Integrating HID® SEOS tokens with your Net2 system

Overview

This configuration is for customers who want to use HID® SEOS tokens whilst still being able to incorporate PaxLocks into the system. This allows external perimeter doors to be secured using SEOS credentials whilst allowing the simplicity and cost effective PaxLocks to be used on internal doors.

Equipment required

HID® Signo™ readers (any reader in the HID® reader range that can read HID® SEOS tokens)

HID® OMNIKEY® 5427 USB desktop reader

Net2 v6.9 or higher

HID® SEOS ISO cards - 5006PGGAN7 H10302

Note: Compatible with a PaxLock Pro, not compatible with Entry.

Reader

HID® Signo™ readers can be used in their default configuration. As long as the reader is set up to read HID® SEOS tokens then it will output the correct data to the Net2 control unit.

The output from the reader when used with the specified HID® tokens will be 37 bit Wiegand. Net2 will automatically accept this output when the system is configured in accordance with this application note.

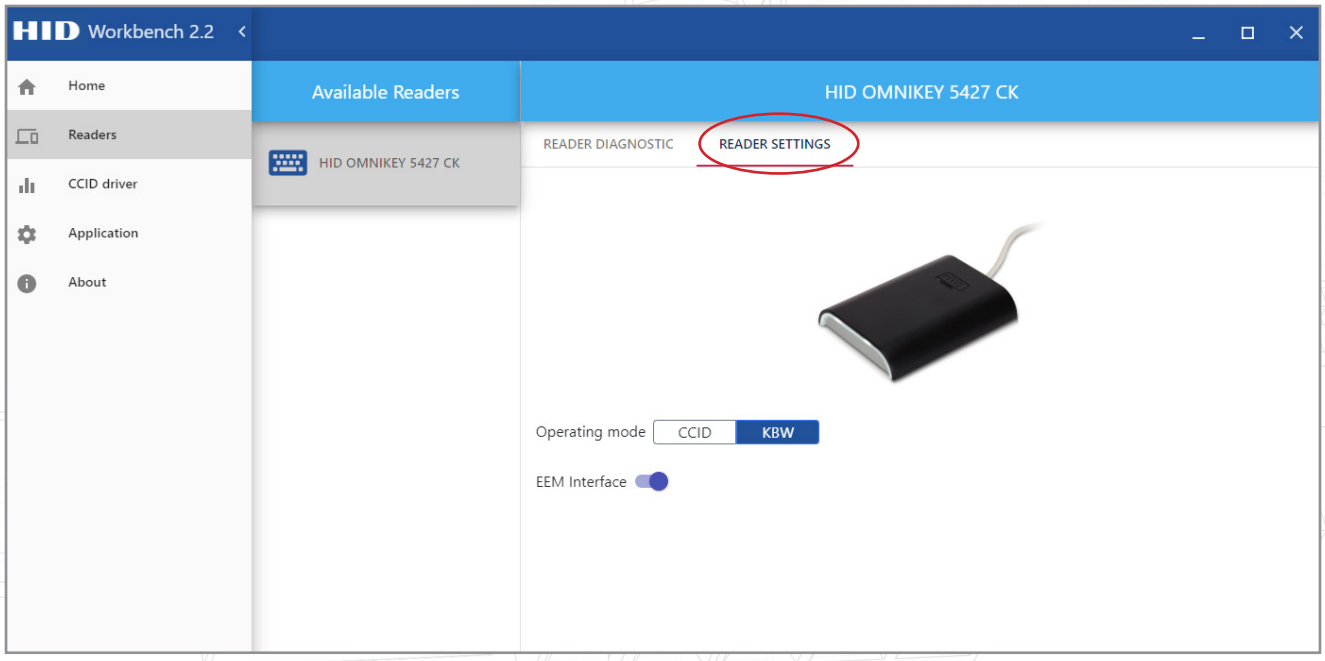
Should the configuration of the reader need to be set up, the configuration app from HID® will need to be used.

