if working with a blank card or Sector. Authentication Key A: Select an option from the drop-down menu. Authentication Key B: Select an option from the drop-down menu. SO Encryption Key: Select an option from the drop-down menu. Note: Only available when writing SE or SR cards. MAD Write Key B: Select an option from the drop-down menu.



7. The wizard is complete. Click **Finish**.
8. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.3.2 MIFARE Classic: custom encoding

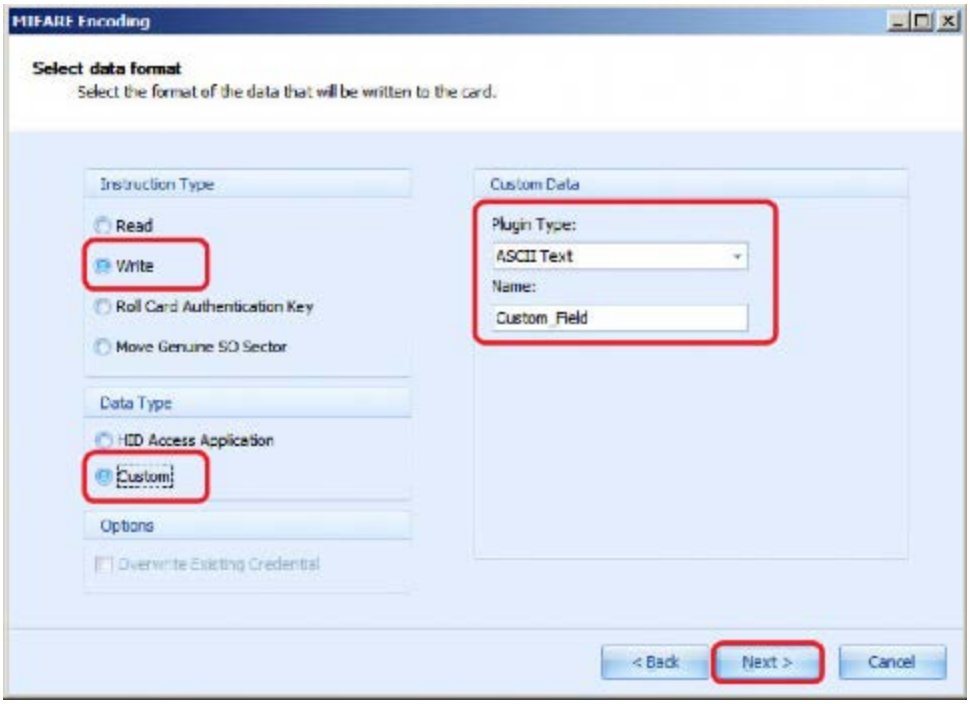
This section covers the Work Instruction wizard for MIFARE Classic, with Custom Encoding.

1. Select the **MIFARE Classic** technology type. Click **OK**.

2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for MIFARE Classic. Click **Next**.
3. **Select Data Format:** You can make selections from the following. When complete, click **Next**.

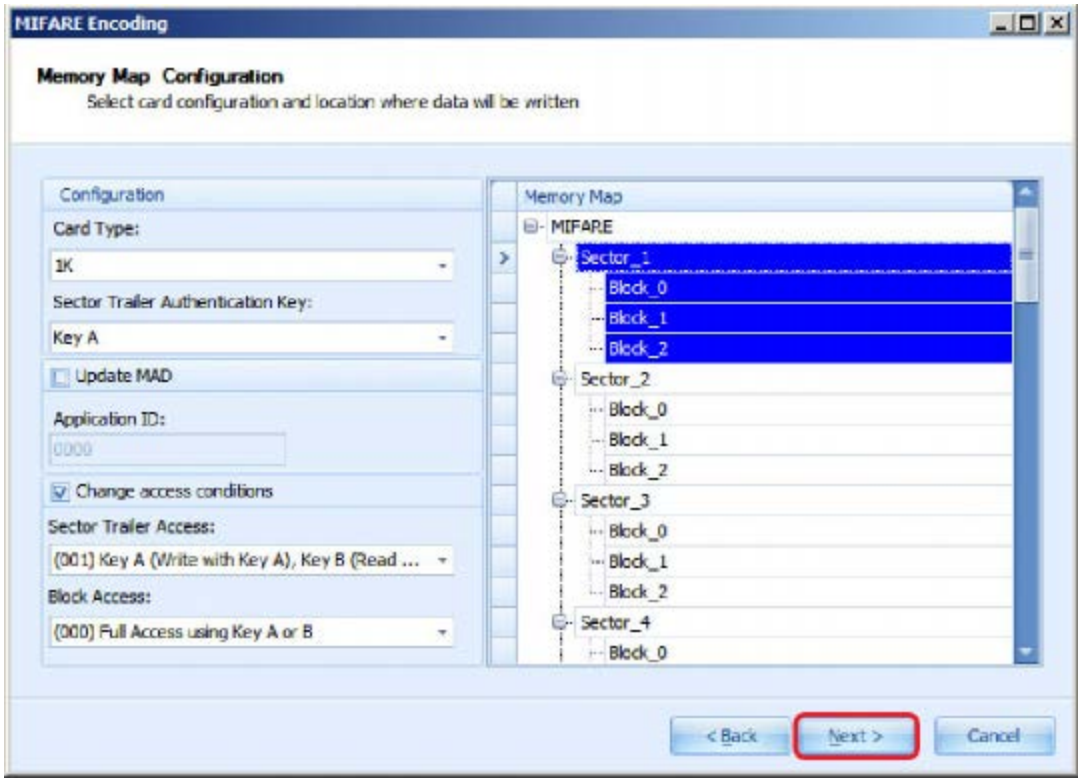
Field	Description
Instruction Type	Read, Write, Roll Card Authentication Key, or Roll Card Authentication Key.
Data Type	For this example **Custom** must be selected.
Options	Not available with **Custom**.
Custom Data	**Plugin Type**: ASCII Text, Hexadecimal Data, Unicode Text, or Integer. **Name**: Modify the Name, if needed. **Note:** Name field constitutes column in Work Order data view.

Note: For this example a **Write/Custom/ASCII Text/Custom_Field** configuration is selected.



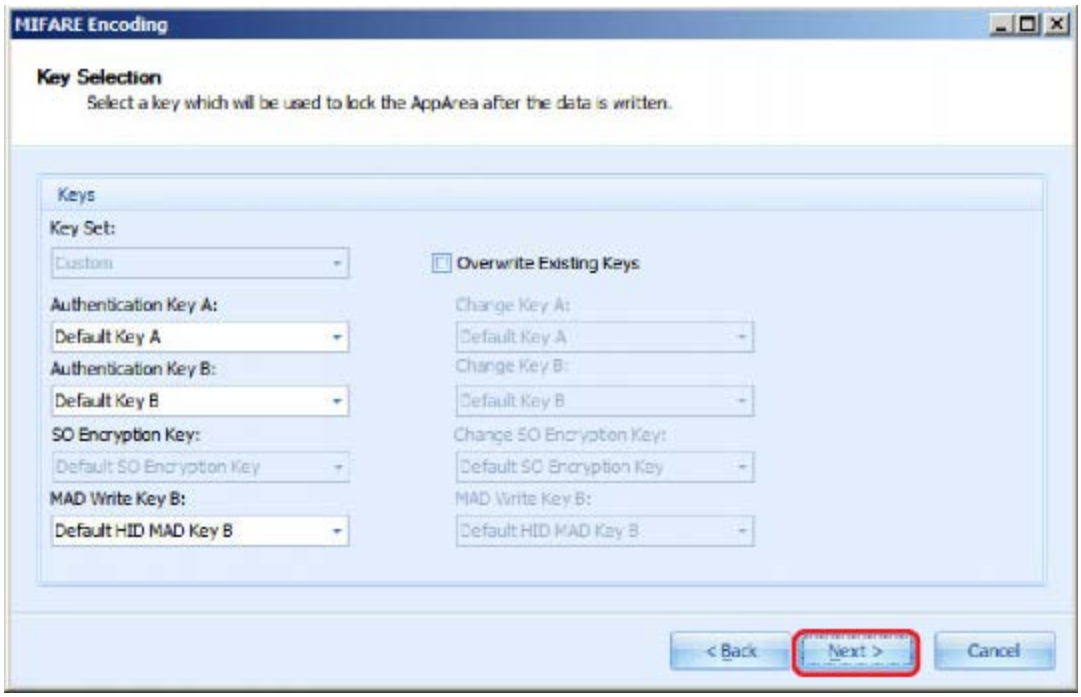
4. **Memory Map Selection:** Select card configuration and location where the data is written. Click **Next**.

Field	Description
Configuration	**Card Type**: 1K, or 4K Sector Trailer Authentication Key: Key A, or Key B
Update MAD	Select the check box to update the MIFARE Application Directory (MAD). **Note:** This is an optional parameter (sector 0 is always reserved for this purpose). **Application ID**: Enter the Application ID your company has registered with NXP to update.
Change access conditions	Select the check box to Change access conditions **Sector Trailer Access**: Select an option from the drop-down menu. **Note:** See the NXP Datasheet for more detail on Sector Trailer. **Block Access**: Select an option from the drop-down menu.
Memory Map	Define (select) the MIFARE Sector/Block (scrollable field). **Note:** The legacy HID application can be encoded on Sector 1. This is a fixed location. The HID SIO application can be encoded in Sector 4 generally, but can be moved.



5. **Key Selection:** Select a key to lock the AppArea after the data is written. Click **Next**.

Field	Description
Keys	Key Set: Not an option. Authentication Keys are the keys currently used to protect the Sector. Select Default if working with a blank card or Sector. Authentication Key A: Select an option from the drop-down menu. Authentication Key B: Select an option from the drop-down menu. SO Encryption Key: Not available with the Custom option. MAD Write Key B: Select an option from the drop-down menu.

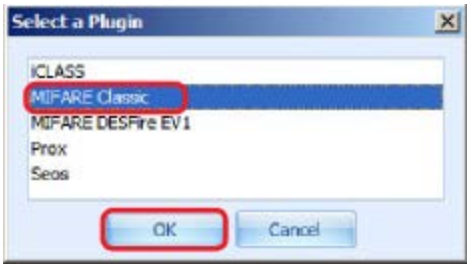


6. The wizard is complete. Click **Finish**.
7. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.3.3 MIFARE Classic: move genuine SO sector

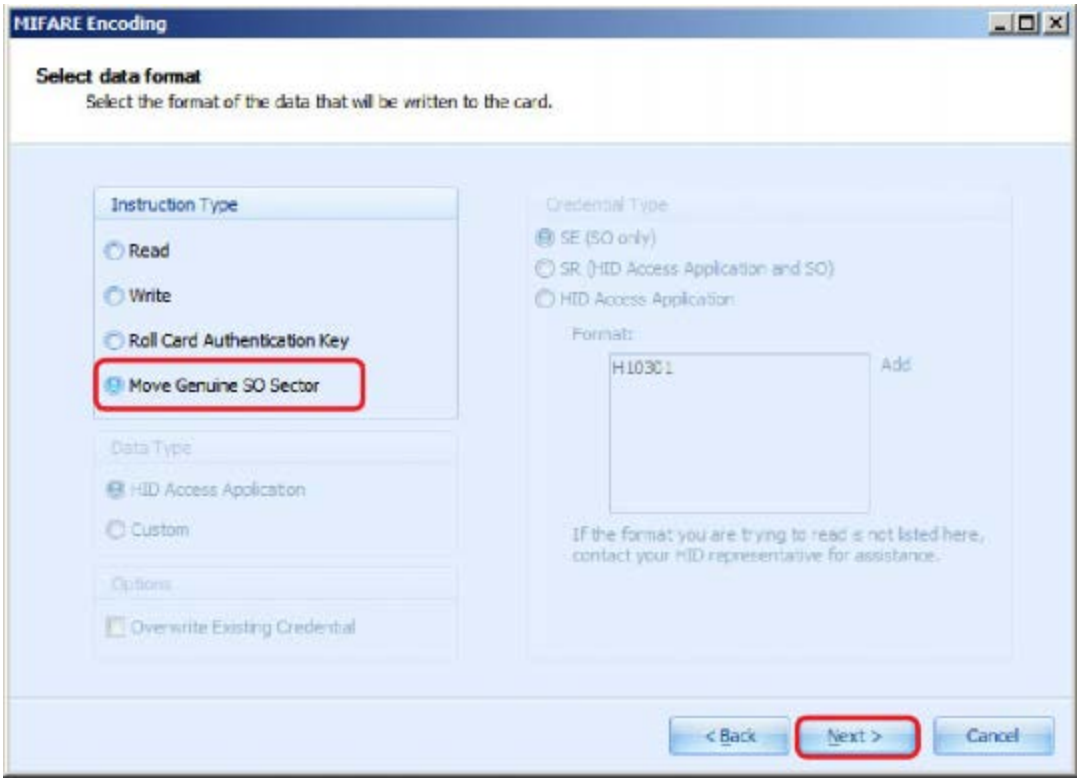
This section covers the Work Instruction wizard for Move Genuine SO Sector process.

1. Select the **MIFARE Classic** technology type. Click **OK**.



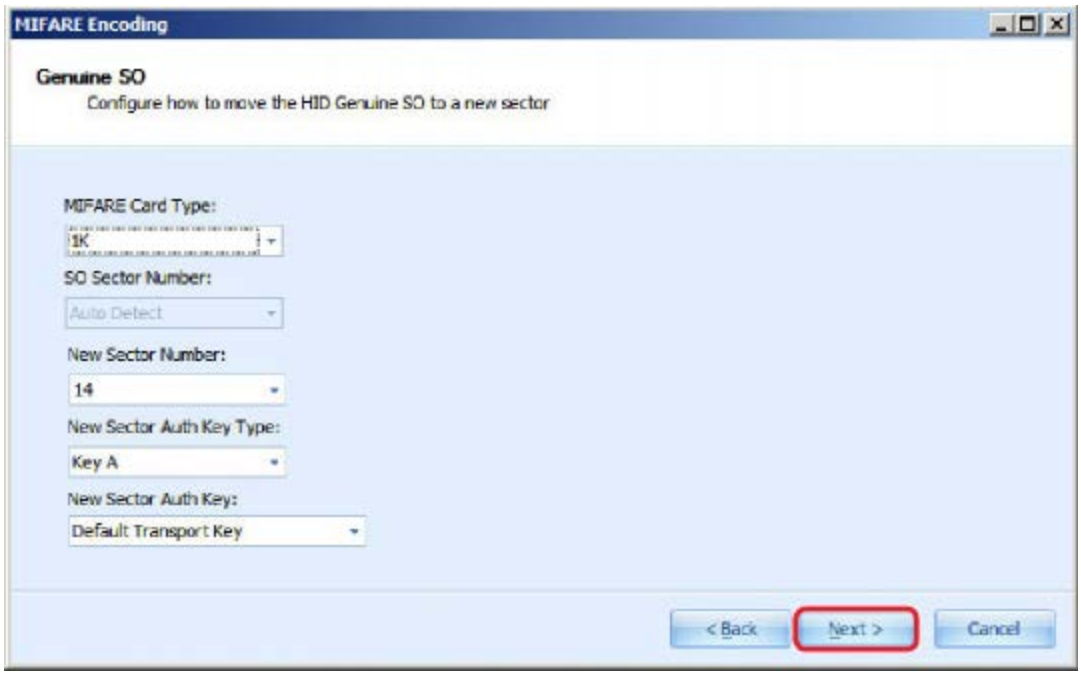
2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for Prox. Click **Next**.
3. **Select Data Format:** Select the following. When complete click **Next**.

Field	Description
Instruction Type	Move Genuine SO Sector



4. Configure the HID Genuine SO to a new sector. Click **Next**.

Field	Description
MIFARE Card Type	Options are: 1K or 4K
SO Sector Number	Auto Detect
New Sector Number	Select new sector number from the drop-down menu. Range is 1-15
New Sector Auth Key Type	Options are: Key A or Key B.
New Sector Auth Key	Options are Default Transport Key, or defined Authentication key. **Note:** If a key is selected other than HID Standard, the reader needs to be configured with the MIFARE Key Set you are using for the SO Sector. See 8.9 Load HID application keys for details.



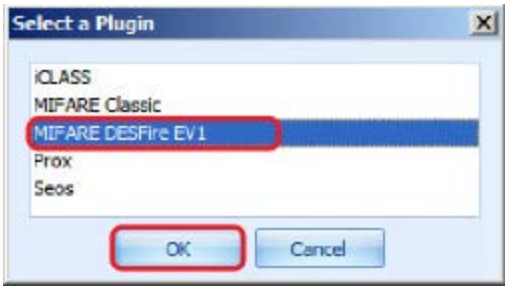
5. When the wizard is complete, click **Finish**.
6. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.4 MIFARE DESFire EV1 work instructions

6.4.1 MIFARE DESFire EV1: HID access application

This section covers the Work Instruction for MIFARE DESFire EV1, with HID Access Application encoding.

1. Select the **MIFARE DESFire EV1** technology type. Click **OK**.

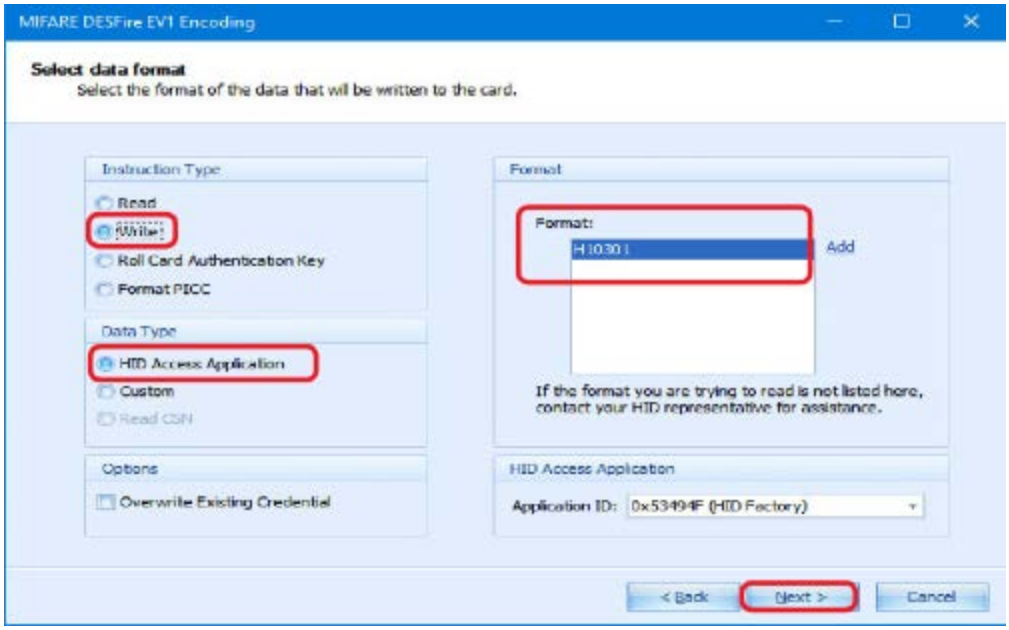


2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for MIFARE DESFire EV1. Click **Next**.

3. **Select Data Format:** You can make selections from the following. When complete click **Next**.

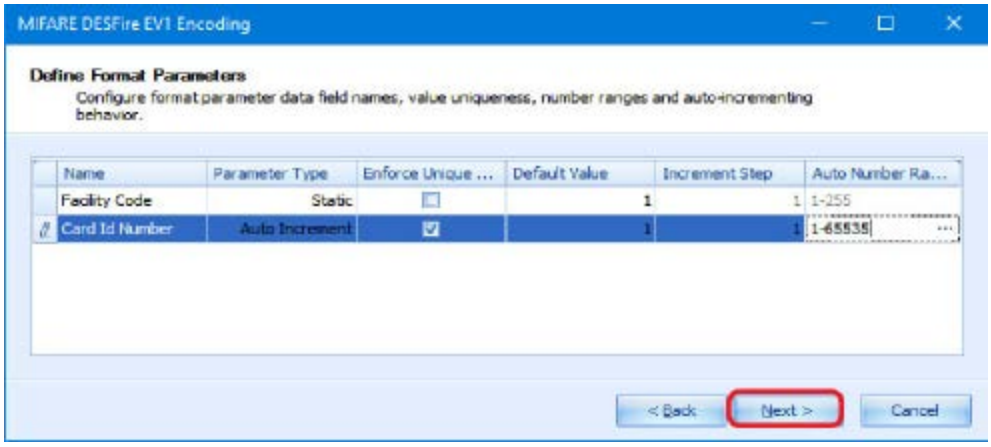
Field	Description
Instruction Type	Read, Write, or Roll Card Authentication Key
Data Type	HID Access Application, or Custom
Options	Overwrite Existing Credential: Allows the iCLASS SE Encoder to write over an application that has already been recorded in the Work Order database.
Format	Select a Format from the list.
HID Access Application	A physical access control (PAC) application that allows a smart card to be used for physical access into a building or secured area. Application ID: The reference identifier for an application on a card.

Note: For this example, a Write/HID Access Application configuration is selected.



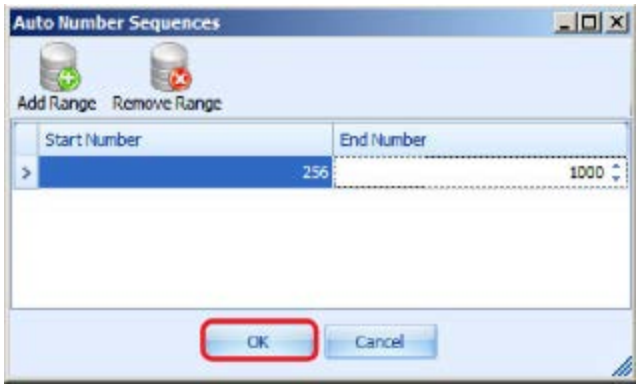
4. **Define Format Parameters:** Select to define each parameter for the chosen format. Select the line to modify. Each parameter is editable with text or from a drop-down menu.

Field	Description
Name	The name is read from the Format file. It is recommended to not change this name unless necessary.
Parameter Type	This can be Auto Increment, Static, or Manual User Entry.
Enforce Unique Numbers	Check this box for a runtime check of the manual value entered to guarantee uniqueness, prior to executing the Work Order.
Default Value	The default Static value for Static and Manual parameters.
Increment Step	The step value used to increment Auto Number sequences.
Auto Numbers	This field sets the Auto Number Sequences for the Work Instruction. The ranges are set by selecting the ellipses (…) and entering the ranges. See following graphic.



Auto number sequences window

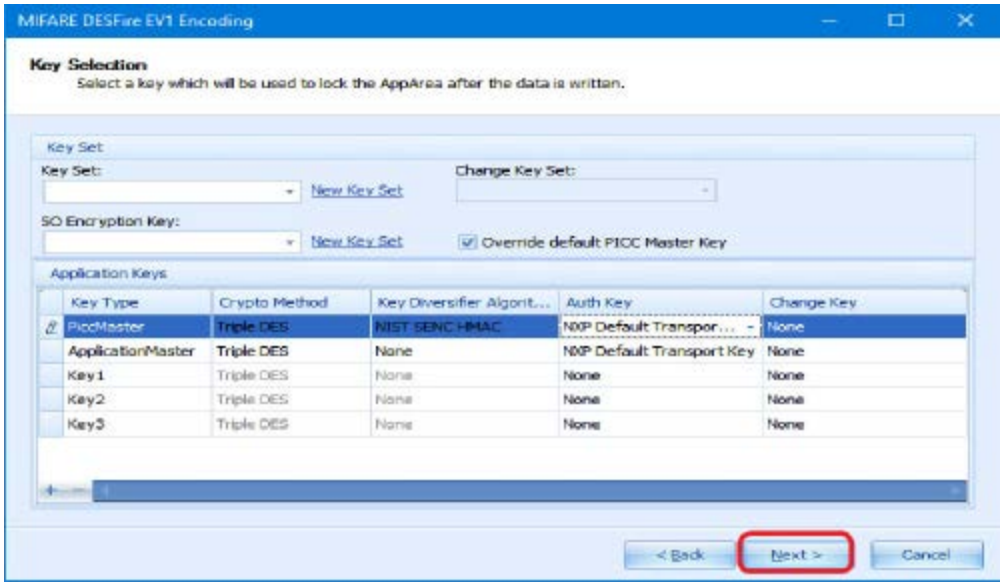
Select **Add Range** and set the range in the editable fields. Click **OK**.



5. Click **Next** to continue with the Wizard.

6. **Key Selection:** Select a key to lock the AppArea after the data is written, and click **Next**.

Field	Description
Key Set	Key Set: Custom or HID defined key sets may be selected Change Key Set: Standard (No option). SO Encryption Key: Key set used to encrypt the SO credential. Standard, Custom, or HID defined key sets may be selected. Override default PICC Master Key: Allows you to override the HID Standard or Elite PICC Master key on a DESFIRE card.
Application Keys	
Key Type	Displays the Key type.
Crypto Method	Triple DES, AES, or 3 Key Triple DES (24 byte keys)
Key Diversifier Algorithm	None, NIST SENC HMAC, NXP AV1 1 Key Triple DES, or NXP AV1 2 Key Triple DES
Auth Key	None, NXP Default Transport Key, or HID SO PICC Master Key. Also custom Auth Key is listed.

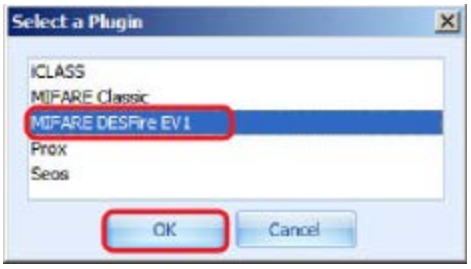


7. The wizard is complete. Click **Finish**.
8. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.4.2 MIFARE DESFire EV1: custom encoding

This section covers the Work Instruction wizard for MIFARE DESFire EV1, with Custom Encoding.

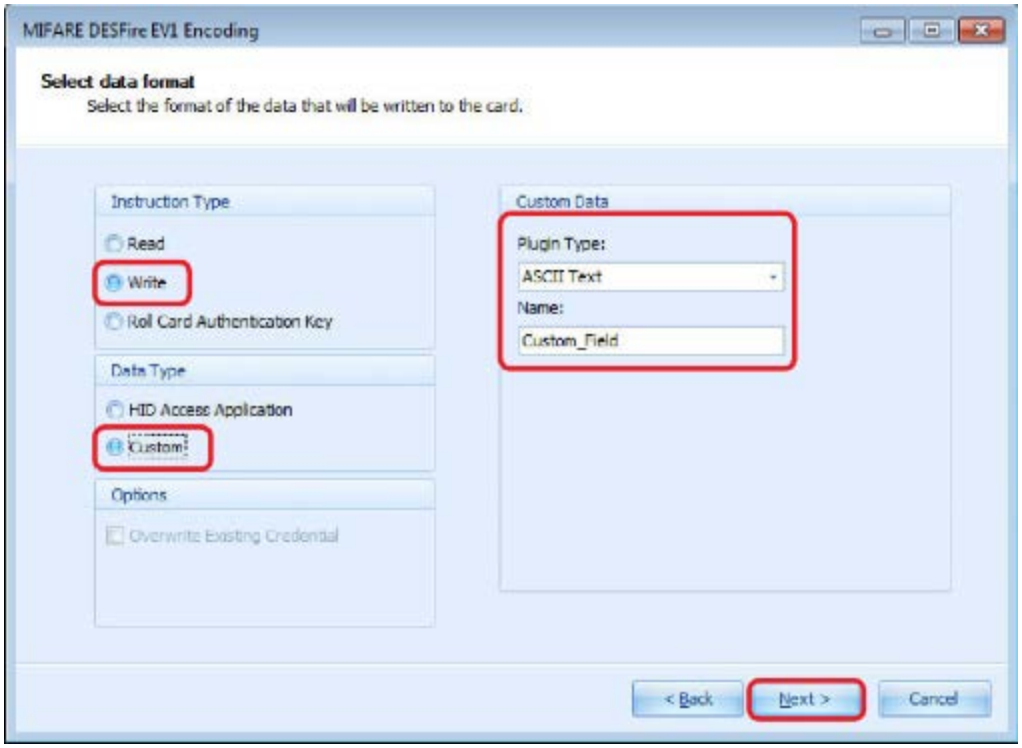
1. Select the **MIFARE DESFire EV1** technology type. Click **OK**.



2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for MIFARE DESFire EV1. Click **Next**.
3. **Select Data Format:** You can make selections from the following. When complete click **Next**.

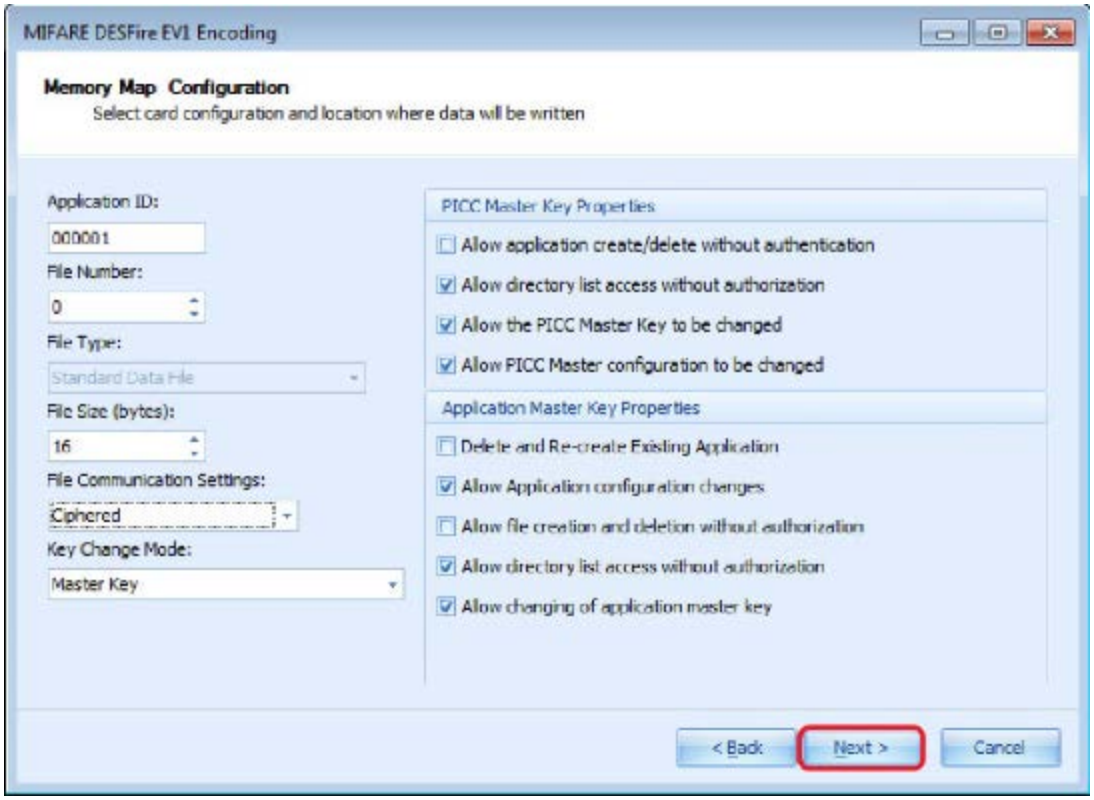
Field	Description
Instruction Type	Read, Write, Roll Card Authentication Key, or Move Genuine SO Sector
Data Type	For this example **Custom** must be selected.
Options	Not available with **Custom**.
Custom Data	**Plugin Type**: ASCII Text, Hexadecimal Data, Unicode Text **Name**: Modify the Name, if needed. Note: Name field constitutes column in Work Order data view.

> **Note:** For this example, a **Write/Custom/ASCII Text/Custom_Field** configuration is selected.



4. **Memory Map Selection:** Select the card configuration and location where the data is to be written. Click **Next**.

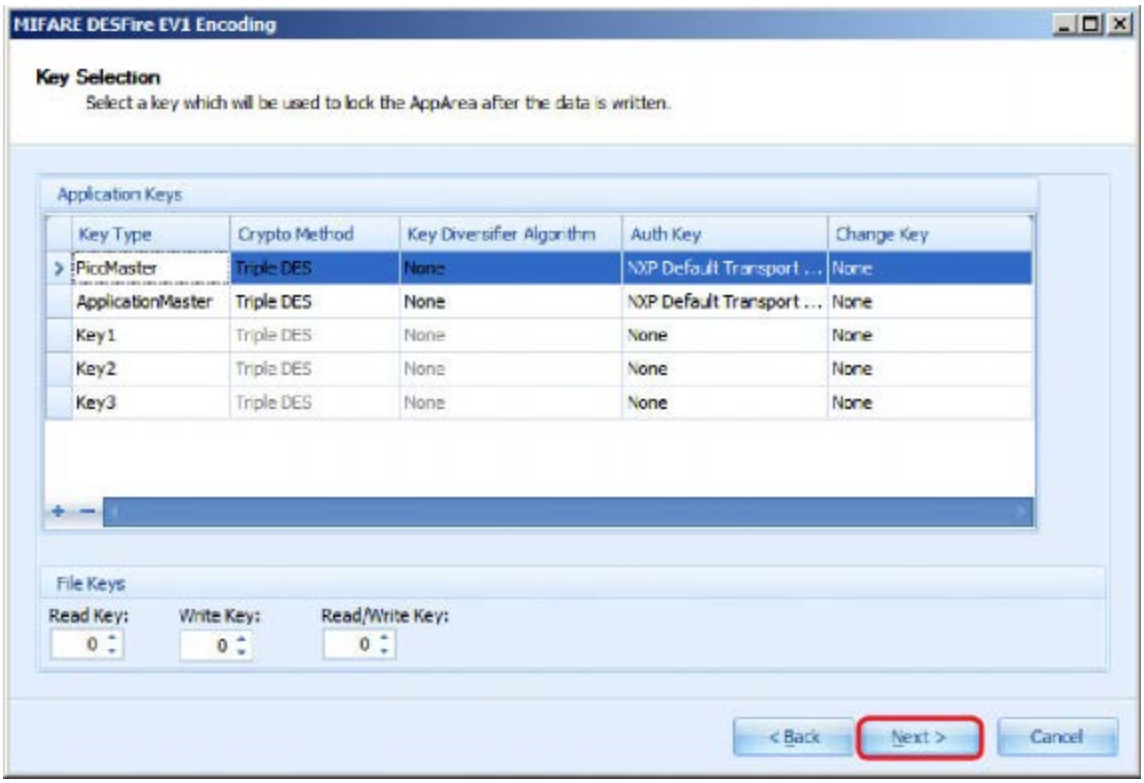
Field	Description
Application ID	Enter the 3-byte Application ID your company has registered with NXP, in hexadecimal form.
File Number	Select the file number (Range 0-31).
File Type	**Standard Data File** is the only supported option.
File Size (bytes)	Select the file size in bytes. Default is 16 bytes.
File Communication Settings	Select **Ciphered** or **Plain** for this example.
Key Change Mode	To change a key, requires authentication with the following: Master Key, Key 1-13, Authenticate with key to be changed, or Do not allow keys to be changed
PICC Master Key Properties	Select the PICC Master Properties from the list. **Note:** These options can only be managed when working with a blank card.
Application Master Key Properties	Select the Application Properties from the list.



5. **Key Selection:** Set the Application Key options in accordance with the NXP datasheets, and click **Next.** All options can be set from the associated drop-down menu.

> **Note:** Selections must abide by the rules you set up for the card.

Field	Description
Application Keys	
Key Type	Displays the Key type.
Crypto Method	Triple DES, AES, or 3 Key Triple DES (24 byte keys)
Key Diversifier Algorithm	None, NXP AV1 1 Key Triple DES, or NXP AV1 2 Key Triple DES
Auth Key	The key used to authenticate to the key specified by Key Type. None: To signify the key is not used. None is only valid for optional Keys 1-13. NXP Default Transport Key: For blank cards, typically NXP Default Transport key is used. Custom Keys: Custom Keys is listed, if they are 16 bytes or larger and have been loaded to the currently selected encoder using the Key Manager. If the card contains non-default keys (either loaded at the factory or by 3rd party), than the proper custom key must be selected that can authenticate for the specified Key Type.
Change Key	The Change Key is used only if you desire that the current key be changed during the encoding operation. None: To signify the key is not changed. NXP Default Transport Key: For blank cards, typically NXP Default Transport key is used. Custom Keys: Custom Keys is listed, if they are 16 bytes or larger and have been loaded to the currently selected encoder using the Key Manager.
File Keys Note: Keys selected in the following must be configured in the Application Keys section above	
Read Key	Select Read Key number (Range 0-13). Default is 0. Note: 0 indicates that the Application Master Key is used to provide access to the file.
Write Key	Select Write Key number (Range 0-13). Default is 0. Note: 0 indicates that the Application Master Key is used to provide access to the file.
Read/Write Key	Select Read/Write Key number (Range 0-13). Default is 0. Note: 0 indicates that the Application Master Key is used to provide access to the file.



6. When wizard is complete, click **Finish**.
7. Return to **5.6 Create a work order**, step 5 to save the Work Order.

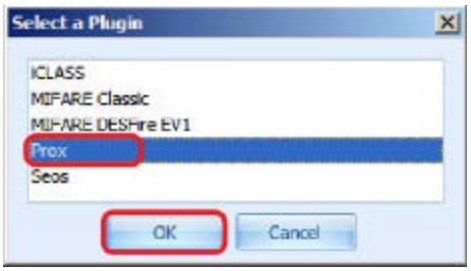
6.5 Prox work instructions

6.5.1 Prox: HID access application

This section covers the Work Instruction wizard for Prox, with the HID Access Application encoding.

Note: This encoding only works with Genuine HID Prox credentials.

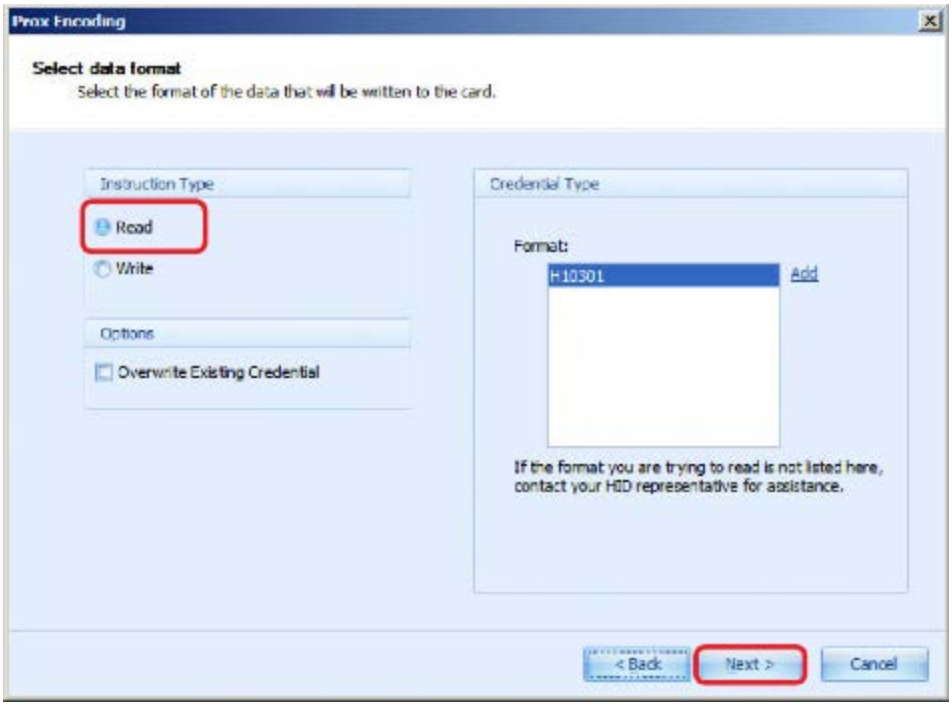
1. Select the **Prox** technology type. Click **OK**.



2. The Work Instruction Wizard opens to allows you to configure the Work Instruction for Prox. Click **Next**.
3. **Select Data Format:** You can make selections from the following. When complete click **Next**.

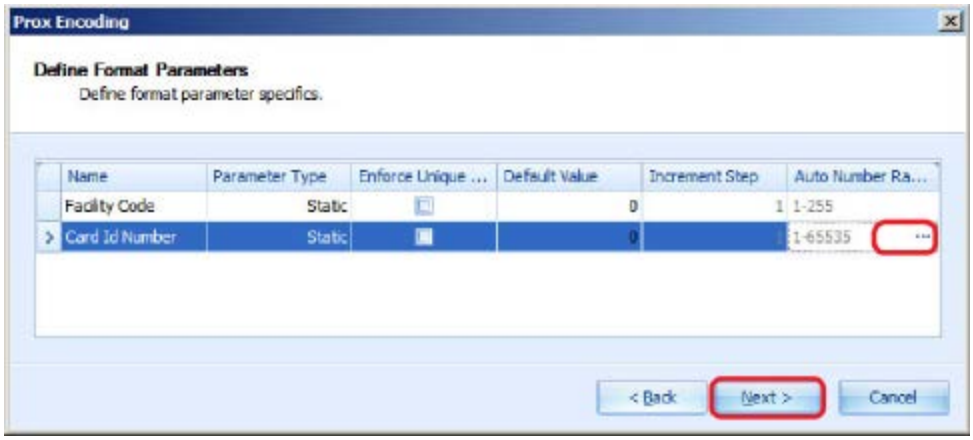
Field	Description
Instruction Type	Read, or Write.
Options	Overwrite Existing Credential: Allows the iCLASS SE Encoder to write over an application that has already been recorded in the Work Order database.
Credential Type	Format: Select a Format from the list.

Note: For this example, a **Read/Format: H10301** configuration is selected.



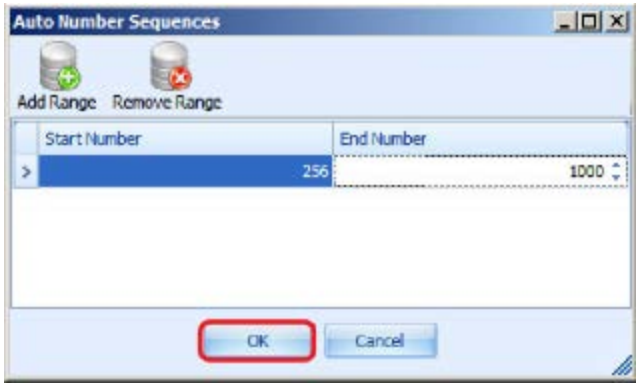
4. **Define Format Parameters:** Define each parameter for the selected format. Select the line to modify, each parameter is editable with text or from a drop-down menu.

Field	Description
Name	The name is read from the Format file. It is recommended to not change this name unless necessary.
Parameter Type	This can be Auto Increment, Static, or Manual User Entry. **Note:** Type is typically determined by the Format file.
Enforce Unique Numbers	Check this box for a runtime check of the manual value entered to guarantee uniqueness, prior to executing the Work Order.
Default Value	The default Static value for Static and Manual parameters.
Increment Step	The step value used to increment Auto Number sequences.
Auto Numbers	This field sets the Auto Number Sequences for the Work Instruction. The ranges are set by selecting the ellipses (…) and entering the ranges (see following graphic).



Auto number sequences window

Select **Add Range** and set the range in the editable fields. Click **OK**.



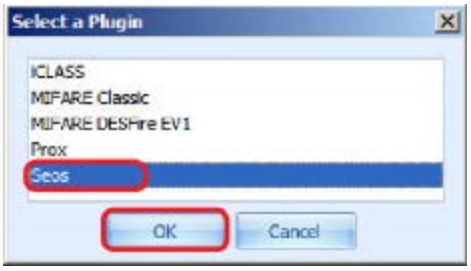
5. Click **Next** to continue with the Wizard.
6. When the wizard completes, click **Finish**.
7. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.6 Seos work instructions

6.6.1 Seos: HID access application

This section covers the Work Instruction wizard for Seos, with the HID Access Application encoding.

