



Nymi Band 3.0 HID Seos

User Guide

2020-09-23

Version 1.1

Table of Contents

Revision history	3
1 Overview	4
Prerequisites	4
1.1. Supported HID Readers	4
2 HID Seos Credential Enrollment	5
2.1. AsureID and Encoder Setup	5
2.2. Loading Encoder Keys and Credits in AsureID	6
2.3. Configuring CP1000 Encoder Settings for Nymi Band 2.0	6
2.4. Creating a Work Order in AsureID	8
2.5. Encoding Nymi Band Seos Credential (Card ID + Facility ID) in AsureID	10
2.5.1. Read Back Nymi Band Seos credential	12
2.5.2. Re-encoding Nymi Band Seos credential	12
2.5.3. Rolling Seos keys on a Nymi Band	13
2.6. Configuring the Readers with Elite Keys	14
3 Nymi Band User Enrollment	15
3.1. Nymi Band User Enrollment	16
3.2. Authentication by Fingerprint	17
3.3. Nymi Band User Unenrollment	17
3.3.1. Removing the Nymi Band's assignment from the user	17
3.3.2. Performing a Delete User Data process	17
3.4. Firmware Upload to the Nymi Band	18
3.5. Log Downloads from the Nymi Band	18
4 Using the Nymi Band for Door Access	19
4.1. Charge the Nymi Band	19
4.2.1. Charging the Nymi Band	19
4.2. Wearing the Nymi Band	20
4.3. Authenticate the Nymi Band	20
4.3.1. Authentication by fingerprint	20
4.4. Using Band for Physical Access	21

5 Troubleshooting and Limitations	22
5.1. Pilot / Security Limitations	22
5.2. Enrollment System Limitations	22
5.3. Resetting the Nymi Band	23
6 PACS Early-Access Addendum	24

Revision history

Version	Date	Revision history
1.0	June 14, 2020	Initial version
1.1	September 17, 2020	Corrections

This guide provides information about using and managing the Nymi Band in HID Seos enabled physical access application environment. It contains workflow information and troubleshooting information that helps you to set up and use the Nymi Band within a HID ecosystem.

Prerequisites

The following components need to be available:

1. Nymi Band 3.0
2. Laptop provided by Nymi to allow local enrollment of the Nymi Bands using the Nymi Band Application (NBA) software.
3. CP1000 (Omnikey 5427UE) USB encoder provided by HID, configured to work with Nymi Bands.

The general workflow of a Seos-enabled Nymi Band is shown below.

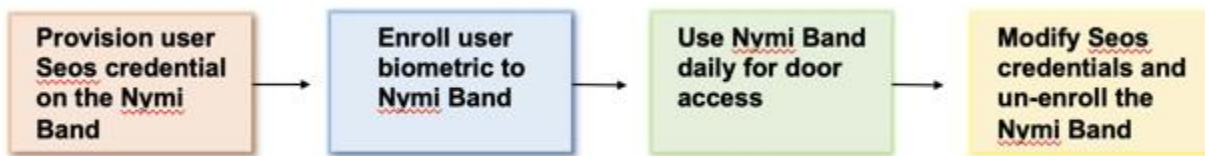


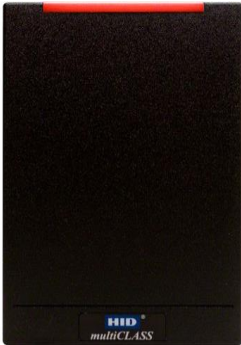

Figure 1.1 - Nymi Band workflow for HID Seos physical access applications

Note: This document strictly pertains to the Nymi Band 3.0 Beta program and is meant for deploying Seos in small Proof-Of-Concept (POC) and pilot projects only.

1.1. Supported HID Readers

The following HID access control readers have been qualified to work with the Seos enabled Nymi Band. Ensure that the HID readers are set up with the RF settings that match the CP1000 encoder.

HID Reader	Description	Reference
------------	-------------	-----------

HID multiCLASS SE RP40	multiCLASS SE® readers simplify migration from legacy technologies with support 125 kHz for HID Prox	
HID iCLASS SE R40	iCLASS SE® R40 is part of HID Global's iCLASS SE platform for adaptable, interoperable access control.	

Note: Most supported readers indicate **iCLASS SE** on the front nameplate of the reader.

2 HID Seos Credential Enrollment

2.1. AsureID and Encoder Setup

To set up AsureID, follow the quick start guide that came with the CP1000 encoder, or follow the steps provided in the AsureID User Guide (PLT-01485). The CP1000 encoder is provided by HID to operate with the Nymi Band. The AsureID **licence key** is printed on the CP1000 encoder quick start guide on page 4, provided by HID. This licence key is used with AsureID for online activation. The initial AsureID credentials are:

- UserID: admin
- password: admin

During the first-time setup of CP1000 encoder, a prompt appears to **provide new admin keys for encoder**. Do the following:

1. Create a passphrase.
2. Generate and save random keys.
3. Save a copy of the three keys in case the encoder needs to be securely restored at some later date.

For more information, see the [HID AsureID Guide](#).

2.2. Loading Encoder Keys and Credits in AsureID

Install iClass SE encoder configuration package (refer to the HID AsureID User Guide).

- Connect CP1000 encoder.
- Launch AsureID, choose **Work Order Manager application**.
- Select **File > Upload Encoder Configuration Package**.