Desktop reader configuration

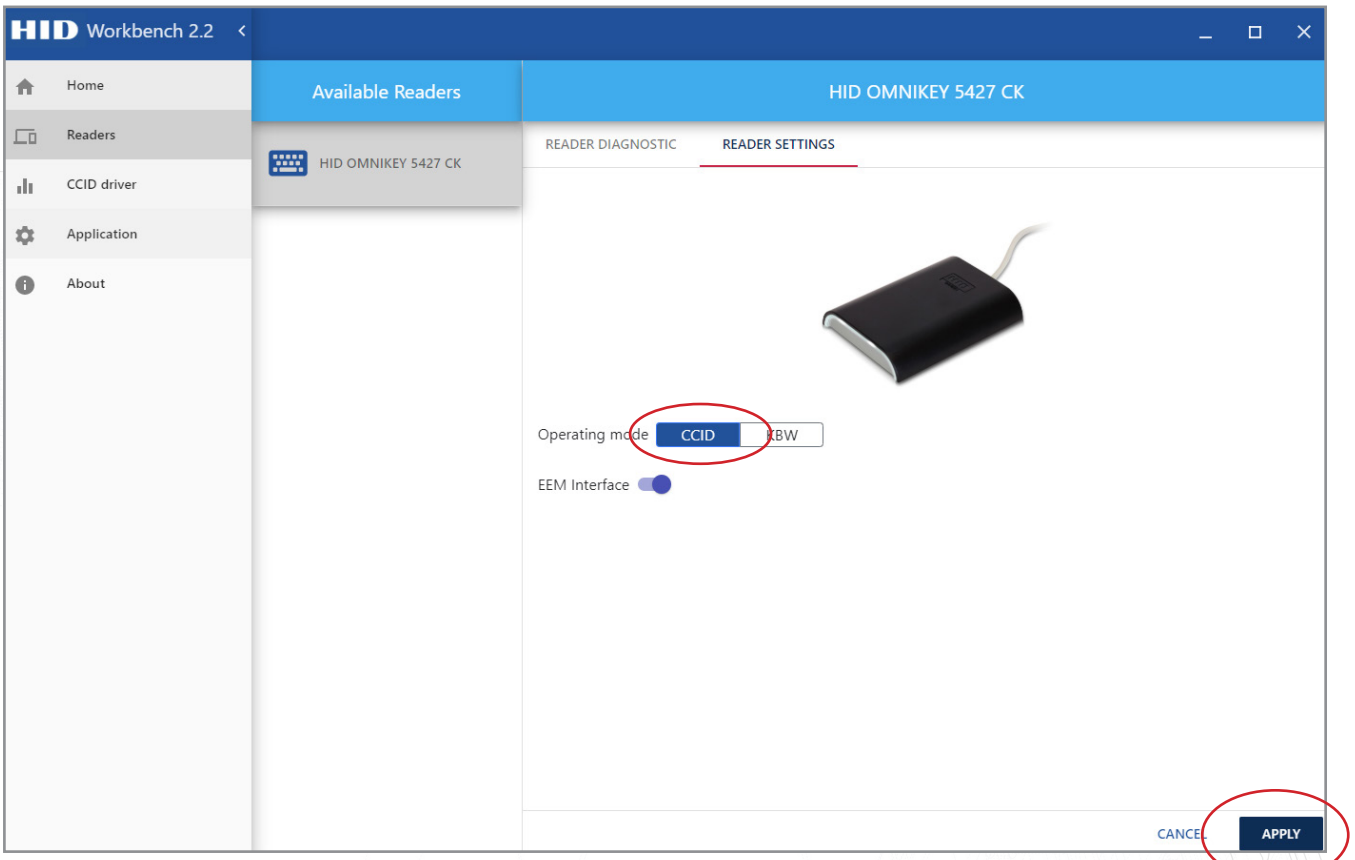
In this configuration we are using two different token numbers taken from the same card. To enable this to work the USB desktop reader must be configured to send the details of both numbers to Net2 during enrolment.

1. The configuration required for this mode to function correctly in Net2 is contained within the configuration file, **'Pax_OmiKey.cfg'** which can be downloaded from www.Paxton.Info/6940
2. To configure the HID® desktop reader you will also need the HID® OMNIKEY® Workbench software
3. In HID® OMNIKEY® Workbench click **'Readers'**