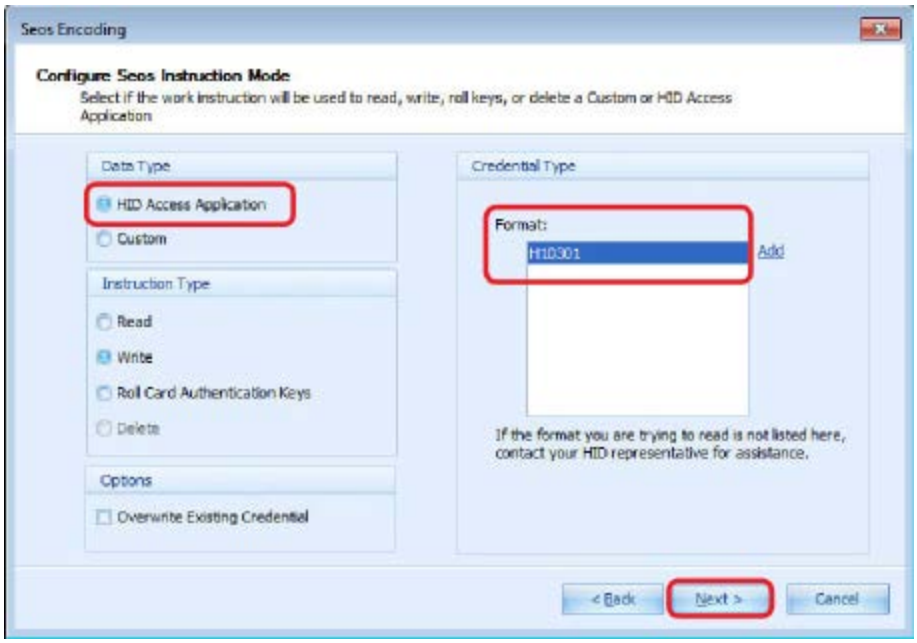
1. Select the **Seos** technology type. Click **OK**.



2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for Prox. Click **Next**.
3. **Configure Seos Instruction Mode:** You can make selections from the following. When complete click **Next**.

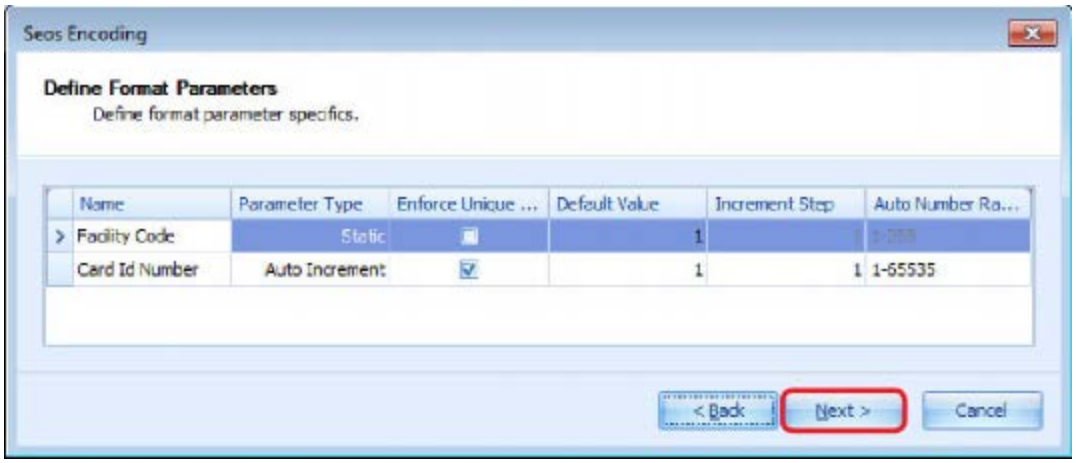
Field	Description
Data Type	HID Access Application, Custom, or Read CSN.
Instruction Type	Read, Write, Roll Card Authentication Key, or Delete. **Note:** Delete is only available for custom encoding.
Options	Overwrite Existing Credential: Allows the iCLASS SE Encoder to write over an application that has already been recorded in the Work Order database. **Note:** This is not recommended if the card number is already printed or engraved onto the credential.
Credential Type	Format: Select a Format from the list.

Note: For this example, a **Write/HID Application** configuration is selected.



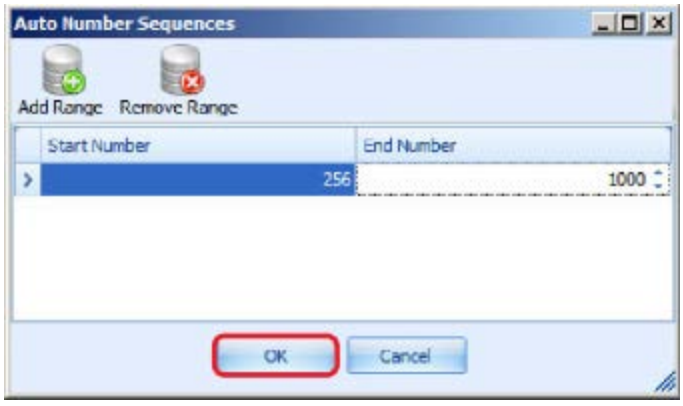
4. **Define Format Parameters:** You select, then customizes each parameter defined for the selected format. Select the line to modify, each parameter is editable with text or from a drop-down menu.

Field	Description
Name	The name is read from the Format file. It is recommended to not change this name unless necessary.
Parameter Type	This can be Auto Increment, Static, Manual User Entry, or Previous Work Instruction. **Note:** Type is typically determined by the Format file.
Enforce Unique Numbers	Check this box for a runtime check of the manual value entered to guarantee uniqueness, prior to executing the Work Order.
Default Value	The default Static value for Static and Manual parameters.
Increment Step	The step value used to increment Auto Number sequences.
Auto Numbers	This field sets the Auto Number Sequences for the Work Instruction. The ranges are set by selecting the ellipses (…) and entering the ranges. See following graphic.



Auto number sequences window

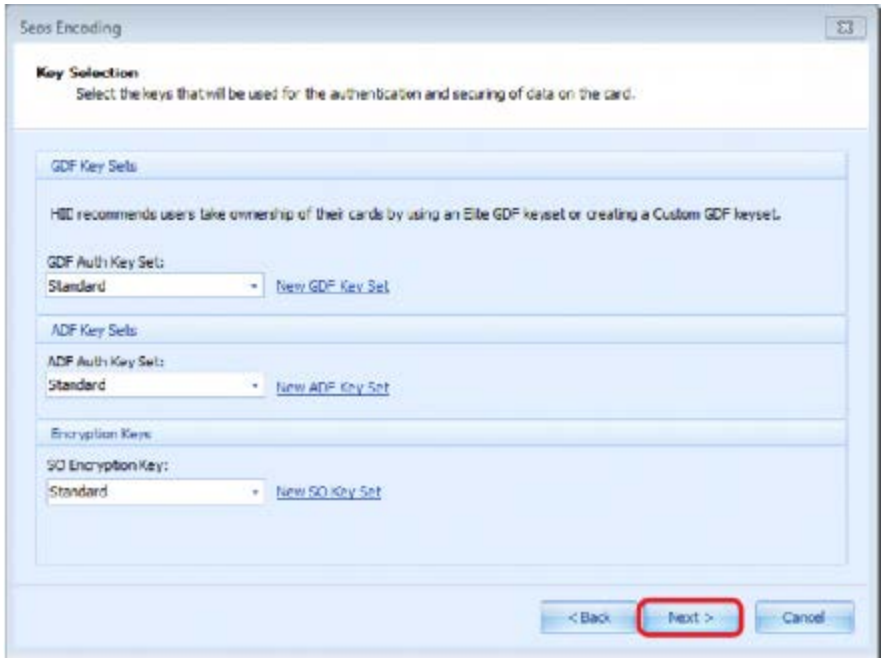
Select **Add Range** and set the range in the editable fields. Click **OK**.



5. Click **Next** to continue with the Wizard.

6. **Key Selection:** Select a key to lock the AppArea after the data is written, and click **Next**.

Field	Description
GDF Key Sets	GDF Auth Key Set: Sets the key set to be used to authenticate to the GDF to grant access to create the ADF for the HID Access Application. If the card presented at the time of encoding has the factory default GDF keys, Asure ID attempts to change the GDF keys.
ADF Key Sets	ADF Auth Key Set: Selects the authentication key set for accessing the ADF in which HID Access Application credential is written.
Encryption Keys	SO Encryption Key: Standard, Custom or HID defined key sets may be selected



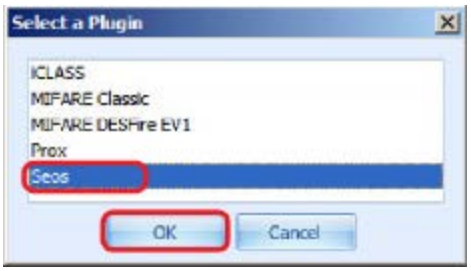
7. The wizard is complete. Click **Finish**.
8. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.6.2 Seos: custom encoding (basic mode)

This section covers the Work Instruction wizard for Seos, with Custom Encoding/Basic Mode. The Basic - Single Key Mode Is designed to be the fastest way for users who are not familiar with the Seos architecture to create a Custom Seos Application. Mainly, this is achieved by requiring you to define only one key, which is used for the Privacy Encryption Key, Message Authentication Code (MAC) and as the Administrator Authentication key used for reading, writing and modifying itself (the authentication key required to change keys during Key Rolling operations).

Note: This mode provides a moderate level of security, but for high-security or complex operations, the Standard Mode should be considered.

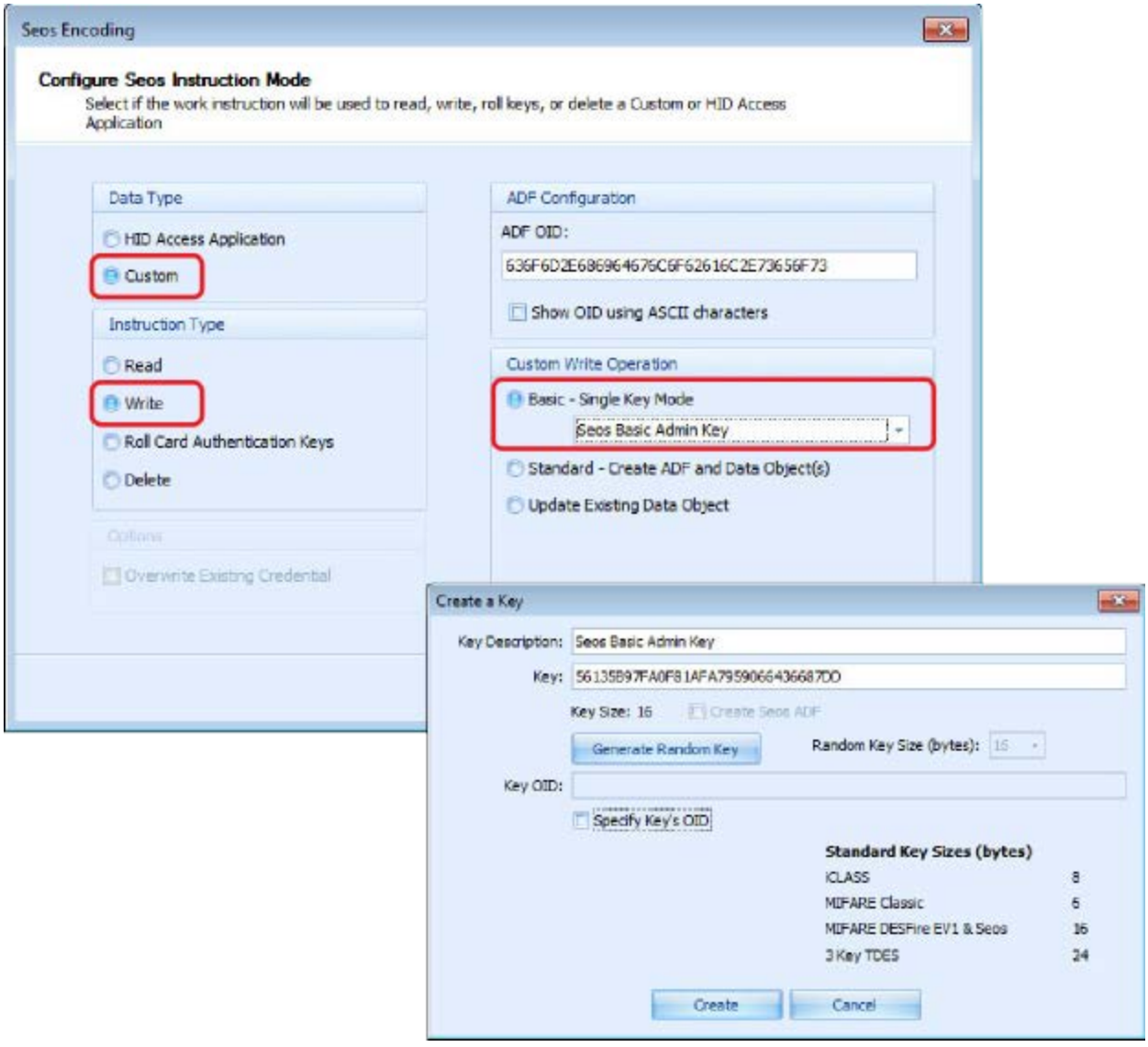
1. Select the **Seos** technology type. Click **OK**.



2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for Prox. Click **Next**.

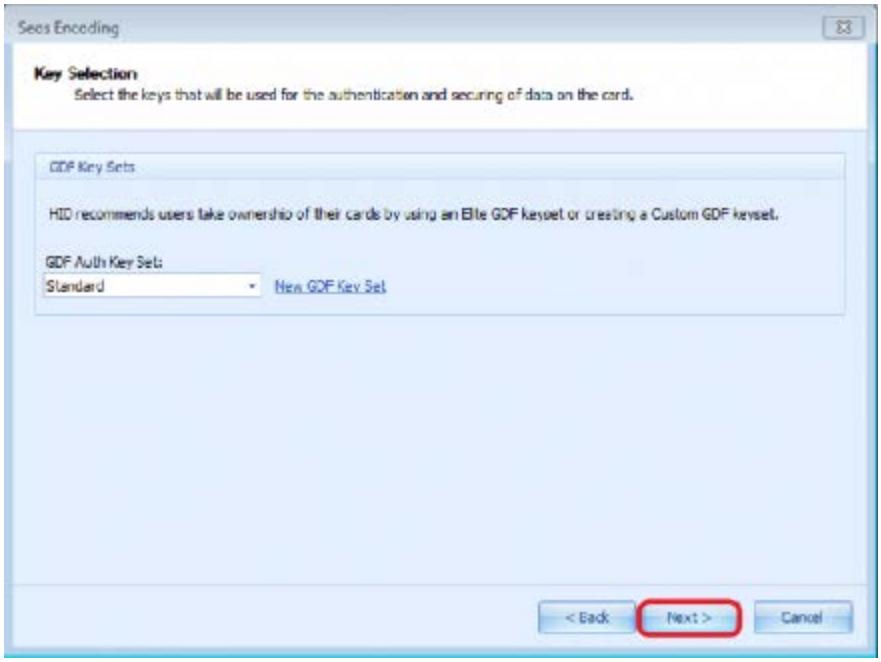
3. **Configure Seos Instruction Mode:** You can make selections from the following. When complete click **Next**.

Field	Description
Data Type	For this example **Custom** must be selected.
Instruction Type	For this example **Write** must be selected.
Options	Not available with **Custom**.
ADF Configuration	**ADF OID**: A number (8 byte minimum) used to reference the application after it is created. **Show OID using ASCII characters**: Displays ASCII characters.
Custom Writer Operation	For this example **Basic - Single Key Mode** must be selected. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu. Once the desired 16-byte Custom Key and description are entered, click **Create**. The key is uploaded to the encoder, after the wizard is completed. Once this key is loaded to the encoder, it can only be referenced by OID, therefore backup the key in a secure place, to configure the back-end system at a later time.



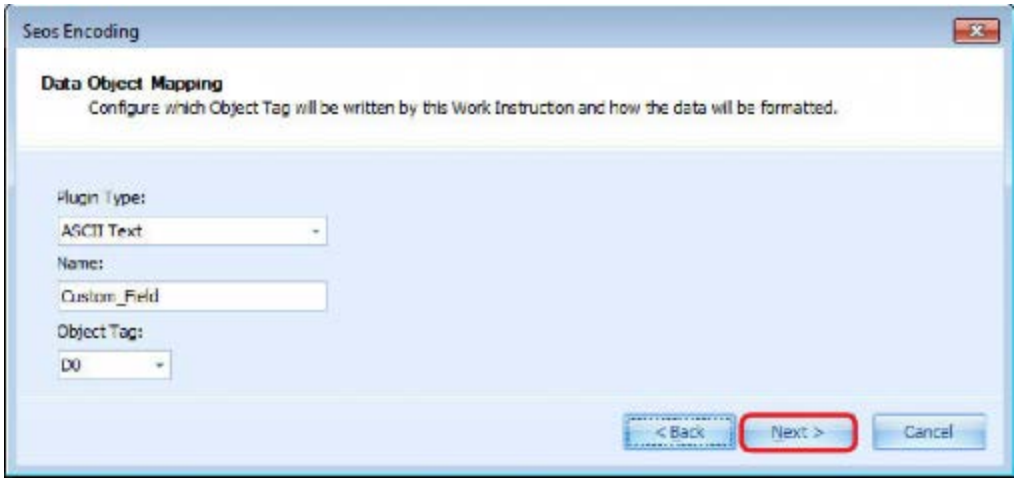
4. **Key Selection:** Select the keys that are used for the authentication and securing of data on the card. Click **Next**.

Field	Description
GDF Key Sets	GDF Auth Key Set: Sets the key set to be used to authenticate to the GDF to grant access to create the ADF for the HID Access Application. If the card presented at the time of encoding has the factory default GDF keys, Asure ID attempts to change the GDF keys.

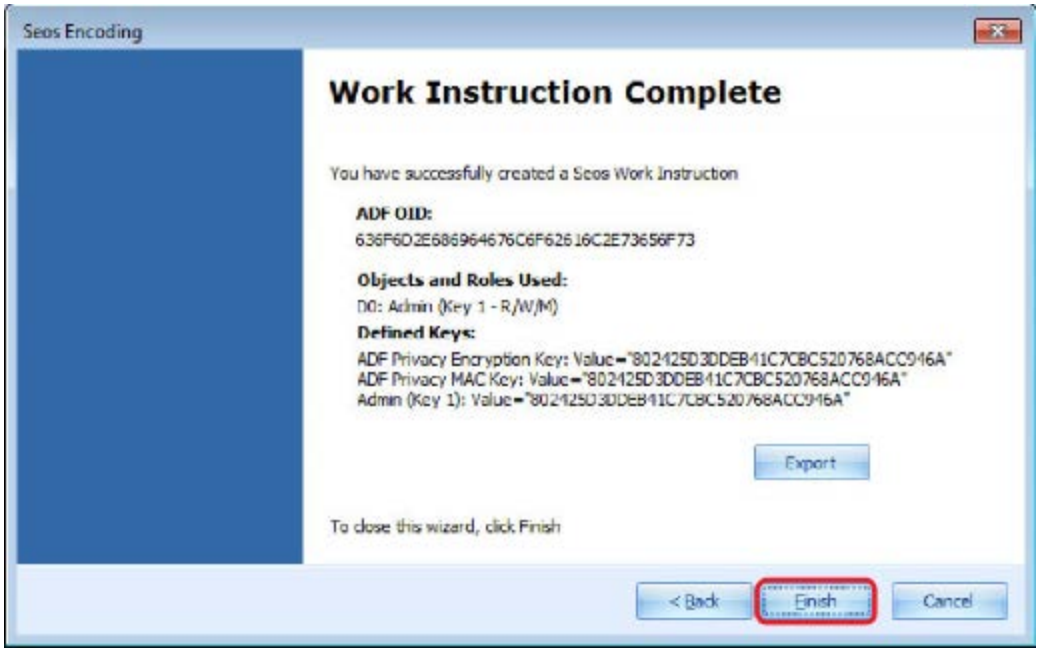


5. **Data Object Mapping:** Configure which Object Tag is written by this Work Instruction and how the data is formatted, and click **Next**.

Field	Description
Plugin Type	This defines how the data is entered in the Work Order Manager or in Data Entry. Options are ASCII Text, Hexadecimal Data, Unicode Text, Signed 64-bit Integer, or Lumidigm Fingerprint Data.
Name	This defines the name of the data field in which you enter the custom data.
Object Tag	The Object Tag in Basic Mode is always **D0**.



6. Review the configuration summary and click Export (to a .txt file) if required. Click **Finish**.

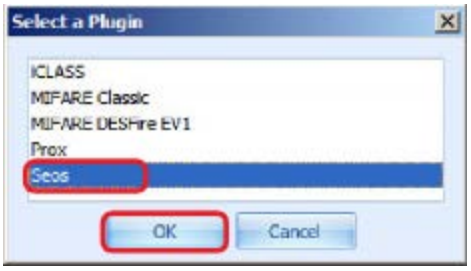


7. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.6.3 Seos: custom encoding (standard mode)

Standard Mode is designed to support advanced Custom Application Configurations. You are not required to have intimate knowledge of the Seos architecture for simpler configurations of Standard Mode, but for more complex configurations it is helpful. Defaults are provided in this mode to create a single key with read/write/change key access to a single object tag.

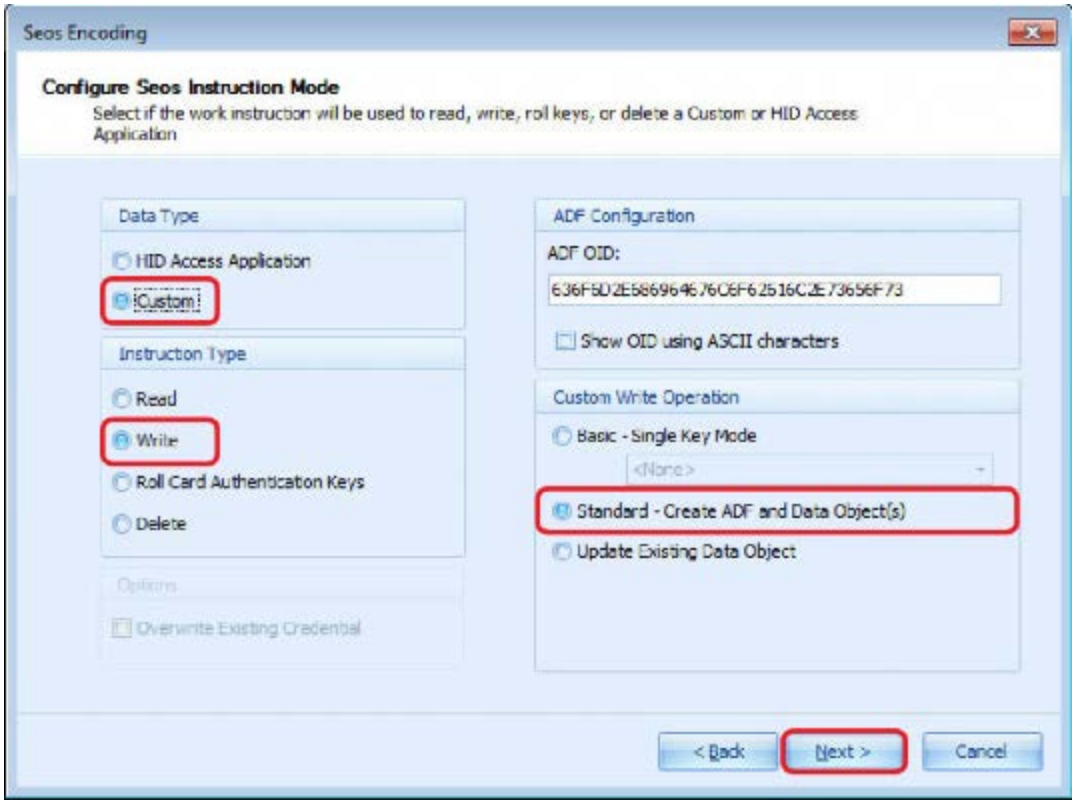
1. Select the **Seos** technology type. Click **OK**.



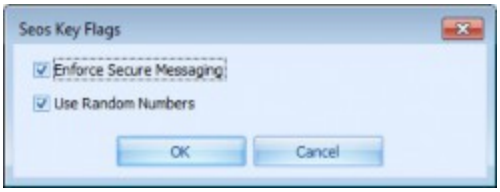
2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for Prox. Click **Next**.

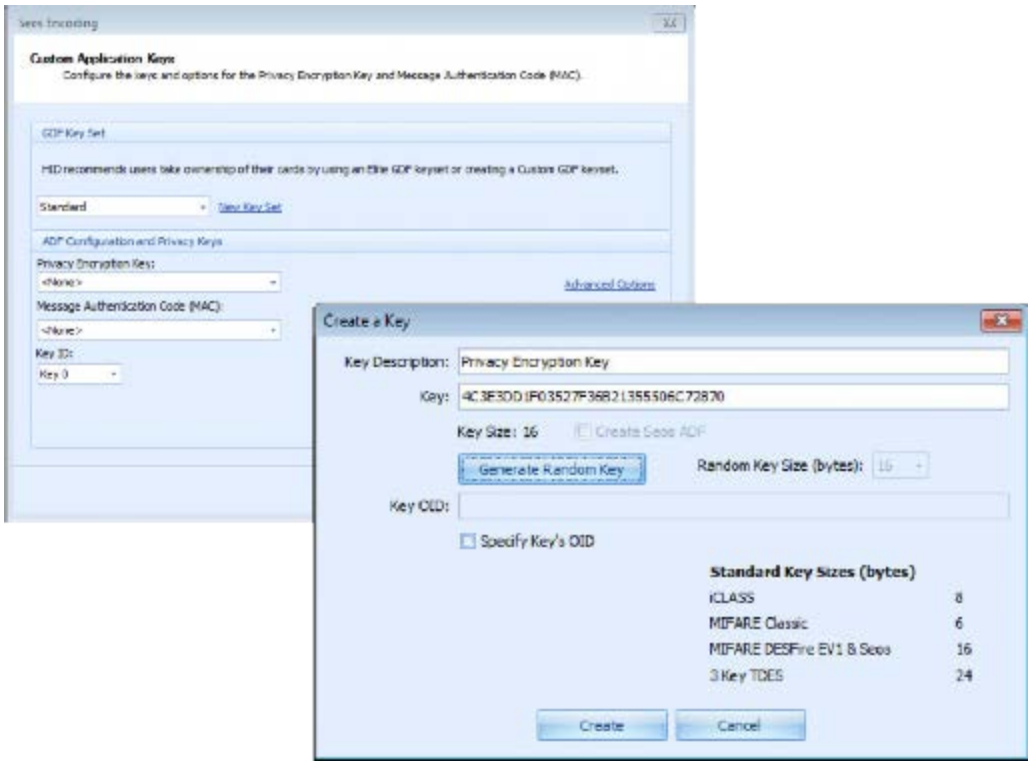
3. **Configure Seos Instruction Mode:** You can make selections from the following. When complete click **Next**.

Field	Description
Data Type	For this example **Custom** must be selected.
Instruction Type	For this example **Write** must be selected.
Options	Not available with **Custom**.
ADF Configuration	**ADF OID**: A number (8 byte min) used to reference the application after it is created. **Show OID using ASCII characters**: Displays ASCII characters.
Custom Writer Operation	For this example **Standard - Create ADF and Data Object(s)** must be selected.



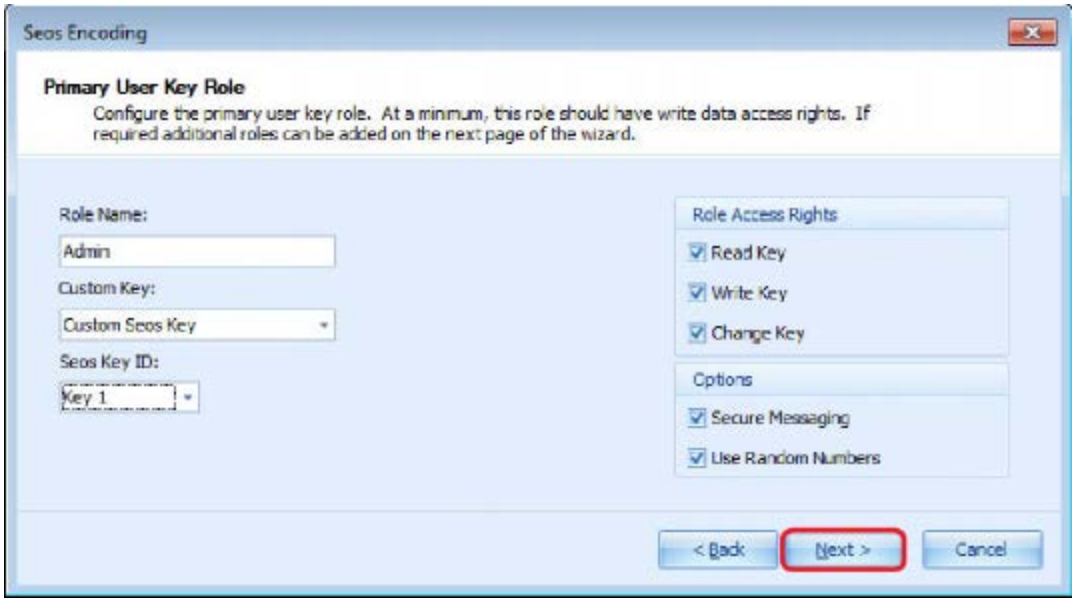
4. **Custom Privacy Keys:** Select a custom key to use as the Privacy Encryption Key and Message Authentication Code, which is created when the ADF is created, and click **Next**.

Field	Description
GDF Key Set	Sets the key set that is used to authenticate to the GDF to grant access to create the ADF for the HID Access Application. If the card presented at the time of encoding has the factory default GDF keys, Asure ID attempts to change the GDF keys.
Privacy Encryption Key	The Privacy Encryption Key is used to encrypt the transactions between the client and the ADF. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu.
Message Authentication Code (MAC)	The Message Authentication Code (MAC) is a 16 byte code appended to the end of encrypted data transmission to protect the integrity of transaction. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu.
Key ID	Select the Key ID in which the Privacy Keys is stored. The default **Key 0** is the Privacy Key ID recommended by HID.
Advanced Options	Advanced Options allows you to set the Seos Key Flags. Default settings are recommended for the Privacy Keys. 



5. **Primary User Key Role:** Define a User Key/Role for accessing the default Data Object, and click **Next.**

Field	Description
Role Name	Rename the Role Name, if desired.
Custom Key	Assign a Custom Key that this Role uses. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu.
Seos Key ID	Select the Key ID for the slot in the ADF this key assumes when the ADF is created.
Role Access Rights	Modify the Role Access Rights as desired. It is recommended that the Primary User Role has Read and Write access (Change Key access is optional). **Read Key**: Is used to authenticate to a Data Object prior to reading its contents. **Write Key**: Is used to authenticate to a Data Object prior to writing its data to it. **Change Key**: Is used to authenticate prior to a Key Roll operation. See 6.7 Work instruction: roll card authentication key for details.
Options	Modify the Options (default options)



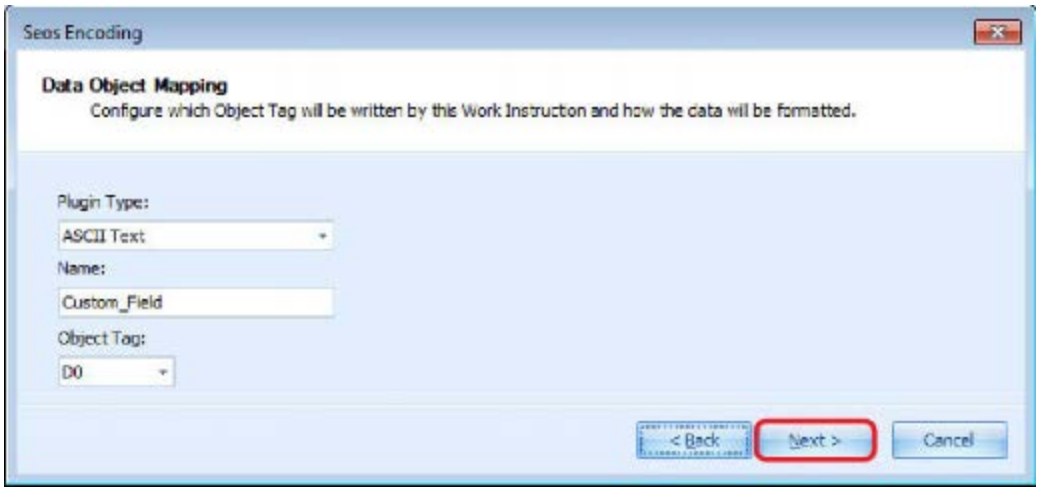
6. **ADF Configuration:** Create and manager User Key Roles and Object Tags. Click **Next**.

Field	Description
Available User Key Roles	Add, Modify and delete User Key Roles. **Note:** At least one User Key Role must be defined and assigned to an Object Tag, before you can continue. Drag and drop User Keys Roles onto an Object Tag in the ADF Configuration pane.
ADF Configuration	Add and remove Object Tags. **Note:** At lease one Object Tag must be defined in the ADF. Action: Allows you to Edit or remove Roles from the ADF Configuration pane.

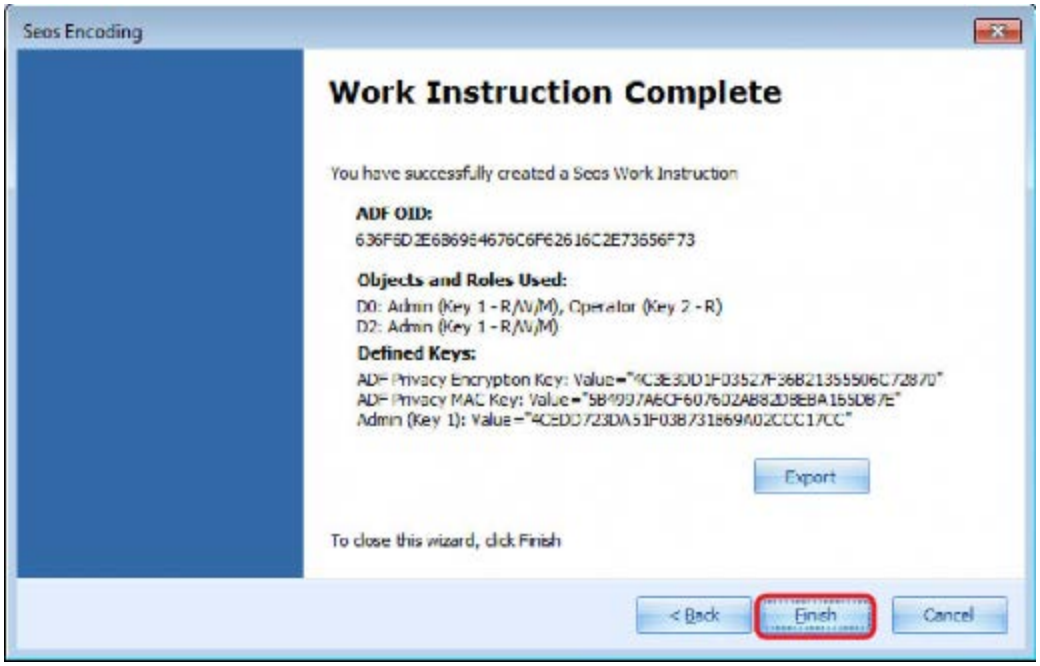
Note: By default the Object Tag D0 is created and the Primary User Role is assigned access to this Object Tag.

7. **Data Object Mapping:** Configure which Object Tag is written by this Work Instruction and how the data is formatted, and click **Next**.

Field	Description
Plugin Type	This defines how the data is entered in the Work Order Manager or in Data Entry. Options are ASCII Text, Hexadecimal Data, Unicode Text, or Signed 64-bit Integer.
Name	This defines the name of the data field in which you enter the custom data.
Object Tag	If more than one Object Tag is defined in the ADF, select which Object Tag this Work Instruction should read or write. The default is **D0**.



8. Review the configuration summary and click Export (to a .txt file) if required. Click **Finish**.

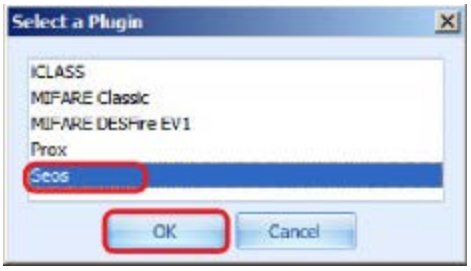


9. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.6.4 Seos: custom encoding (update existing data object)

To update a card where the ADF already exists, or if the ADF has multiple objects and was created in a previous Work Instruction, then a distinct type of write operation is required to update the data object only and not modify any existing keys or data objects.

1. Select the **Seos** technology type. Click **OK**.

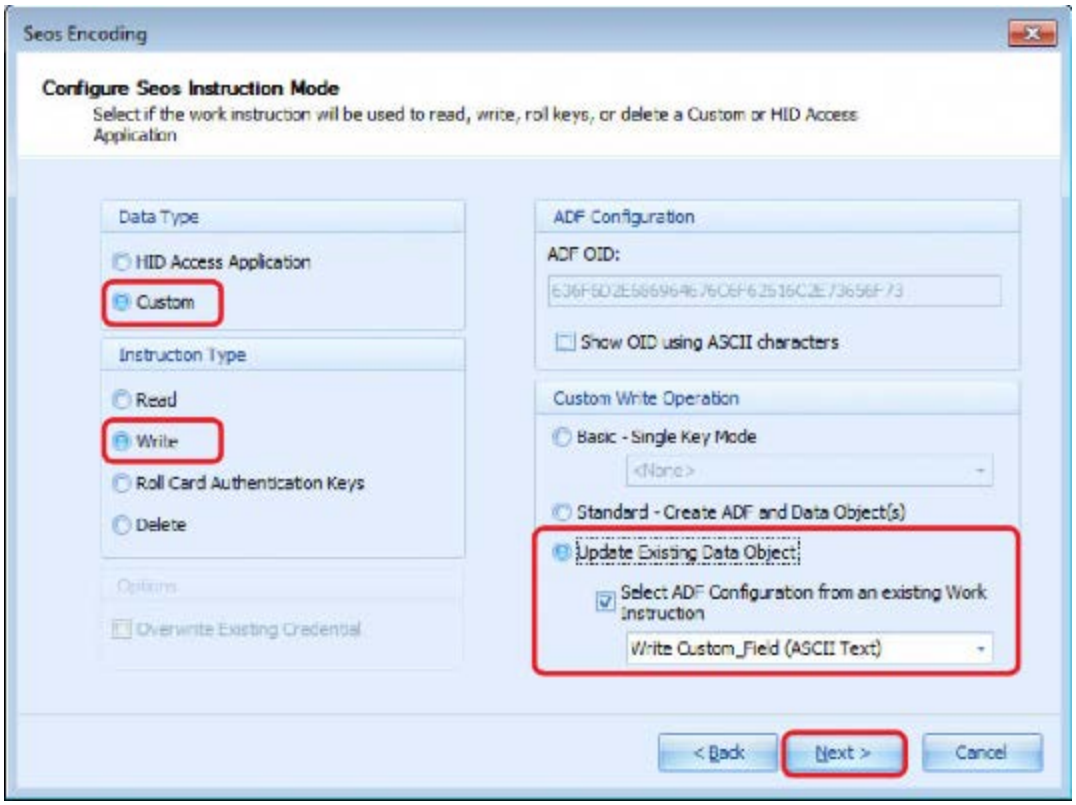


2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for Prox. Click **Next**.

3. **Configure Seos Instruction Mode:** You can make selections from the following. Click **Next.**

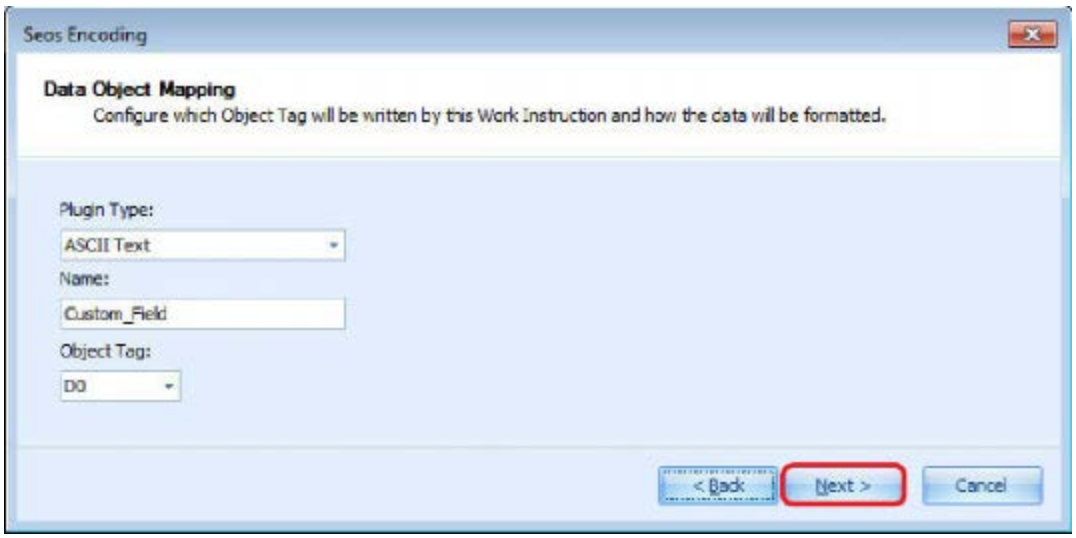
Method 1—(configure ADF using an existing work instruction)

Field	Description
Data Type	For this example **Custom** must be selected.
Instruction Type	For this example **Write** must be selected.
Options	Not available with **Custom.**
ADF Configuration	**ADF OID**: A number (8 byte minimum) used to reference the application after it is created. **Show OID using ASCII characters**: Displays ASCII characters.
Custom Writer Operation	For this example Update Existing Data Object must be selected. Additionally select the **Select ADF Configuration from an existing Work Instruction** option. Select the Work Instruction from the pull-down menu. **Note:** This checkbox is only present if there another Seos Custom Write Work Instruction was created prior to this Work Instruction.

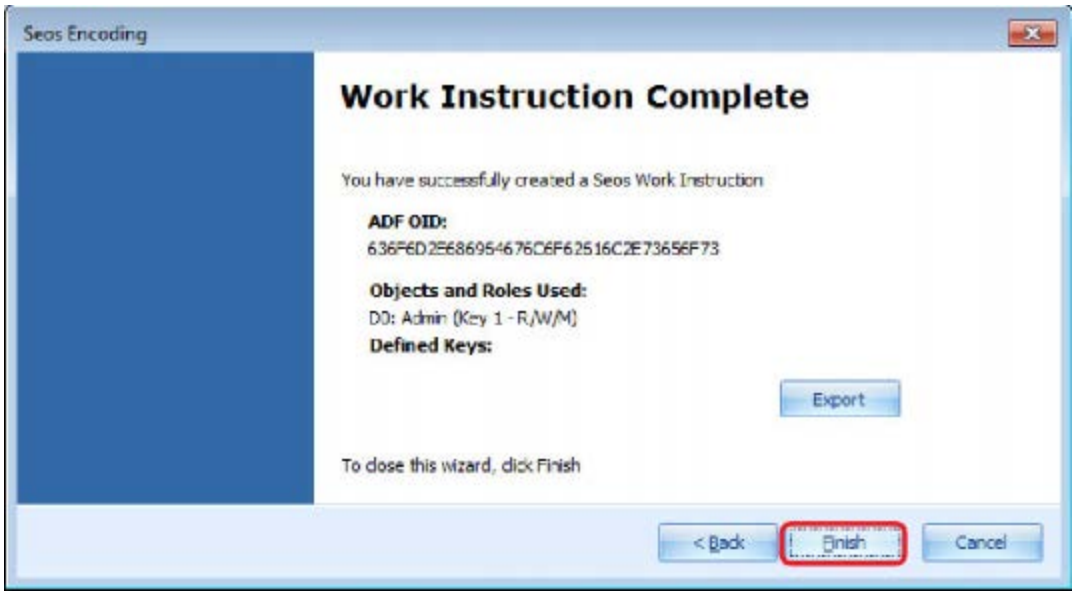


4. **Data Object Mapping:** Configure which Object Tag is written by this Work Instruction and how the data is formatted, and click **Next**.

Field	Description
Plugin Type	This defines how the data is entered in the Work Order Manager or in Data Entry. Options are ASCII Text, Hexadecimal Data, Unicode Text, or Signed 64-bit Integer.
Name	This defines the name of the data field in which you enter the custom data.
Object Tag	Select desired Object Tag, if more than one has been defined in a Previous Work Instruction. Otherwise type in the desired Object Tag, if the **Select ADF Configuration from an existing Work Instruction** (on the *Configure Seos Instruction Mode* window) option is not checked.