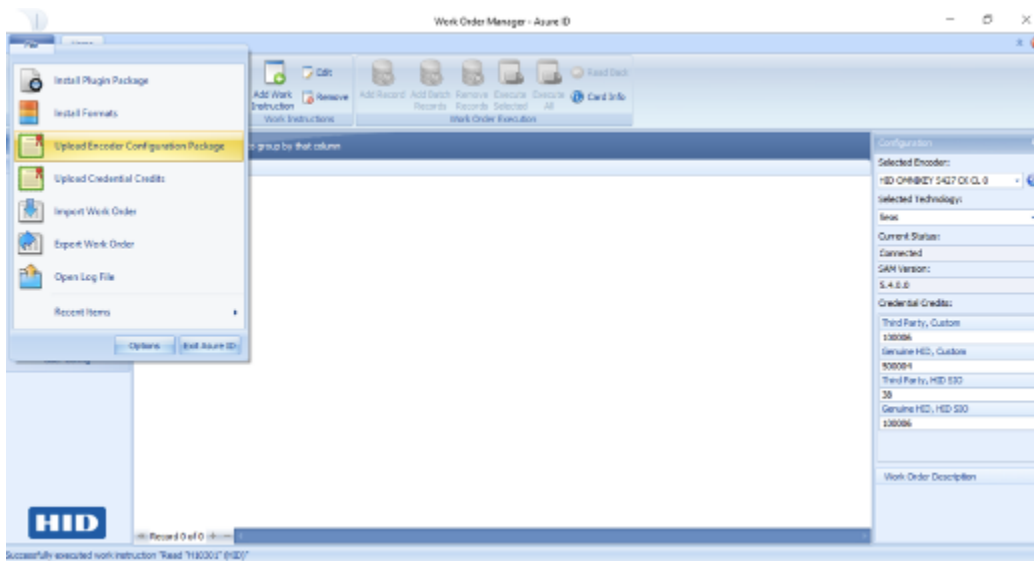


Figure 2.1 - Uploading encoder configuration package

2.3. Configuring CP1000 Encoder Settings for Nymi Band 2.0

Note: This step is not required for use with Nymi Band 3.0

Use the following settings to configure the CP1000 encoder for the Nymi Band.

1. Connect the CP1000 encoder
2. With appropriate drivers installed, open the **Encoder Management** console in a web browser at the default address <http://192.168.63.99>
3. Navigate to the Contactless Config > Polling tab, and then
 1. **Check ISO/IEC 14443 Type A**, and deselect all other protocols.

4. Navigate to the Contactless Config > ISO14443A tab, and then
 1. Modify **register 10** with the **value 03**.
5. Select the **System Config** tab
 1. Click **Apply Changes**.
 2. Click **Store Changes**.
 3. Click **Reboot System**.