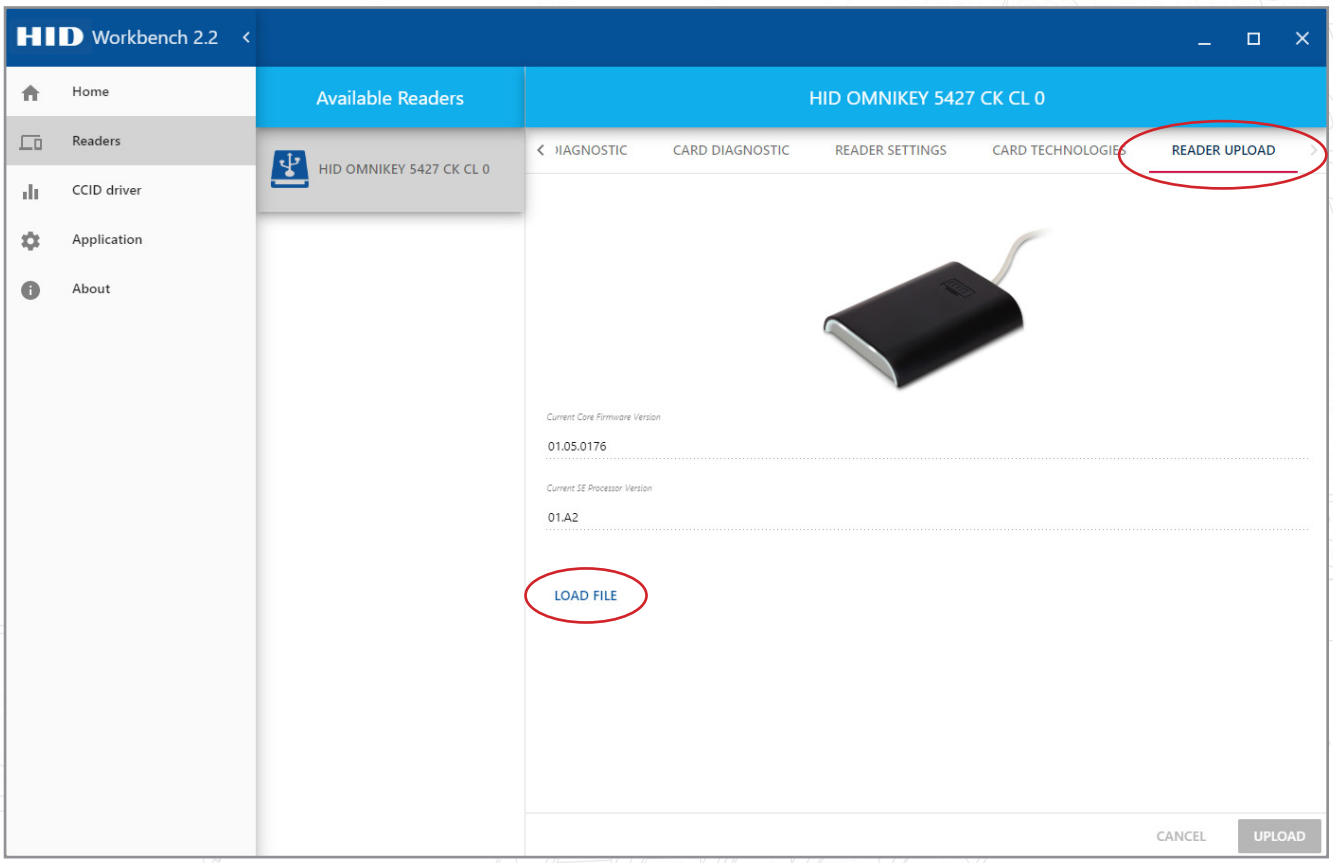
4. Click **'Reader settings'**



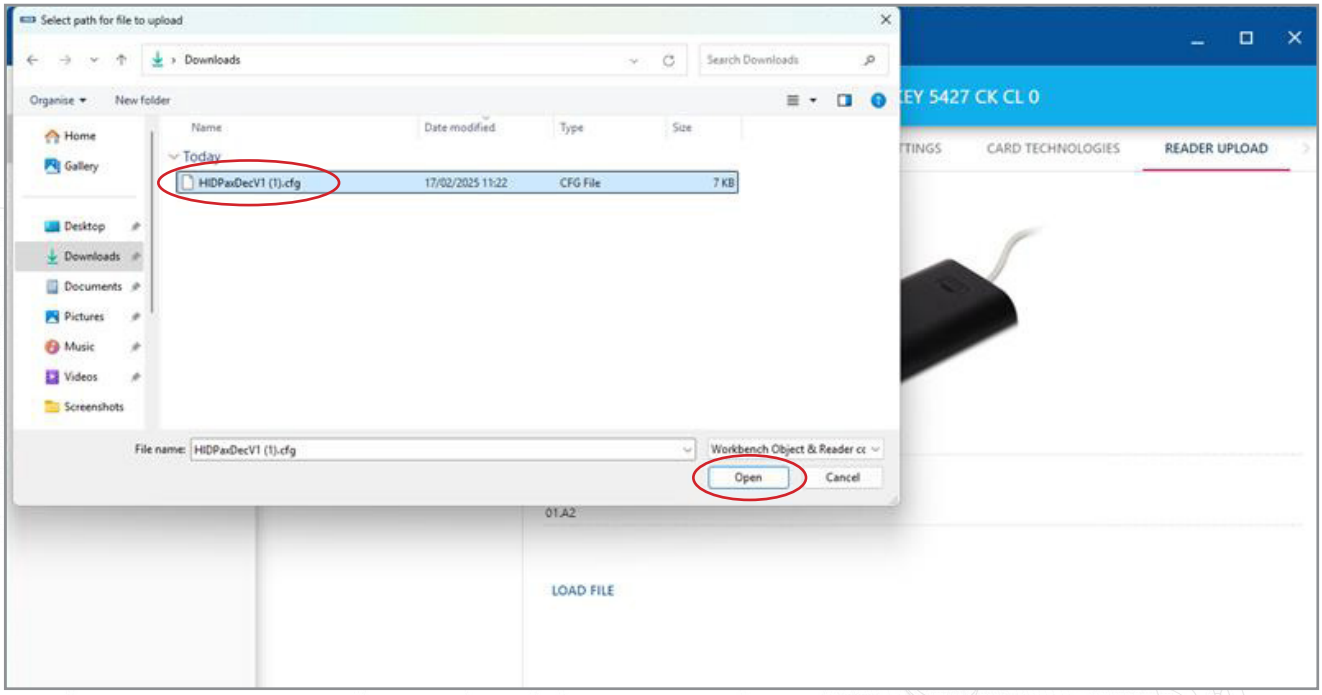
5. Change the operating mode to **'CCID'** and click **'Apply'**