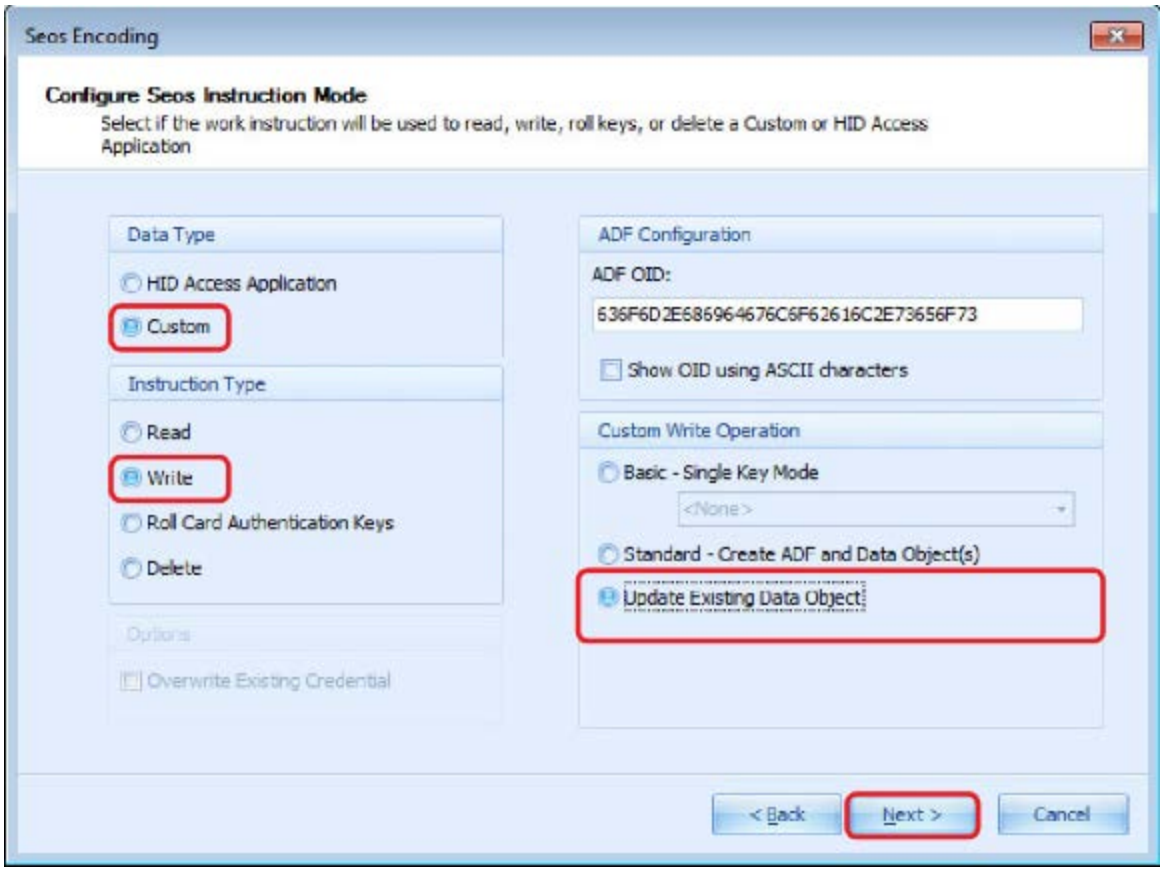
5. Review the configuration summary and click **Export** (to a .txt file) if required. Click **Finish**.



6. Return to **5.6 Create a work order**, step 5 to save the Work Order.

Method 2—(configure ADF manually)

Field	Description
Data Type	For this example **Custom** must be selected.
Instruction Type	For this example **Write** must be selected.
Options	Not available with **Custom**.
ADF Configuration	**ADF OID**: A number (8 byte minimum) used to reference the application after it is created. **Show OID using ASCII characters**: Displays ASCII characters.
Custom Writer Operation	For this example Update Existing Data Object must be selected. Additionally select the **Select ADF Configuration from an existing Work Instruction** option. Select the Work Instruction from the pull-down menu. **Note:** This checkbox is only present if there another Seos Custom Write Work Instruction was created prior to this Work Instruction.

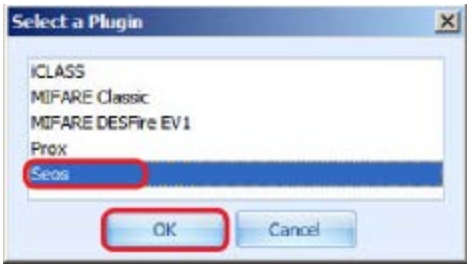


7. Go to **6.6.3 Seos: custom encoding (standard mode)**, steps 4–9.

6.6.5 Seos: custom encoding (rolling custom Seos keys)

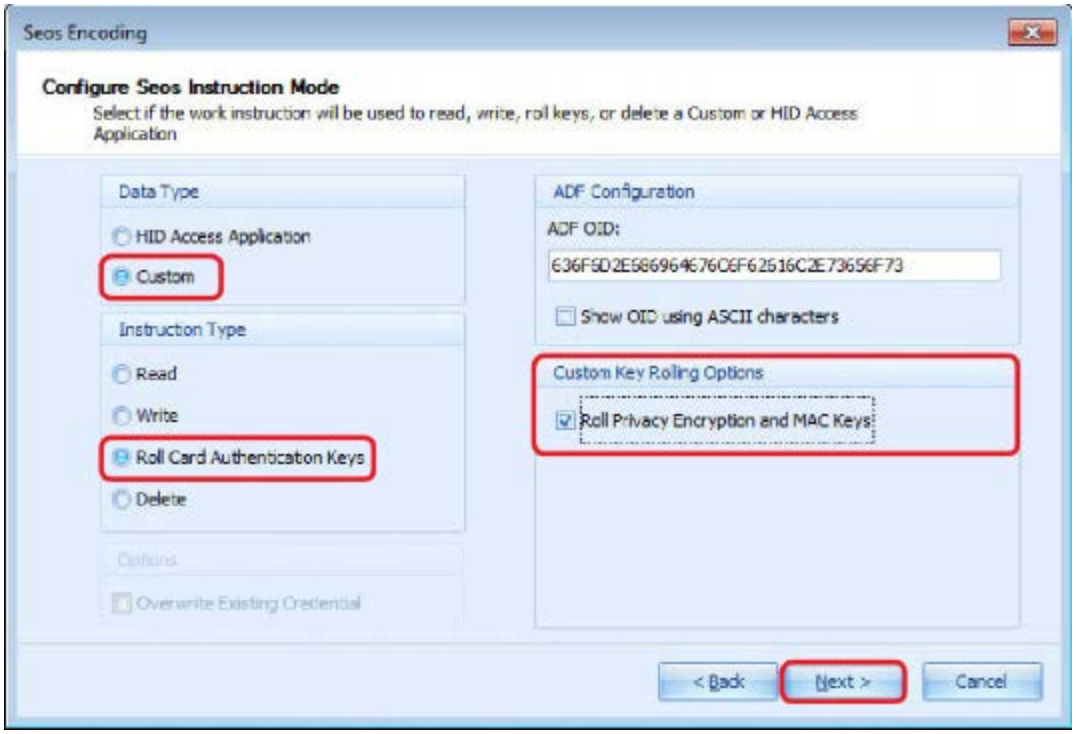
This operation changes 1 or more keys present in an ADF.

1. Select the **Seos** technology type. Click **OK**.



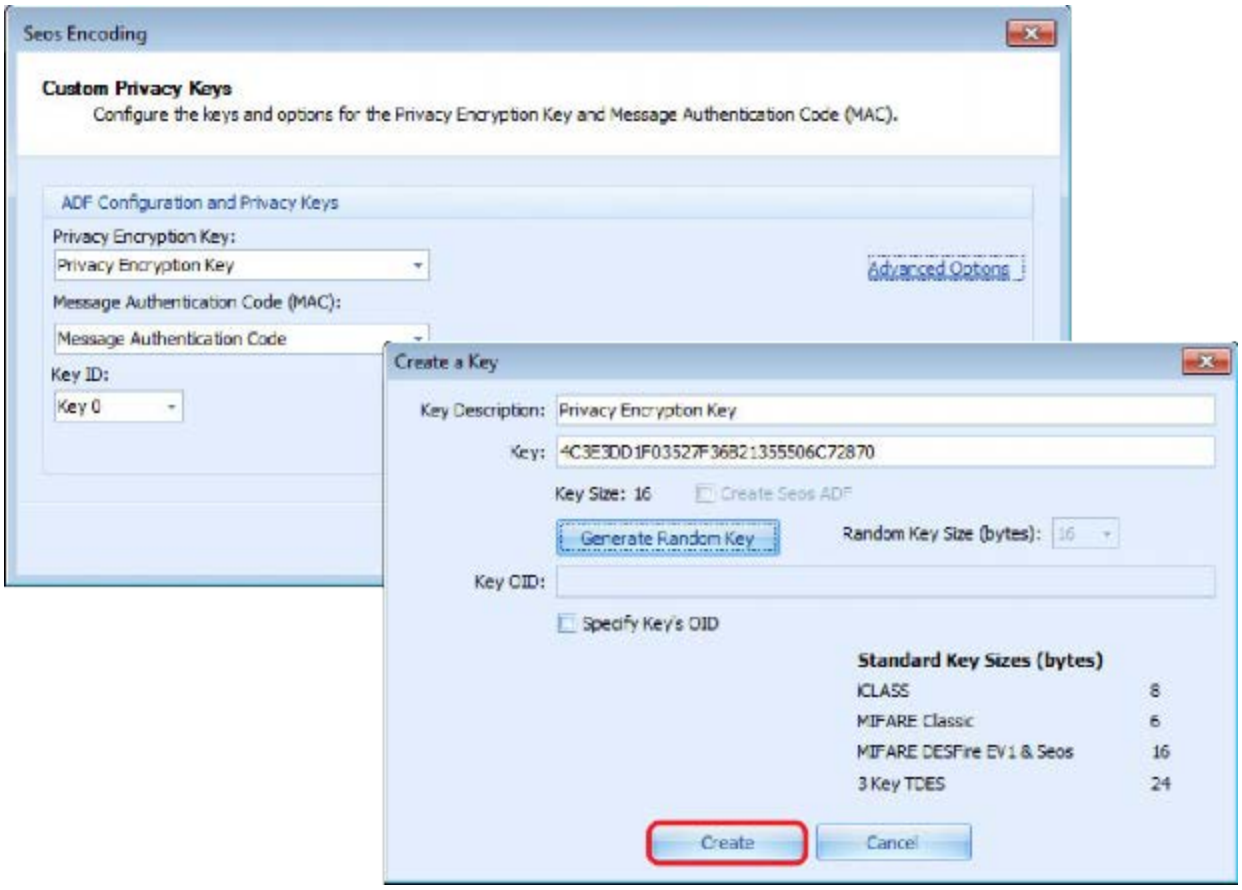
2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for Prox. Click **Next**.
3. **Configure Seos Instruction Mode:** You can make selections from the following. Click **Next**.

Field	Description
Data Type	For this example **Custom** must be selected.
Instruction Type	For this example **Roll Card Authentication Keys** must be selected.
Options	Not available with **Custom**\.
ADF Configuration	**ADF OID**: A number (8 byte minimum) used to reference the application after it is created. **Show OID using ASCII characters**: Displays ASCII characters.
Custom Key Rolling Options	For this example **Roll Privacy Encryption and MAC Keys** must be selected.



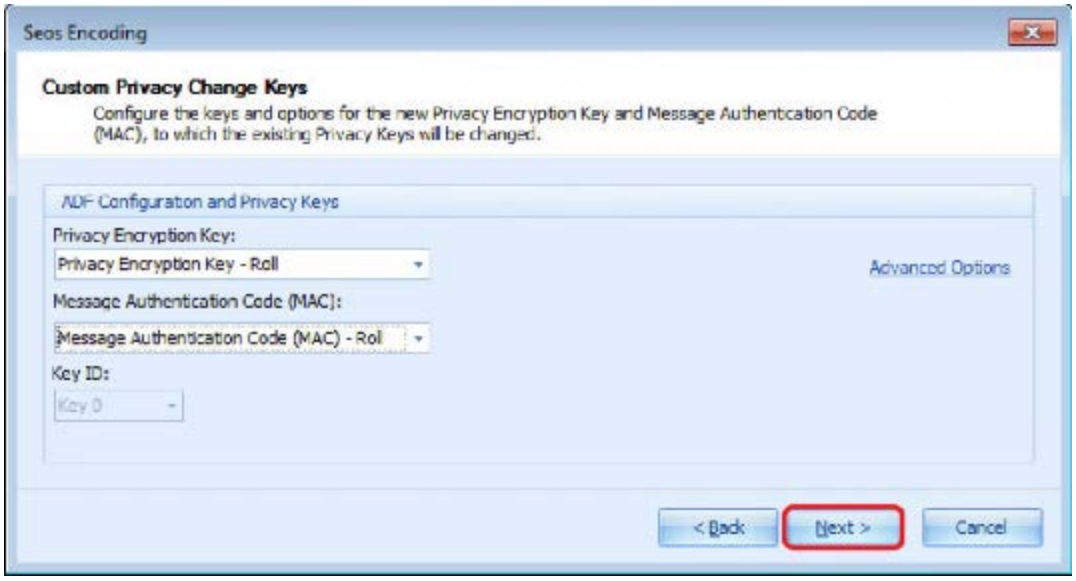
4. **Custom Privacy Keys:** Select a custom key to use as the Privacy Encryption Key and Message Authentication Code, which is created when the ADF is created, and click **Next**.

Field	Description
Privacy Encryption Key	The Privacy Encryption Key is used to encrypt the transactions between the client and the ADF. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu.
Message Authentication Code (MAC)	The Message Authentication Code (MAC) is a 16-byte code appended to the end of encrypted data transmission to protect the integrity of transaction. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu.
Key ID	Select the Key ID in which the Privacy Keys is stored. The default **Key 0** is the Privacy Key ID recommended by HID.
Advanced Options	Advanced Options allows you to set the Seos Key Flags. Default settings are recommended for the Privacy Keys. 

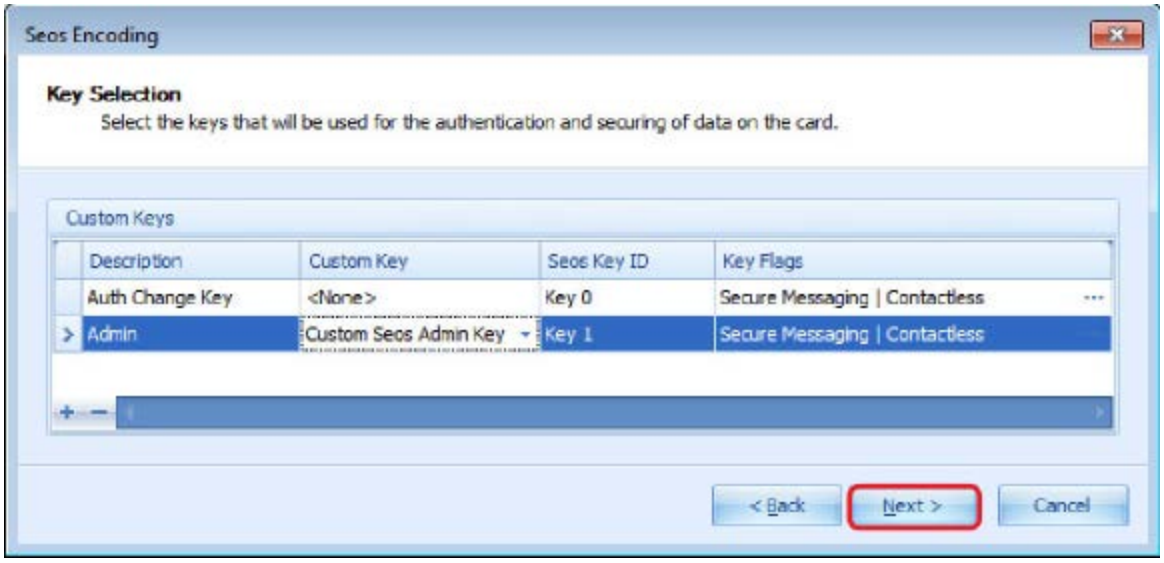


5. **Custom Privacy Change Keys:** If the Roll Privacy Encryption and MAC Keys check box was selected in step 3, the Custom Privacy Change Keys window is displayed. Define the new Privacy Encryption Key and MAC, and click **Next**.

Field	Description
Privacy Encryption Key	The Privacy Encryption Key is used to encrypt the transactions between the client and the ADF. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu.
Message Authentication Code (MAC)	The Message Authentication Code (MAC) is a 16 byte code appended to the end of encrypted data transmission to protect the integrity of transaction. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu.
Key ID	This option is not available on this window.
Advanced Options	Advanced Options allows you to set the Seos Key Flags. Default settings are recommended for the Privacy Keys. 



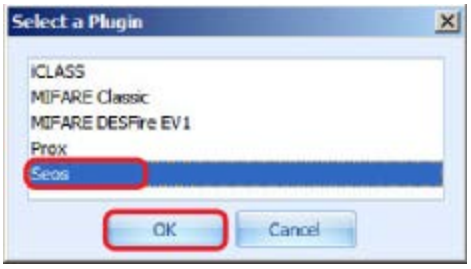
6. **Key Selection:** Select the Keys that are used for the authentication and securing of data on the card, and click **Next**.



7. The wizard is complete. Click **Finish**.
8. Return to **5.6 Create a work order**, step 5 to save the Work Order.

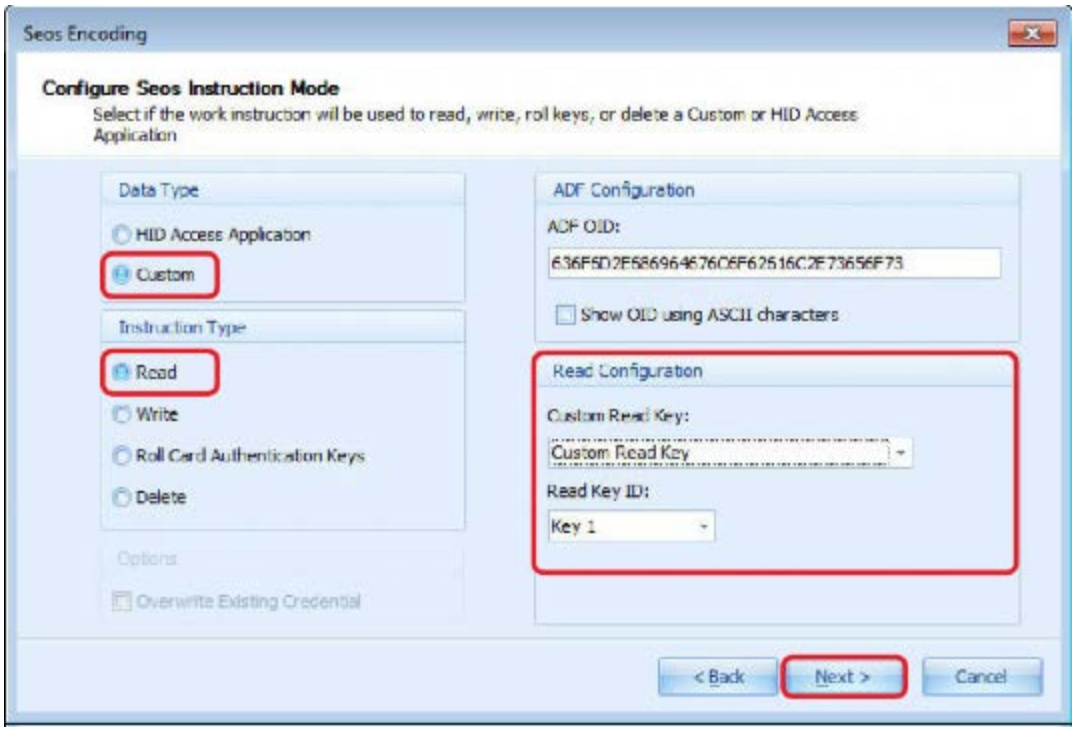
6.6.6 Seos: reading a Seos data object from a custom ADF

1. Select the **Seos** technology type. Click **OK**.



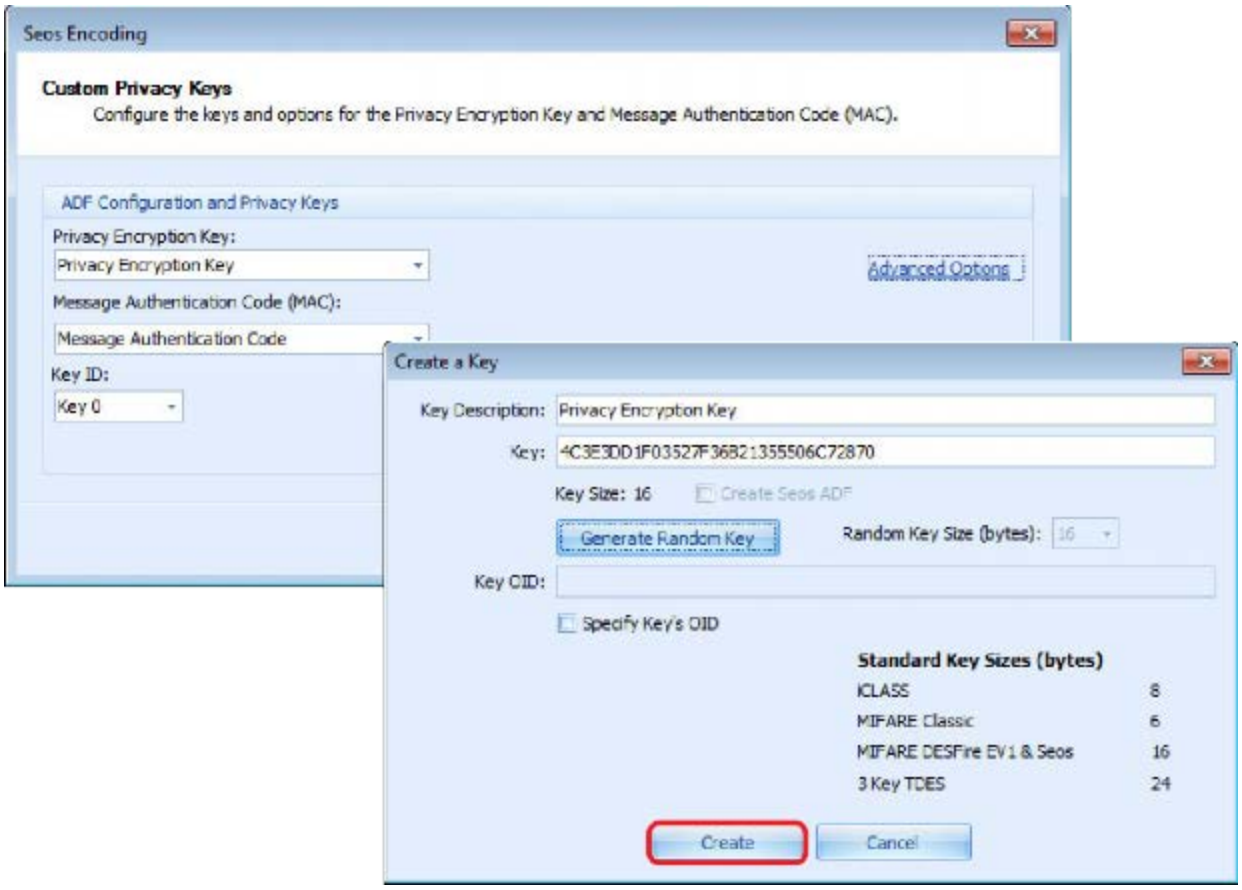
2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for Prox. Click **Next**.
3. **Configure Seos Instruction Mode:** You can make selections from the following. Click **Next**.

Field	Description
Data Type	For this example **Custom** must be selected.
Instruction Type	For this example **Read** must be selected.
Options	Not available with **Custom**\.
ADF Configuration	**ADF OID**: A number (8 byte minimum) used to reference the application after it is created. **Show OID using ASCII characters**: Displays ASCII characters.
Read Configuration	**Custom Read Key**: Specify the Custom Read Key which are used to authenticate to the ADF to read the Data Object. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu. **Read Key ID**: This Read Key is to be referenced in the ADF.



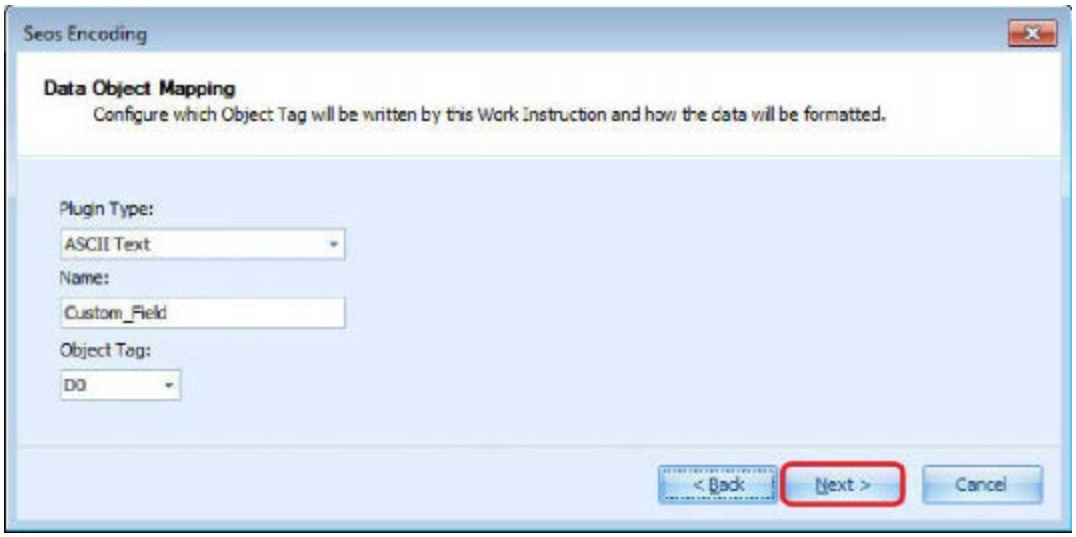
4. **Custom Privacy Keys:** Select a custom key to use as the Privacy Encryption Key and Message Authentication Code, which is created when the ADF is created, and click **Next**.

Field	Description
Privacy Encryption Key	The Privacy Encryption Key is used to encrypt the transactions between the client and the ADF. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu.
Message Authentication Code (MAC)	The Message Authentication Code (MAC) is a 16 byte code appended to the end of encrypted data transmission to protect the integrity of transaction. **Note:** If the desired key is not defined, select **<Create New Key>** from the drop-down menu.
Key ID	Select the Key ID in which the Privacy Keys are stored. The default **Key 0** is the Privacy Key ID recommended by HID.
Advanced Options	Advanced Options allows you to set the Seos Key Flags. Default settings are recommended for the Privacy Keys. 



5. **Data Object Mapping:** Configure which Object Tag is written by this Work Instruction and how the data is formatted, and click **Next**.

Field	Description
Plugin Type	This defines how the data is entered in the Work Order Manager or in Data Entry. Options are ASCII Text, Hexadecimal Data, Unicode Text, or Signed 64-bit Integer.
Name	This defines the name of the data field in which you enter the custom data.
Object Tag	Type in the Object Tag, from which the data is read. Default is **D0**.

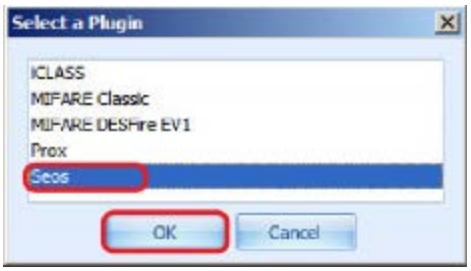


6. When the wizard completes, click **Finish**.
7. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.6.7 Seos: deleting a custom ADF

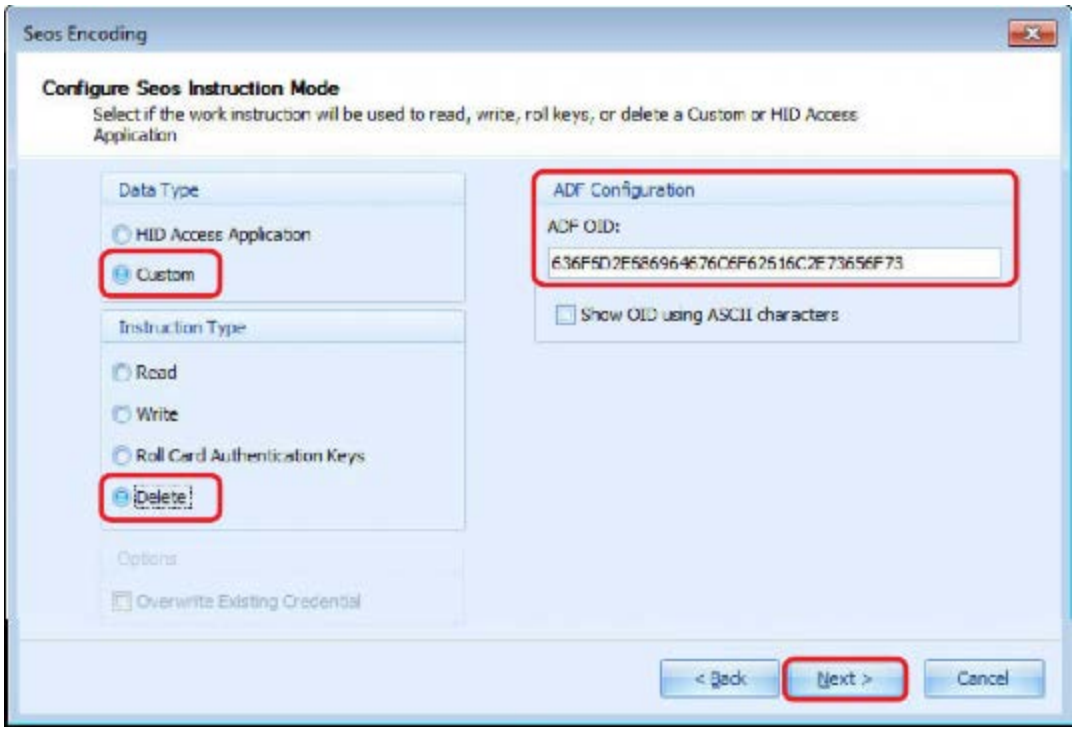
Important: This operation deletes any data associated with an ADF and the ADF itself and should only be performed if the ADF and its data is no longer required.

1. Select the **Seos** technology type. Click **OK**.



2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for Prox. Click **Next**.
3. **Configure Seos Instruction Mode:** Make selections from the following. Click **Next**.

Field	Description
Data Type	For this example **Custom** must be selected.
Instruction Type	For this example **Delete** must be selected.
Options	Not available with **Custom**\.
ADF Configuration	**ADF OID**: A number (8 byte minimum) used to reference the application after it is created. **Show OID using ASCII characters**: Displays ASCII characters.



4. **Key Selection:** Select the keys that are used for the authentication and securing of data on the card. Click **Next**.

Field	Description
GDF Key Sets	GDF Auth Key Set: Select the key set to use to authenticate to the GDF to grant access to delete the ADF containing the application.

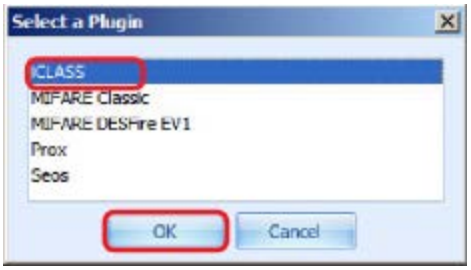
5. When the wizard completes, click **Finish**.
6. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.7 Work instruction: roll card authentication key

This section covers the Work Instruction wizard for Roll Card Authentication Key Encoding for iCLASS, MIFARE Classic, MIFARE DESFire EV1, and Seos.

Note: If a key is selected other than HID Standard, the reader does not need to be configured with the appropriate Key Set you are using. See **8.9 Load HID application keys** for details.

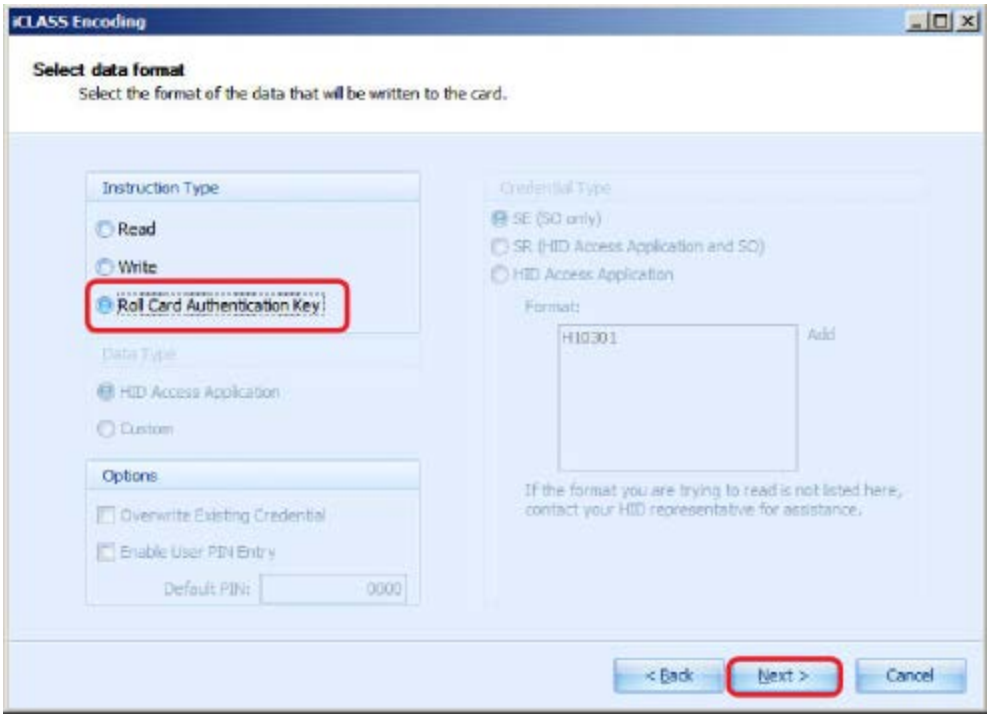
1. Select the technology type. Click **OK**.



2. The Work Instruction Wizard opens to allow you to configure the Work Instruction for Prox. Click **Next**.
3. **Select Data Format:** You can make selections from the following. Click **Next**.

Field	Description
Instruction Type	Select **Roll Card Authentication Key** for this option.
Data Type	Not available. Seos - HID Access Application
Credential Type	Not available

Note: The screenshot below is using the iCLASS technology. This window is slightly different with other technologies (MIFARE, Seos, etc.).

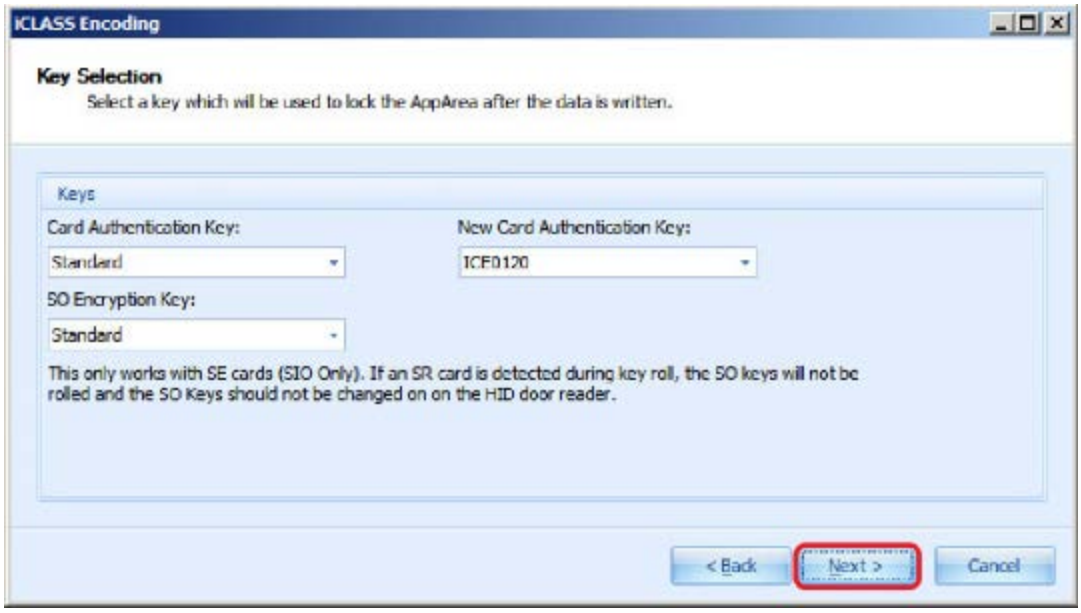


4. **Key Selection:** Select a key to lock the AppArea after the data is written. Click **Next**.

iCLASS key selection

The following section is the Key Selection window for iCLASS Encoding.

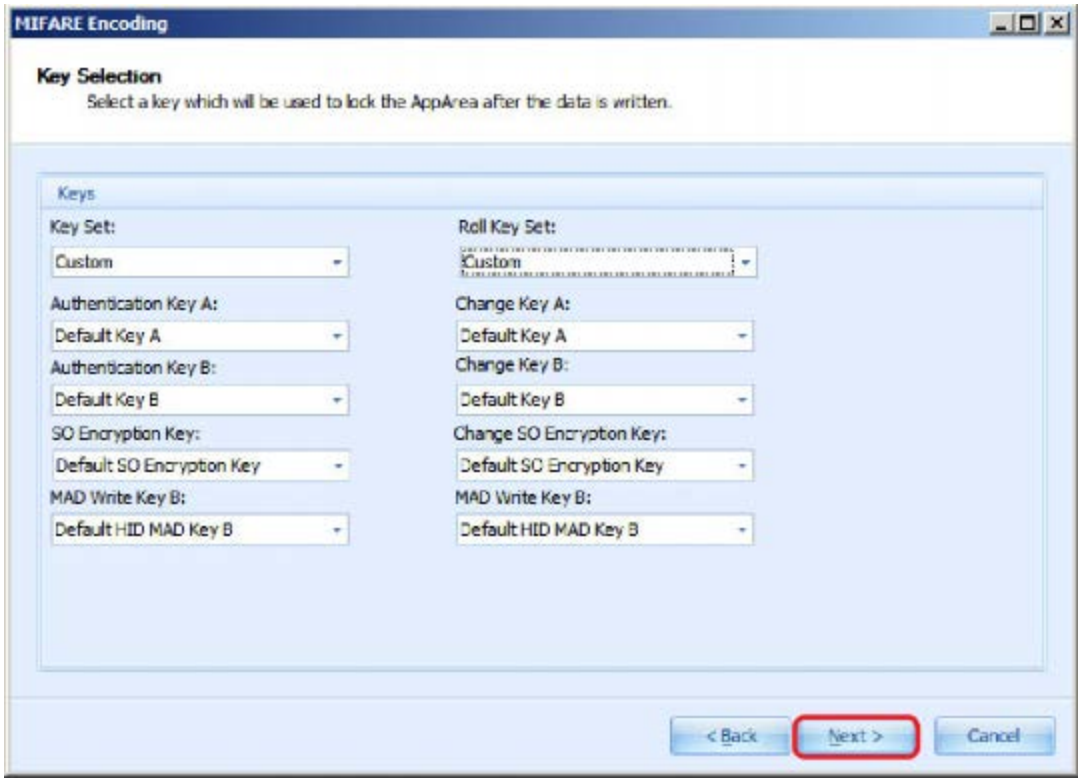
Field	Description
Key	Card Authentication Key: Standard, or HID defined Key Sets may be selected New Card Authentication Key: Standard, or HID defined Key Sets may be selected SO Encryption Key: Standard, or HID defined Key Sets may be selected



MIFARE Classic key selection

The following section is the Key Selection window for MIFARE Classic Encoding.

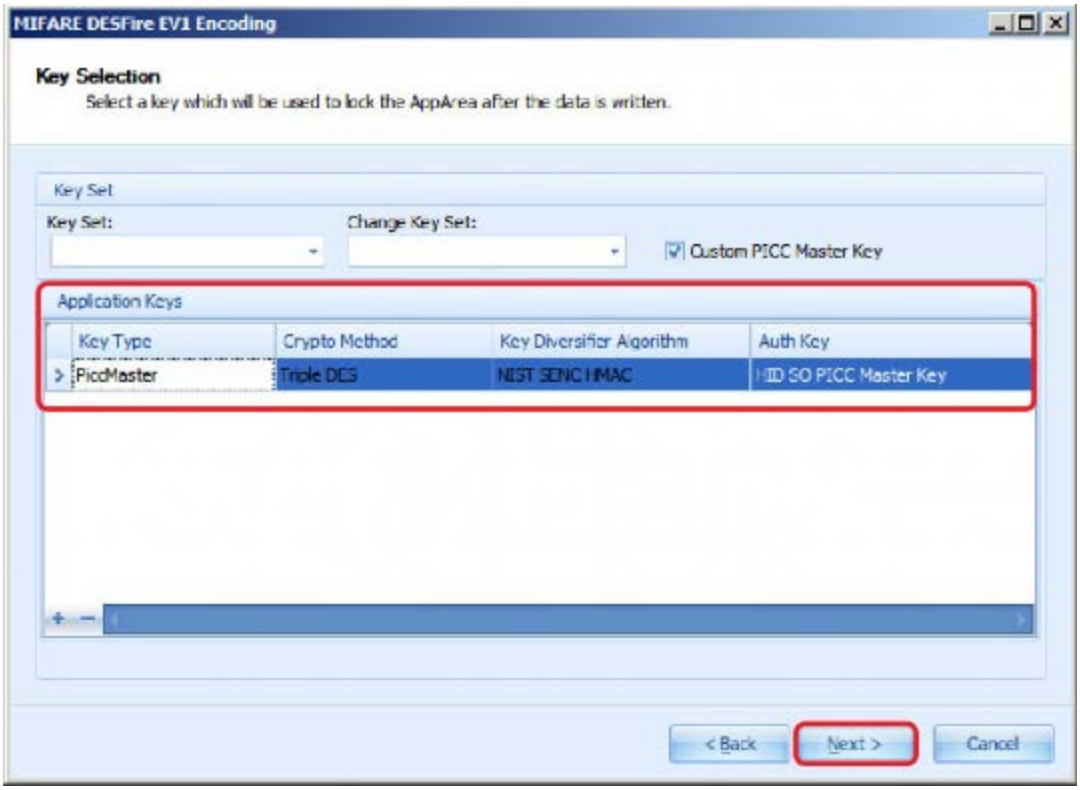
Field	Description
Keys	**Key Set**: Custom, Standard, or HID defined Key Sets may be selected. **Roll Key Set**: Custom or HID defined Key Sets may be selected. **Authentication Key A**: Select an option from the drop-down menu. **Change Key A**: Select an option from the drop-down menu. **Authentication Key B**: Select an option from the drop-down menu. **Change Key B**: Select an option from the drop-down menu. **SO Encryption Key**: Select an option from the drop-down menu. **Change SO Encryption Key**: Select an option from the drop-down menu. **MAD Write Key A**: Select an option from the drop-down menu. **MAD Write Key B**: Select an option from the drop-down menu.



MIFARE DESFire EV1 key selection

The following section is the Key Selection window for MIFARE DESFire EV1 Encoding.

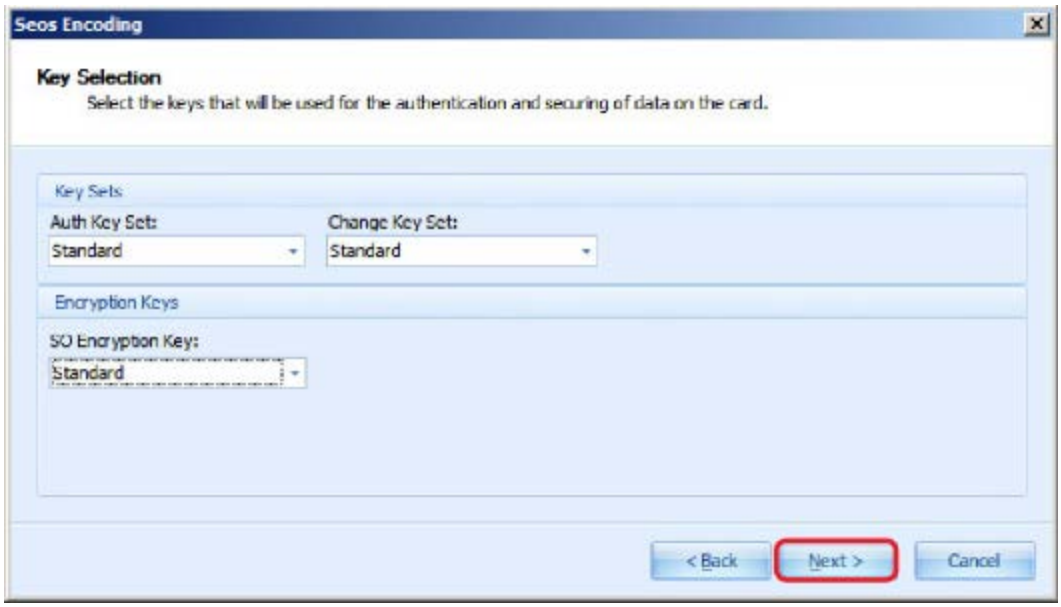
Field	Description
Keys	Key Set: Standard or HID defined Key Sets may be selected. Change Key Set: Standard or HID defined Key Sets may be selected. Custom PICC Master Key: Select to open the Application Keys section for configuration (see section circled below).