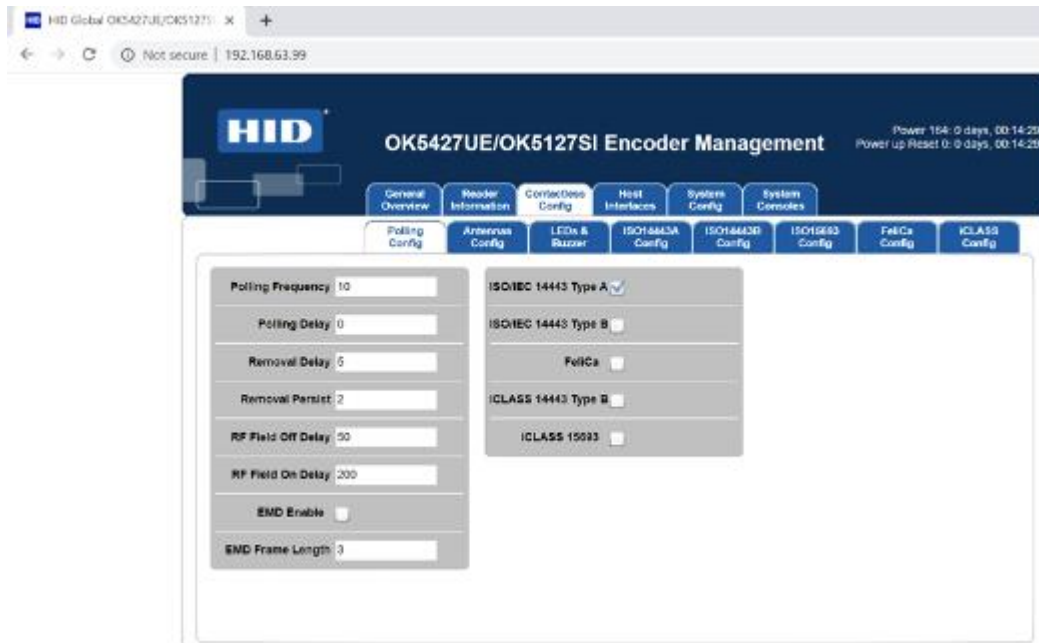


Figure 2.2 - Configuring CP1000 encoder protocol settings

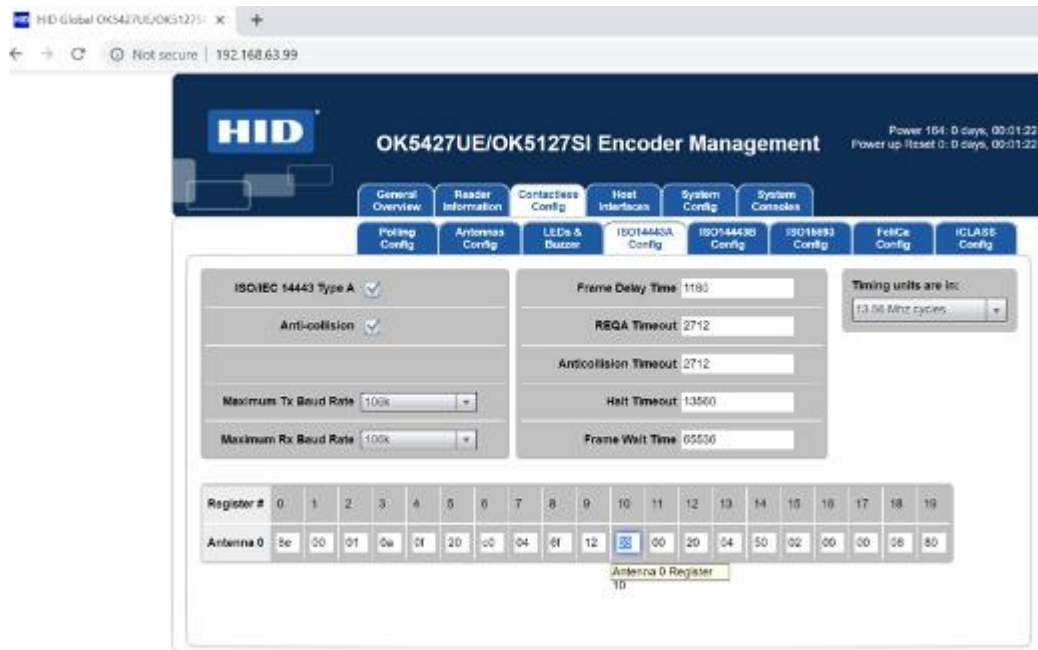


Figure 2.3 - Configuring CP1000 encoder RF settings

2.4. Creating a Work Order in AsureID

To create a word order in AsureID follow these steps:

1. Connect CP1000 encoder.
2. Launch AsureID, choose **Work Order Manager**.
3. From the overhead menu click **New > Seos**, then **OK**.
4. In the Seos encoding window click **Next**.
 1. Select **HID Access Application**
 2. Select **Write**
 3. Select **credential type format** (e.g., H10301)
 4. Then click **Next**
5. On the **Define Format Parameters** screen, assign appropriate facility code and card ID rules, and then click **Next**.
6. In the **Key Selection** step, select appropriate GDF, ADF, and SO keys, and then click **Next**.
7. Click **Finish**, then save and name the template for later use.