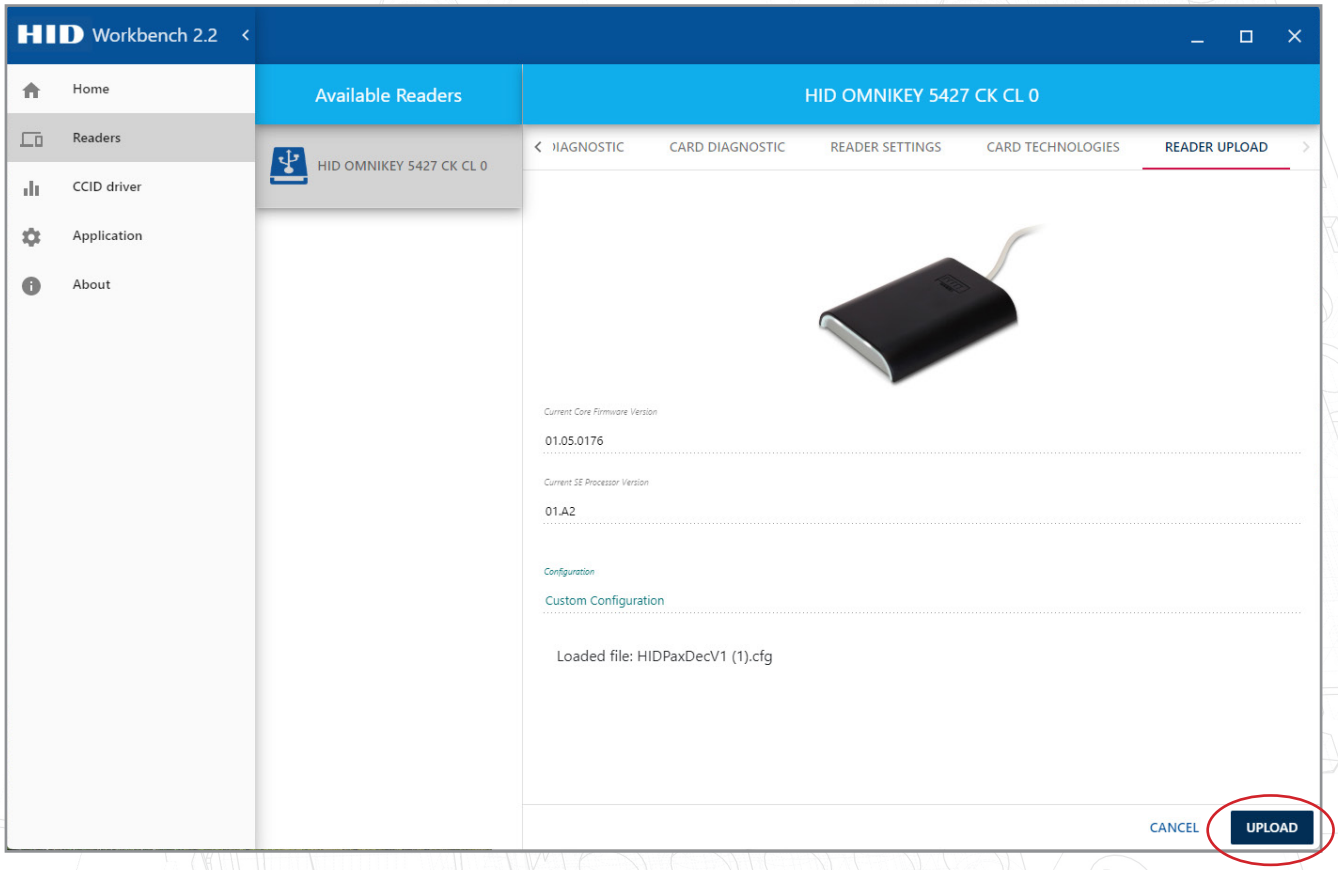
6. Click on **'HID® OMNIKEY® 5427 CK CL 0'**, scroll across to **'Reader upload'** and click **'Load File'**



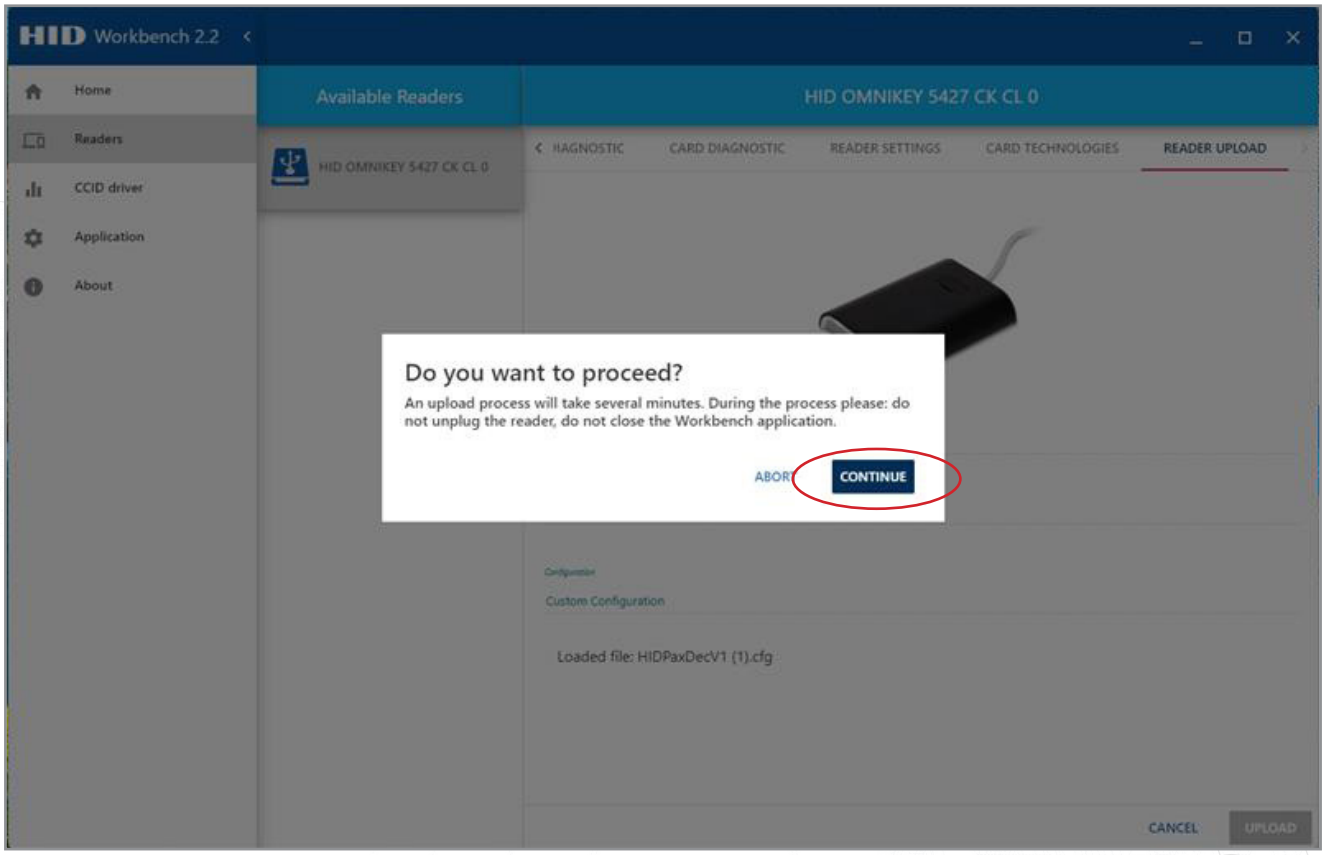
7. Select the file **Pax_OmiKey.cfg** Click **'Open'**