Seos key selection

The following section is the Key Selection window for Seos Encoding.

Field	Description
Key Sets	Auth Key Set: Standard or HID defined Key Sets may be selected. Change Key Set: Standard or Custom Key Sets may be selected.
Encryption Keys	SO Encryption Key: Standard or HID Standard Key Sets may be selected.



5. When the wizard is complete, click **Finish**.
6. Return to **5.6 Create a work order**, step 5 to save the Work Order.

6.8 Multi-technology card support

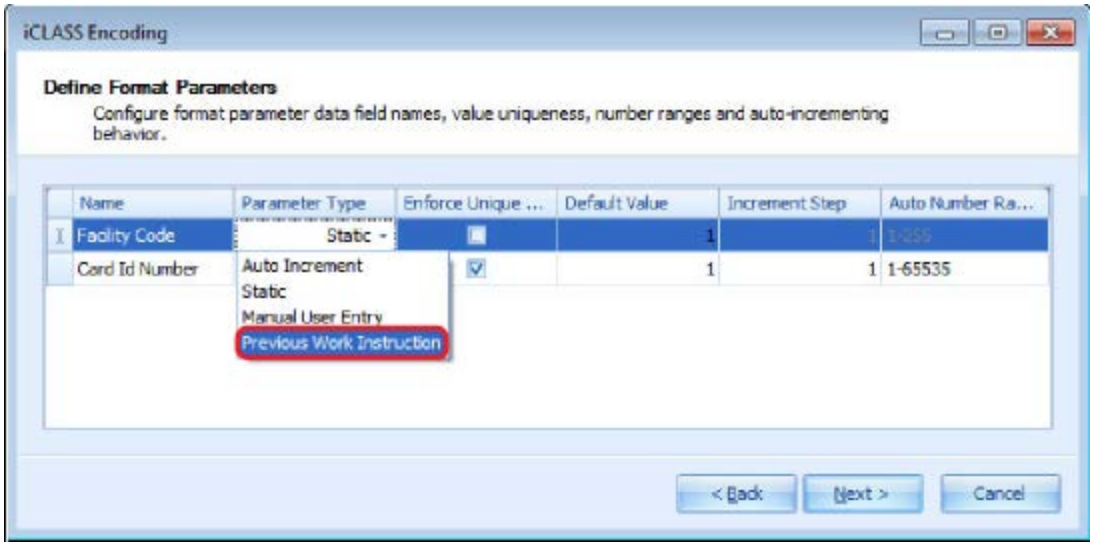
To support multiple technology cards, a Work Order can contain multiple Work Instructions for multiple encoding operations for a single technology. For instance, to read a multi-technology Prox/iCLASS card you would first add a Prox Work Instruction and then add an iCLASS Work Instruction. For more information on creating work instructions, see **Work instruction wizard**.

Note: A special feature exists to read the PACS credential from one technology (for instance Prox) and write the same formatted credential into another technology supported by the card (for instance iCLASS).

For example,

1. Open a Work Order then select Add Work Instruction.
2. Select the Prox technology type from the list and use the Work Instruction Wizard to create a Prox Read instruction with the desired format. Save the Work Instruction.
3. Next, Select Add Work Instruction and use the Work Instruction Wizard to create another work instruction.
4. Select the iCLASS technology type from the list and use the Work Instruction Wizard to create an iCLASS Write - HID Access Application instruction.

   Note: You must select the same format as in the Prox Read instruction in step 2 above.
5. On the Define Format Parameters page, select the Previous Work Instruction option for the Parameter Type field. Do this for each parameter in the grid. This routes the PACS credential data read from the Prox instruction into the iCLASS instruction.



6. Complete the Wizard selections and save the Work Order.

Note: These parameters are set to read-only in the Work Order Manager to prevent you from manually entering data, which could be overwritten.

Section 07

Key Management

7.1 Introduction

The following section covers all aspects of the Key Management environment.

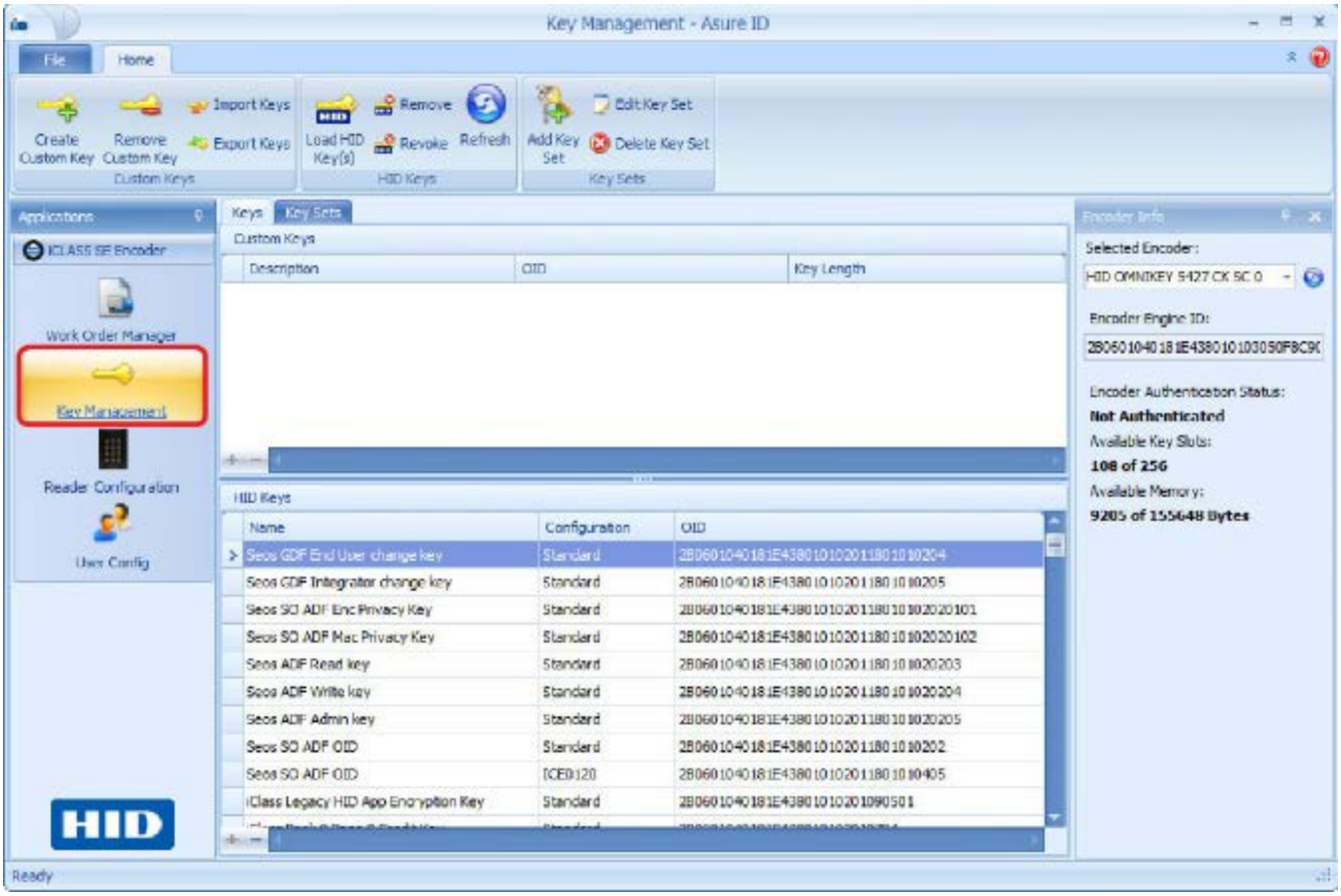
There is a limit to the number of and Keys (HID and Custom) that can be stored on the iCLASS SE Encoder. The Available Key Slots and Memory is easily monitored on the **Encoder Info** panel.

It is recommended that this space be managed by:

- Loading only keys that are needed for your configuration.
- Exporting and/or removing custom and HID Keys that are not longer required.

7.2 Key Management Home tab

The Key Management Home tab contains the following areas.



7.2.1 Key Management toolbar

The Key Management module of the CP1000 Desktop Encoder allows you to view and manage the HID and Custom Keys.

Toolbar Function	Description
Create Custom Key	Allows you to create or randomly generate a key. See 7.4 Create key.
Remove Custom Key	The general rule is keys are not removed or deleted. However, if the number of stored keys reaches its limit (number/size), it may be required to remove keys that are not required. See 7.5 Remove selected key. **Note:** Custom Keys should be exported before removing them from the system.
Import Keys	Allows you to Import Custom Keys exported from another file. **Note:** You must share the same Admin Keys and passwords to share Custom Keys. See 7.6 Import keys and key sets.
Export Keys	Allows you to securely export (save) the Custom Keys and Admin Keys for backup and recovery. See 7.7 Export keys.
Load HID Key(s)	Allows you to load a file containing encrypted HID keys targeted to a specific encoder. The names and locations of the files are required. Once loaded, the HID keys appear on the HID Keys pane. See 7.8 Load HID keys.
Remove	Allows you to remove the selected HID key or keys from the selected encoder. See 7.9 Remove HID keys.
Revoke	Allows you to load the key revocation list to the encoder. See 7.10 Revoke HID keys.
Refresh	Allows you to reload keys from the encoder. See 7.11 Refresh HID key list.
Add Key Set	Allows you to add a Key Set to create a grouping of custom keys. See 7.12 Add key set.
Edit Key Set	Allows you to edit a Key Set. See 7.13 Edit key set.
Delete Key Set	Allows you to delete a Key Set from the Key Set pane. See 7.14 Delete key set.

7.2.2 Encoder Info panel

The Key Management **Encoder Info** panel displays information about the CP1000 Desktop Encoder currently connected to the computer.

Field	Description
Selected Encoder	All available encoders are listed in the drop-down list. Click the **Refresh** to refresh the type of encoder.
Encoder Engine ID	The ID of the selected encoder is displayed. Credentials are linked to this Encoder Engine ID.
Encoder Authentication Status	The Authentication function is normally an automatic function. However, if **Not Authenticated** is displayed, or if the encoders are changed, this process allows the authentication of the new iCLASS SE Encoder.
Available Key Slots	The number of HID and Custom keys stored on the encoder. As keys are loaded and removed, the information is shown on the Encoder Info panel.
Available Memory	The amount of memory available on the encoder.

7.3 Key Manager File tab

The **Key Manager File** tab contains specific options for this module.

Option Function	Description
Upload Credential Credits	The Upload Credential Credits allows the upload of Credential Credits provided by HID Global. See 4.4 Upload encoder configuration package.
Sync Encoder	See 7.10 Revoke HID keys for detailed information.
Change Encoder Admin Keys	See 7.16 Change encoder Admin keys for detailed information.
Open Log File	Allows you to view the log file of events for the Asure ID CP1000 Edition application.

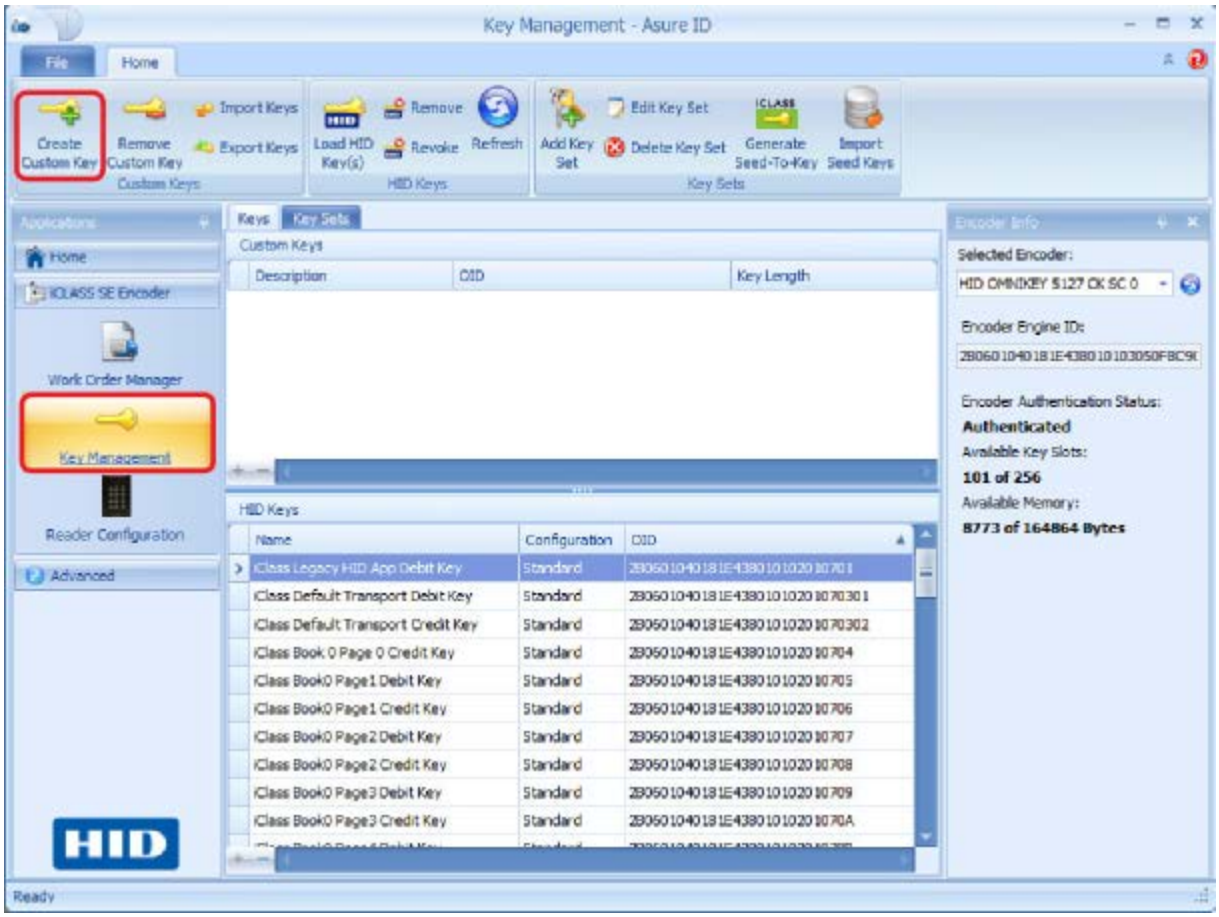
7.4 Create key

The Create Key process allows you to define and save a new Custom Key to the iCLASS SE Encoder.

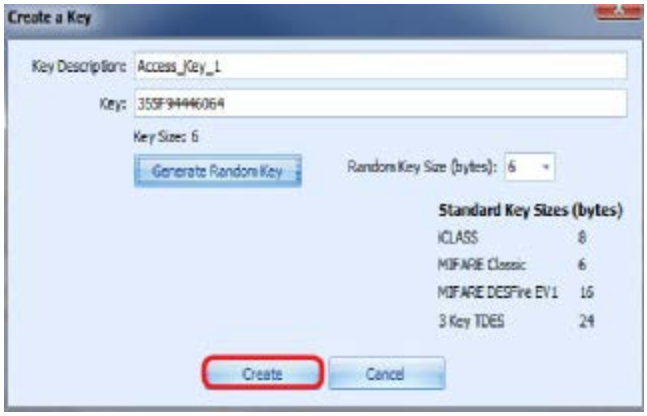
> **Note:** When a Custom Key is created, it is encrypted and stored in the Asure ID native database and uploaded on demand in the following situations:

- A new Encoder is used to encode a credential
- An encoder which previously contained the key became full and the key was backed-up and deleted to make room for a new key.

1. Select the **Key Management** module.
2. Click **Create Custom Key** from the toolbar.

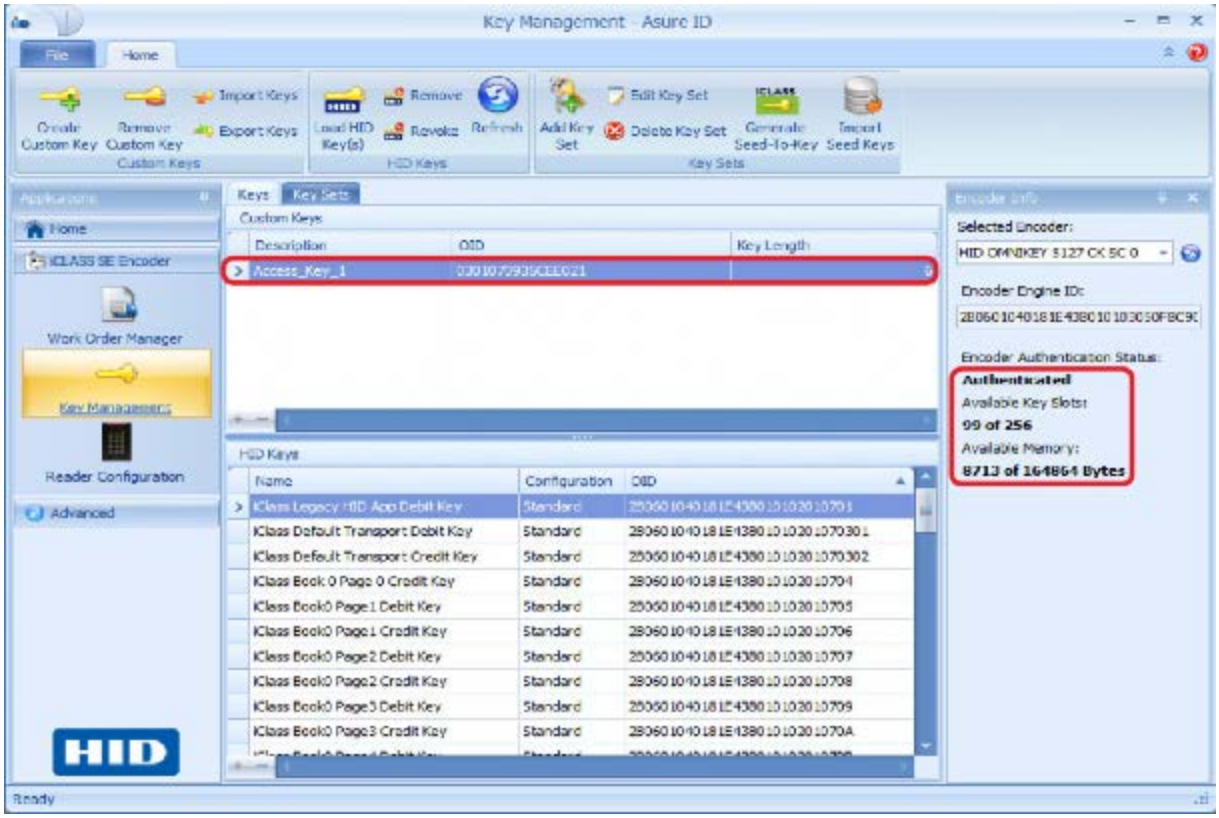


3. Enter the following information on the Create a Key window and click **Create**.



Field	Description
Key Description	Enter a description for the key.
Key	This can either be manually entered (hexadecimal) or click **Generate Random Key**, which generates a key based on the Random Key Size field and fills the field.
Random Key Size (bytes)	From the drop-down menu set the key size value. The following are technology and encoder key sizes: • MIFARE = 6 bytes • MIFARE DESFire = 16 bytes • iCLASS Authentication = 8 bytes • iCLASS Encryption = 16 bytes • DES = 8 bytes • 2kTDES = 16 bytes • 3kTDES = 24 bytes • AES = 16 bytes • Encoder Configuration Keys = 16 bytes • SO Keys = 16 bytes

4. The new Key is created and is displayed in the **Custom Keys** pane.
   The **Available Key Slots** and **Available Memory** display the updated status.

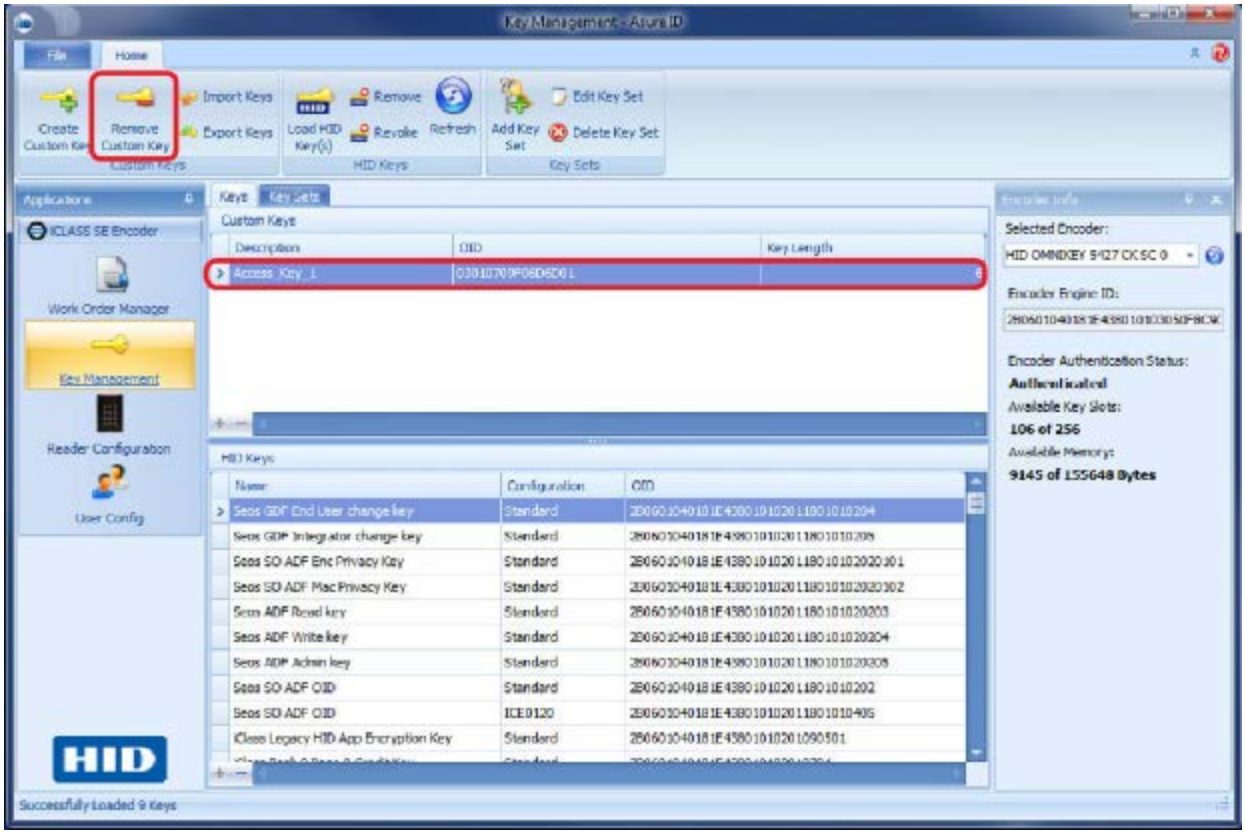


7.5 Remove selected key

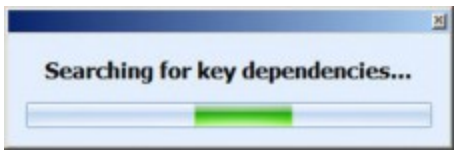
The general rule is Keys are not removed or deleted. However, if the number of stored keys reaches its limit (number/size), it may be required to remove keys that are not required.

> **Note:** Custom Keys should be exported before removing them from the system. See **7.7 Export keys** for more information.

1. Select the **Key Management** module.
2. Select the Key to be removed.
3. Click **Remove Custom Key** from the menu bar.

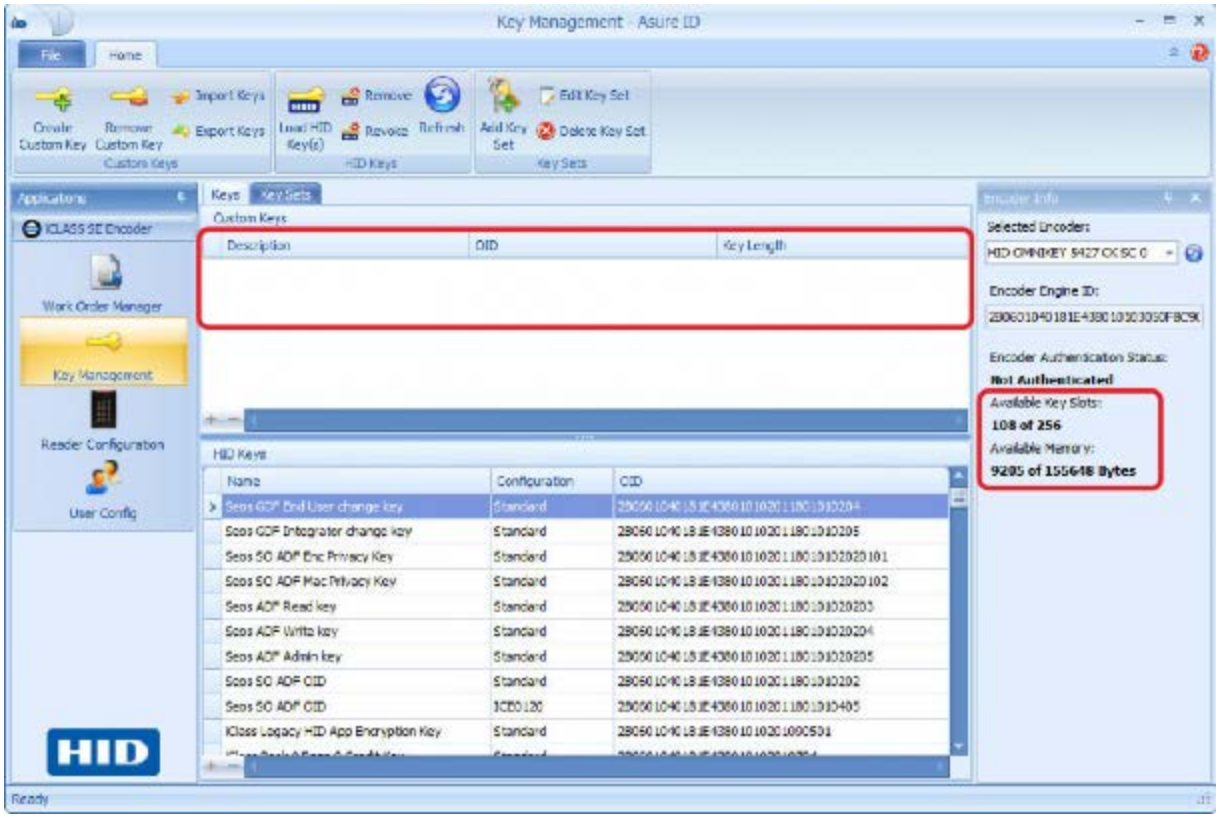


4. A Working progress bar is displayed.



5. When complete, the Key is removed from the encoder and no longer appears on the list.

> **Note:** The **Available Key Slots** and **Available Memory** displays the updated status.



7.6 Import keys and key sets

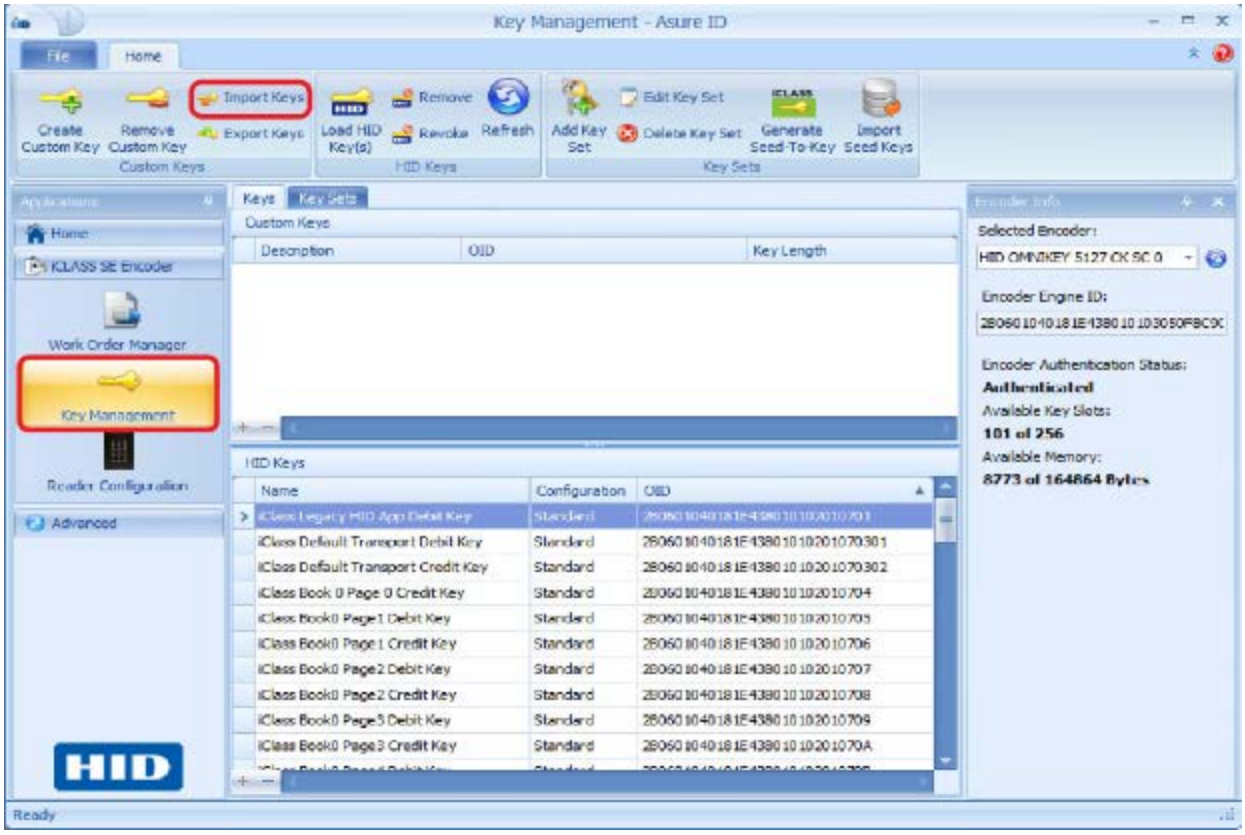
The Import Keys tool allows you to import Custom Keys and Key Sets exported from an iCLASS SE Encoder. To import Custom Keys from a file on a computer or USB flash drive, use the following steps.

> **Important: To import keys/key sets to another device, that device must have the same SNMP Admin keys as the device from which the custom keys were originally exported and each workstation must have the same PIN Code.**

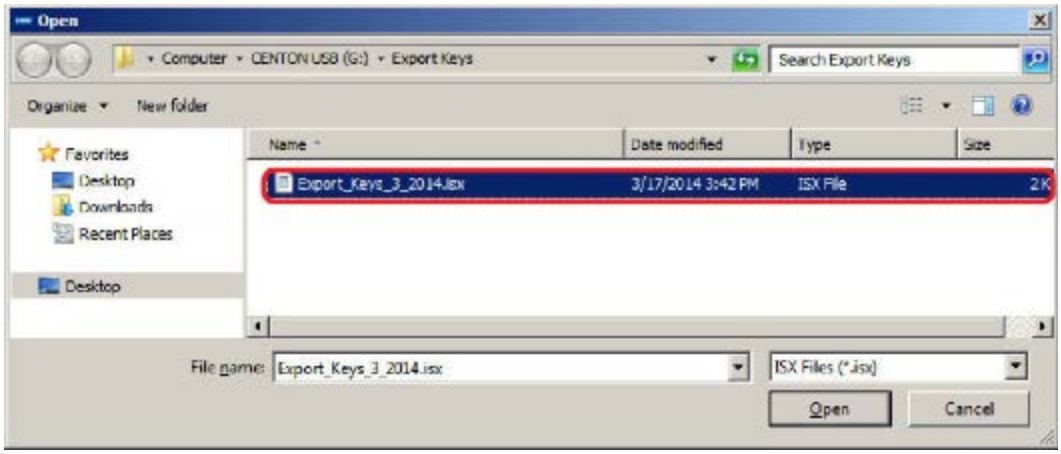
You must enter the 4-9 digit code to securely access the Custom Keys from a workstation. This code should be the same across all workstations where custom keys are automatically synchronized.

> **Note:** The SNMP encoder Admin keys must also match on all workstations where custom keys are automatically synchronized.

1. Select **Key Management**.
2. Select **Import Keys** from the menu bar.



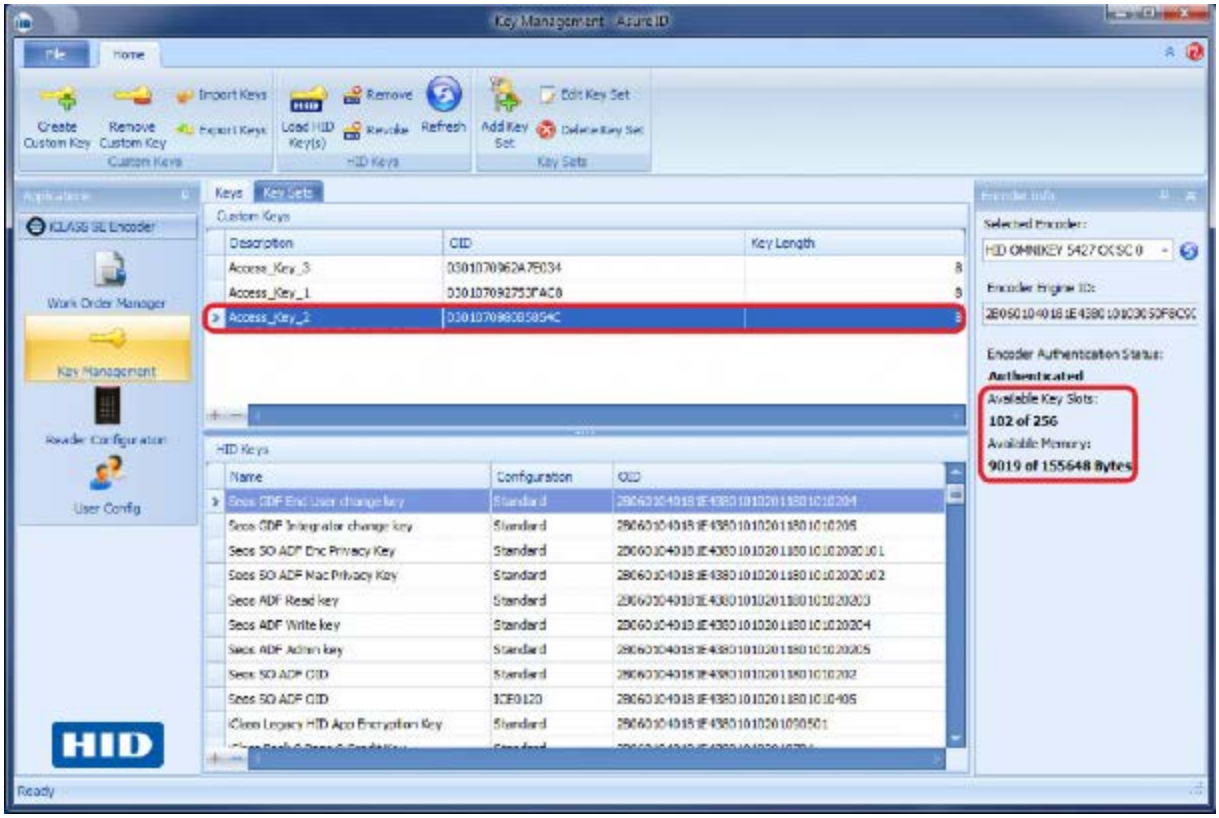
3. Locate the file previously saved in **7.7 Export keys**. Double-click the file to import.



4. Enter the password set for the keys, if required. Click **OK**.

5. The Keys are displayed in the Custom Keys list.

> **Note:** The **Available Key Slots** and **Available Memory** displays the updated status.



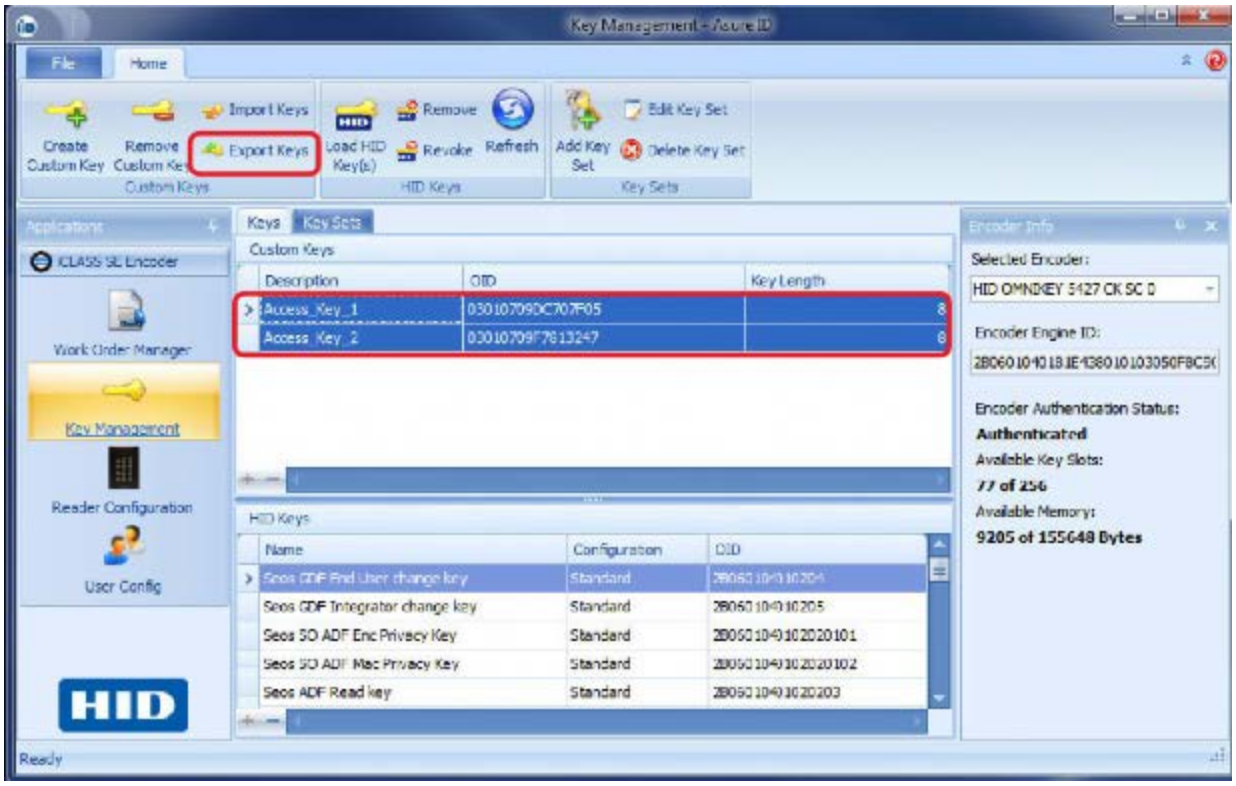
7.7 Export keys

The **Export Keys** tool allows you to securely export (save) the Custom Keys and Admin Keys for backup and recovery.

> **Important: If the PC hosting the application fails, you lose access to the encoder which stores the credential credits and custom keys, therefore it is important that you record these keys in a secure location for future reference.**

Admin Keys are required if the PC running this application, is no longer functioning. These keys are entered when this application is loaded on a new PC to reconnect to the encoder, otherwise credential credits and other important information is lost and the encoder needs to be returned to HID to be restored to factory settings.

1. Select the **Key Management** > **Export Keys**.



2. Select any or all of the following: **Export Custom Keys**, **Export Key Sets**, **Export Admin Keys** and click **OK**.

3. The Password window only appears when the **Export Admin Keys** is selected. Enter a password (twice) to access the file, and click **OK**.

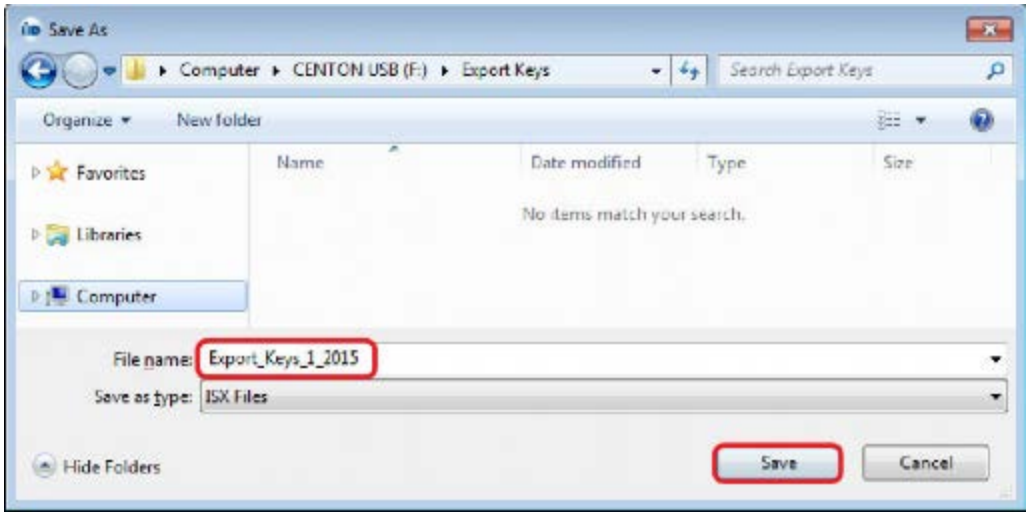
   > **Note:** Make note of this password for future access to this file.

4. Browse to a location to save the file.

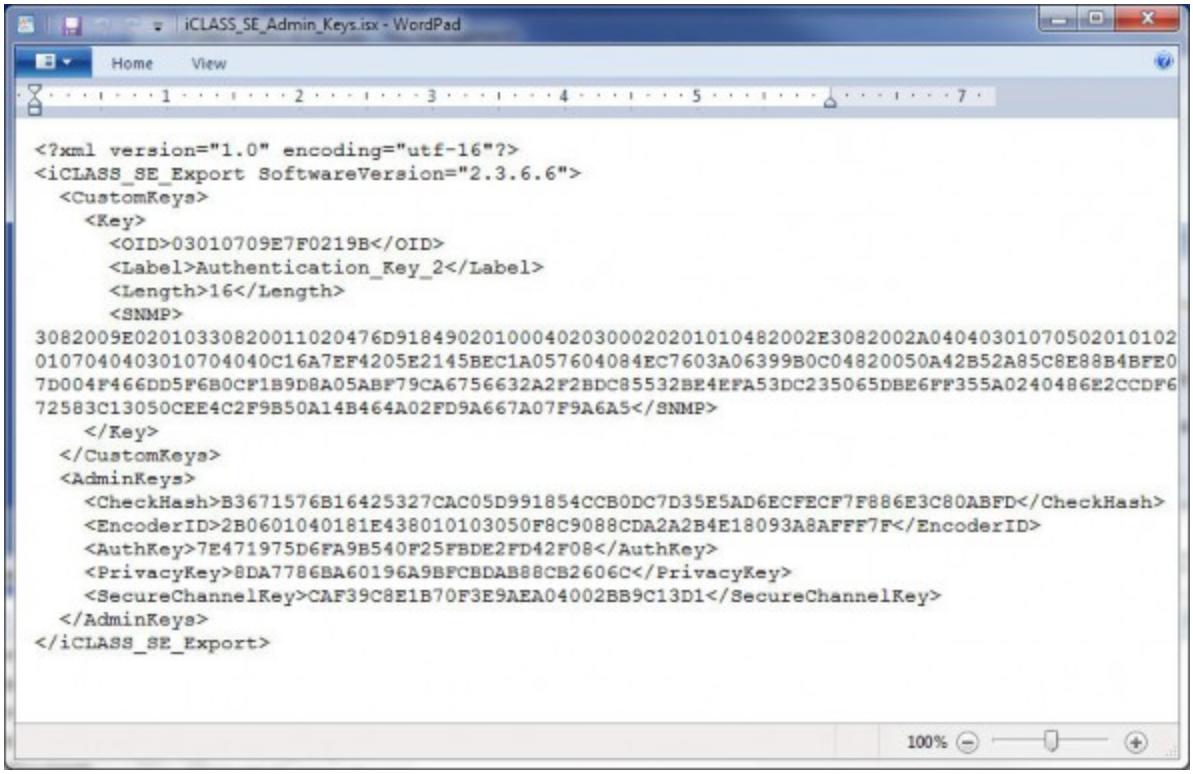
   > **Note:** It is recommended that this file be saved in a secure location along with backup information.