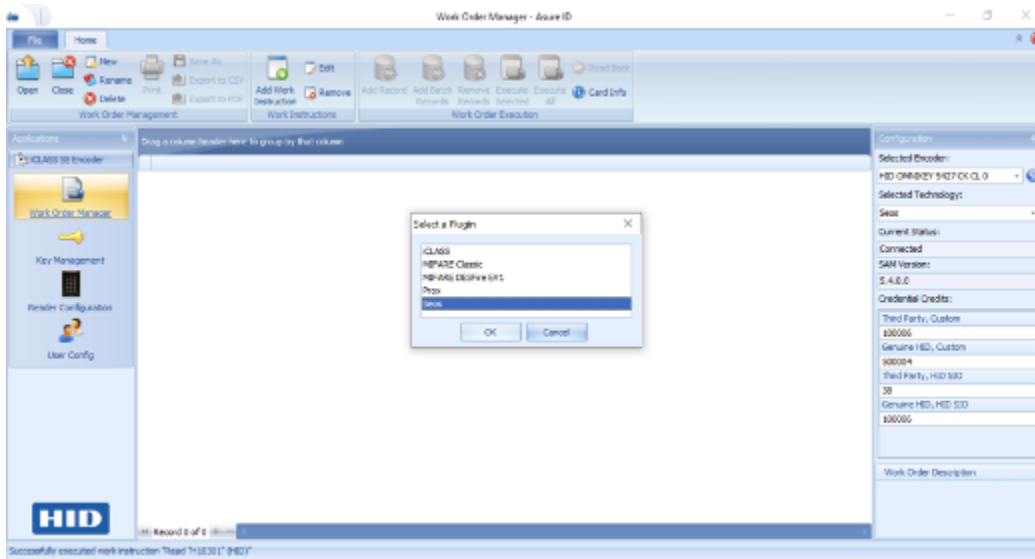


Figure 2.4 - Creating a seos work order

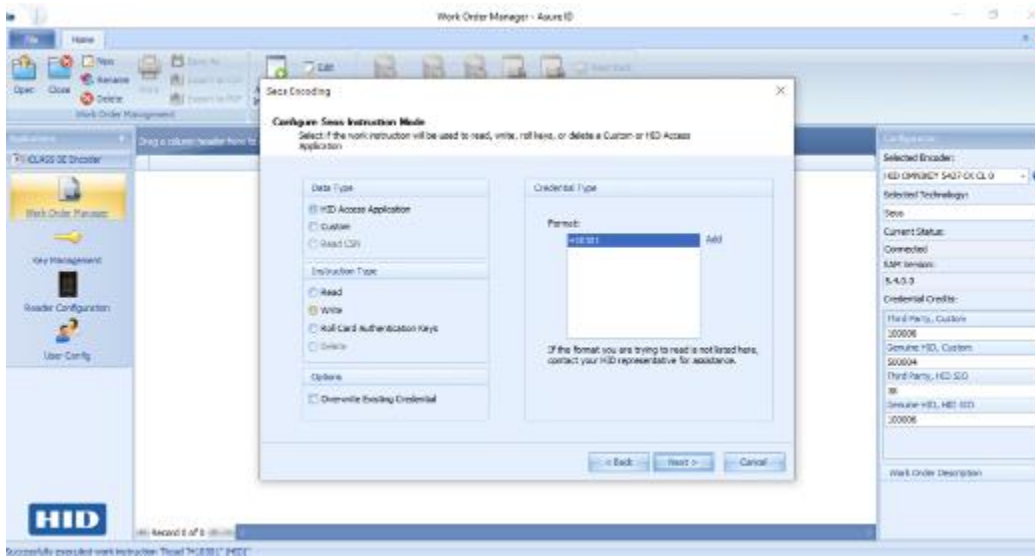


Figure 2.5 - Work order configuration, Seos instruction mode

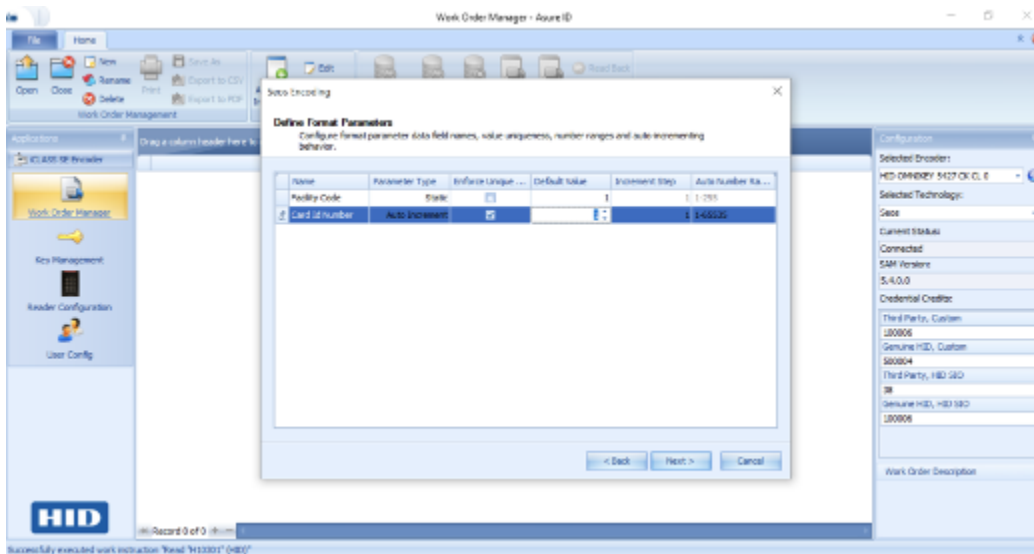


Figure 2.6 - Work order configuration, define format parameters

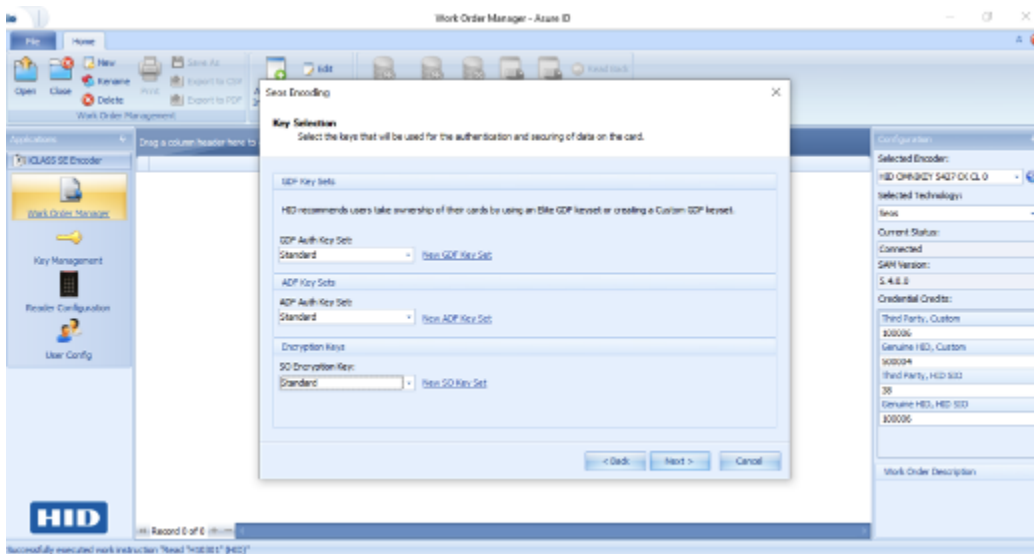


Figure 2.7 - Work order configuration, key selection

2.5. Encoding Nymi Band Seos Credential (Card ID + Facility ID) in AzureID

Following these steps to encode the Nymi Band Seos credentials:

1. Ensure that the Nymi Band is unenrolled and on the Nymi Band charger.

Alternatively, an enrolled Nymi Band can be encoded if worn on the user's wrist after having been authenticated.

2. Connect CP1000 encoder and launchASUREID.
3. InASUREID, select **Work Order Manager** and open the previously saved Work Order to encode Nymi Band.
4. Select appropriate entry from list (e.g., Facility Code 10, Card Number 7).
5. Place Nymi Band onto the encoder with the display facing the top side of the encoder.
6. Click **Execute Selected**.
7. A pop-up window with the encoding status is displayed. Wait for the encoding to complete.
8. The Nymi Band can now be enrolled and used to register the Nymi Band's **Facility Code** and **Card Number** with the access control system.