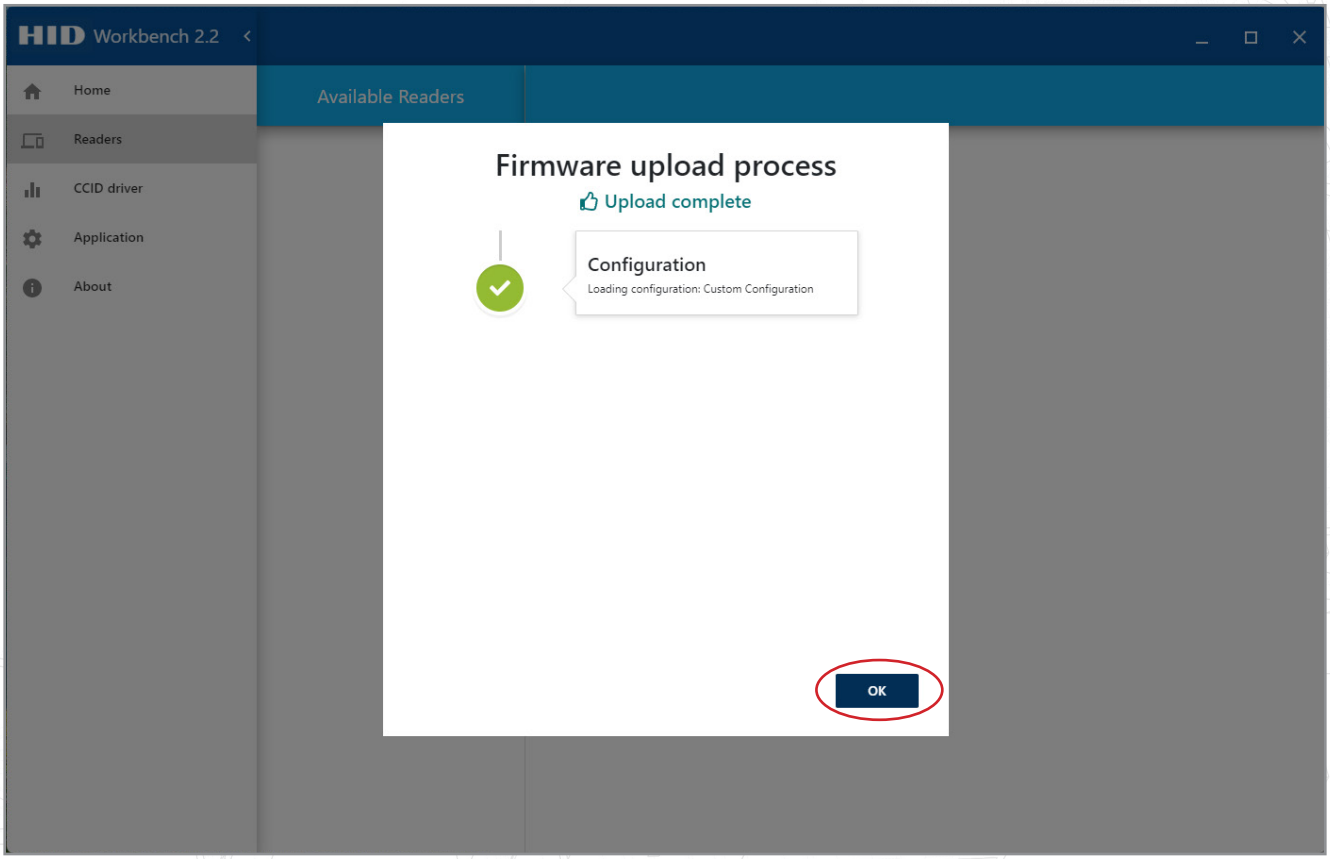
8. Click **'Upload'**



9. Click **'Continue'**



10. Click **'OK'** to close the application



Now that the USB desktop reader is configured correctly it will deliver two token credentials to Net2 whenever a token is presented to it.

Tokens

The tokens for this integration need to be **"HID® SEOS™ ISO cards - 5006PGGAN7 H10302"**, this ensures that the tokens have a static UID and a unique 37 bit number encoded into the secure memory.

Note: "HID® SEOS™ ISO cards - 5006PGGAN7 H10302" is the ordering reference from HID® and should be used when purchasing tokens.

HID® readers will read the secure credential, PaxLocks will read the static UID.

When enrolled using the Custom DTR two credentials will be created for each token, one for the secure credential and one for the UID.