5. Enter a name for the file, and click **Save**

> **Important: The Admin Keys are encrypted and cannot be entered into Asure ID or any 3rd party application in their encrypted form. Therefore, it is imperative that you have a secure backup (hard copy) of the Admin keys, if the encoder is to be used in a 3rd party system.**



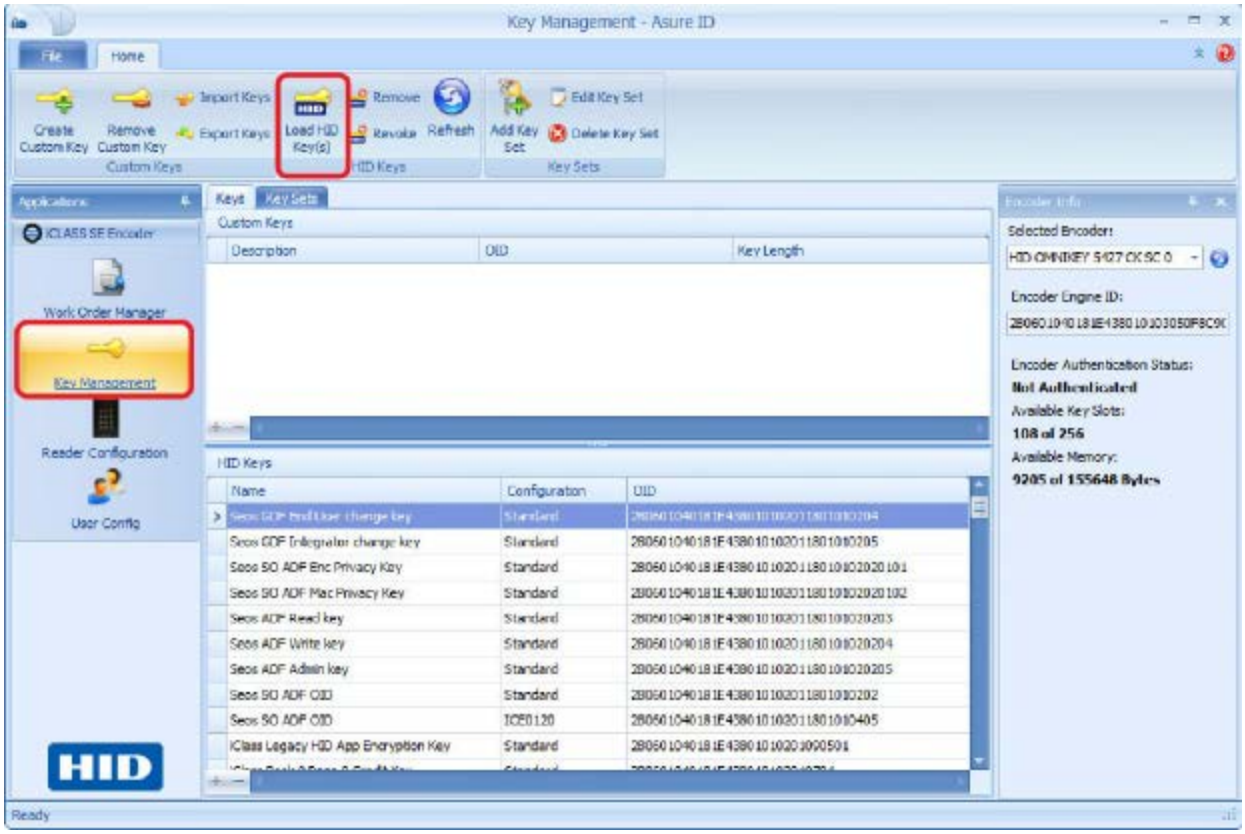
This file can now be used to Import Keys to an iCLASS SE Cp1000 Encoder. See **7.6 Import keys and key sets** for information on this process.



7.8 Load HID keys

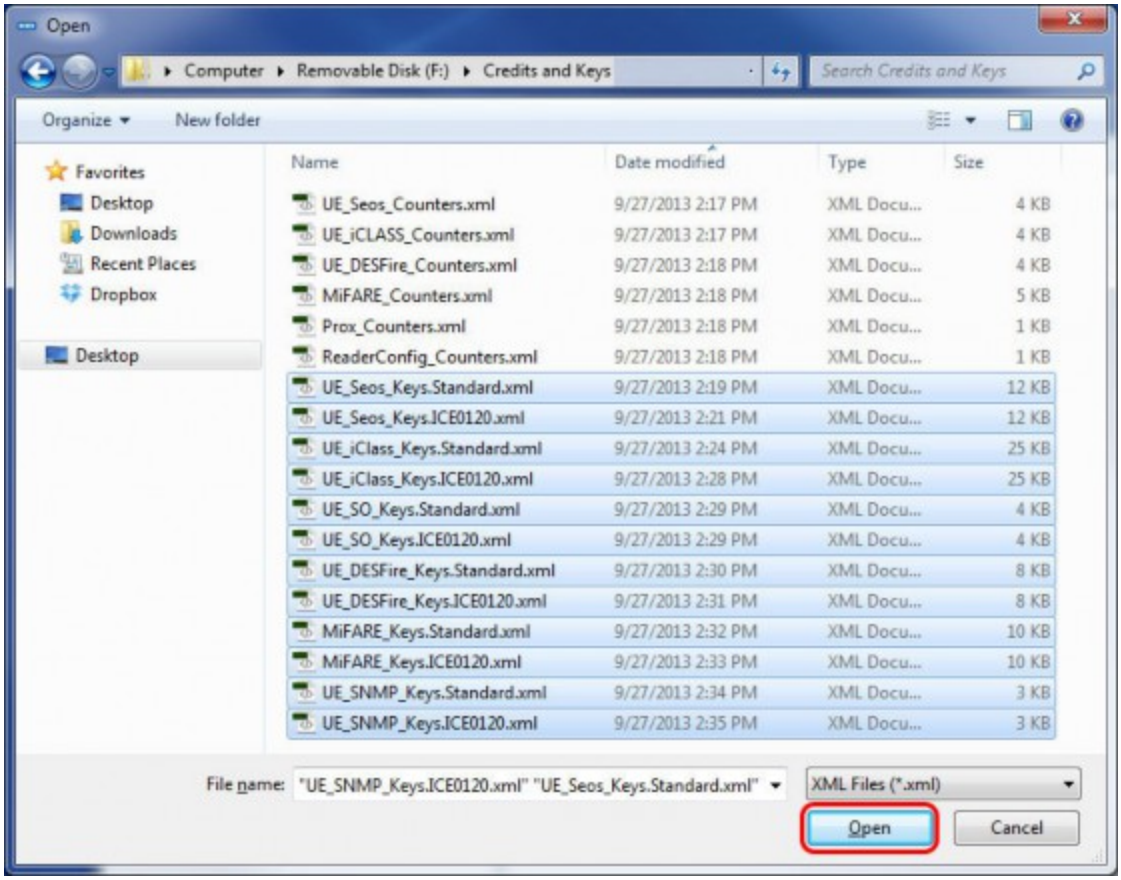
The **Load HID Key(s)** feature allows you to securely upload the HID Keys by using an .ise or .xml file. The following process loads the HID managed keys to the iCLASS SE CP1000 Encoder.

1. Select **Home** tab > **Key Management** > **Load HID Key(s)**.

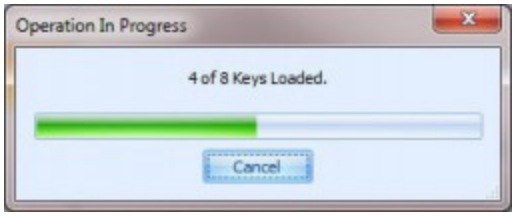


2. Browse to and select the Keys ordered from HID Global.

3. Select the files to be loaded, and click **Open**.

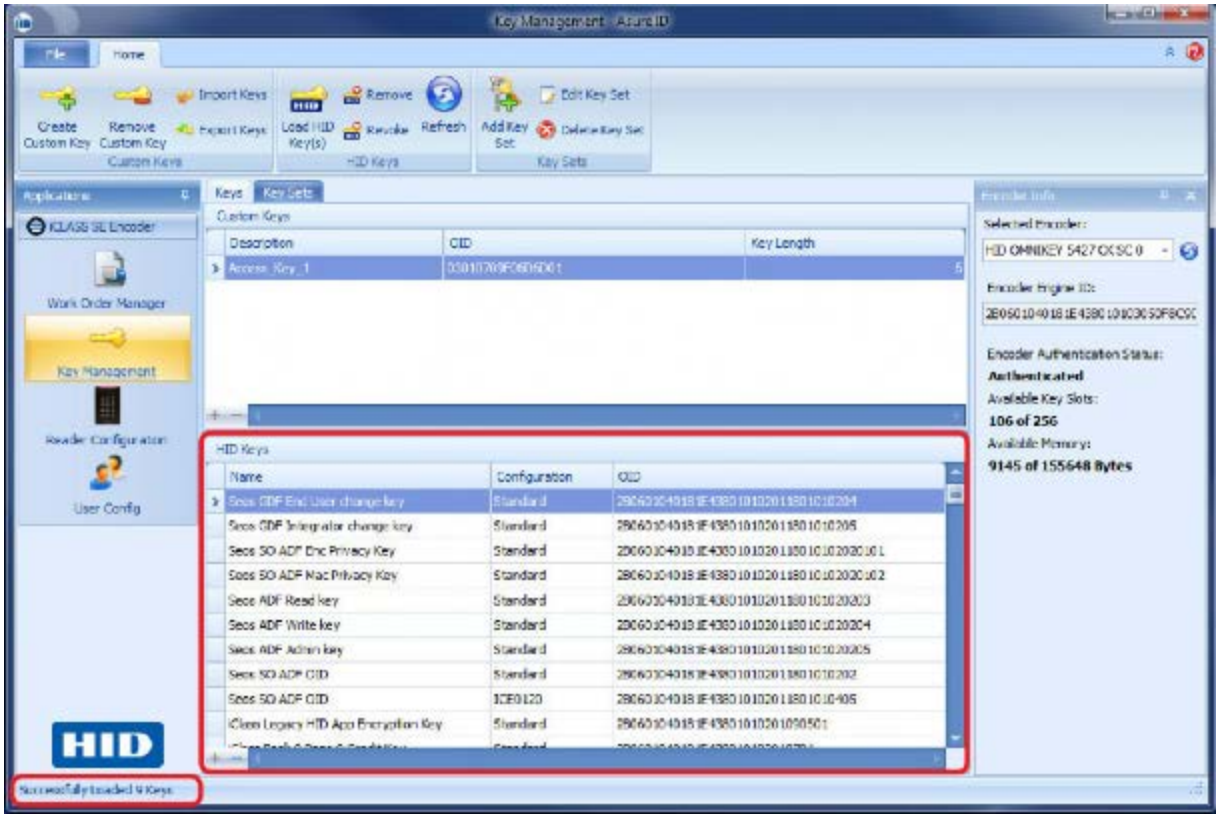


4. A progress bar is displayed as keys are loaded.



5. When the Keys are successfully loaded, a message is displayed at the bottom of the window.

6. After the upload is complete, the installed Keys are displayed on the **HID Keys** pane.



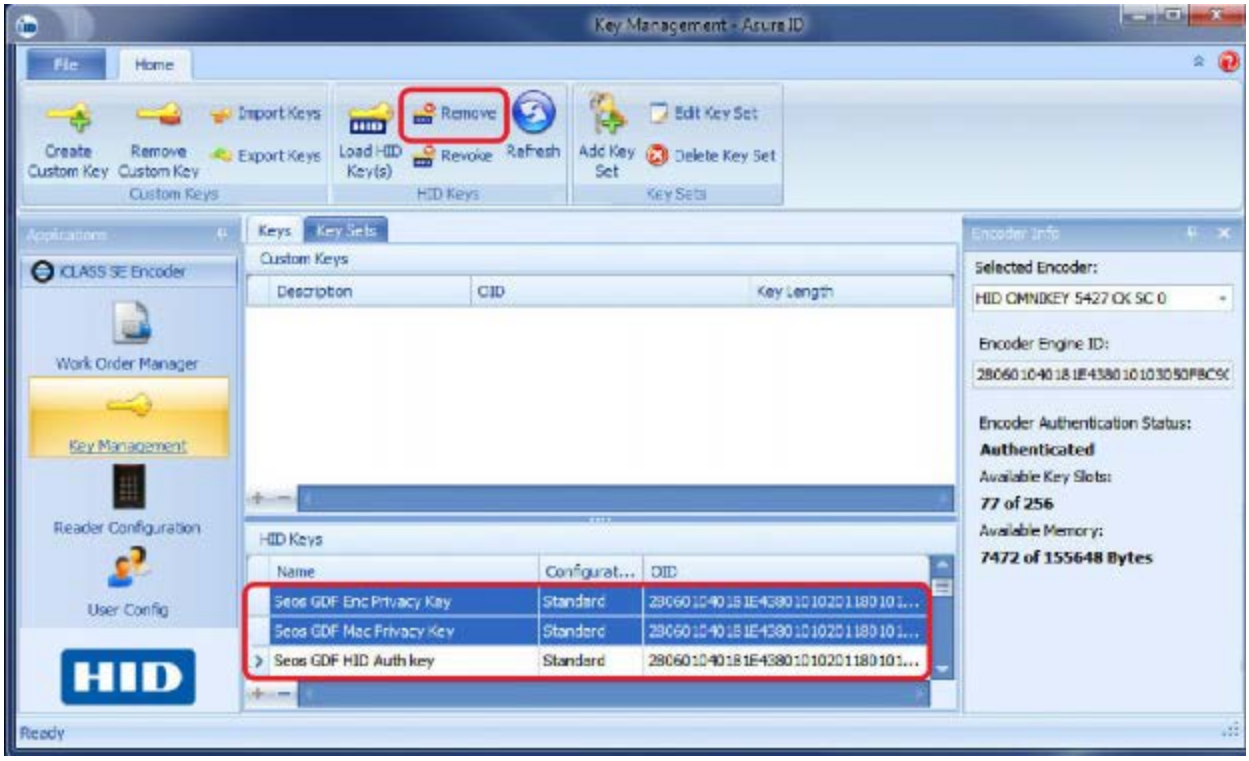
7.9 Remove HID keys

The Remove tool allows you to remove specific HID Keys from the iCLASS SE CP1000 Encoder.

1. Select **Home** tab > **Key Management**.
2. Select the HID Keys to be removed from the HID Keys pane.

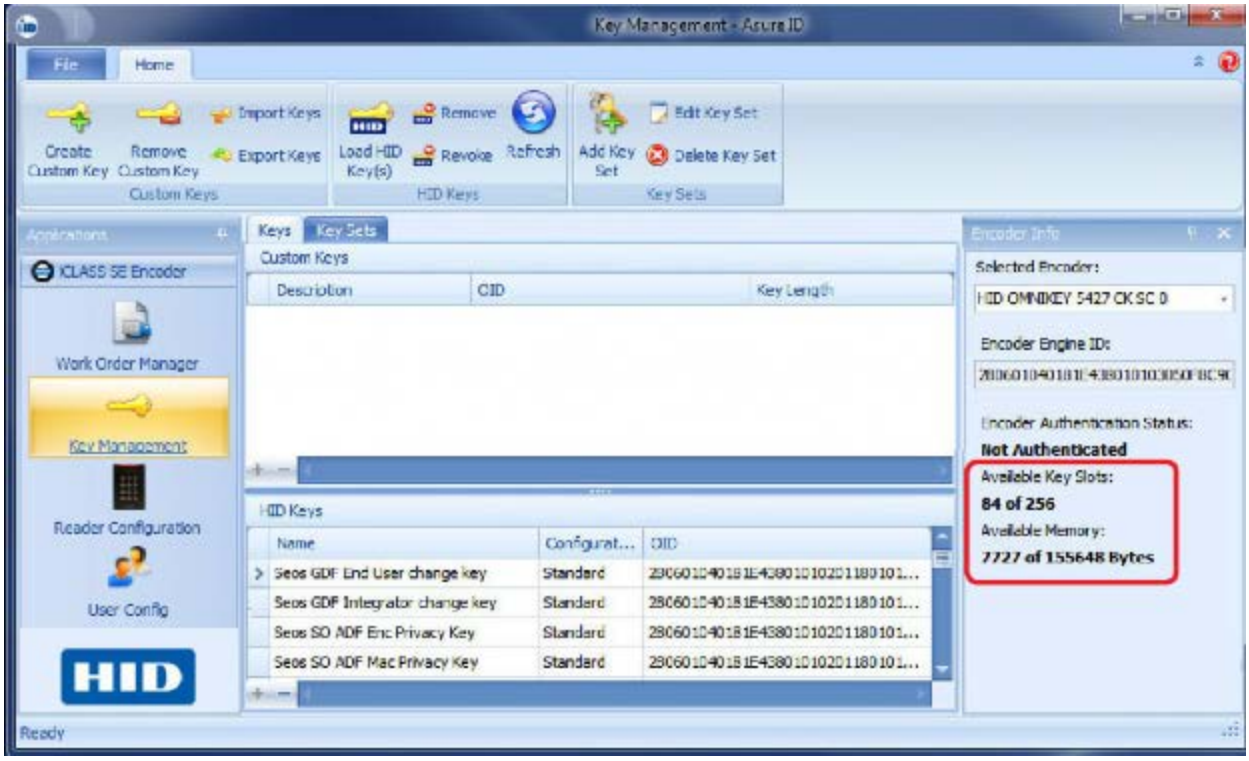
   > **Note:** This includes selecting the line that contains the arrow (**>**).

3. Click **Remove** from the menu bar.



4. The selected keys are removed (in this example it was the last remaining keys).

Note: The Available Key Slots and Available Memory display the updated status.



7.10 Revoke HID keys

The Revoke tool, allows the loading of a Key Revocation list. You would receive this list from HID Technical Support and is only used with their assistance.

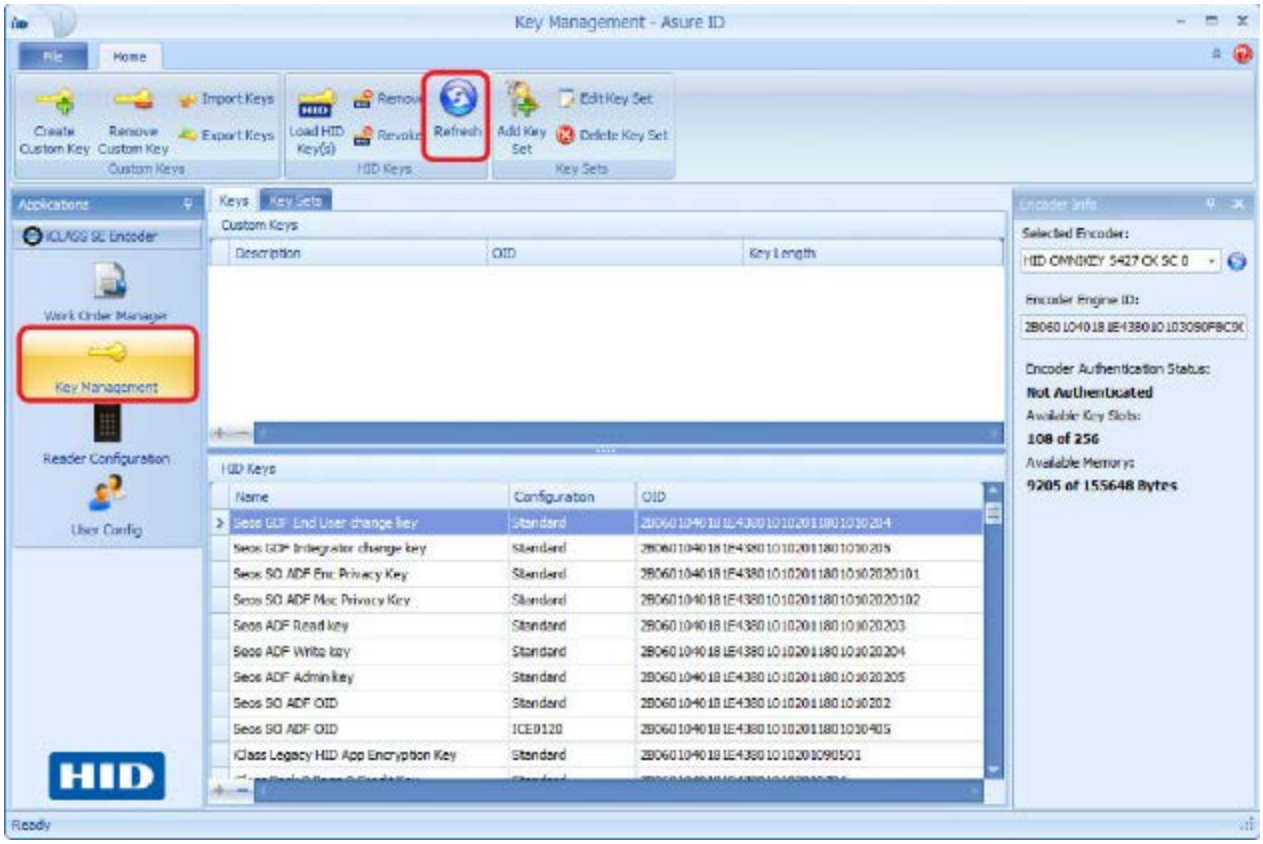
If there is a need to revoke HID keys, a request to HID Global is made and a Key Revocation List is created, and delivered to you. To perform a revocation, follow the steps below.

1. Select the **Key Management** module.
2. Select **Revoke**.

3. Once HID Keys have been revoked, they are not allowed to be reinstalled on the device.

7.11 Refresh HID key list

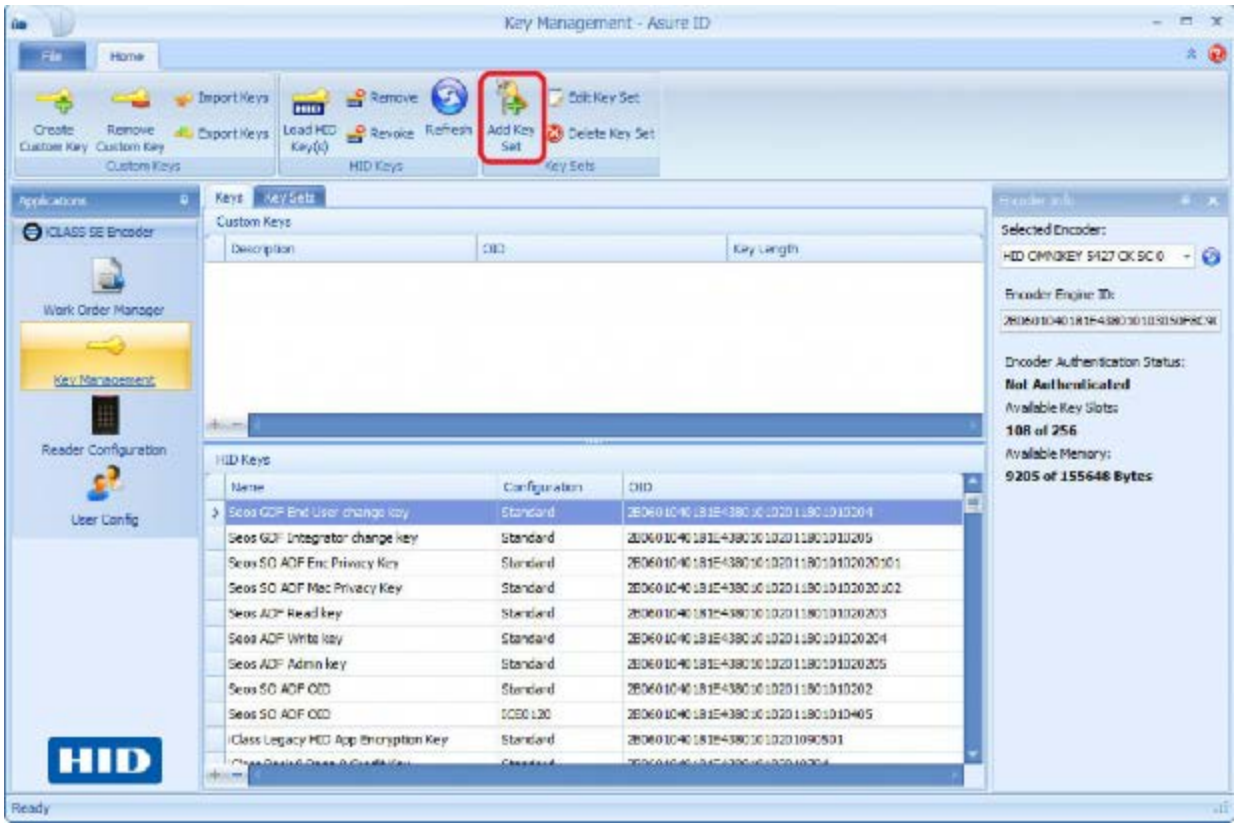
1. Oftentimes it is necessary to refresh the list of keys. This often occurs when after Custom Keys have been added or deleted. When you select Refresh, all HID Keys and Keysets are updated from the current database.
2. Select **Home** tab > **Key Management**.
3. Select **Refresh**.
4. The Keys are reloaded from the encoder.



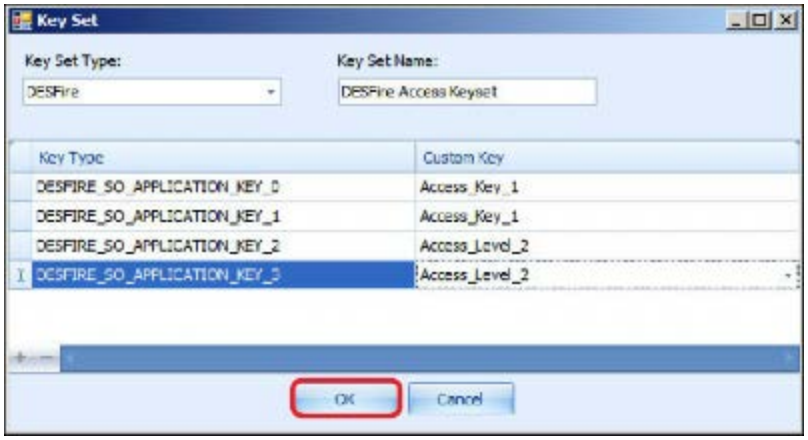
7.12 Add key set

Key Sets are created as a means to group keys for the HID applications to simplify deployment.

1. Select **Home** tab > **Key Management**.
2. Select **Add Key Set**.

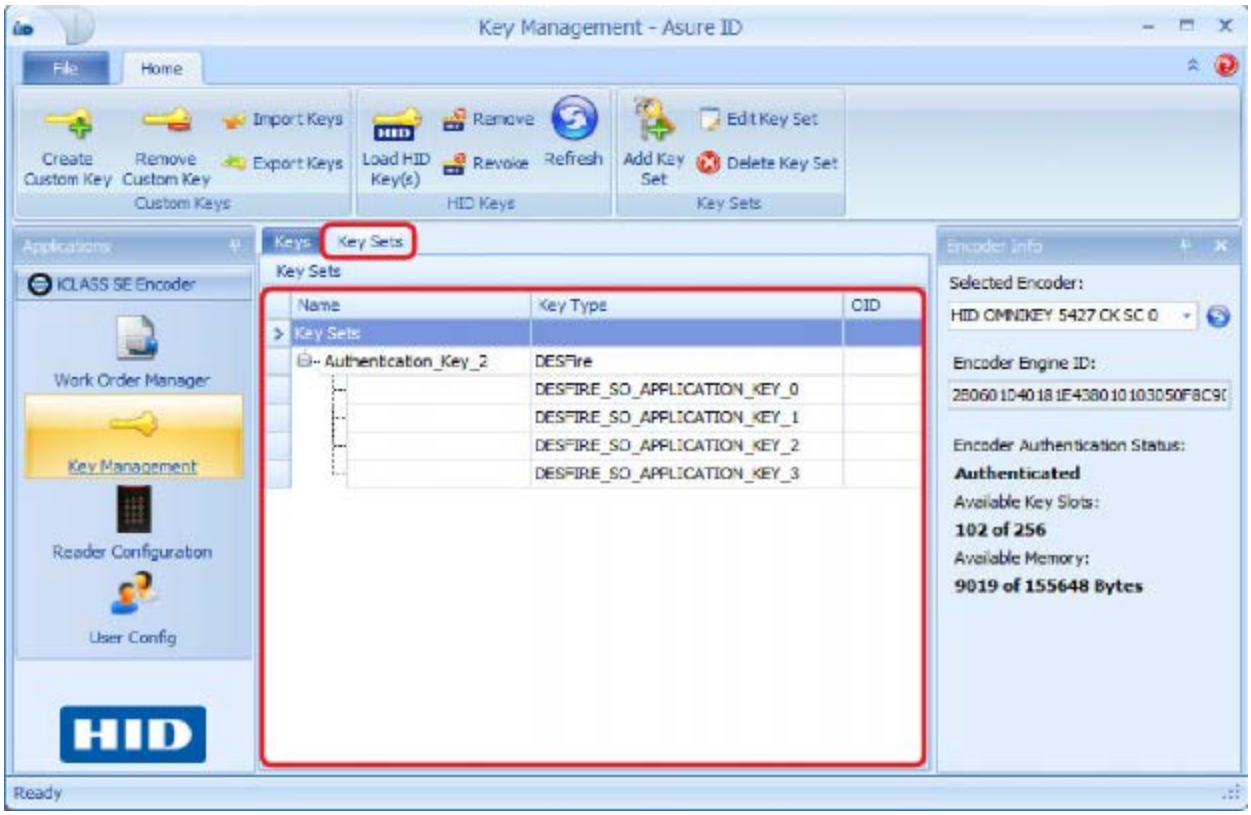


3. Define the Key Set. Click **OK**.



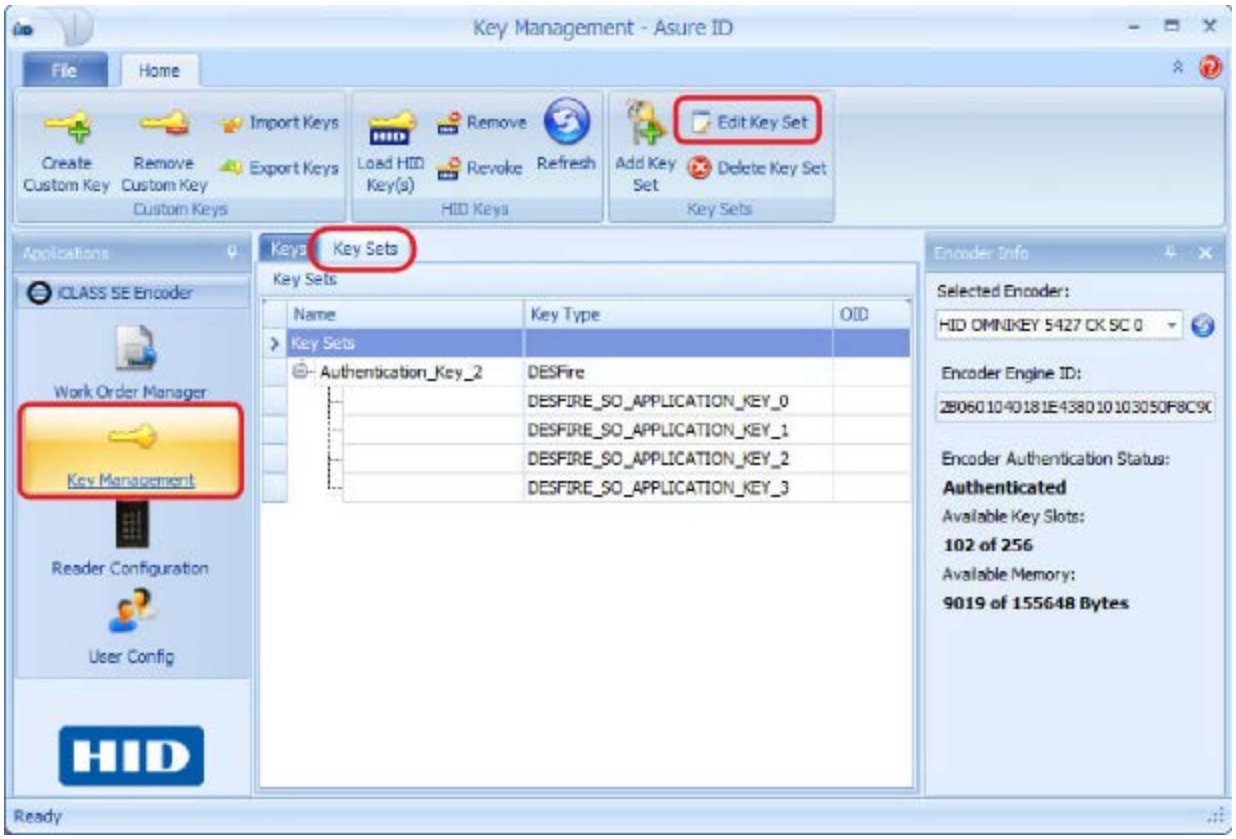
Field	Description
Key Set Type	Select the technology type: DESFire, iCLASS, MIFARE, Seos, or SO.
Key Set Name	Enter a Name for this Key Set.
Key Type	Select a Key Type from the list.
Custom Key	Select a **Custom Key or HID Key** from the drop-down menu.

4. The Key Set created is displayed on the **Key Sets** tab.

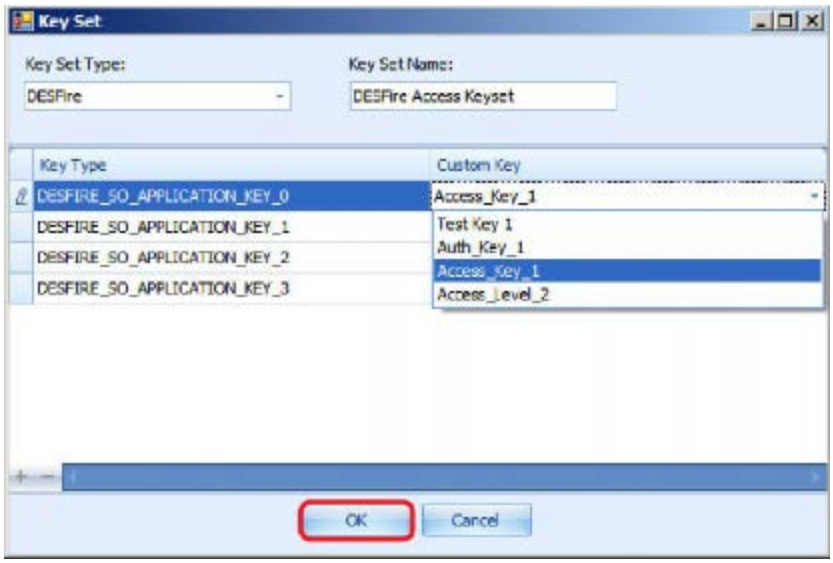


7.13 Edit key set

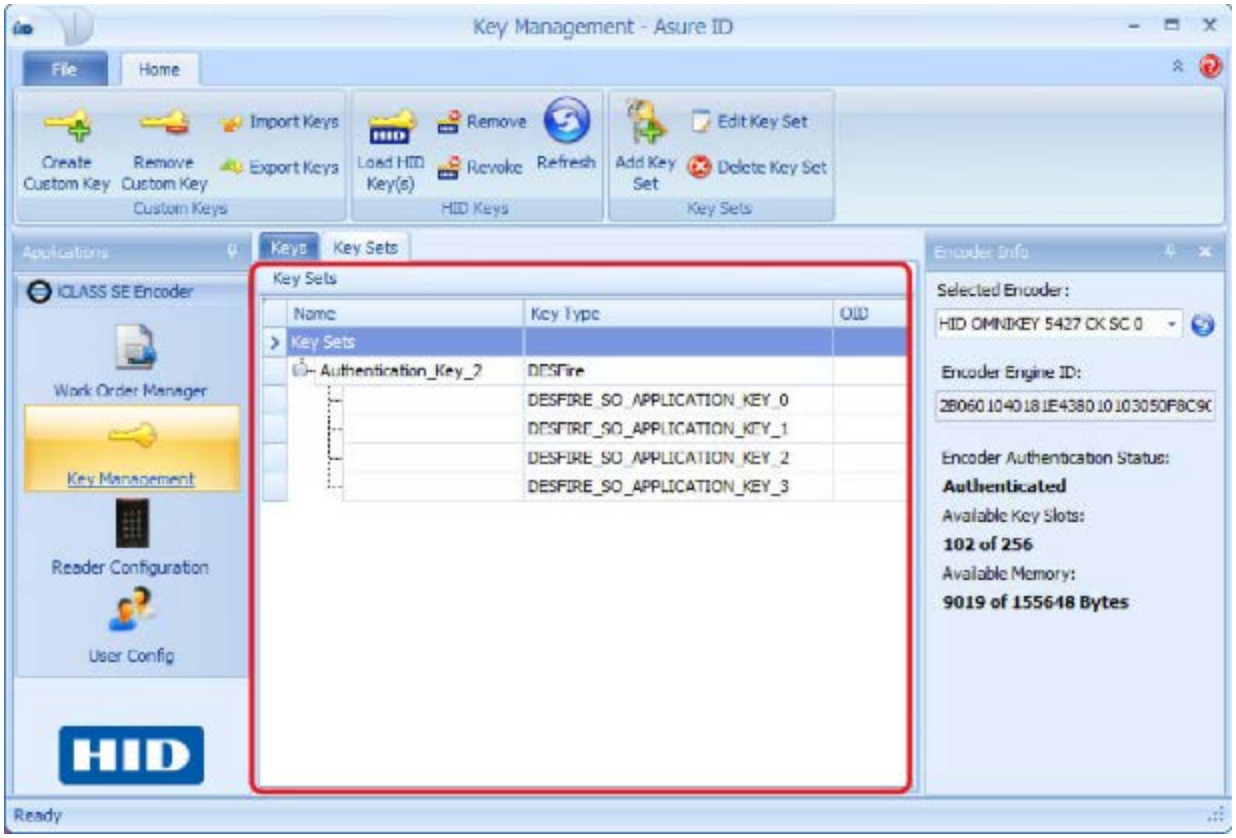
1. Select **Key Management** > **Key Sets** tab.
2. Select a Key Set to modify.
3. Click **Edit Key Set** from the menu bar



4. Edit the Key Set as needed. Click **OK**.

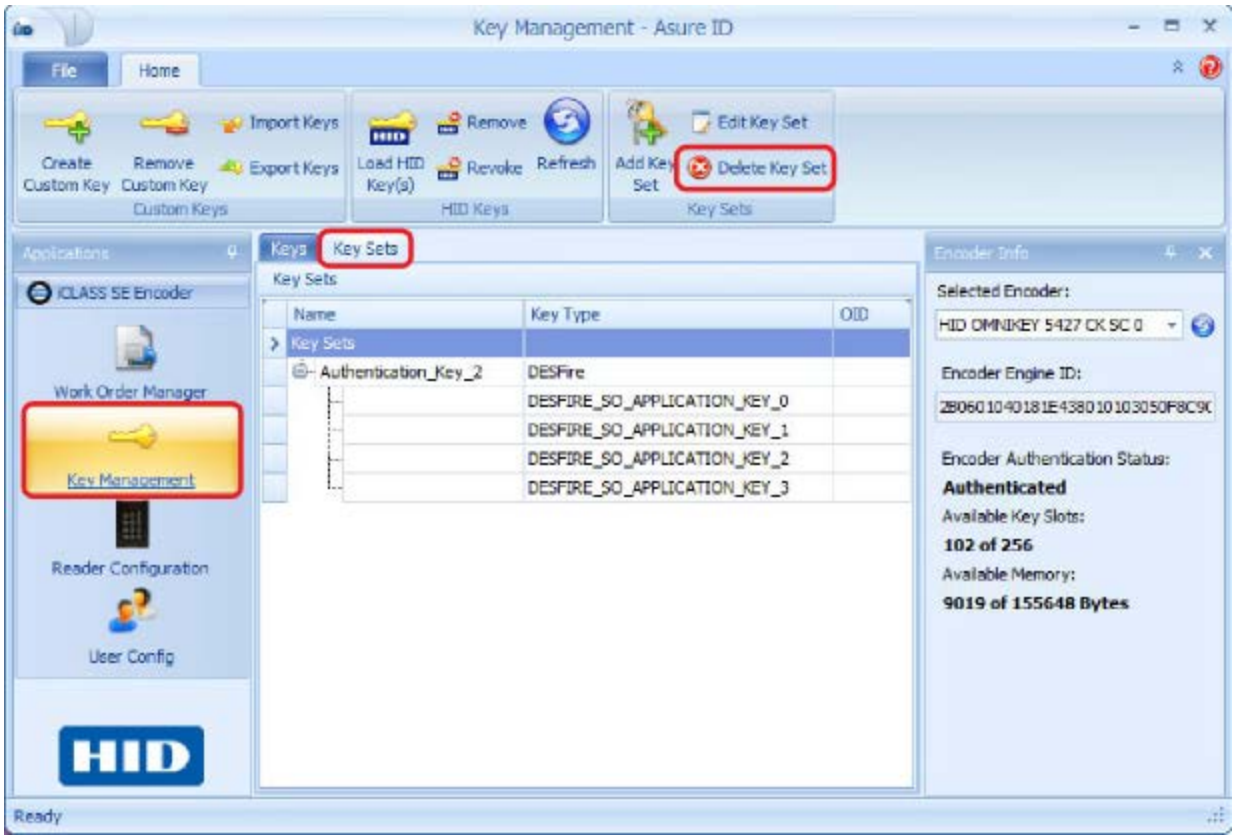


5. The **Key Sets pane** displays the changes.

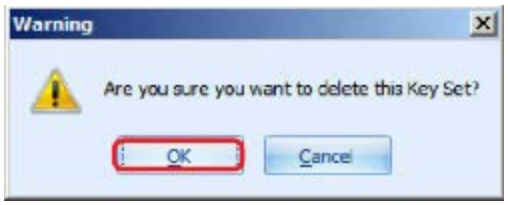


7.14 Delete key set

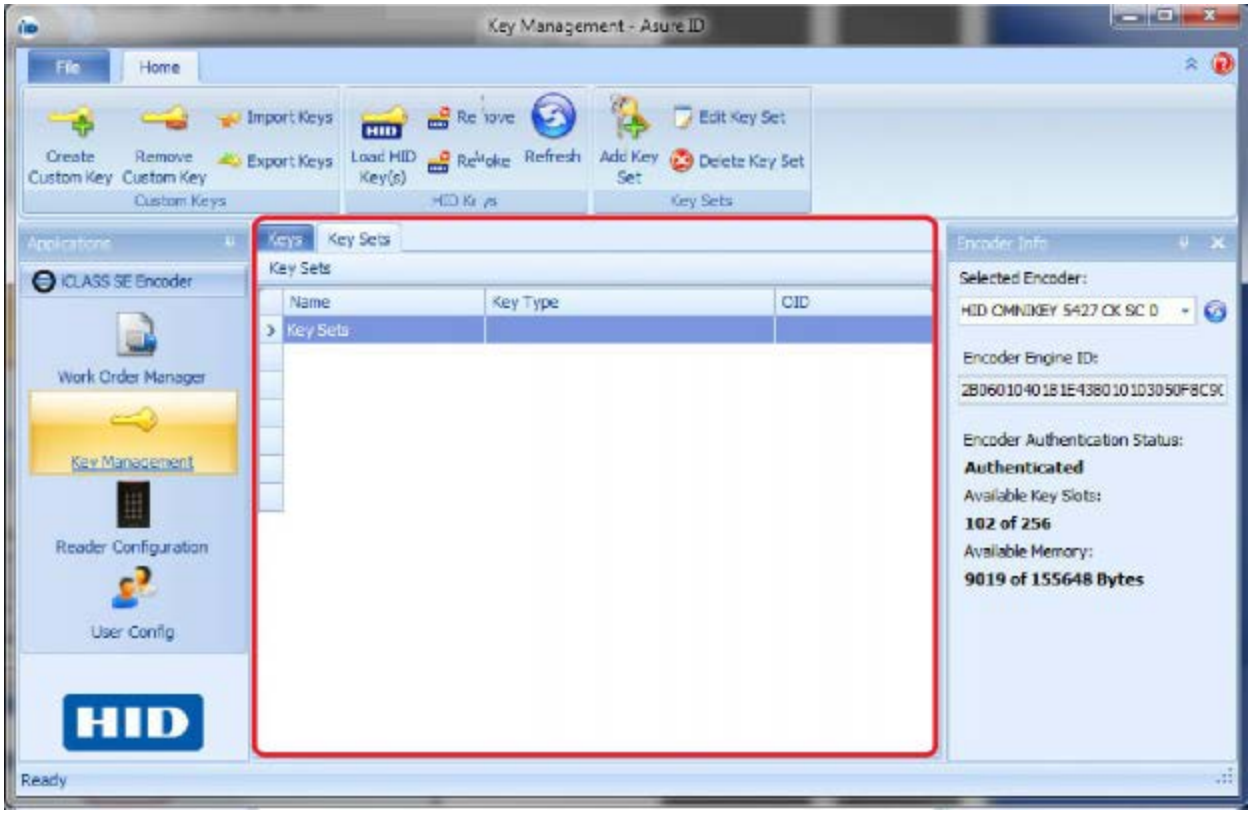
1. Select **Key Management** > **Key Sets** tab.
2. Select a Key Set to delete.
3. Click **Delete Key Set**.