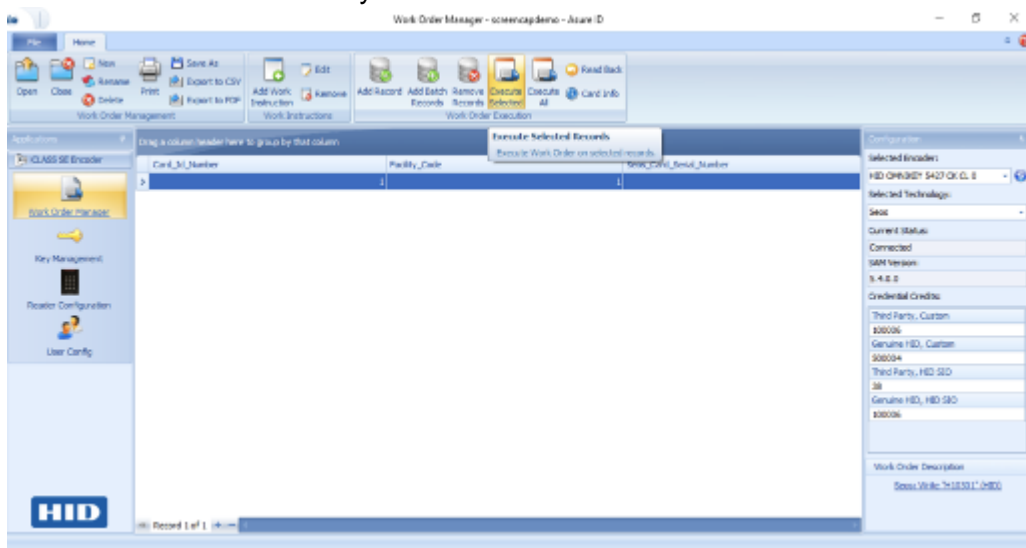


Figure 2.8 - Work order execution

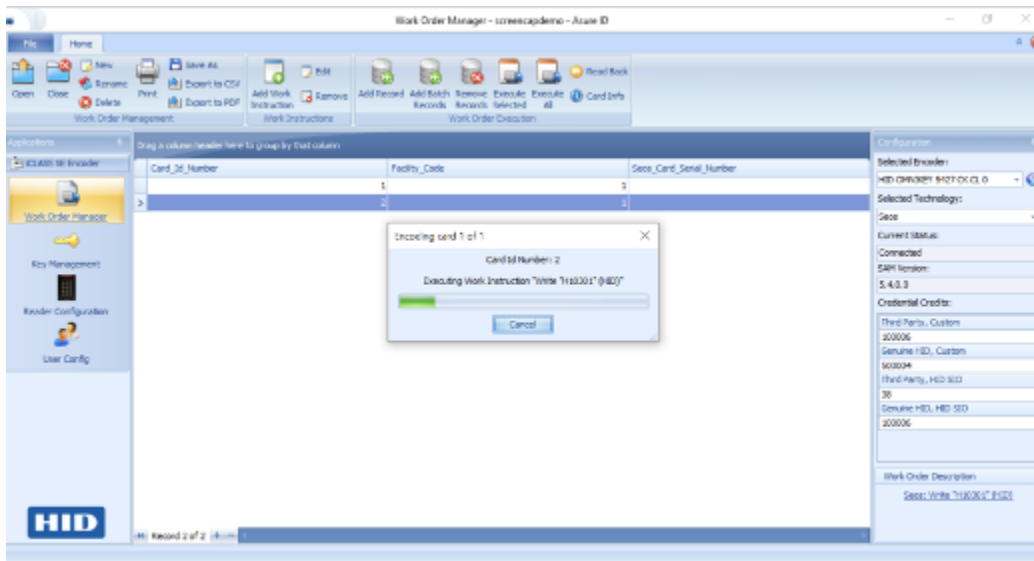


Figure 2.9 - Work order execution, in progress

2.5.1. Read Back Nymi Band Seos credential

To confirm the Facility Code and Card Number on the Nymi Band, with a work order open, click a record to highlight it, then click the **Read Back** button.

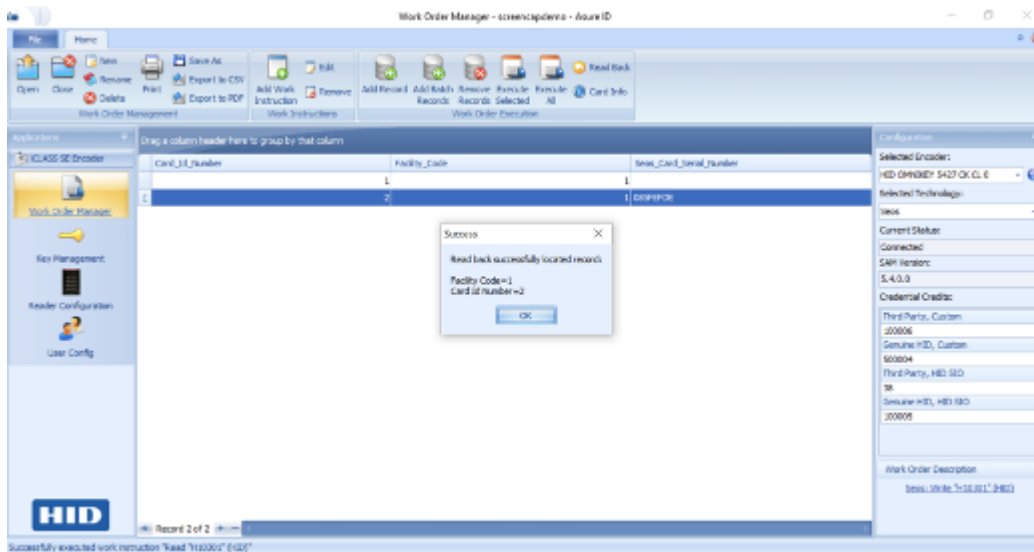


Figure 2.10 - Card credential read back

2.5.2. Re-encoding Nymi Band Seos credential

Overwriting the Seos credential with a new Facility Code and Card Number is possible by creating a work order (section 3.4), with **Overwrite Existing Credential** enabled in the **Options** section of the work order.

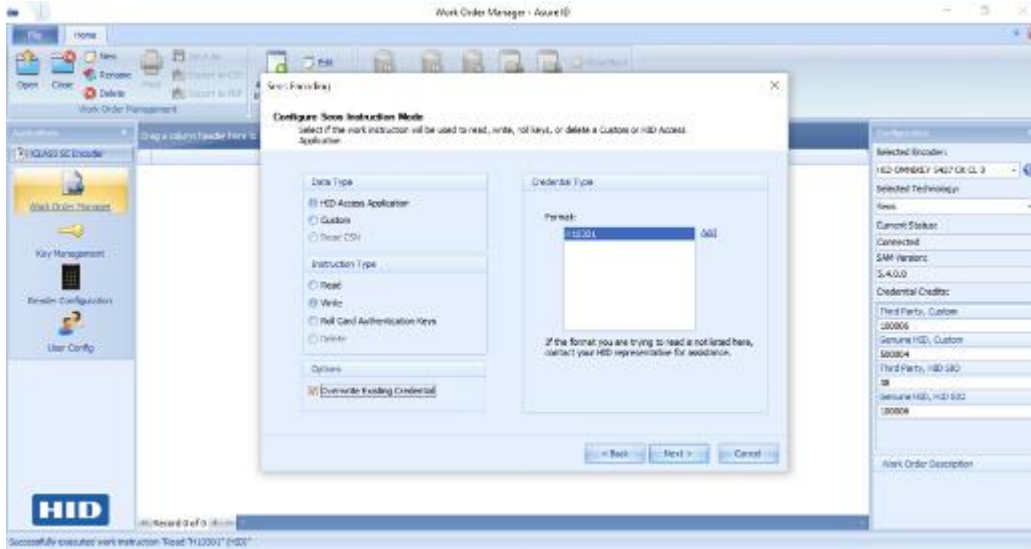


Figure 2.11 - Work order configuration, overwrite existing credential

2.5.3. Rolling Seos keys on a Nymi Band

If keys have been changed previously and need to be written with the standard key set, or the work order requires that the keys be rolled, a **Roll Keys** work order may be created and executed.