Net2 Software configuration

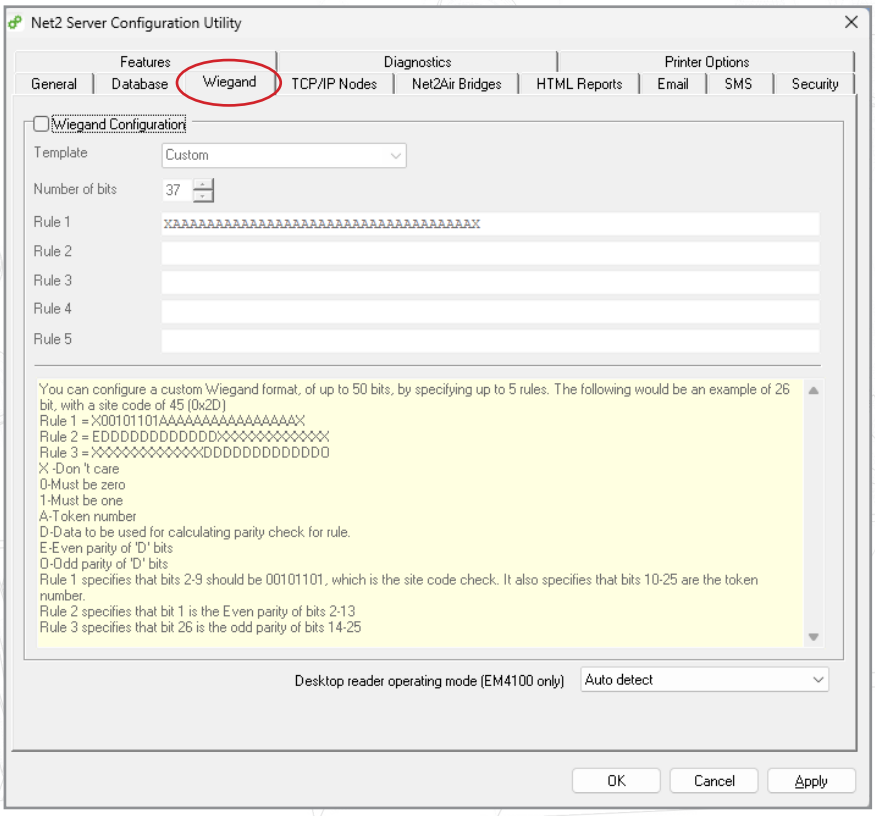
Setting up Net2

All ACU's that will have HID® readers connected need to be setup to be in Wiegand Custom mode.

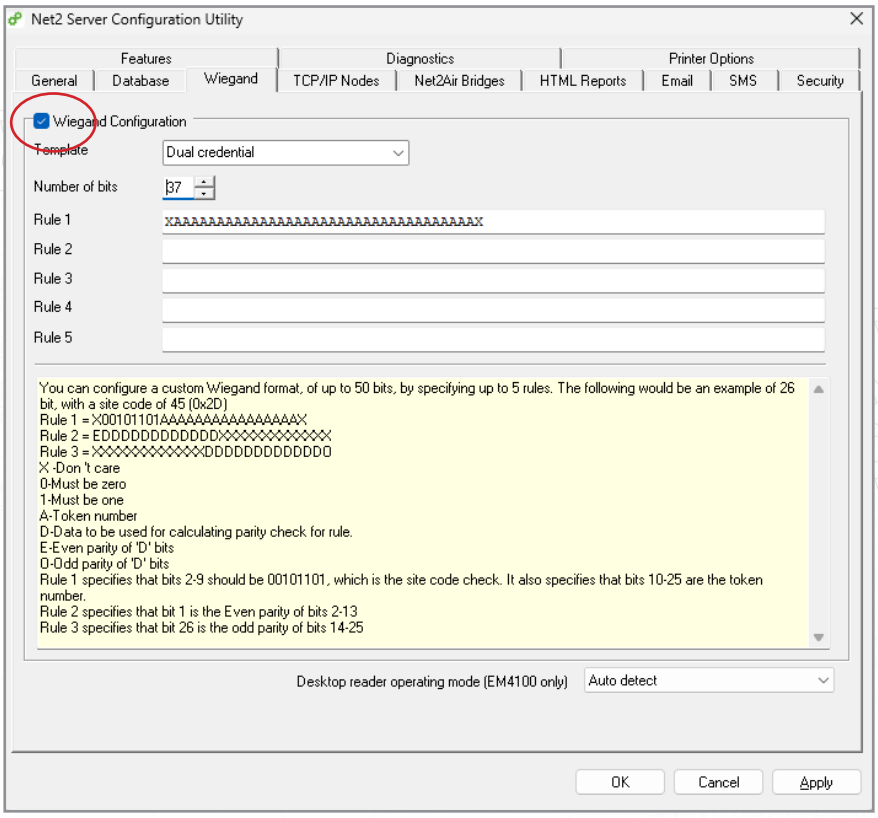
Note for Paxlocks: If Paxlocks using older versions of firmware are reset, a standard Paxton token, that is valid on the system, will need to be used to bind the Paxlock to the Net2 system, the HID® tokens cannot be used until you have updated to v6.9.