4. Click **OK** to verify the deletion.



5. The Key Set is no longer displayed in on the **Key Sets** tab.



7.15 Sync encoder

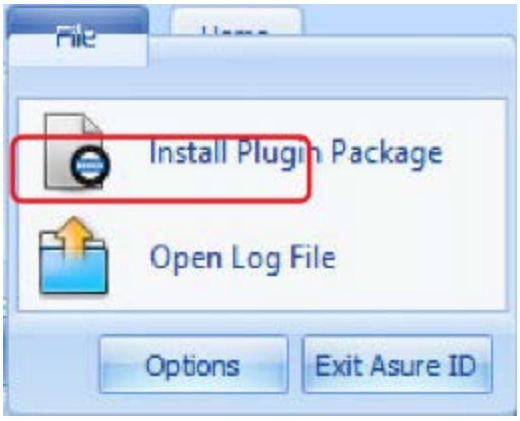
The following information describes how to synchronize the Database to the iCLASS SE CP1000 Desktop Encoder.

The need to synchronize the database to the encoder is required if you have connected a new/different iCLASS SE encoder. The encoder configuration is stored on the encoder and only copied on the database. This type of change would create a circumstance where the encoder and the database on the PC are not in-sync.

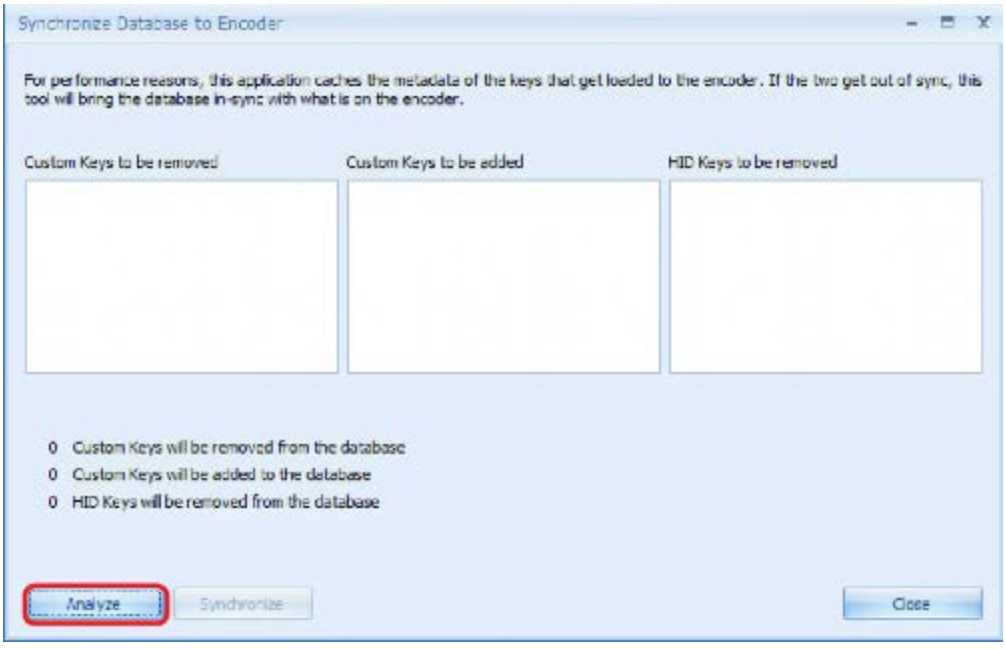
The fact that the encoder and database are out-of-sync may not be apparent, as there is no indicator that they are out-of-sync. Additionally the keys (custom and HID) from the first encoder continues to display on the second encoder, as this information is coming from the database.

Note: The application allows the creation of a Work Order in this circumstance using the keys from the first encoder. However, when you execute the Work Order you receive an error (authentication or no key available). The following process synchronizes the database with the current encoder attached to the PC.

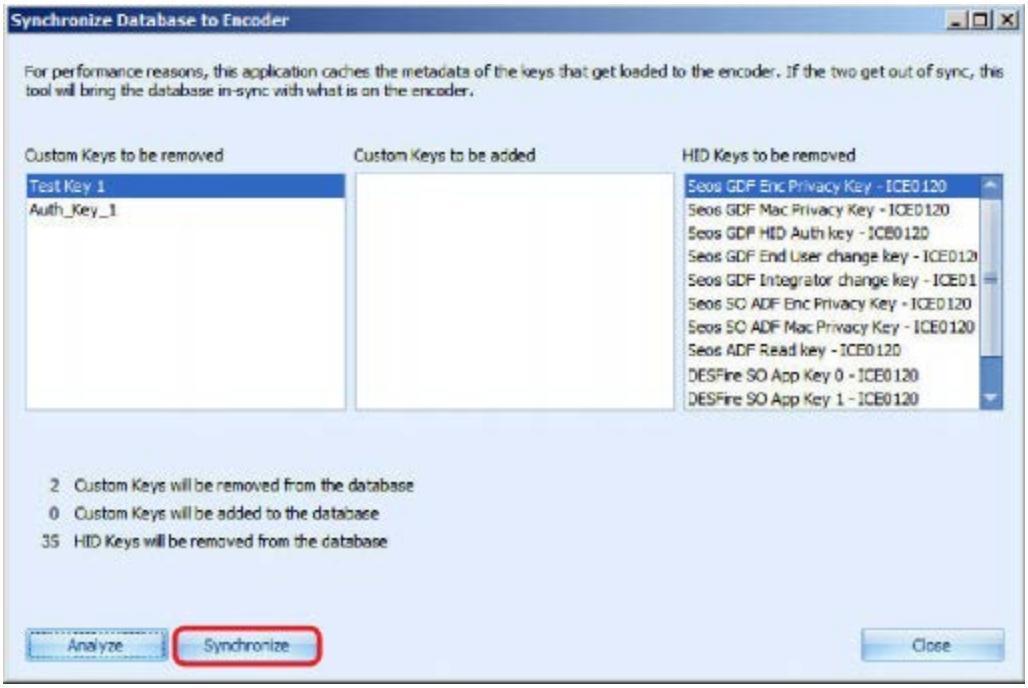
1. Select **Key Management** > **File** tab.
2. Select the **Sync Encoder** option.



3. Click **Analyze**. The current state of the Database and Encoder is analyzed.



4. The analysis displays what has been determined that is out-of-sync. Click **Synchronize**.

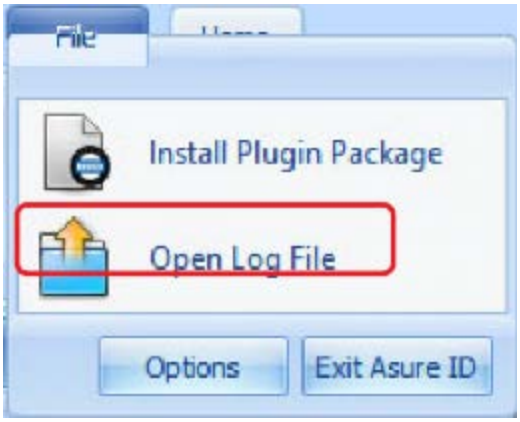


5. The custom keys in the database are now synchronized and the window returns to its original state (before the analysis).
   The HID keys need to be re-installed to complete the synchronization. For more information see **7.8 Load HID keys**.

7.16 Change encoder Admin keys

For security purposes you should change the Administrative Keys on this device.

1. Select **Key Management** > **File** tab.
2. Select the **Change Encoder Admin Keys** option.



3. Enter the Admin Keys on the **Provide New Admin Keys for Encoder** window. This can be done by entering (copy/paste) keys that have been saved earlier.
4. Optionally you can generate random keys, click **Generate Random Keys**.

5. Click **OK**.

Important: It is important that you record these keys for future reference, in a secure location. These keys are required if the PC hosting the application fails. These keys are entered when this application is loaded on a new PC to reconnect to the iCLASS SE Encoder, otherwise credential credits and other important information is lost.

Section 08

Reader configuration

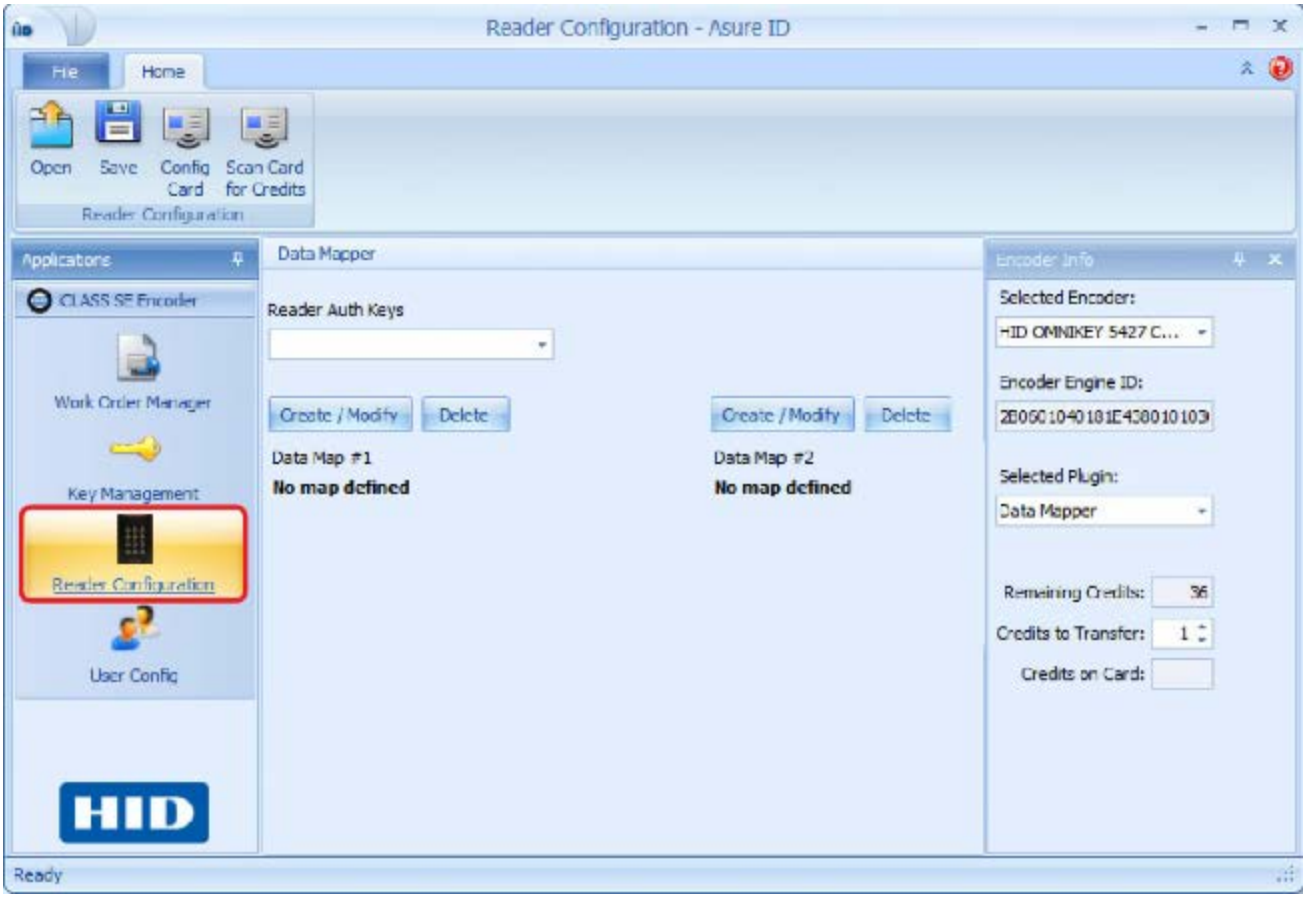
8.1 Introduction

The Reader Configuration module is used to create the Reader Data configuration cards (for both keys and reader limited settings). The application allows you to change the keys or behavior of a Reader.

8.2 Reader Configuration Home tab

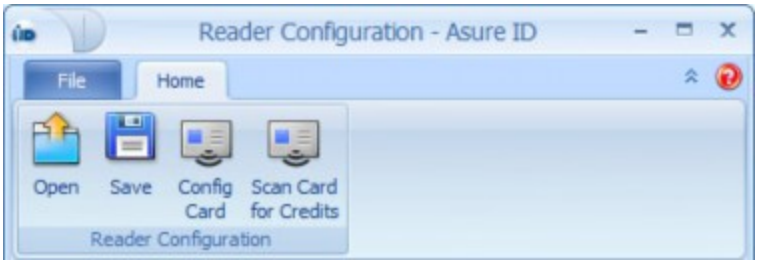
The Reader Configuration main window contains the following areas.

Note: The center pane, changes dramatically with the selection of the **Selected Plugin** (Data Mapper, Elite Prep Card, or Load HID Application Keys) field.



8.2.1 Reader Configuration toolbar

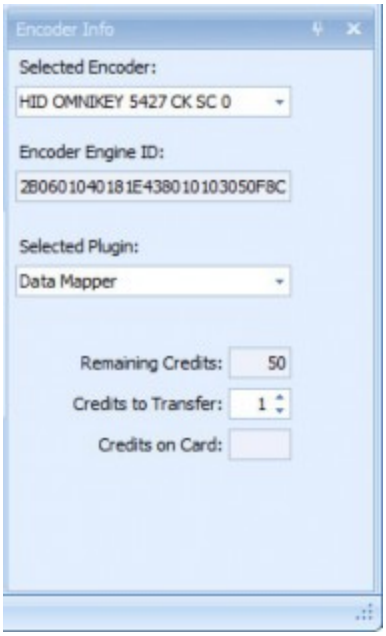
The Reader Configuration toolbar of the CP1000 Desktop Encoder allows you to create the Reader Data configuration cards (for both keys and reader limited settings). The application allows you to change the keys or behavior of a Reader.



Field	Description
Open	Open a Reader configuration.
Save	Save a Reader configuration.
Config Card	Encode a Configuration card with the information displayed in the window below, with the number of credits designated to transfer.
Scan Card for Credits	Scans the card for the number of available (unused) credits on the configuration card.

8.2.2 Encoder Info panel

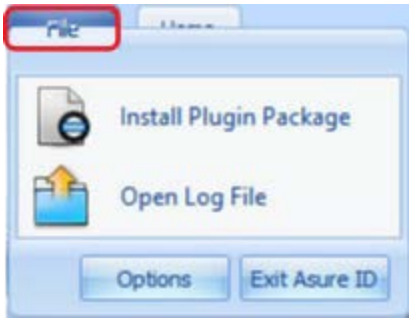
The Key Management **Encoder Info** panel displays information about the CP1000 Desktop Encoder currently connected to the computer.



Field	Description
Selected Encoder	Displays/selects the current Encoder to configure.
Encoder Engine ID	Displays the Engine ID of the current Encoder selected above.
Selected Plugin	Data Mapper: See 8.4 Data Mapper for detailed information. Elite Prep Card: See 8.6 Elite Prep card for detailed information. Load HID Application Keys: See 8.9 Load HID application keys for detailed information. iCLASS Legacy Config Card: See 8.7 Reader options config card for detailed information. Reader Options Config Card: See 8.8 iCLASS legacy config card.
Remaining Credits	Displays the number of available credits. **Note:** These credits are loaded on to the iCLASS SE Encoder with the other credits delivered with the encoder, or ordered from HID.
Credits to Transfer	Designates the number of credits to be loaded onto the configuration card. **Note:** This is the number of times that the card can be used in the field to program a door reader.
Credits on Card	The number of credits that are available (unused) on the card. This number is displayed after the Config Card process is completed or after a Scan Card for Credits process.

8.3 Reader Configuration File tab

The **Reader Configuration File** tab contains specific options for this module.

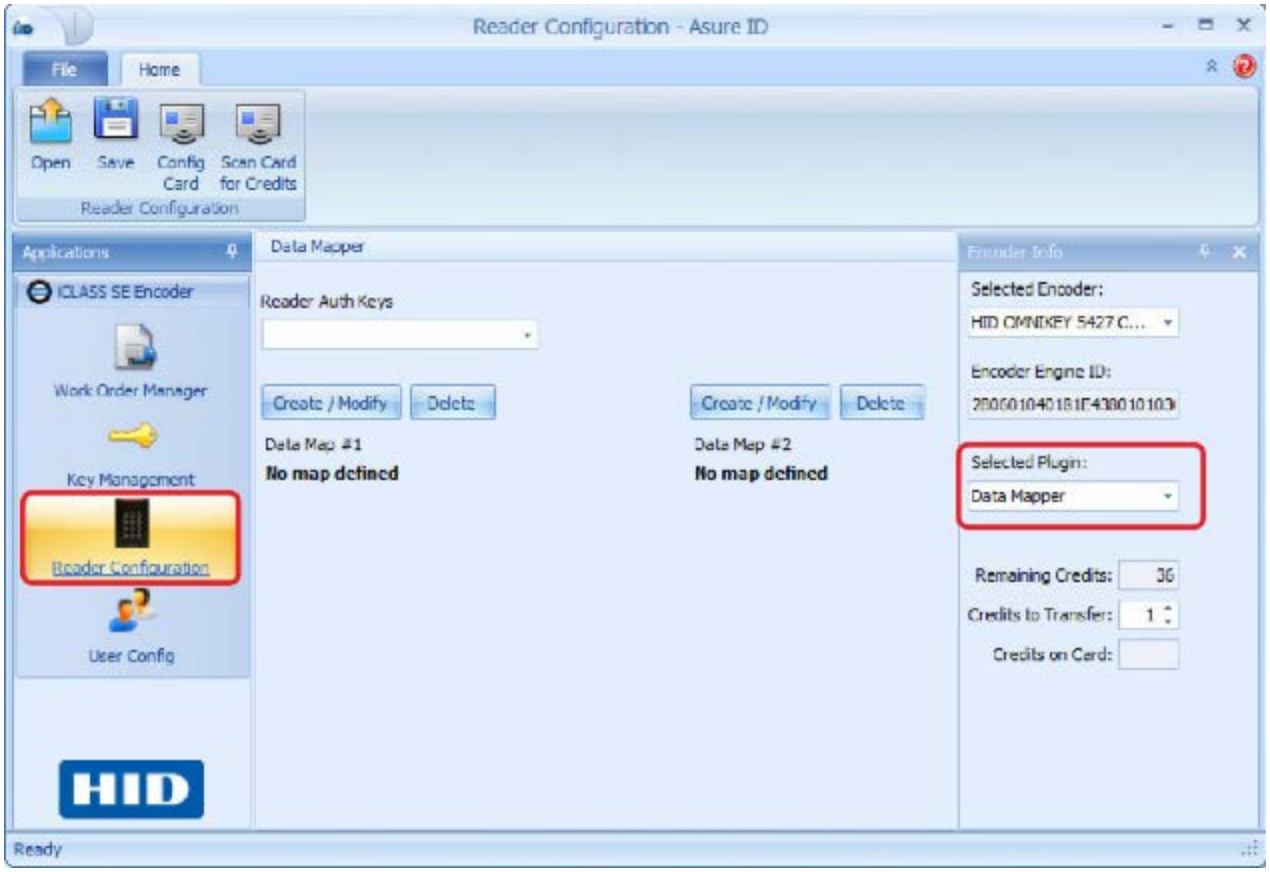


Option Function	Description
Install Plugin Package	The **Install Plugin Package** is a bundle of files that installs all the necessary plugins for the encoder.
Open Log File	The **Open Log File** allows you to view the log file of events for the Asure ID CP1000 Edition application.

8.4 Data Mapper

This process loads the Data Mapper information to the Reader Data Config Card. This is generally used with a 9XXXWXXEKX0324 or 9XXXMXXEKX0324 reader to configure the reader for custom MIFARE Classic or MIFARE DESFire EV1 credential cards.

1. Select **Reader Configuration** module.
2. Select **Data Mapper** from the *Selected Plugin* field.

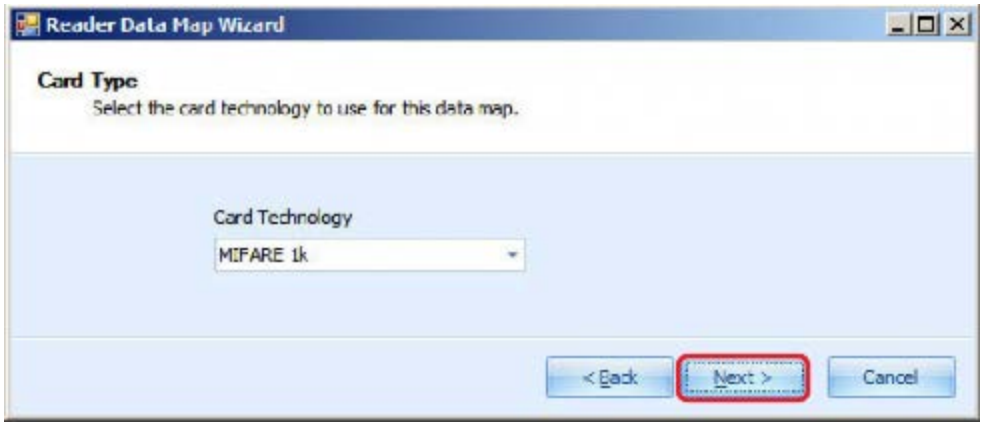


3. Select the Reader Auth Keys. This is the key used by the reader to authenticate the configuration card and read/apply the configuration to the reader. Most readers utilize the Standard option unless you have modified the Reader Auth Keys.
4. Two Data Mapper configurations can be created (Data Map #1 and Data Map #2 shown above). Click **Create / Modify** for each as needed. This opens the Data Mapper Wizard.

8.5 Data Mapper wizard

1. Click **Next** to continue.

2. Select the Card Technology from the drop-down menu.
3. Click **Next**.

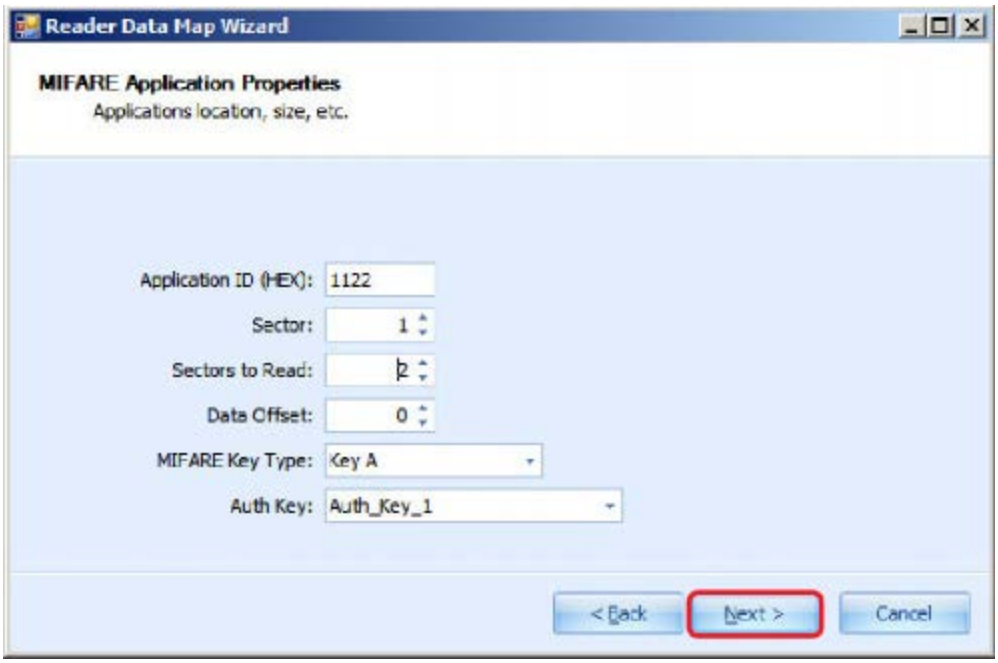


4. Enter the Application Properties.

MIFARE 1k / MIFARE 4k application properties window

The following window appears when the MIFARE (1k or 4k) Card Technology has been selected.

Field	Description
Application ID (HEX)	Enter an Application ID (3-byte Hex value).
Sector	The Sector number box sets the sector number where the application is loaded. Range is: 1k: 0 - 15 4k: 0 - 39
Sectors to Read	Instructs the encoder on the number of consecutive sectors to be read. Range is: 1k: 0 - 15 4k: 0 - 39
Data Offset	Instructs the encoder on the number of bytes to ignore before applying subsequent data manipulation operations.
MIFARE Key Type	Select from the drop-down menu. Options are: Key A or Key B.
Auth Key	Sets the actual custom key to be loaded to the encoder for authenticating the read operation. **Note:** The keys in this list are created in the Create key process. Only keys created with the Key Size for that technology appears. For example a key created with a 6 Byte size would appear for MIFARE.

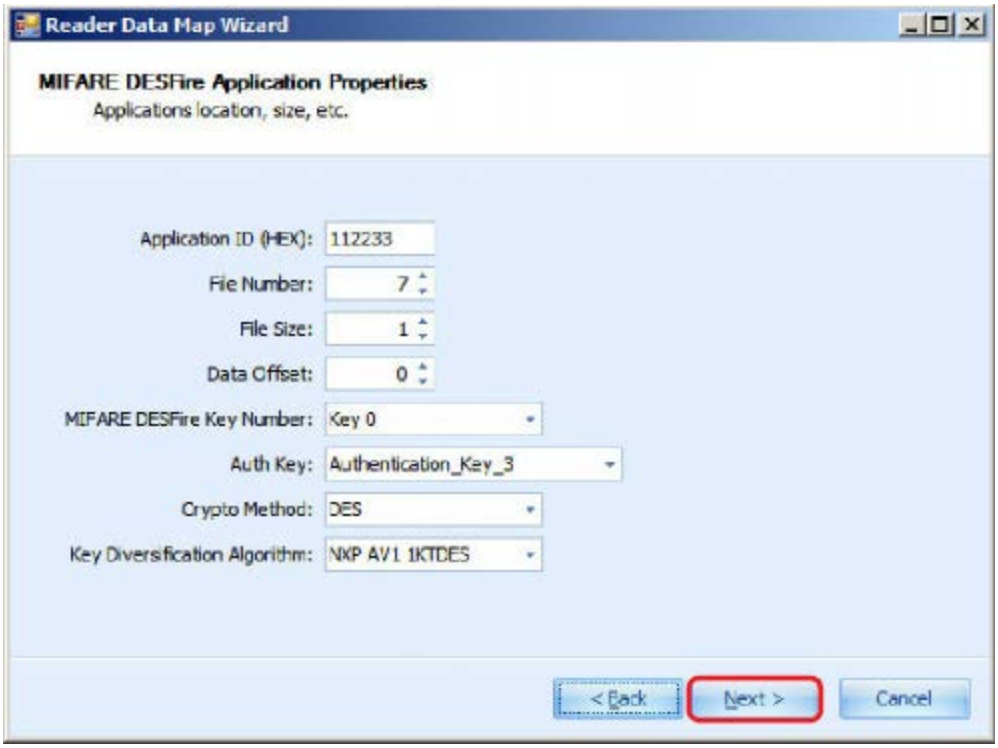


MIFARE DESFire 0.6 / MIFARE DESFire EV1 application properties window

The following window appears when the MIFARE DESFire (.06 or EV1) Card Technology has been selected.

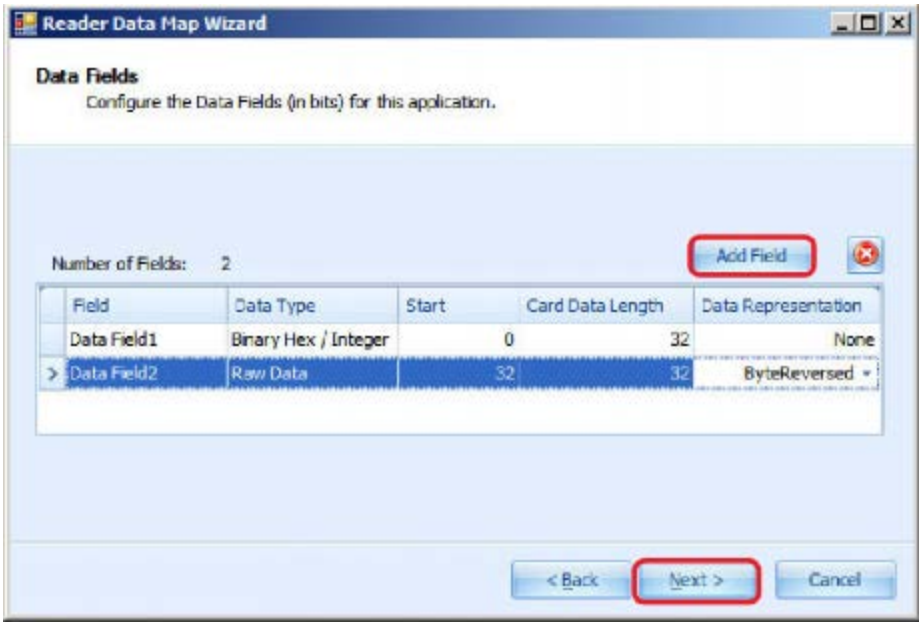
Field	Description
Application ID (HEX)	Enter an Application ID (3-byte Hex value).
File Number	Range is 0 - 31
File Size	Range is 0 - 240 bytes
Data Offset	Range is 0 - 256 bits

Field	Description
MIFARE DESFire Key Number	Select from the drop-down menu. Options are Key 0 through Key 13 or select Free File Access if authentication is not required.
Auth Key	Select key from the drop-down field. The keys in this list are created in the Create key process. Only keys created with the Key Size for that technology appears. For example a key created with a 16 Byte size would appear for MIFARE DESFire.
Crypto Method	Options are: None, DES, or AES (AES is available with MIFARE DESFire EV1 only).
Key Diversification Algorithm	Options are: None, NXP AV1 1KTDES, NXP AV1 2KTDES, or NXP AV1 AES128 (AES 128 is available with MIFARE DESFire EV1 only).
File Transmission Type	Options are Plain or Cipher.



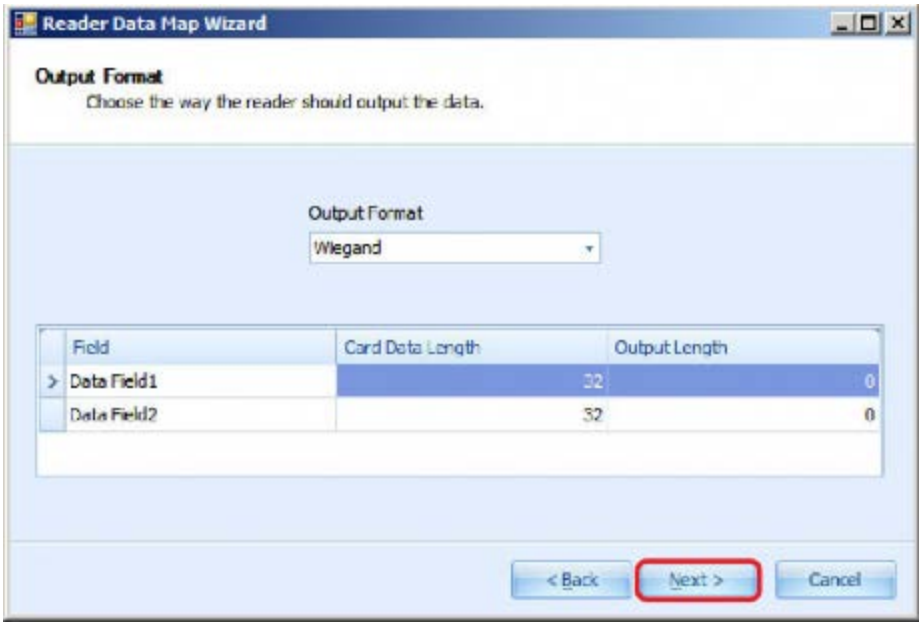
5. When the Application Properties wizard is complete, click **Next**.
   The options on the **Data Fields** window determine the data manipulation operations performed by the encoder prior to reporting the data to the access control system.
   The data read from the card can be split into multiple fields, each with its own conversion operation.
6. Click **Add Field**. A new field row is listed. Each field has the following options:

7. Click **Next**.



Field	Description
Field	Names the Data Field and is auto-incremented when selecting Add Field. It is recommended this name be left at its default setting.
Data Type	Determines how the encoder is to interpret and convert the data in the field. The following options are supported in the encoder: Raw Data - no conversion Binary Hex/Integer - the bytes are interpreted as an integer BCD Nibble - binary-coded decimal, each Nibble (half byte) represents a digit BCD Byte - binary-coded decimal, each full byte represents a digit ASCII Decimal - each byte is an ASCII numeric character ABA Track II as String - mag stripe track 2 format
Start	Specifies the starting bit number in the data field. Combined with the Card Data Length field (specified in bits), it defines the actual data in the data field that is to be manipulated and reported to the access control system. This is not the same as the Data Offset parameter set on the previous page. Default value of 0.
Card Data Length	See description above (Start). Default value of 0.
Data Representation	Allows the reversal of the order of bytes before applying the conversion specified in the Data Type field. Options are: None and ByteReversed.

8. Set the Output Format. Click **Next**.



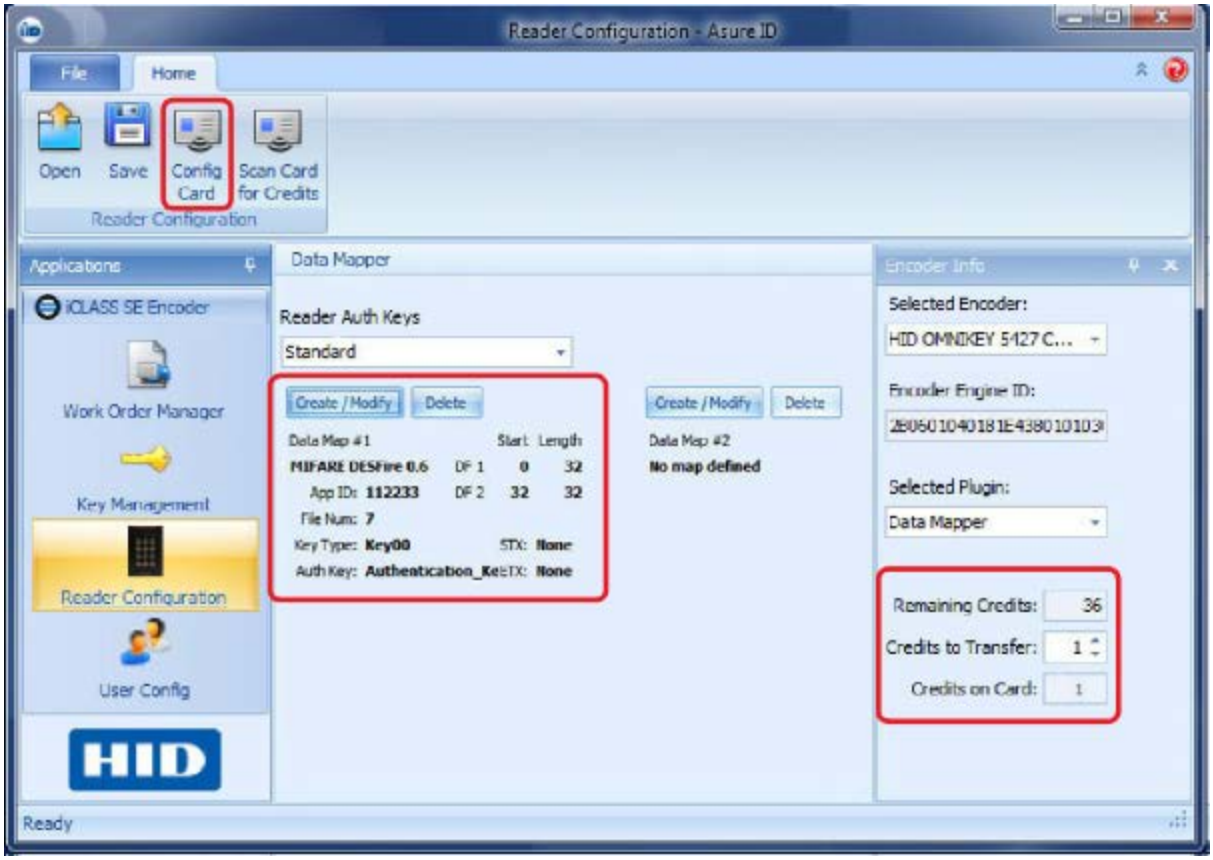
Field	Description
Output Format	Determines the format. The following options are supported on the encoder: • Wiegand If the *Data Type* is set to Binary Hex/Integer on previous page, the least significant bits are sent. The maximum *Output Length* is 32. When the input data is Raw Data, the maximum *Output Length* is 255. • ABA Track II If the *Data Type* is set to Binary Integer on previous page, *Output Length* represents the number of BCD digits to send. Every digit is sent as a 5 bit character (4 data bits and 1 parity bit) as defined in ABA Track II. *Output Length* is max 10 digits. When the input data is raw data then *Output Length* represents the number of bits to send. No conversion is done. The bits are sent as is. *Output Length* is max 255 bits. • ASCII Dec If the *Data Type* is set to Binary Integer on previous page, the least significant digits are sent. *Output Length* represents the number of digits to send. Every digit is send as a character. *Output Length* is max 10 characters. When the input data is raw data the data is sent as is. *Output Length* represents the number of characters to send. The maximum number of characters is 32.
Field	This field is auto-filled from the previous window.
Card Data Length	This field is auto-filled from the previous window.
Output Length	Sets the length of the data transmission.

9. Configure the Start and Stop bits for the Wiegand transmission. Click **Next**.

Field	Description
STX Bit	Adds a bit at the start of the data transmission Options are: None, Fixed Bit-Logic 0, Fixed Bit-Logic 1, Even Parity, Odd Parity
Bit Number	STX computed from bit 0 to Bit Number.
ETX Bit	Adds a bit at the end of the data transmission Options are: None, Fixed Bit-Logic 0, Fixed Bit-Logic 1, Even Parity, Odd Parity
Bit Number	ETX computed from bit number to end of data.

10. Data Map wizard is complete. Click **Finish**.

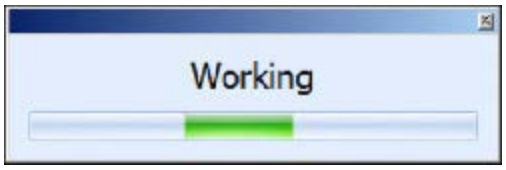
11. The information populates the Data Mapper pane.



12. Select the number of Credits in the **Credits to Transfer** field.

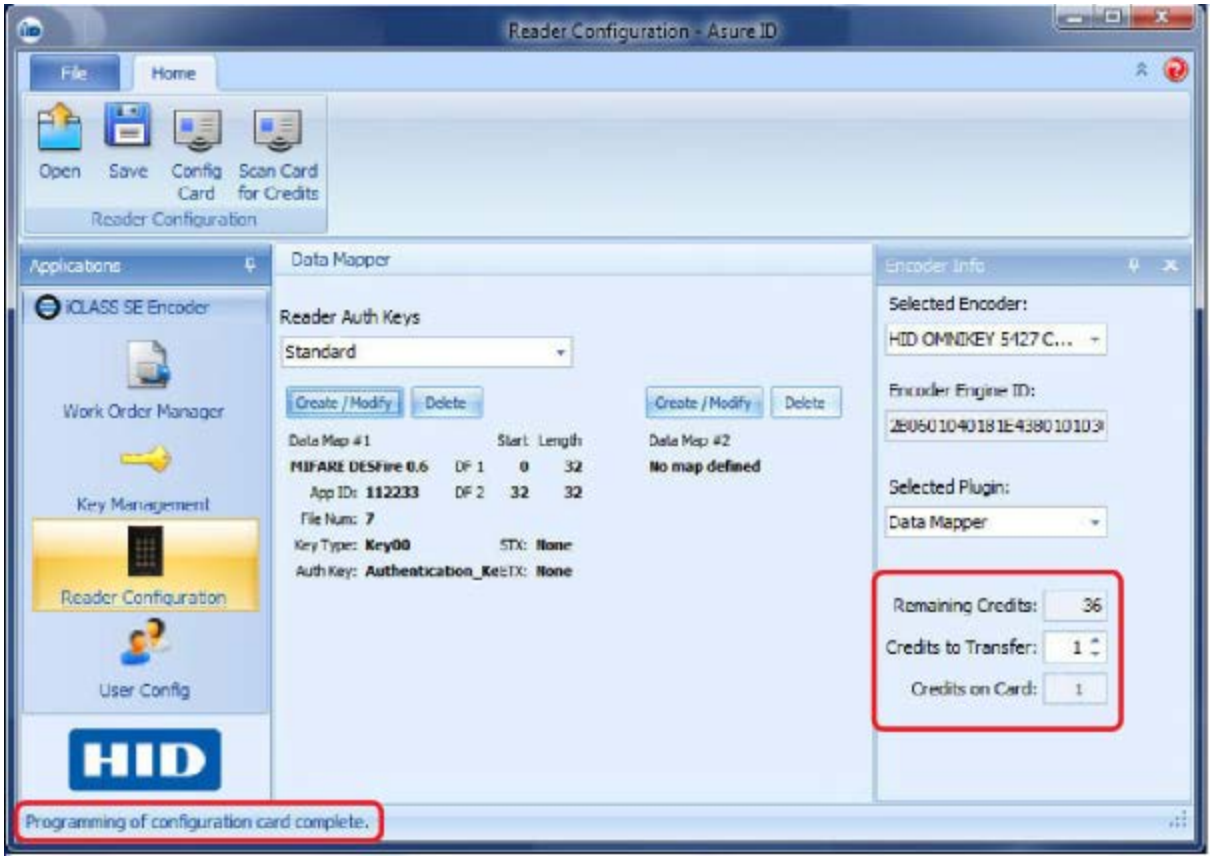
> **Note:** Each Encoder configuration transaction is one credit. This is the number of Encoders that can be configured using this configuration card.

13. Place a **Reader Data** card on the Encoder. See *Credential Programmer How to Order Guide* to order the Reader Data card, part number: 0501600475-READER.
14. Click **Config Card**.
15. A **Working** status is displayed.



16. When complete, a message is displayed at the bottom of the window stating **Programming of configuration card complete**.

    The **Remaining Credits** are decreased by the number of credits that were transferred. **Credits on Card** increases by the number of credits that were transferred to the card.



See **8.10 Programming the reader** to continue.

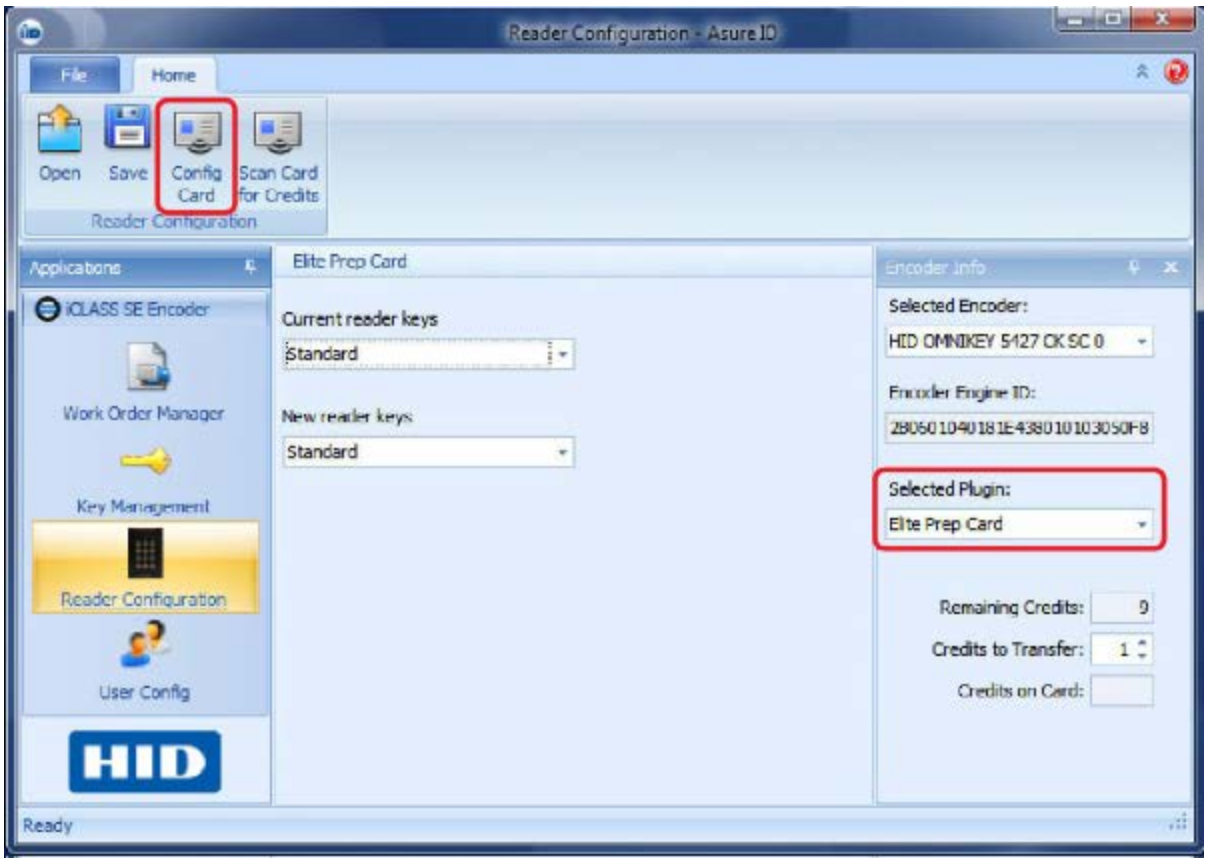
8.6 Elite Prep card

This Configuration Plugin sets the Reader Configuration Key used to authenticate future Configuration cards. This is a means to privatize or localize Encoder configuration authorizations.