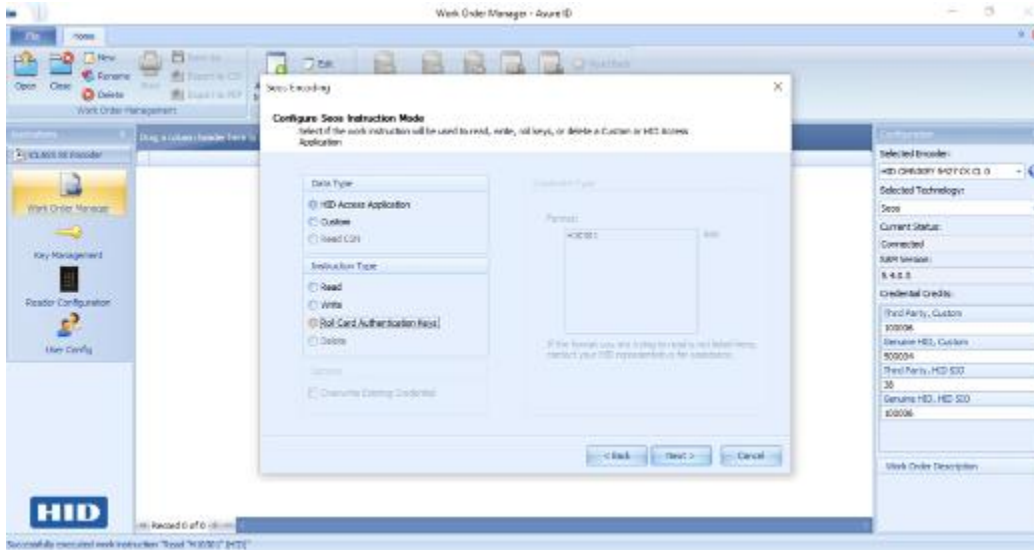


Figure 2.12 - Work order configuration, roll card keys



2.6. Configuring the Readers with Elite Keys

If applicable, to configure a mobile-ready iClass SE door reader with Elite keys, power cycle the reader and apply the reader configuration card within five seconds of powering on the reader.

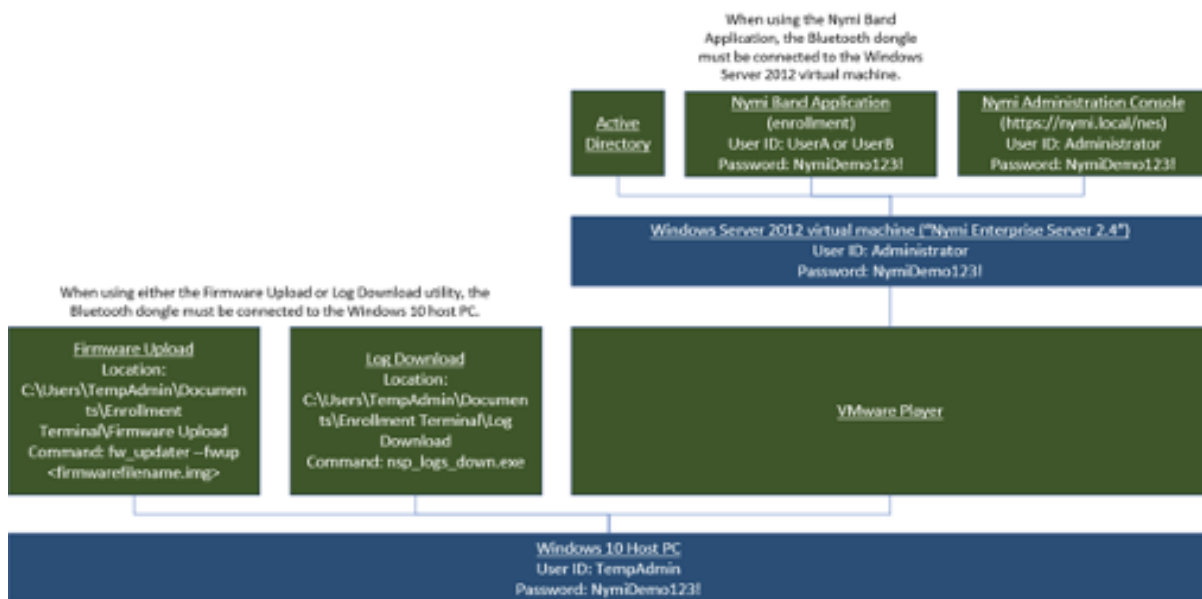
3 Nymi Band User Enrollment

A Nymi Band can only be used after it has been biometrically enrolled to a user. For production use, the Nymi Enterprise Edition (NEE) software is integrated into the customer's Active Directory (AD) environment, and the customer enrolls the users based on pre-existing AD credentials.

In a beta test or POC environment, Nymi may provide a notebook computer with AD, NEE and other utilities already configured. Accounts for users (UserA, UserB, UserC, etc.) are already set up on the AD, and Nymi Band users can enroll using these user credentials.

The content of the notebook is documented in the diagram below. The credentials (user ID and password) necessary to access the system and enroll the Nymi Bands are:

- Windows 10 host PC: user ID is `TempAdmin`
- Windows Server 2012 virtual machine: user ID for the administrator account is `Administrator`
- Windows Server 2012 virtual machine: user ID for the user accounts used to enroll the Nymi Bands are `UserA` and `UserB`
- All credentials in the notebook computer share the same password: `NymiDemo123!`. This is acceptable since the notebook contains no sensitive data and is not connected to a production AD.