Wiegand rule setup

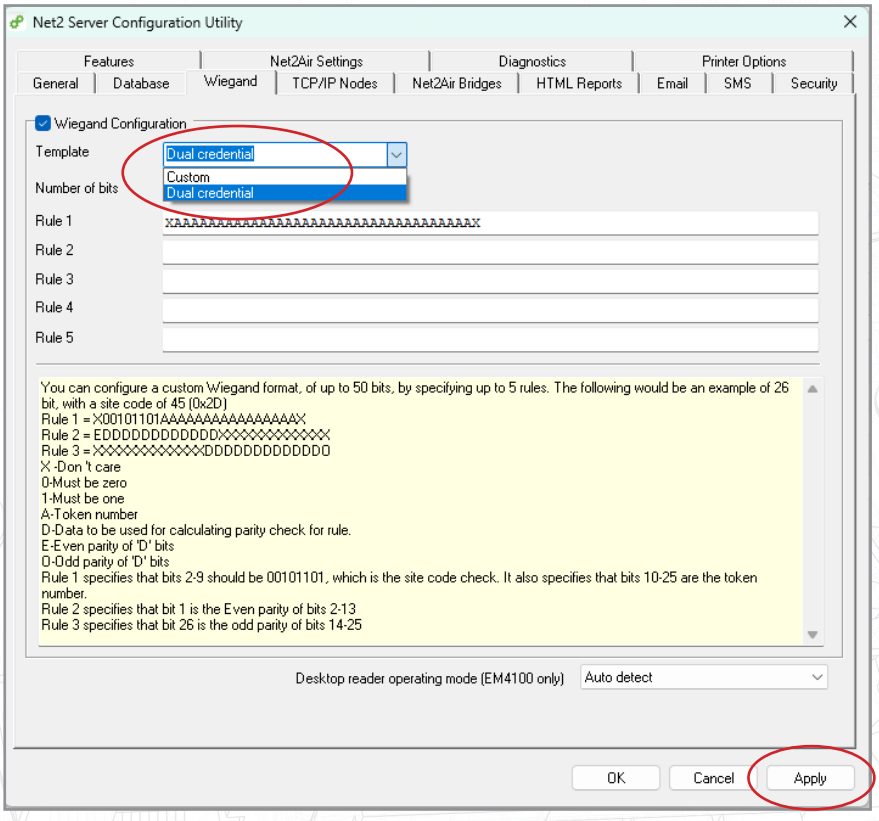
1. Login to the Net2 server Configuration Utility
2. Click on the **'Wiegand'** tab