1. Select **Reader Configuration** module.
2. Select **Elite Prep Card** from the *Selected Plugin* drop-down menu.
3. Select the Keyset from the **Current reader keys** drop-down, that matches the encoder configuration keys currently deployed in the reader.
4. Select the Keyset to be deployed from the **New reader keys** drop-down.
5. Select the number of Credits in the **Credits to Transfer** field.

   > **Note:** Each Reader configuration transaction is one credit. This is the number of Encoders that can be configured using this configuration card.

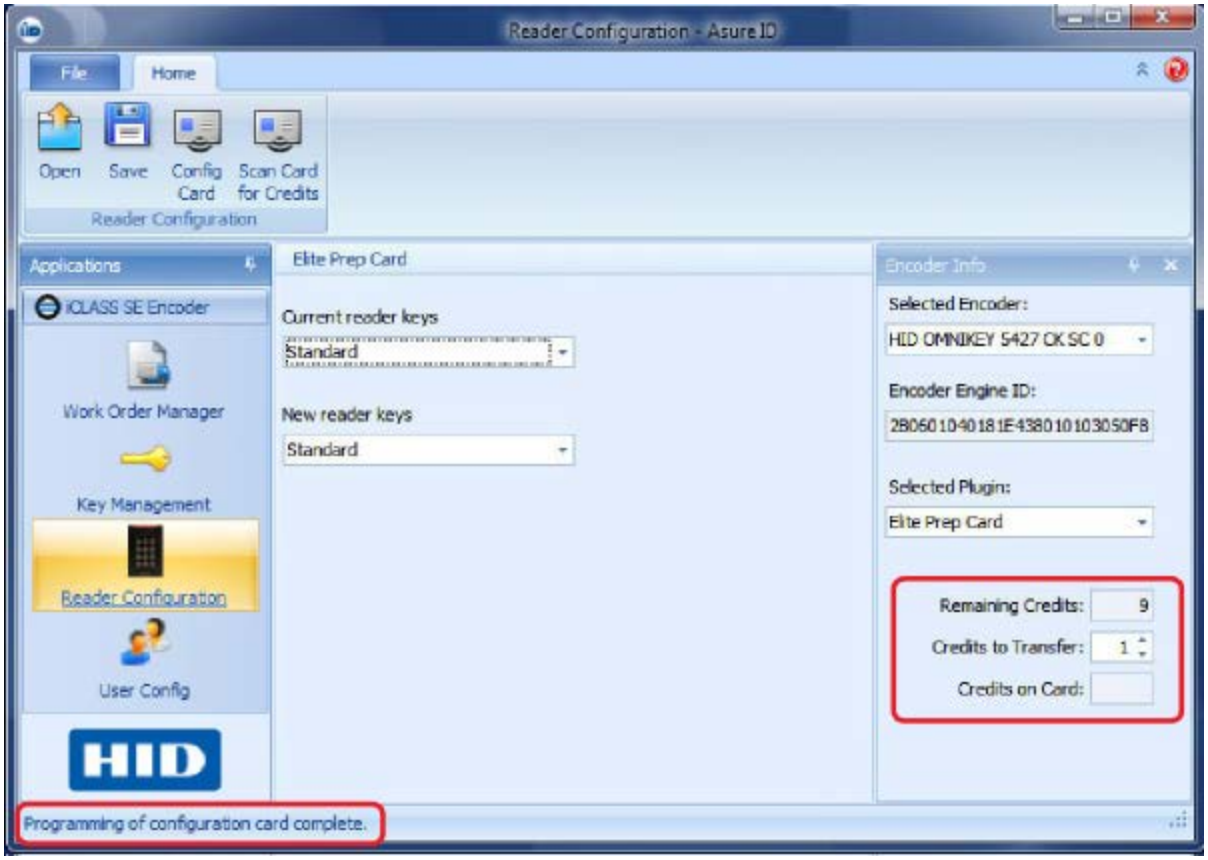
6. Place an **Elite Prep** card on the Encoder. See *Credential Programmer How to Order Guide* to order the Elite Prep card, part number: 0501600475-ELITE.
7. Click **Config Card**.



8. A **Working** status is displayed.

9. When complete, a message is displayed at the bottom of the window stating **Programming of configuration card complete**.

   The **Remaining Credits** decreases by the number of credits that were transferred. **Credits on Card** increases by the number of credits that were transferred to the card.



See **8.10 Programming the reader** to continue.

8.7 Reader options config card

This Configuration Plugin allows you to generate Config Cards for customer specific configuration files.

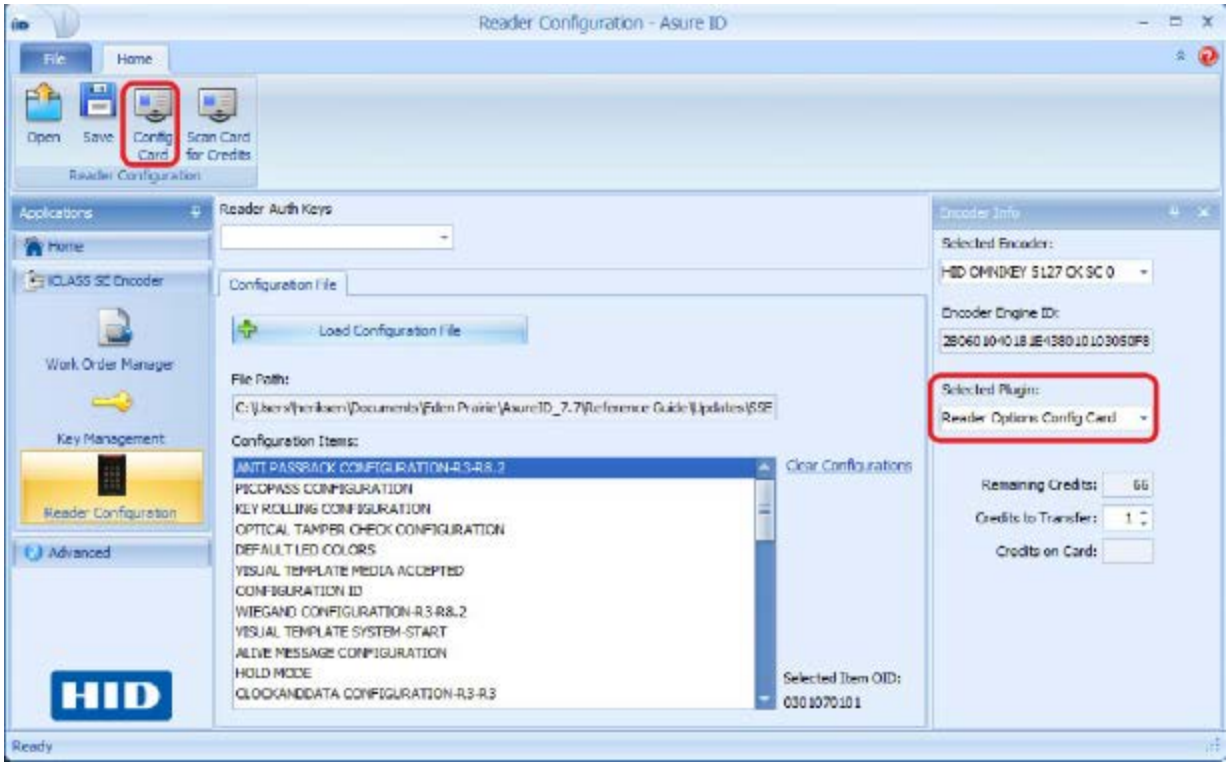
1. Select **Reader Configuration** module.
2. Select **Reader Options Config Card** from the Selected Plugin drop-down menu.
3. Click **Load Configuration File** and browse to find the .ccxml or .eccxml file from HID Global.

   > **Note:** The file information populates the **Configuration Items** field.

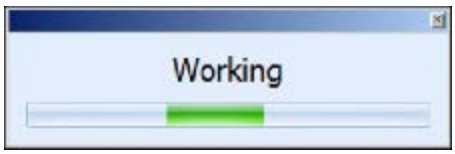
4. Select the number of Credits in the **Credits to Transfer** field.

   > **Note:** Each Reader configuration transaction is one credit. This is the number of Readers that can be configured using this configuration card.

5. Place an **Reader Data Card** on the Encoder. See *Credential Programmer How to Order Guide* to order the Reader Data card, part number: 0501600475-READER.
6. Click **Config Card** from the menu bar.

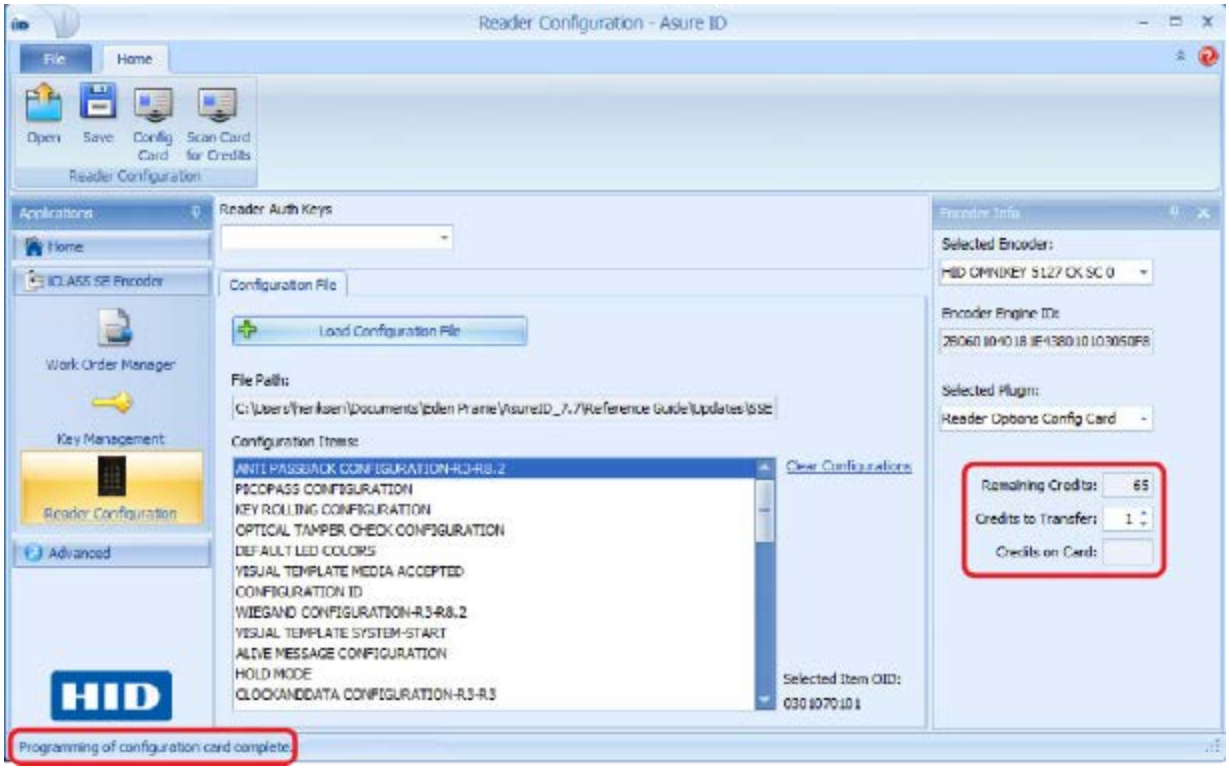


7. A **Working** status is displayed.



8. When completed a message is displayed at the bottom of the window stating **Programming of configuration card complete**.

   The **Remaining Credits** decreases by the number of credits that were transferred. **Credits on Card** increases by the number of credits that were transferred to the card.



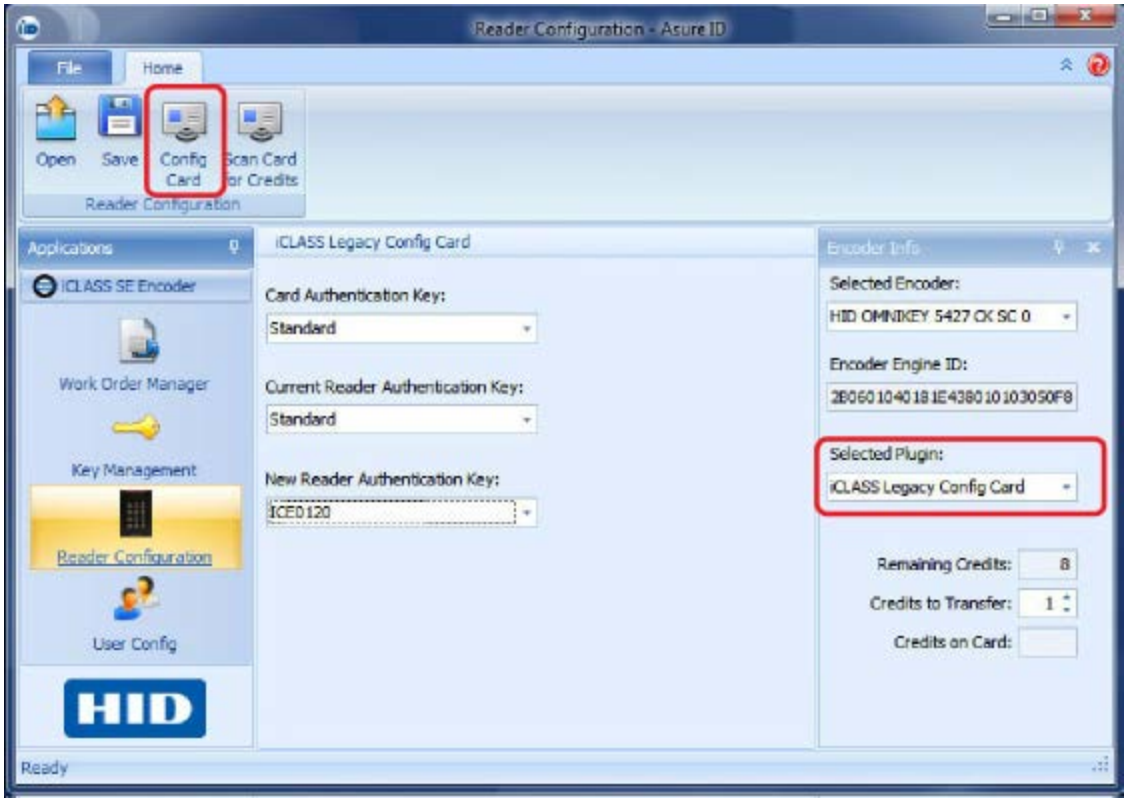
See **8.10 Programming the reader** to continue.

8.8 iCLASS legacy config card

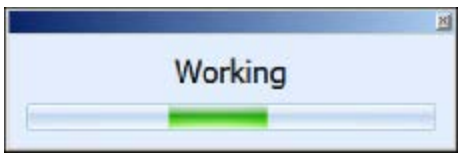
This Configuration Plugin sets the Reader Configuration Key used to authenticate Legacy Configuration cards. This is a means to privatize or localize Encoder configuration authorizations.

1. Select **Reader Configuration** module.
2. Select **iCLASS Legacy Config Card** from the Selected Plugin drop-down menu.
3. Select the Keyset from the **Card Authentication Key** drop-down that matches the encoder configuration keys currently deployed in the reader.
4. Select the Keyset from the **Current Reader Authentication Key** drop-down that matches the encoder configuration keys currently deployed in the reader.
5. Select the Keyset to be deployed from the **New Reader Authentication Keys** drop-down.
6. Select the number of Credits in the **Credits to Transfer** field.

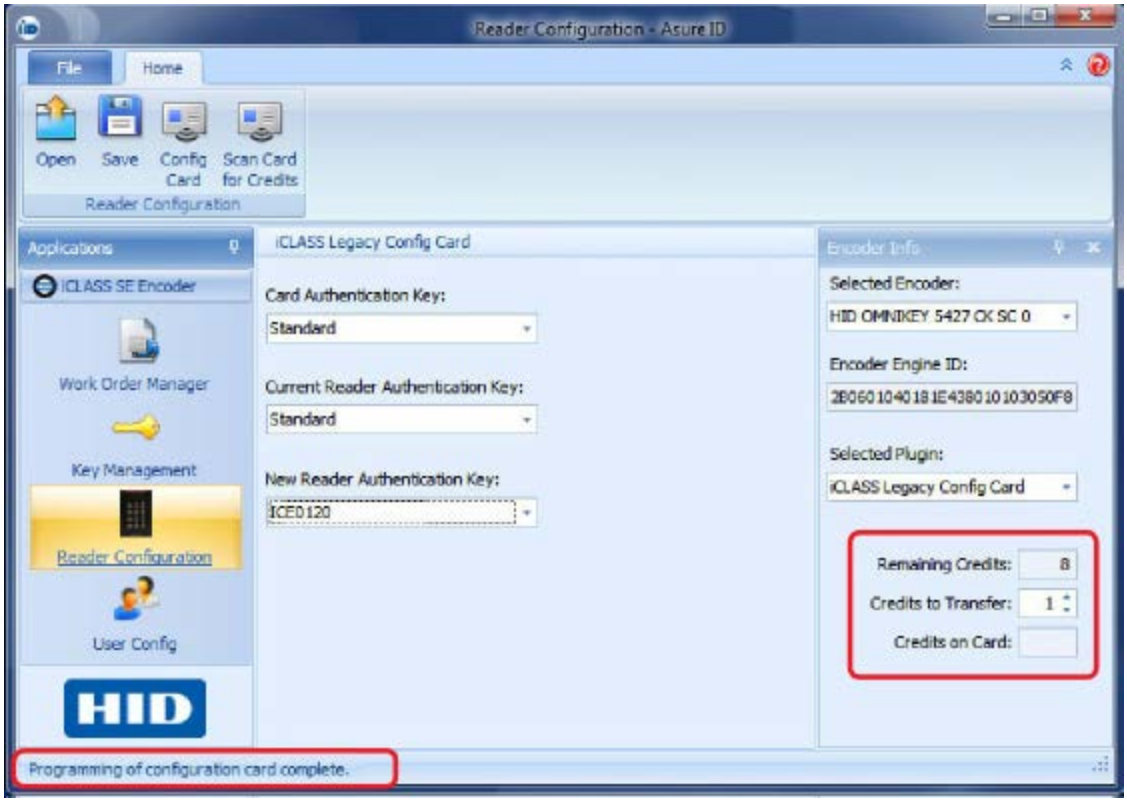
   Note: Each Reader configuration transaction is one credit. This is the number of Encoders that can be configured using this configuration card.
7. Place an **iCLASS Legacy Card** on the Encoder. See *Credential Programmer How to Order Guide* to order the iCLASS Legacy card, part number: 2000PCCNN-LEGACY.
8. Click **Config Card** from the menu bar.



9. A **Working** status is displayed.



10. When complete a message is displayed at the bottom of the window stating **Programming of configuration card complete**. The **Remaining Credits** decreases by the number of credits that were transferred. **Credits on Card** increases by the number of credits that were transferred to the card.

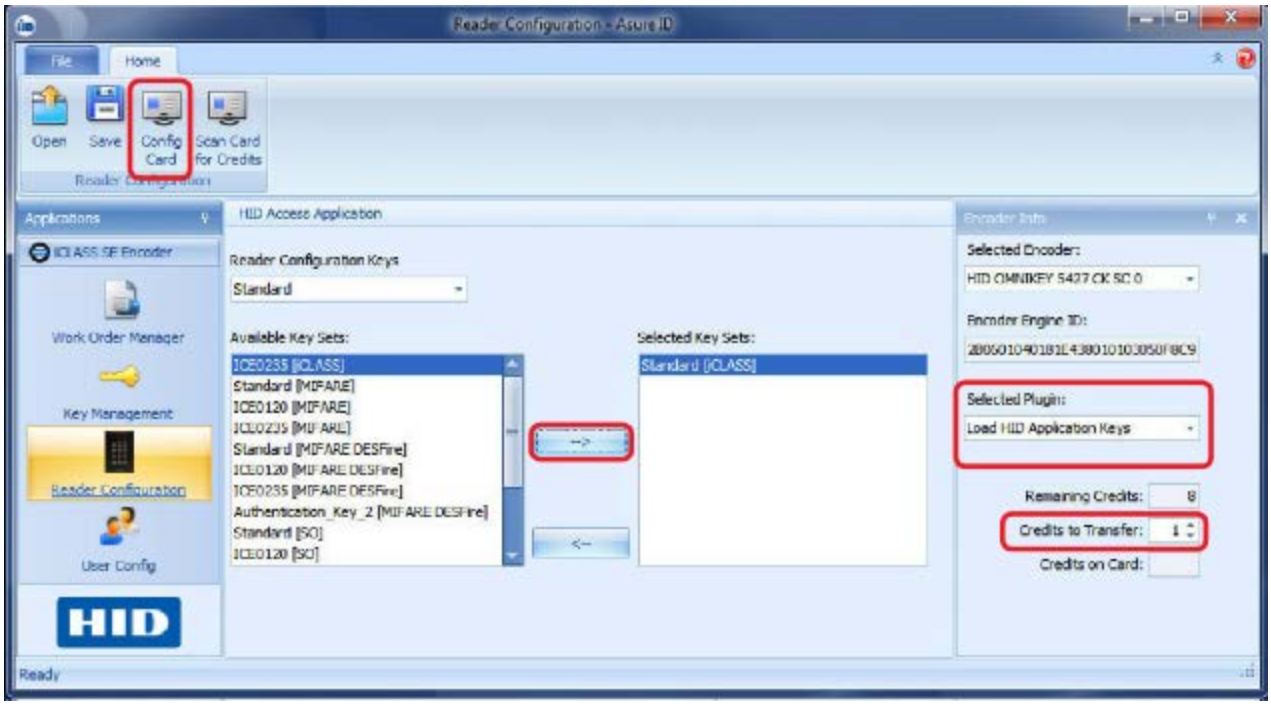


See **8.10 Programming the reader** to continue.

8.9 Load HID application keys

This Configuration Plugin is designed to load media and application keys to one or more Encoders.

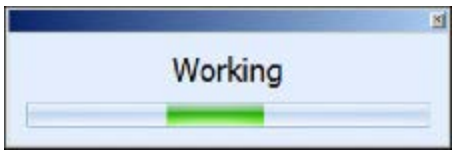
1. Select **Reader Configuration** module.
2. Select **Load HID Application Keys** from the *Selected Plugin* drop-down menu.
3. Select the currently deployed Reader Configuration Keys from the drop-down menu.
4. Select the desired keys from the *Available Key Sets* (left) panel, click the **arrow** which appears in the **Selected Key Sets**(right) panel.



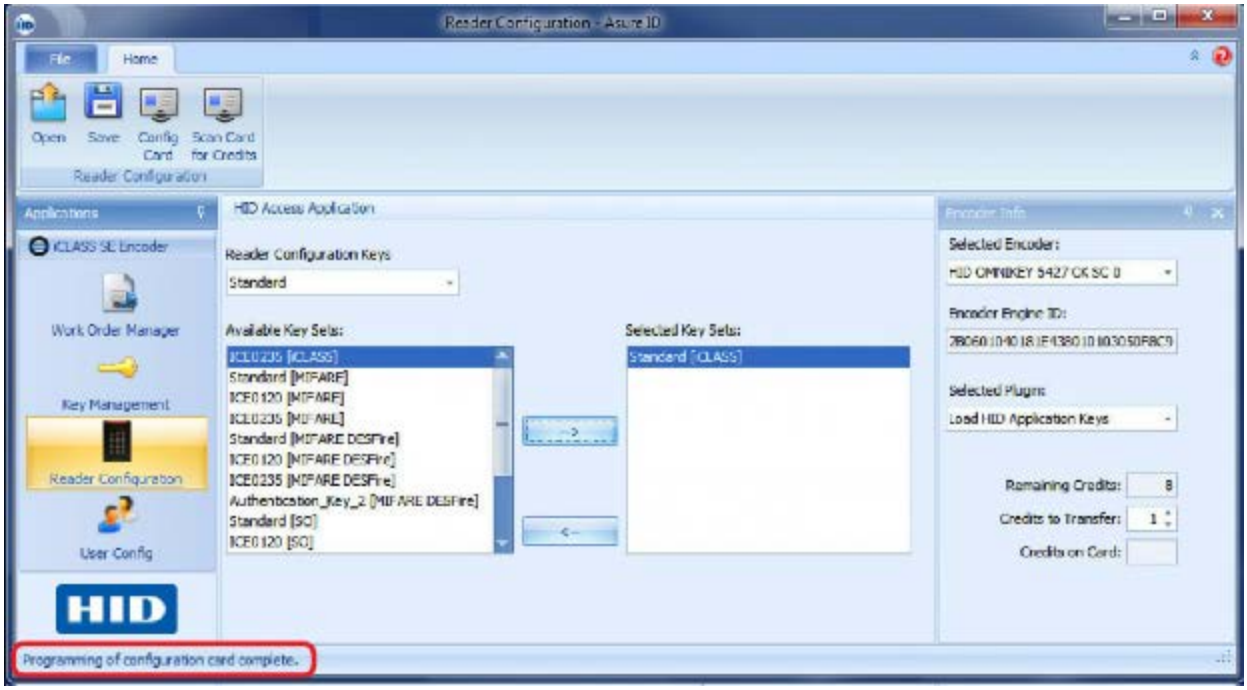
5. Select the number of Credits in the **Credits to Transfer** field.

> **Note:** Each Encoder configuration transaction is one credit. This is the number of Encoders that can be configured using this configuration card.

6. When complete, place a **Reader Data** card on the Encoder. See *Credential Programmer How to Order Guide* to order the Reader Data card, part number: 0501600475-READER.
7. Click **Config Card**.
8. A **Working** status is displayed.



9. When complete, a message is displayed at the bottom of the window stating **Programming of configuration card complete**. The **Remaining Credits** decreases by the number of credits that were transferred. **Credits on Card** increases by the number of credits that were transferred to the card.



See **8.10 Programming the reader** to continue.

8.10 Programming the reader

Once the cards have been configured, use the following steps to configure the reader to one of these cards:

1. Cycle the power on the reader.
2. During the first 5 seconds after the power cycle, the LED shows purple. Present the ELITE PREP Config Card to the reader and hold it.
3. The reader flashes an LED sequence of red, green, and amber along with several beeps.
4. When the LED flashes red/blue intermittently, remove the card.

You should re-label the reader to note that it has been configured.

Section 09

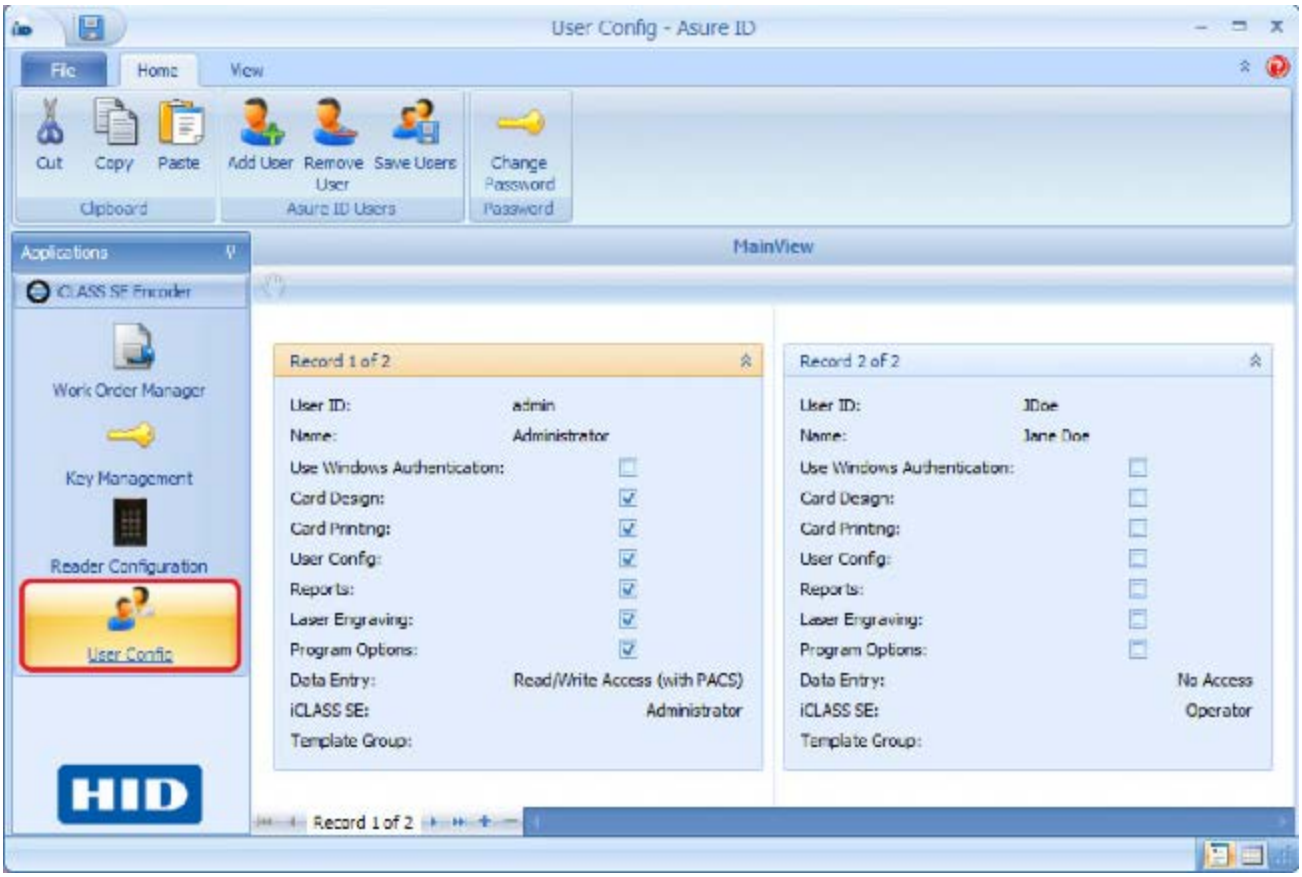
User Config module

9.1 Introduction

The User Config module manages all the User Records, configuration and passwords.

9.2 User Config Home tab

The User Config Home tab contains the following areas.



9.2.1 User Config Home toolbar

The User Config module of the CP1000 Desktop Encoder allows you to manager the records and passwords of the users.

Toolbar Function	Description
Cut	Allows you to copy the user record to the clipboard and delete the record.
Copy	Copies the user record to the clipboard
Paste	Pastes a user record from the clipboard
Add User	Adds a user to the Asure ID application. See 9.5 Add a user.
Remove User	Removes a user from the Asure ID application. See 9.6 Remove a user.
Save Users	Saves all users to the Asure ID application. See 9.7 Edit a user.
Change Password	Allows you to change a password. See 9.8 Change password.

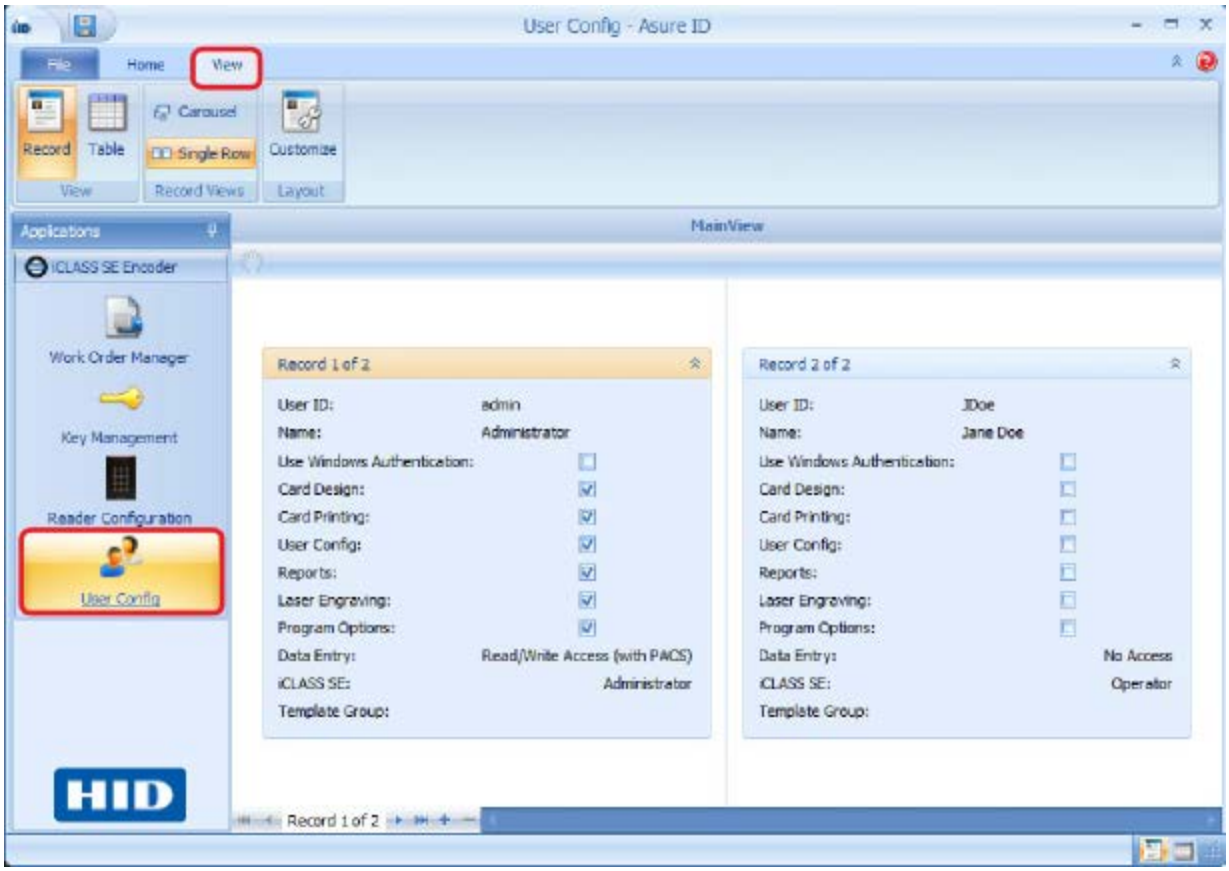
9.3 User Config File tab

The **User Config File** tab allows you to Add, Save, and Remove Users. See information listed above.

9.4 User Config View tab

To manage Users Records, you can select from a variety of options. To modify the View complete the following tasks:

1. Select **User Config** > **View** tab.
2. Select the preferred viewing options.

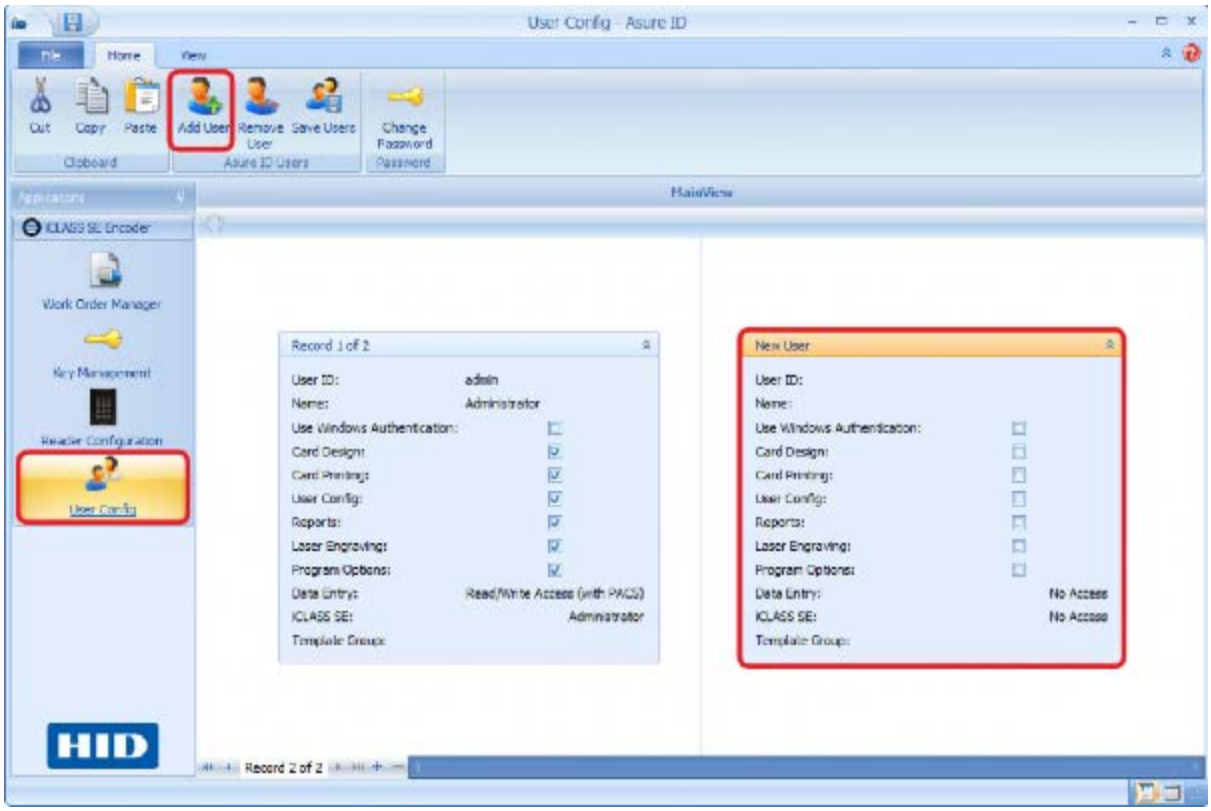


Option	Description
Record	The Record view shows records individually, and the organization of the screen is in a non-overlapping frame window. Combined with options from the Record Views group, this option is the default view and remains combined with your last chosen Record Views choice until you chose another view.
Table	The Table view allows you to see all records in a grid view with columns and rows. Check boxes appear to indicate User preferences.
Carousel	The Carousel record view allows you to display multiple images in a single area of the Main View window. When selected, the record appears to be on a rotating carousel. Navigate through the User Records by using the scroll bar at the bottom of the window.
Single Row	The Single Row record view allows you to select records by using the scroll bar at the bottom of the window.
Customize	Layout Customize allows you to customize the view of the User Records list. It offers options to create a customized view by using drag-and-drop and customization menus. Preview the custom view from the View Layout tab.

9.5 Add a user

The application is provided with an Admin level user configured. If a general operator level user, with limited access is needed, use the following instructions.

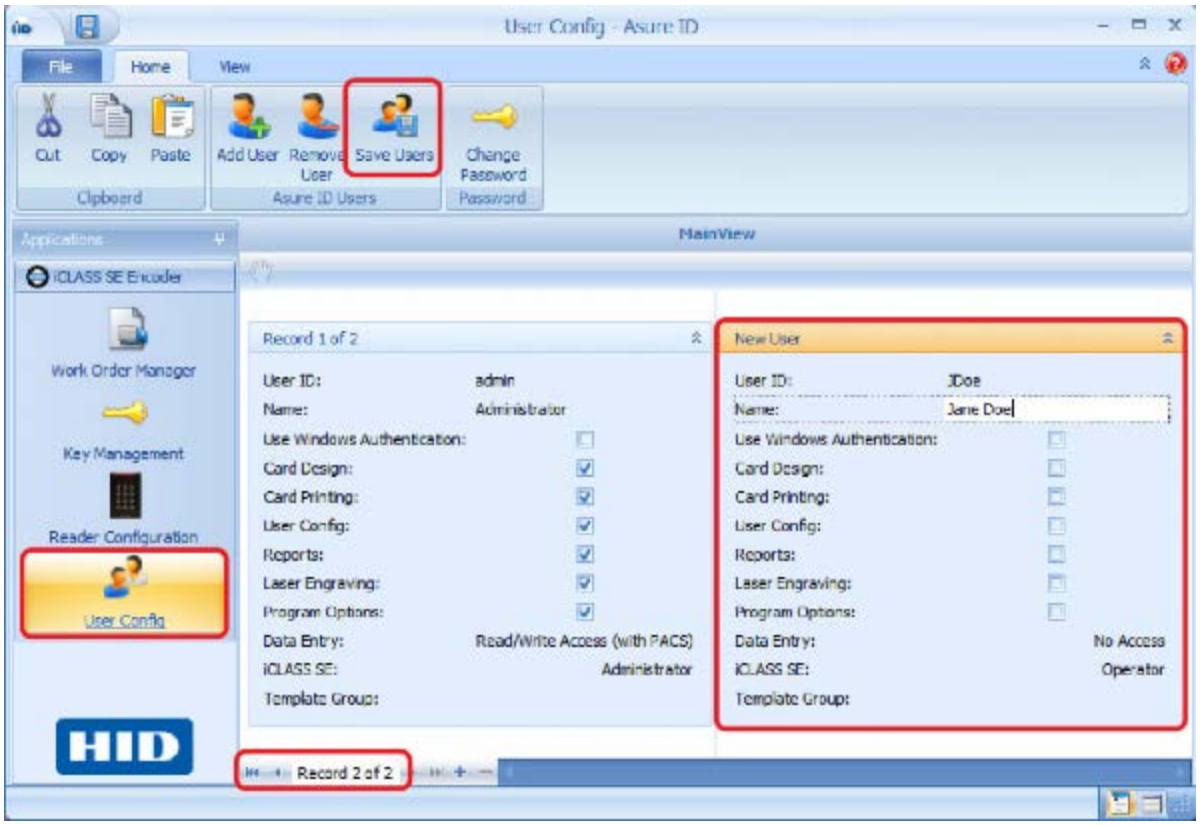
1. Select **User Config** > **Add User**.
2. A blank **New User** record is displayed.
3. Enter the specific configuration for the new user.



Field	Description
User ID	Enter a **User ID** (wand over User ID for the field to appear).
Name	Enter a user **Name** (wand over Name for the field to appear).
Use Windows Authentication	**This option enables Windows Authentication**. If selected the User ID must match the type of encoder Authentication.
Program Options	This option allows this user to have access to program options.
iCLASS SE	The **iCLASS SE** option allow you to select a Security Level (User Role) for each user. **No Access** - Does not allow access to the application. **Administrator** - Sets the user access level at Administrator. There is no restriction to this level. **Operator** - Sets the user access level at Operator. This level restricts configuration, but allows the user to execute Work Orders.