The Bluetooth dongle is always physically attached to the PC. It is connected to only one operating system at any given time, and the connection is configured within the VMware player



Figure 3.1 - Enrollment station block diagram

In order to access the Windows Server 2012 virtual machine, please do the following:

1. From the Windows 10 host PC's desktop, click the Nymi Enterprise Server 2.4 icon. This starts the VMware Player application.
2. From the VMware Player screen, right-click the Nymi Enterprise Server 2.4 virtual machine listed on the left.
3. Select **Power On** from the drop-down menu. Windows Server 2012 starts in the VMware Player window.
4. From within the window, access the Windows Server 2012 using CTRL-ALT-INSERT.
5. When operations that require Windows Server 2012 are completed, you can return to the host PC by right-clicking the Nymi Server 2.4 icon, and selecting the **Suspend** option.

3.1. Nymi Band User Enrollment

Launch the **Nymi Band Application** under the Windows Server 2012 virtual machine. Log into the application using the UserA or UserB credential (one for each user), as documented in section 2. Follow the on-screen instructions to enroll the user. For further instructions, please refer to the **Nymi Band Enrollment** section of the *Nymi Enterprise Edition Administration Guide*.

3.2. Authentication by Fingerprint

When the screen displays the fingerprint, the employee holds their finger on the square fingerprint sensor and surrounding fingerprint bezel for about 15 seconds, while the Nymi Band displays **HOLD FINGER**.

When the Nymi Band displays one of the following icons, the employee identity was successfully authenticated, and the employee can remove their finger from the fingerprint sensor and fingerprint bezel.

If the authentication fails, the Nymi Band vibrates and the **RETRY** message appears. When the fingerprint icon appears, the employee can try to authenticate again.

If the fingerprint authentication fails, ensure the following considerations:

- Employee's finger and the sensor are clean and dry.
- Employee's finger is still on the sensor and bezel during the authentication period.
- Employee does not lift their finger off the sensor or bezel during the authentication period.

3.3 Nymi Band User Unenrollment

To unenroll a Nymi Band from a user, two operations need to be performed:

- Remove the Nymi Band's assignment from the user
- Perform a Delete User Data process

3.3.1. Removing the Nymi Band's assignment from the user

1. In the NES Administrator Console, select **Users**.
2. In the **Search** field, type the full or partial username, first name, or last name of the employee.
3. Click **Find**. The Users page displays the user, or a list of users that match the search criteria.
4. Select the name of the user.

3.3.2 Performing a Delete User Data process

1. Remove the Nymi Band from the wrist of the user, and then attach the Nymi Band to a charger.
2. On the Nymi Band, hold the bottom button until you see the **Delete User Data** message on the screen (about 10 seconds).
3. Continue to hold the bottom button until the Nymi Band vibrates quickly twice and the User Data Deleted message appears on the screen.

Biometric authentication does not work for the user after you complete the Delete User Data process. To use the Nymi Band again, the user must enroll the Nymi Band by using the Nymi Band Application



Note: If you perform a Delete User Data process on a Nymi Band and attempt to re-enroll it, users will see the following message, *A Nymi Band has been assigned to (user name), however it cannot be found.* To proceed, you need to delete the Nymi Band from NES and re-enroll.

3.4. Firmware Upload to the Nymi Band

In the event that a firmware update to the Nymi Band is required, please refer to the **Updating Nymi Band Firmware Overview** section of the Nymi Enterprise Edition Administration Guide for further instructions.

3.5. Log Downloads from the Nymi Band

Nymi may request for logs to be retrieved from a Nymi Band for diagnostic purposes.

1. Ensure that the Nymi Band is connected to a charger and is within Bluetooth range of the notebook computer.
2. From the Windows 10 host PC, start a command prompt, and go to the `C:\Users\TempAdmin\Documents\Enrollment Terminal\Log Download` directory.
3. Run the **Services** application, and stop the **Nymi Bluetooth Service** service.
4. Run the `nsp_logs_download.exe` application. The logs are saved in the same directory as `fwlog_day_date_time_year.log`.
5. Restart the **Nymi Bluetooth Service** service.

4 Using the Nymi Band for Door Access

4.1. Charge the Nymi Band

The NymiBand is charged by placing it on a Nymi Band charger. The Nymi Band receives power from standard USB-A ports. It takes about two **hours** to fully charge the Nymi Band. A fully-charged Nymi Band has a battery life of about **three days**. When a Nymi Band has a drained battery, it will not respond to any button presses. The Nymi Band shows a charging icon when connected to the charging cable.

USB charger requirements:

- Regulated voltage of 5V, independent of the number of ports or connected devices.
- Source a minimum of 150mA for each device, independent of the number of ports or connected devices.



Figure 4.1 – Nymi Band Charger

4.2.1 Charging the Nymi Band

1. Plug the charging cable into the USB port on your computer or a UL-certified USB wall charger. A light appears in the center bottom of the charger indicating that it is receiving power.
2. Hold the other end of the charging cable near the port on the back of the tracker until it attaches magnetically. Make sure the pins on the charging cable align with the port on the back of your Nymi Band. The Nymi Band vibrates indicating that it is receiving power.
3. Push the bottom button on the Nymi Band to view the amount of battery charge that is on the Nymi Band.



Figure 4.2 - Charging battery indicator

4. When the Nymi Band is fully charged, disconnect the charging cable from the Nymi Band.



Figure 4.3 - Full battery indicator

4.2. Wearing the Nymi Band

Put on the Nymi Band like a watch. The Nymi Band should be fitted snugly on the user's wrist. Gently push on the Nymi Band and make sure it does not have excess overhang over the wrist. The sensors on the back of the Nymi Band detects whether the Nymi Band is being worn.