Field	Description
Card Design	These options do not apply to the iCLASS SE Encoder users.
Card Printing	
User Config	
Reports	
Laser Engraving	
Data Entry	
Template Group	

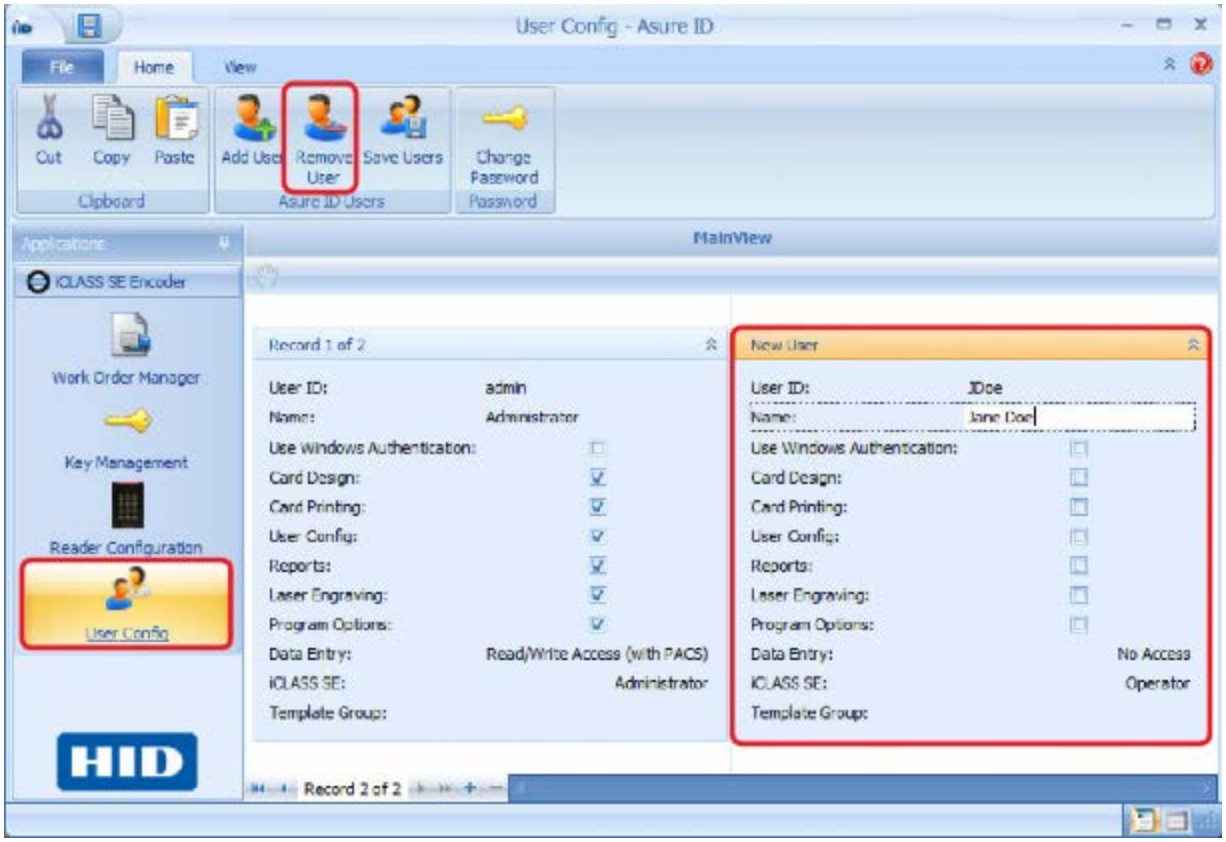
4. Select **Save Users** from the menu bar.
5. The new user is now listed on the **Main View** window. The Record identifier in the bottom of the window updates to reflect the number of records created in the application.



9.6 Remove a user

To remove/delete an existing user, complete the following steps:

1. Select **User Config** module.
2. Select a User Record to remove/delete. Depending on the view, and the number of Users, this may require you to scroll through the list.
3. Select **Remove User** from the menu bar.

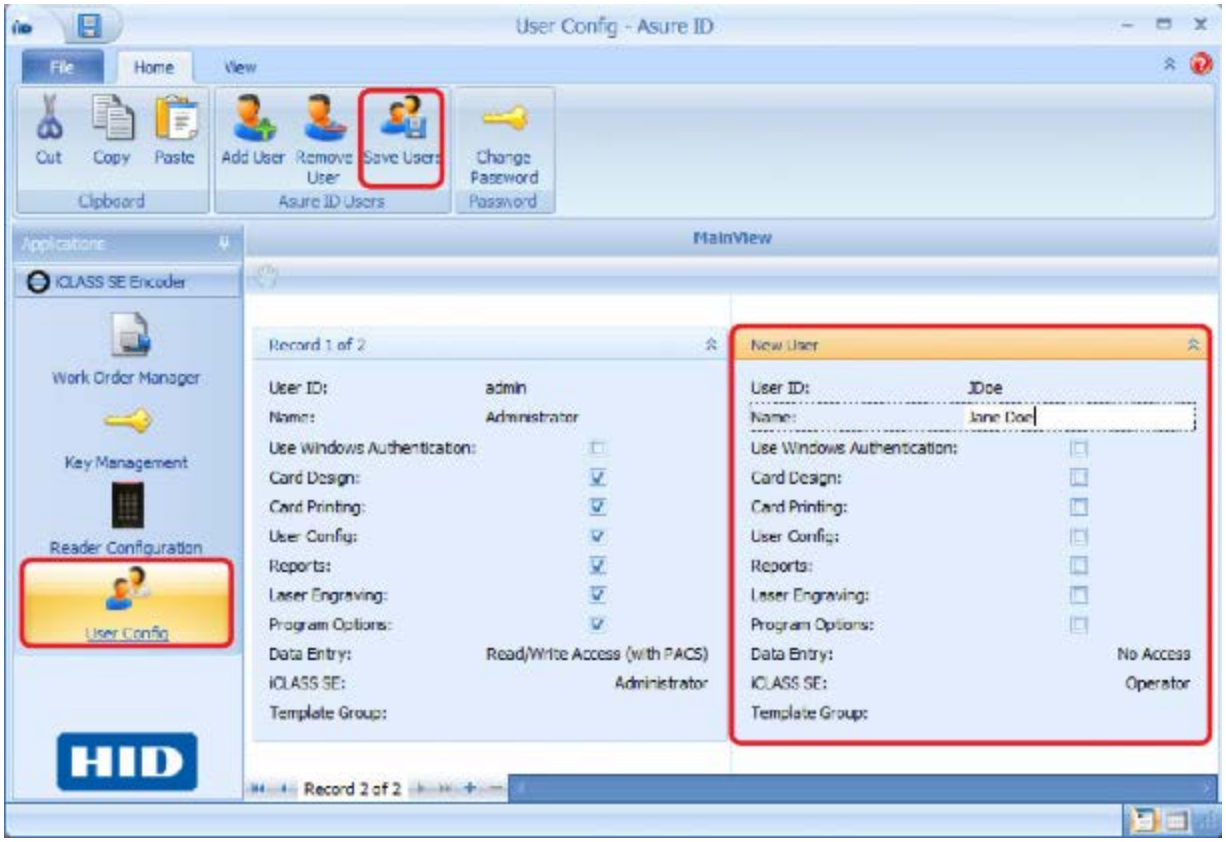


4. Click **Yes** to verify the deletion. The User's Record is removed from the list.

9.7 Edit a user

To edit an existing user, complete the following steps:

1. Select the **User Config** module.
2. Select a User Record to modify. Depending on the view, and the number of Users, this may require you to scroll through the list.

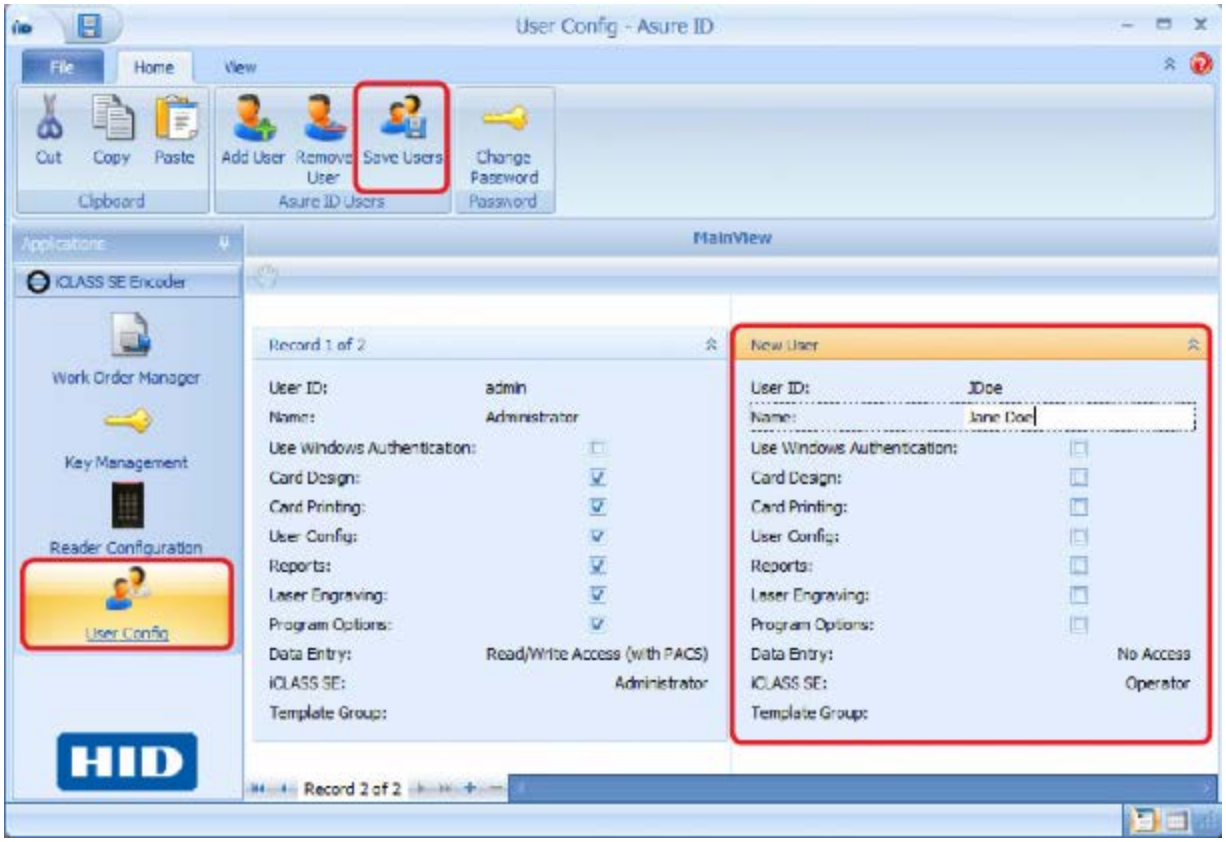


3. Modify the record.
4. Select **Save Users** from the menu bar.

9.8 Change password

To modify a password complete the following steps:

1. Select the **User Config** module.
2. Select a User Record to modify the password. Depending on the view, and the number of Users, this may require you to scroll through the list.
3. Select **Change Password** from the menu bar.



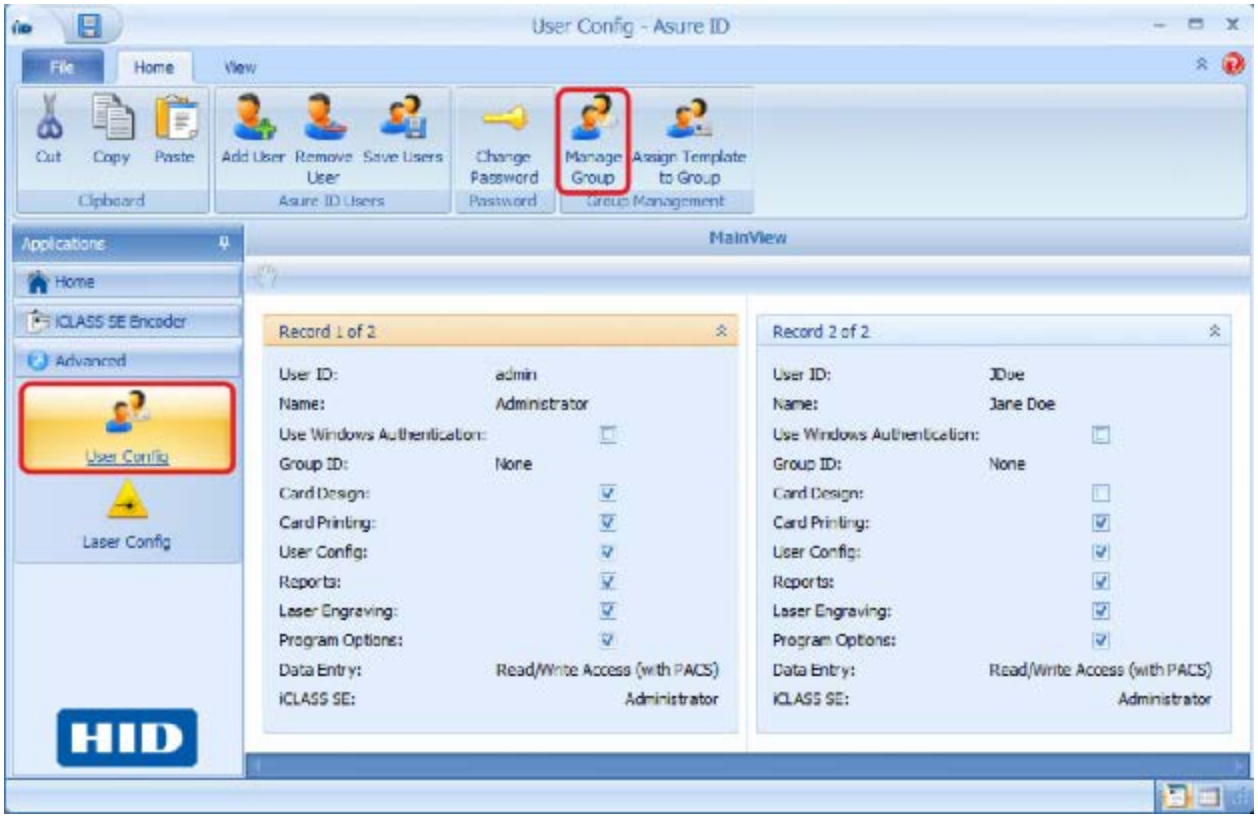
4. Enter the new password twice, and click **OK**.

Important: When creating a new Admin user, or changing an Admin password, it is important that this password is saved in a secure location. At this time there is no password reset feature in place.

9.8.1 Manage groups

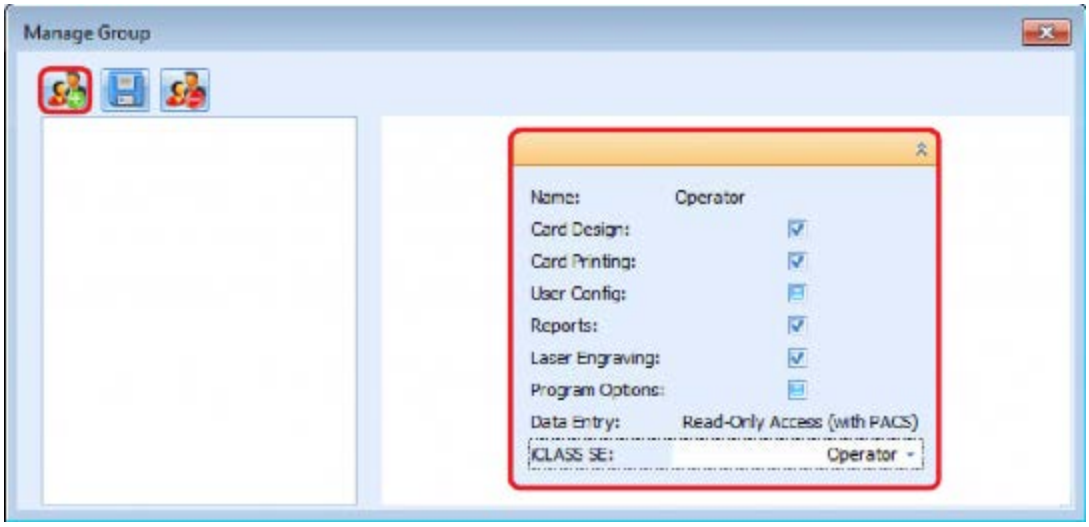
To add, save, or delete a user group, complete the following steps:

1. Select **User Config** module.
2. Select **Manage Group** from the menu bar.



3. A blank **Manage Group** window with the Add, Save, and Delete user group icons are displayed. Select the **Add Group** icon.

4. A blank User Group window is displayed. Enter the specific configuration for the new group.



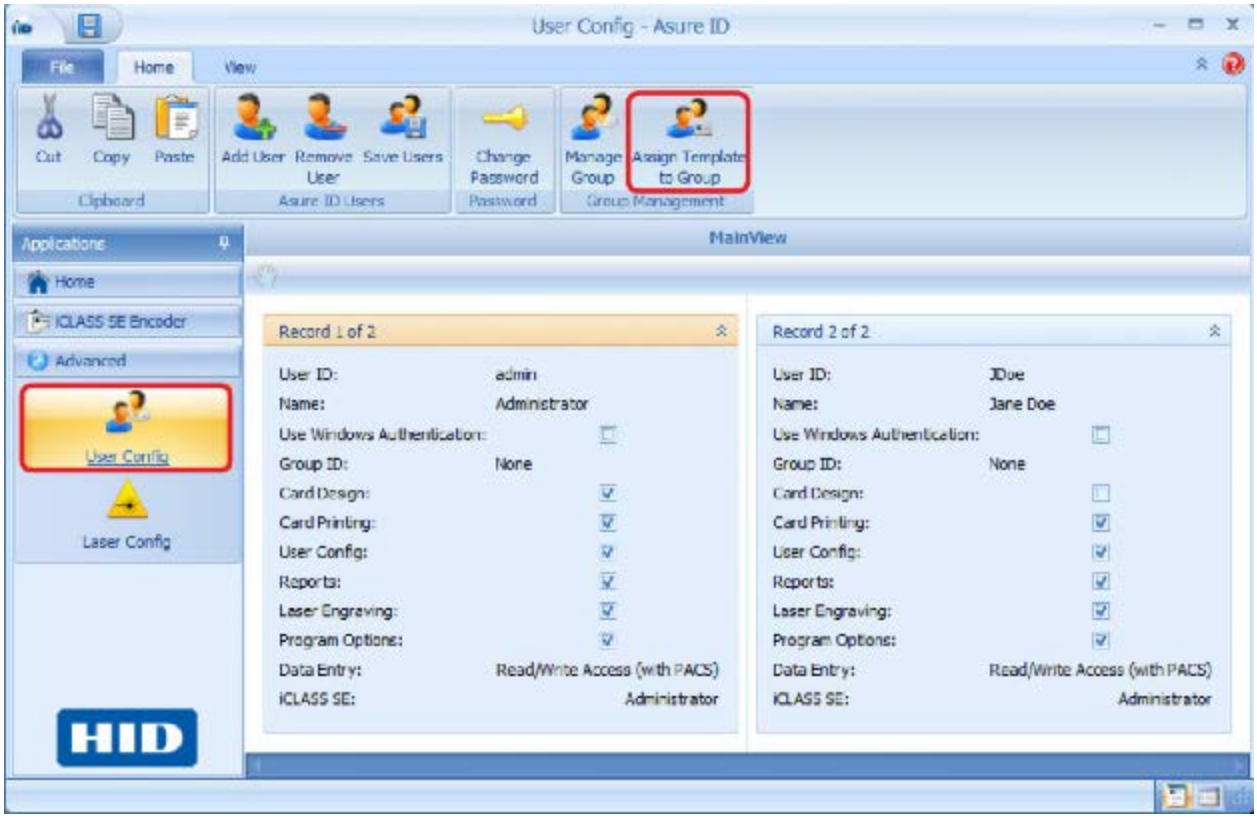
Field	Description
	Add User Group. Opens a blank User Group window.
	Save User Group. Saves any changes made to the Add Group window.
	Delete User Group. Deletes the selected User Group.
Name	Enter a **Name** for this group (wand over Name for the field to appear).
Card Design	These options allow this group to have access to program options.
Card Printing	
User Config	
Reports	
Laser Engraving	
Program Options	
Data Entry	This option sets the Data Entry access level. • No Access • Read/Write Access (with PACS) • Read/Write Access (no PACS) • Read-Only Access (with PACS) • Read-Only Access (no PACS)
iCLASS SE	The **iCLASS SE** option allow you to select a Security Level (User Role) for each group. • **No Access** - Does not allow access to the application. • **Administrator** - Sets the group access level at Administrator. There is no restriction to this level. • **Operator** - Sets the group access level at Operator. This level restricts configuration, but allows the group to execute Work Orders and Encoding.

5. Click the **Save** icon. The group name is added to the list.

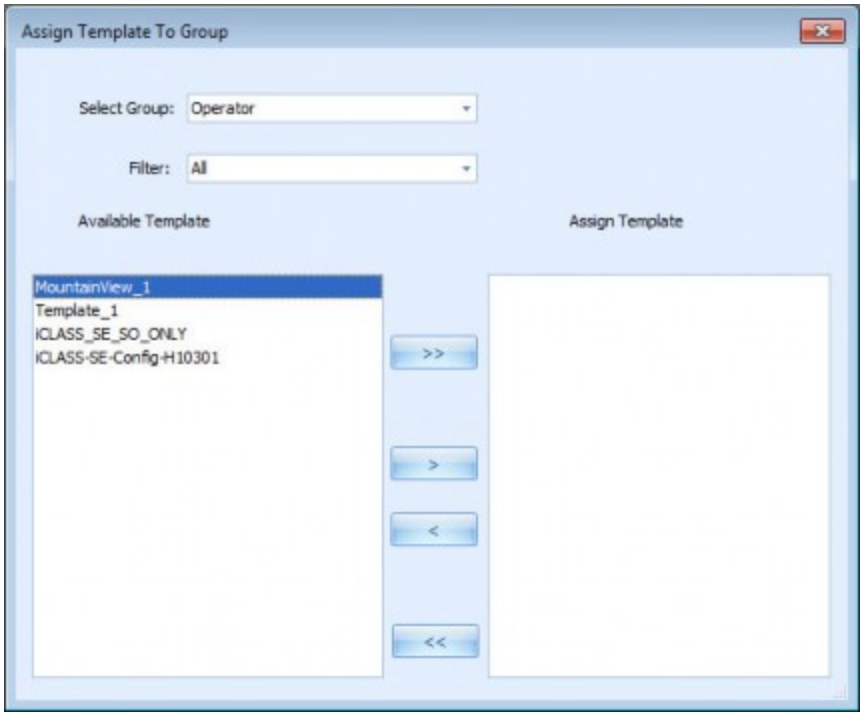
9.8.2 Assign a template to a group

To assign a card template or work order to a group, complete the following steps:

1. Select **User Config** module.
2. Select **Assign Template to Group** from the menu bar.



The **Assign Template To Group** window is displayed.



Field	Description
Select Group	Select the group to assign a template to.
Filter	Select the type of template to assign to this group. • All: Displays all Asure ID and SE Encoder Work Order templates. • Asure ID Card Template: Shows only Asure ID templates. • iClass SE Work Order: Shows only SE Encoder Work Order templates.
Available Template	Select the name of the template to assign to this group and use the arrow keys to move the name of the available template to the Assign Template field. Template names can be moved one at a time or they can all be moved at the same time by clicking the double arrow key.
Assign Template	The template assigned to this user group.

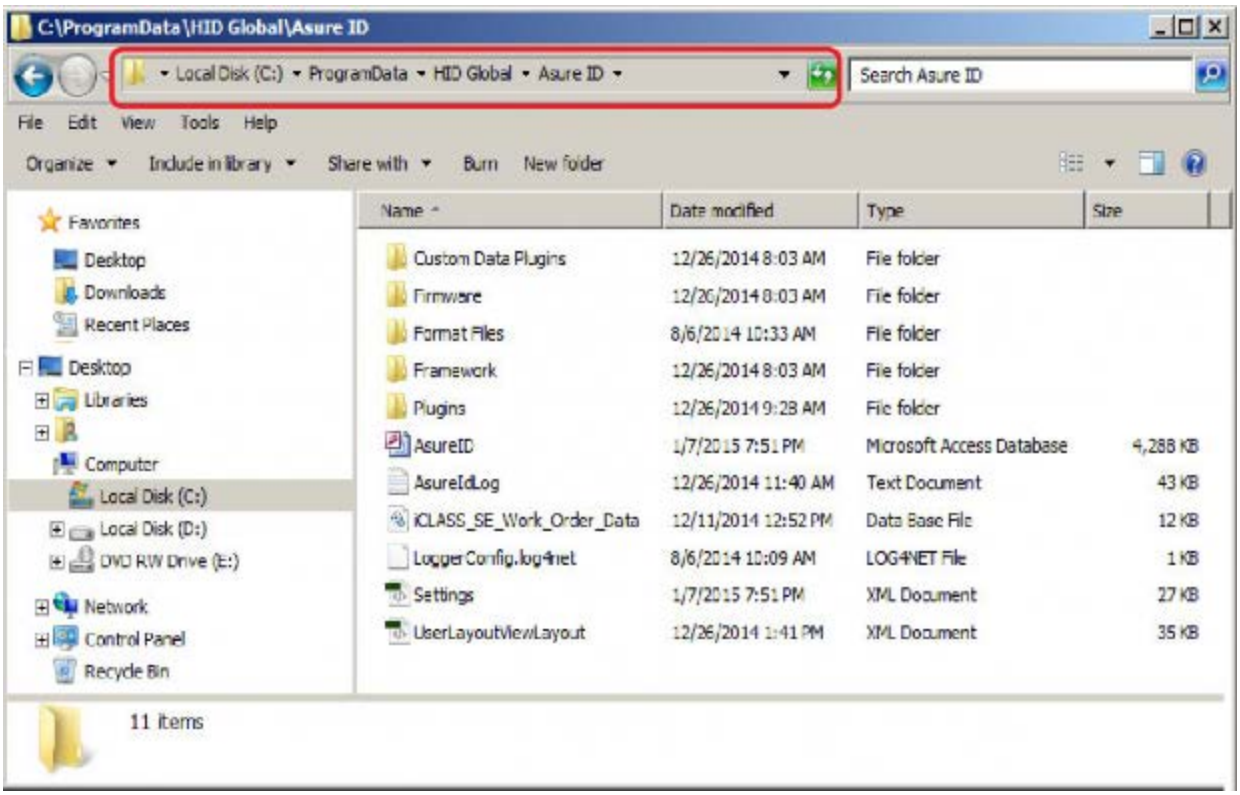
Section 10

User Config module

10.1 Backup and recovery

HID Global recommends that you backup the iCLASS SE Encoder folder at the following location: C:\ProgramData\HID Global\AsureID

This folder contains all the essential files to recover from loss of the PC or other issues with the application.

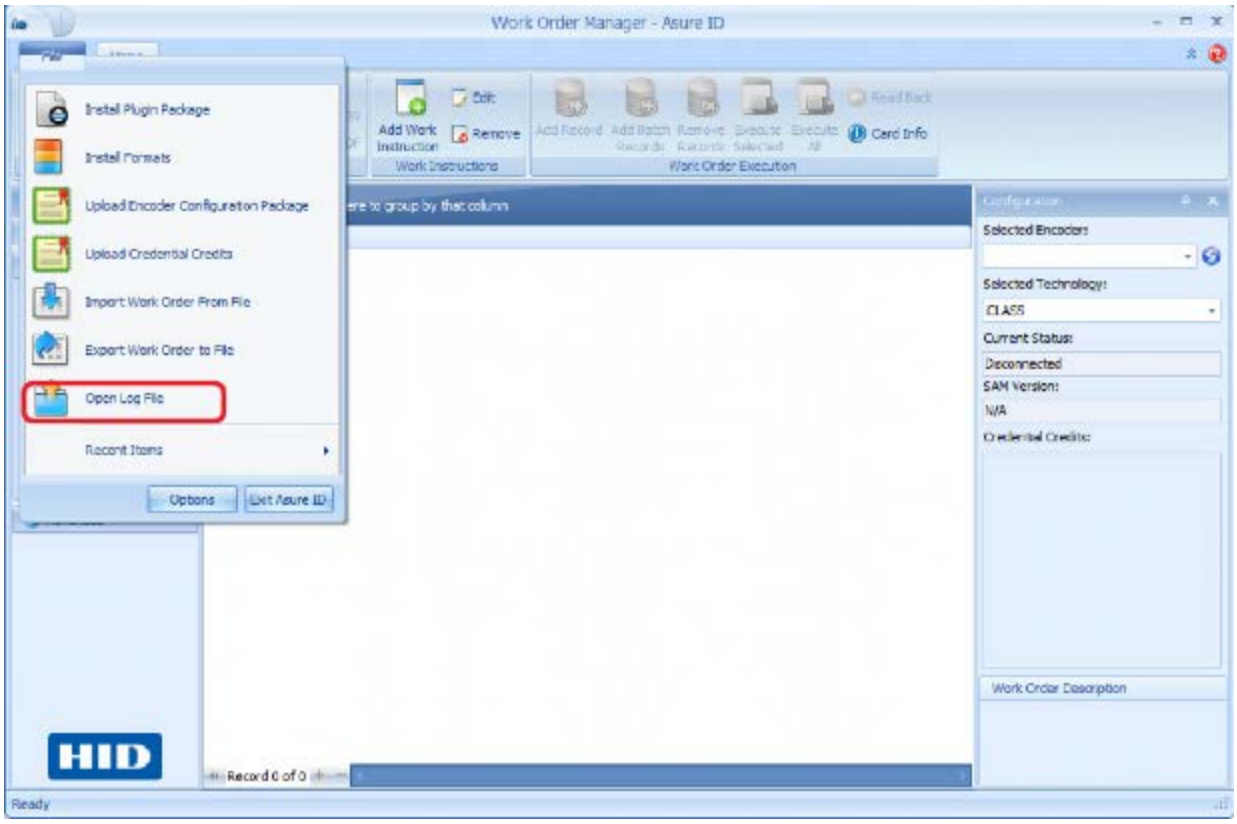


Note: The Administration Keys should be kept in the same secure location. For instructions to export (save) Administration and Custom Keys, see **7.7 Export keys**.

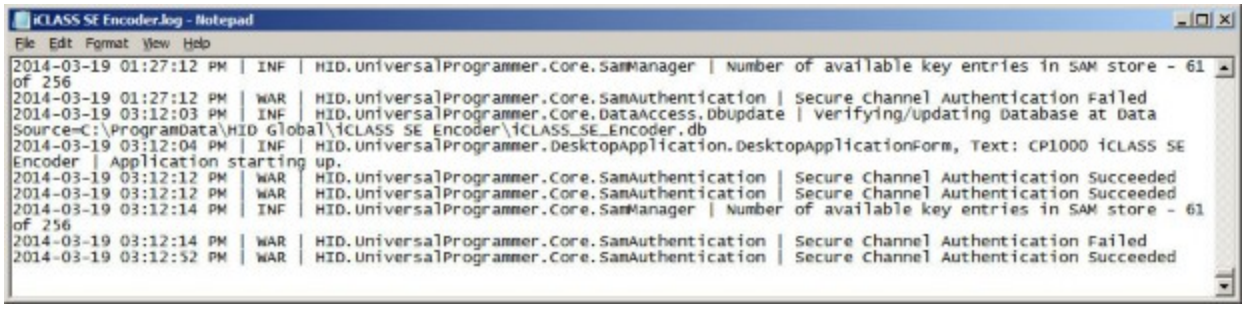
10.2 Log files

The log files are provided as a standard troubleshooting tool. The following procedure accesses the log file through the application.

1. Select **Work Order Manager** > **File** tab > **Open Log File**

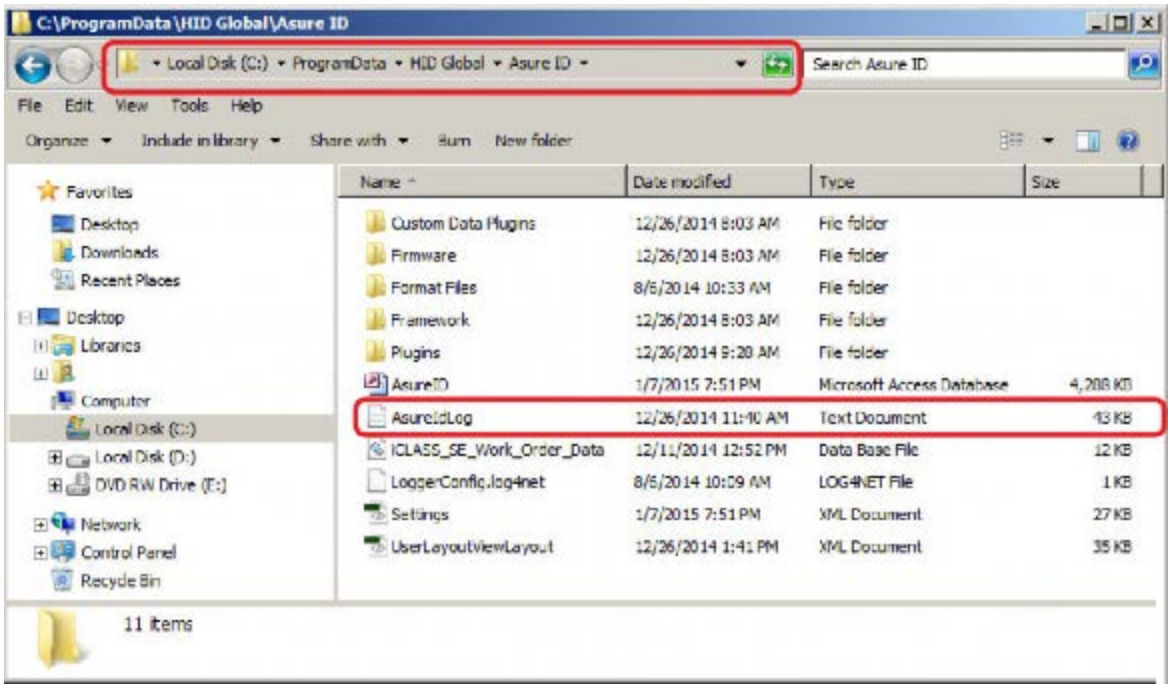


2. The Log file is displayed.



3. You can copy/save the log file, for reference or to send to HID Global Technical Support for assistance.

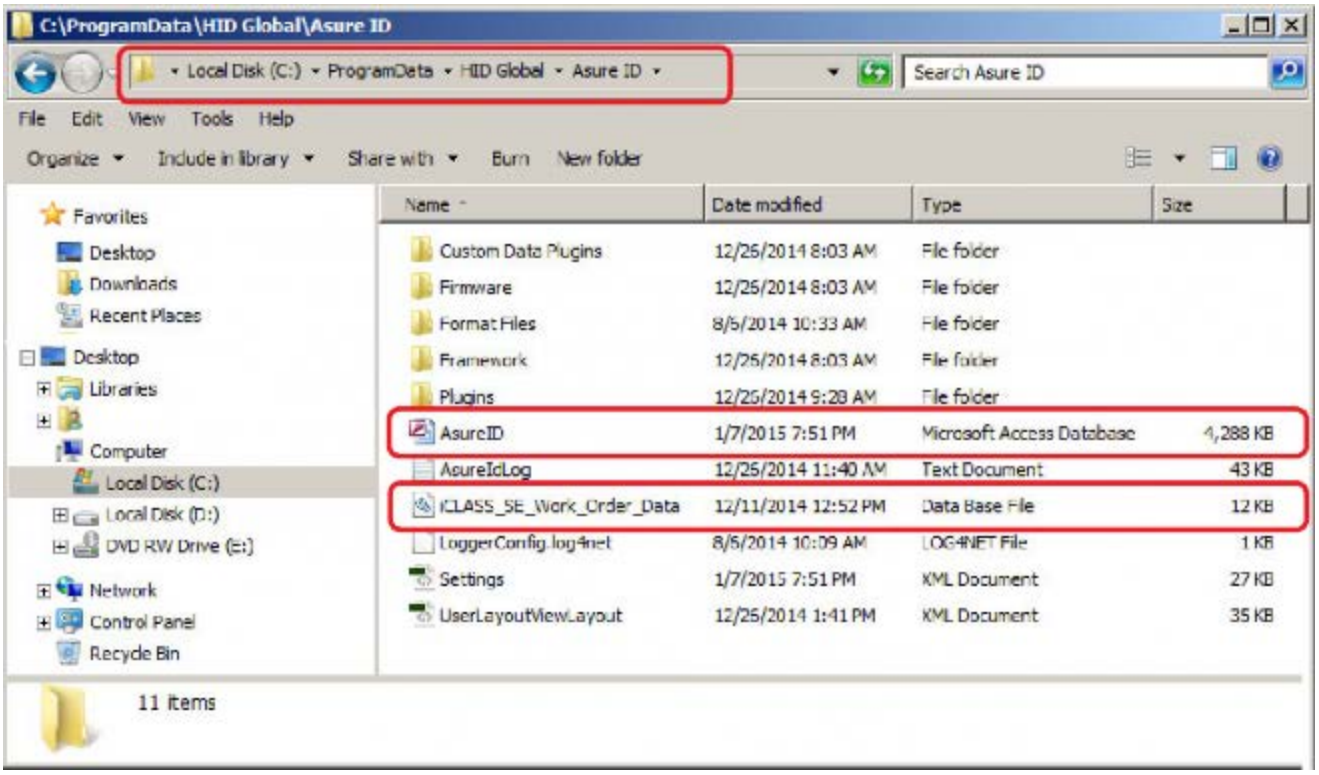
4. If you are not able to access the Asure ID Application, the log file can be found at the following location:
   C:\ProgramData\HID Global\Asure ID



10.3 Database

The database for this application can be found at the following location:

C:\ProgramData\HID Global\Asure ID



Note: This database should be backed up and stored at a secure location. See **10.1 Backup and recovery**.

10.3.1 Supported Databases

The native databases supported are:

- Microsoft Access, 2000 and 2002/2003
- Microsoft SQL Server 2000, 2005, 2008, 2012, 2014, 2016, and 2017
- Oracle 9i and 11g

10.3.2 Synchronize database to encoder

The need to synchronize the database to the encoder, is required if you have connected a new/different iCLASS SE encoder. The encoder configuration is stored on the encoder and only copied on the database. This type of change would create a circumstance where the encoder and the database on the PC are not in-sync.

The fact that the encoder and database are out-of-sync may not be apparent, as there is no indicator that they are out-of-sync. Additionally the keys (custom and HID) from the first encoder continues to display on the second encoder, as this information is coming from the database.

> **Note:** The application allows the creation of a Work Order in this circumstance using the keys from the first encoder. However, when you execute the Work Order you receive an error (authentication or no key available).

For more information on how to synchronize the database with the current encoder attached to the PC, see **7.16 Change encoder Admin keys**.

10.4 Exceptions and error codes

The following are exceptions or error codes that may be presented with the Encoder product. An action is provided to resolve the error, however if the error cannot be cleared, save the log file (see **10.2 Log files**) and contact HID Technical Support.

Exception or Error Message	Situation	Meaning	Action
erInvalidStoreOperation	Encoding	Encoder is missing keys and/or credential counters to complete the operation.	Request keys or credits from HID.
Failed to upload the configuration file to the SAM. See log file for details.	Uploading Keys or Credential Counters	Key package was created for an encoder with a different engine ID.	Request keys or credits from HID for specified encoder.
The Encoder Engine IDs do not Match	Uploading Keys or Credential Counters	Key package was created for an encoder with a different engine ID.	Request keys or credits from HID for specified encoder.
The specified encoder name is not recognized.	Encoding/Managing Keys	Encoder is unplugged or malfunctioning.	1. Make sure correct encoder is selected 2. Reset encoder 3. Restart desktop application
N/A	No encoders listed in Selected Encoders list box	Encoder was not plugged in when application was launched.	Select refresh next to the drop-down list to request the system search for active encoders.
N/A	Current Status in Configuration window reads "Disconnected" for a specified technology.	Applets have not been uploaded or have been cleared from SAM.	1. Navigate to Options > Plugins. 2. If the Applet Version for the specified technology reads "Unavailable", click the hyperlink to upload dlls for the plugin to the SAM.
The smart card cannot be accessed because of other connections outstanding	Any activity involving communication with the encoder	Another application is accessing the encoder.	Close any other applications that may be accessing the encoder.
Configuration of unconfigured iCLASS cards not allowed by encoder.	Encoding iCLASS	iCLASS Configuration file was not configured to allow configuration of Unconfigured cards when the encoder was flashed at the factory.	Encoder must be shipped to HID and SAMPrePersoTool must be used to upload modified UE_iClass_Configuration.xml to encoder with the Value of the "Allow Configuration of Blank Cards" attribute set to "01".

Exception or Error Message	Situation	Meaning	Action
Error: target card has not been configured	Encoding iCLASS	Configuration of Unconfigured iCLASS cards has not been activated in the Work Instruction	1. Open Work Instruction Wizard and change the Expected Card Type from Configured to Unconfigured. 2. Select the desired Card Configuration (2k, 16k/2, etc.) 3. Verify that encoder has been configured to allow configuration of Unconfigured cards (see "Configuration of unconfigured iCLASS cards not allowed by encoder." above for details).
Error: target card has already been programmed	Encoding	Work Instruction is not configured to overwrite cards that have already been programmed.	Open the Work Instruction wizard and check the "Overwrite Existing Credential" checkbox.
Error: unable to authenticate	Encoding	Keys on the card do not match the authentication keys specified in the work order.	1. Go to Key Management and verify that required keys have been installed. 2. Open Work Order and verify that proper authentication key/keysets are in use. 3. Verify correct card is on encoder.
Error: no credentials remain. Contact your HID representative to purchase additional credentials.	Encoding	Credential counters have been exhausted for given technology.	Contact Tech Support to purchase additional credential credits.
Error: data size is larger than the size allocated to be written to the card.	Encoding iCLASS Custom Data	Not enough memory blocks were selected in the Work Instruction Wizard to support the size of the data you are attempting to write to the card.	Open the iCLASS Work Instruction Wizard and allocate more memory blocks for the custom data field, if not enough blocks exist, consider reducing the size of the data being written to the card, or purchasing cards with larger memory size (16k vs. 2k, etc.).
Unable to authenticate Master Key to retrieve list of app IDs.	Encoding DESFire SO Credential	PICC Master key in Work Instruction does not match the PICC Master Key on the card.	1. If card uses Elite keys, add Elite keys/keyset and select in Work Order. 2. If card uses Custom keys, add Custom keys/keyset and select in Work Order.
HID Access Application already exists. Cannot overwrite without turning on Allow Overwrite Existing in the Work Instruction.	Encoding DESFire SO Credential	Work Instruction is not configured to overwrite cards that have already been programmed.	Open the Work Instruction wizard and check the Overwrite Existing Credential checkbox.
Error: unable to authenticate the HID Access Application.	Reading DESFire SO Credential	Keys on the card do not match the authentication keys specified in the work order. Card may be using Elite or Custom keys or card may be blank.	1. If card uses Elite keys, add Elite keys/keyset and select in Work Order. 2. If card uses Custom keys, add Custom keys/keyset and select in Work Order.

Exception or Error Message	Situation	Meaning	Action
An error occurred creating the Legacy HID Access Application. See log file for details.	Encoding MIFARE Credential	An error occurred attempting prepare the sector for the Legacy HID Access App (setting the keys and sector access bits).	1. Verify the proper keys exist on the encoder. 2. Verify the HID Access Application sector has not already been written to by another application.
An error occurred creating the SO HID Access Application. See log file for details.	Encoding MIFARE SO Credential	An error occurred attempting prepare the sector for the SO HID Access App (setting the keys and sector access bits).	1. Verify the proper keys exist on the encoder (this includes the SO keys). 2. Verify the HID Access Application sector has not already been written to by another application.
Error: unable to modify sector trailer. See log file for details.	Encoding MIFARE Custom Data	An error occurred attempting to modify the sector trailer.	Verify that the sector trailer access currently on the card allows the trailer bits to be modified.
An error occurred writing MAD. See log file for details.	Encoding MIFARE Credential or Custom Data	An error occurred attempting to update the MIFARE Application Directory (MAD).	Verify that the MAD sector (0) on the target card has not already been written to by another application with non-MAD data.
An error occurred during media personalization. See log file for details.	Encoding an iCLASS SR custom data to an iCLASS SE card	An error occurred attempting to write SR data to an SE card	Present the correct iCLASS SE card to the encoder.

Glossary

Term	Description
AES	Advanced Encryption Standard The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, The key size used for an AES cipher specifies t<Not Used>he number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows: 10 cycles of repetition for 128-bit keys. 12 cycles of repetition for 192-bit keys. 14 cycles of repetition for 256-bit keys.
APDU	Application Protocol Data Unit
AEAD	Authenticated Encryption with Associated Data
CPO	Custom Product Offering
DES	Data Encryption Standard DES is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations. Although this is considered "strong" encryption, many companies use "triple DES", which applies three keys in succession.
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
MAD	MIFARE Application Directory
PACS	Physical Access Control Solutions
SAM	Secure Application Module
SE	SIO-Enabled or Secure Element
SIO	Secure Identity Object
SNMP	Simple Network Management Protocol
SO	Secure Object - Can have more than one per SIO
TDES	Triple Data Encryption Standard Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.
Top up	An amount of credentials, credits, keys, etc., loaded on the encoder to raise or maintain a desired/required level.
UI	User Interface
UID	Unique Identification Number

Revision history

Date	Description	Revision
February 2024	Minor updates.	B.0
May 2020	Update Reader Data card part numbers in Section 8.	A.9
October 2018	Update to Asure ID 7.8 software version.	A.8
July 2017	Update to Asure ID 7.7.3 software version.	A.7
March 2015	Update to Asure ID 7.6 software version.	A.6
January 2015	Update due to new Asure ID CP1000 Edition Software.	A.5
June 2014	SI information added to the User Guide.	A.4
March 2014	Software Release 2.4 (SP1).	A.3
September 2013	Software Release 2.3.6 (Prox update).	A.2
August 2013	Initial release.	A.1
July 2013	Beta release.	A.0

hidglobal.com

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

PLT-01067, Rev. B.0

Part of ASSA ABLOY