Figure 4.4 - How to wear the Nymi Band

4.3. Authenticate the Nymi Band

To use the Nymi Band to perform tasks, the user must authenticate to the Nymi Band. How the user authenticates depends on the group policy configuration. Once a Nymi Band is authenticated on the user's wrist, removing it automatically de-authenticates and deactivates the physical access interface.

4.3.1. Authentication by fingerprint

When the screen displays the fingerprint icon, the user holds their finger on the square fingerprint sensor and surrounding fingerprint bezel for about 15 seconds. When the Nymi Band vibrates, the user identity is successfully authenticated, and the user can remove their finger from the fingerprint sensor and fingerprint bezel. If the authentication fails, the Nymi Band vibrates and the **RETRY** message appears. The user can try to authenticate again.

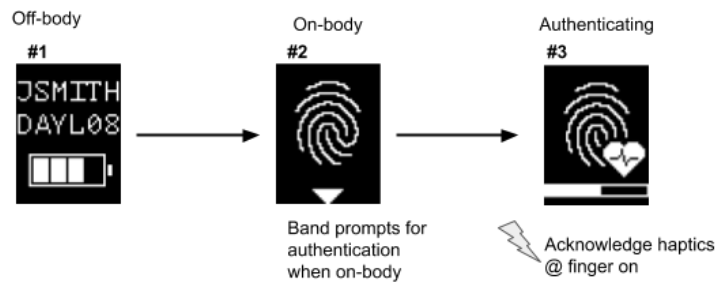


Figure 4.5 - Nymi Band Authentication Screens

If fingerprint authentication fails, ensure the following:

- User's finger and the sensor are clean and dry.
- Keep your finger still on the sensor during authentication.
- Do not lift your finger from the sensor during authentication.

4.4. Using Band for Physical Access

The physical access feature is active when the enrolled Nymi Band is in an authenticated state. In addition, if the Nymi Band is unbound and on a charge supporting credential encoding, the physical access feature is available.

1. Tap and hold the face of the Nymi Band to the center of the HID Seos reader.
2. Hold the Nymi Band in place for a minimum of one second until the reader shows a purple light, then green and sounds two beeps.

If the reader shows green light (no purple light) and beeps only once, remove the Nymi Band from the reader and try again.

Note: You can retry the tap and hold process multiple times if there is a 2 second wait period between taps.

5 Troubleshooting and Limitations

5.1. Pilot / Security Limitations

To ease Seos encoding with Nymi Band 3.0, *unenrolled* Nymi Bands can be encoded with Seos credentials when connected to a charger. This poses a potential security risk that customers must understand and agree to for the duration of their Pilot engagement.

In the future, Nymi intends to address this limitation by locking access to Seos credentials on unenrolled bands, requiring system administrators to unlock the credential prior to assigning to a new user.

This implementation results in the following:

1. A Delete User Data (section 3.3.2) process puts the Nymi Band into an unenrolled state where user biometrics and data have been deleted but Seos credentials are retained. Access to Seos credentials continue to be available over NFC when an unenrolled Nymi Band is connected to a charger. This means Seos credentials can be used for physical access in an unenrolled, unauthenticated state if a system administrator has not taken action to remove privileges for the Seos credential in question in their physical access control system.
2. A previously enrolled Nymi Band will retain its old Seos credential after a Delete User Data action has been performed. When a new user enrolls to the Nymi Band, the same Seos credential will be made available to them. It is up to the system administrator to re-assign the Seos credential to the new user in their physical access control system to avoid inadvertent access to the previous user's physical access privileges.

Note that while enrolled, the Seos credential is only made available when the Nymi Band is authenticated on the enrolled user's wrist.

5.2. Enrollment System Limitations

- The Log Download or Firmware Upload are command-line utilities running on the Windows 10 host (physical PC), whereas AD, Nymi Enterprise Server (NES) and the Nymi Band Application (NBA) run in a virtual machine, under Windows Server 2012.
- The NBA is not qualified to run under Windows Server 2012 for production use, however it is acceptable in this case.
- There are performance (speed) limitations due to the notebook computer and virtualized environment. In particular, the NBA may take up to 15 seconds to start. This is not representative of production performance.
- There is one Bluetooth dongle attached to the enrollment notebook, and it is shared between the host operating system (Windows 10) and the virtual machine's operating system (Windows



Server 2012). The selection is made in the VMware application, which runs under the host operating system. If the Log Download or Firmware Upload application is being used, then the dongle must be logically connected to the host operating system. When the NBA is being used, the dongle must be logically connected to the virtual machine's operating system.

5.3. Resetting the Nymi Band

If the Nymi Band is unresponsive or is behaving in an unusual way, place the Nymi Band on the charger and hold the **top** button for 10 seconds to restart the Nymi Band. Please contact a member of the Nymi field support team so that a log may be retrieved from the Nymi Band to help diagnose the issue. If the Nymi Band is unresponsive after removing from the charger, it may need to charge for a full two hours.

6 PACS Early-Access Addendum

The Nymi Bands provided for PACS early access users to beta Nymi software, and may encounter operational issues. If the Nymi Band is not recognized by the HID reader and access is not granted, please ensure that the Nymi Band is authenticated and is held up against the centre of the HID reader for about one second, until the LED turns purple and access is granted.

Note: The LED might turn to a different colour, depending on the configuration of the reader.

If repeated attempts remain unrecognized, please perform the following:

1. Remove the Nymi Band from your wrist, and connect it to a charger.
2. Press and hold the top button for about 10 seconds, until the word **RESTART** flashes on the screen. The following figure shows the RESTART message.



The restart process takes about 10 seconds to complete. Next, authenticate to the Nymi Band. Afterwards, the Nymi Band is recognized by the HID reader. In rare cases, the Nymi Band may restart without notice. When this occurs, wait for the restart to complete and then authenticate to the Nymi Band. Afterwards, the Nymi Band should be recognized by the HID reader.

Performance of the Nymi solution is undergoing constant improvements. For any inquiries, including the availability of firmware performance updates, please contact your Nymi representative.