3. Enable **'Wiegand configuration'**

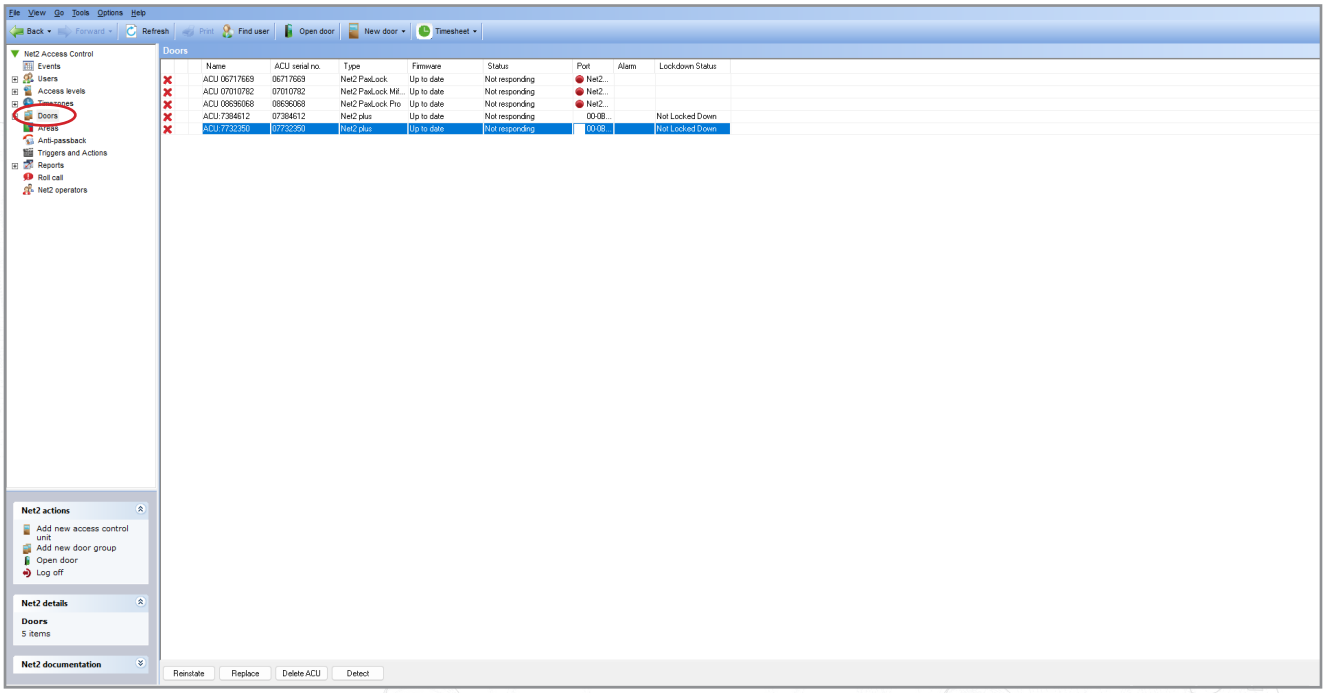


4. Click the **'Template'** drop down, select **'Dual Credential'** and click **'Apply'.**

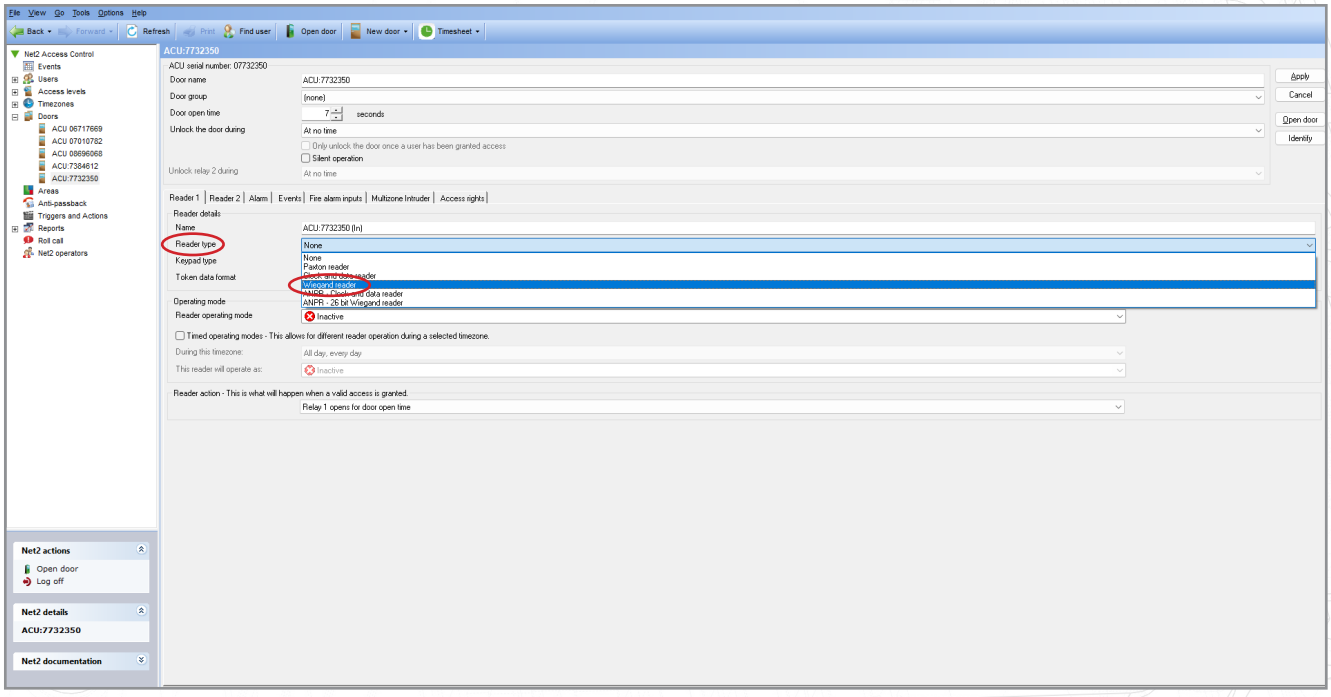


Setting up the doors

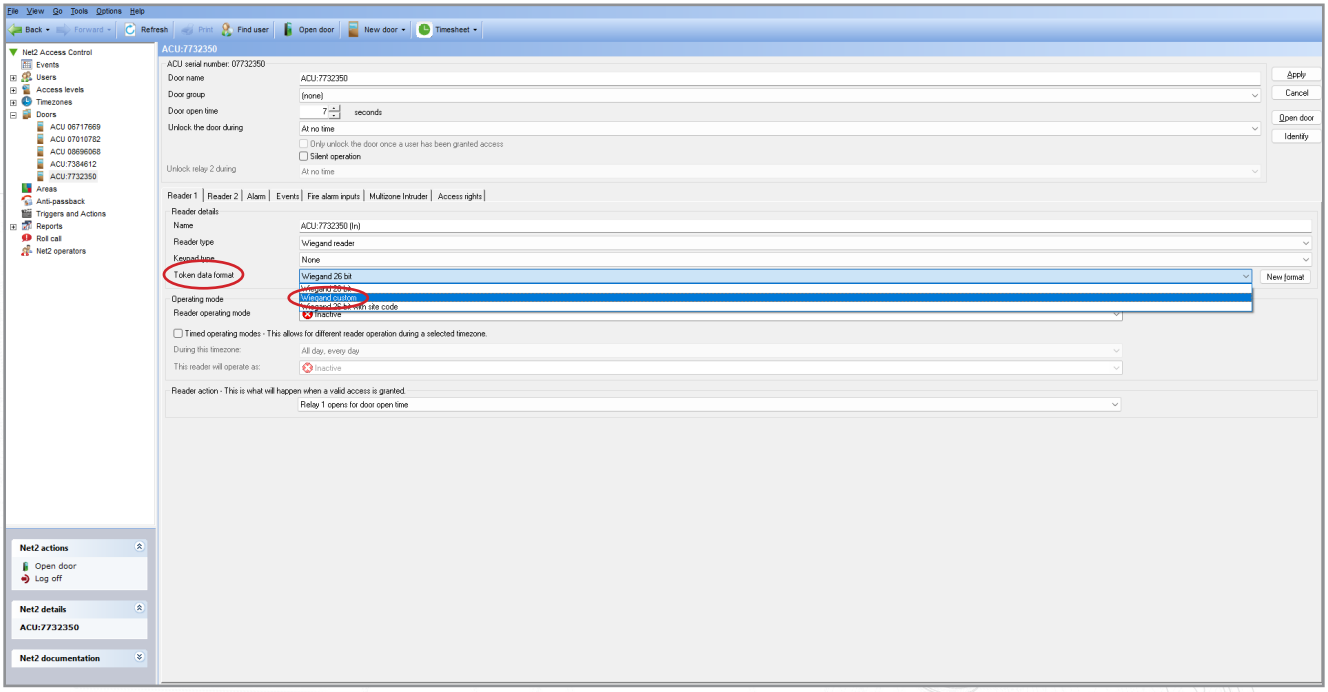
1. Login to the Net2 and select a **'Door'**



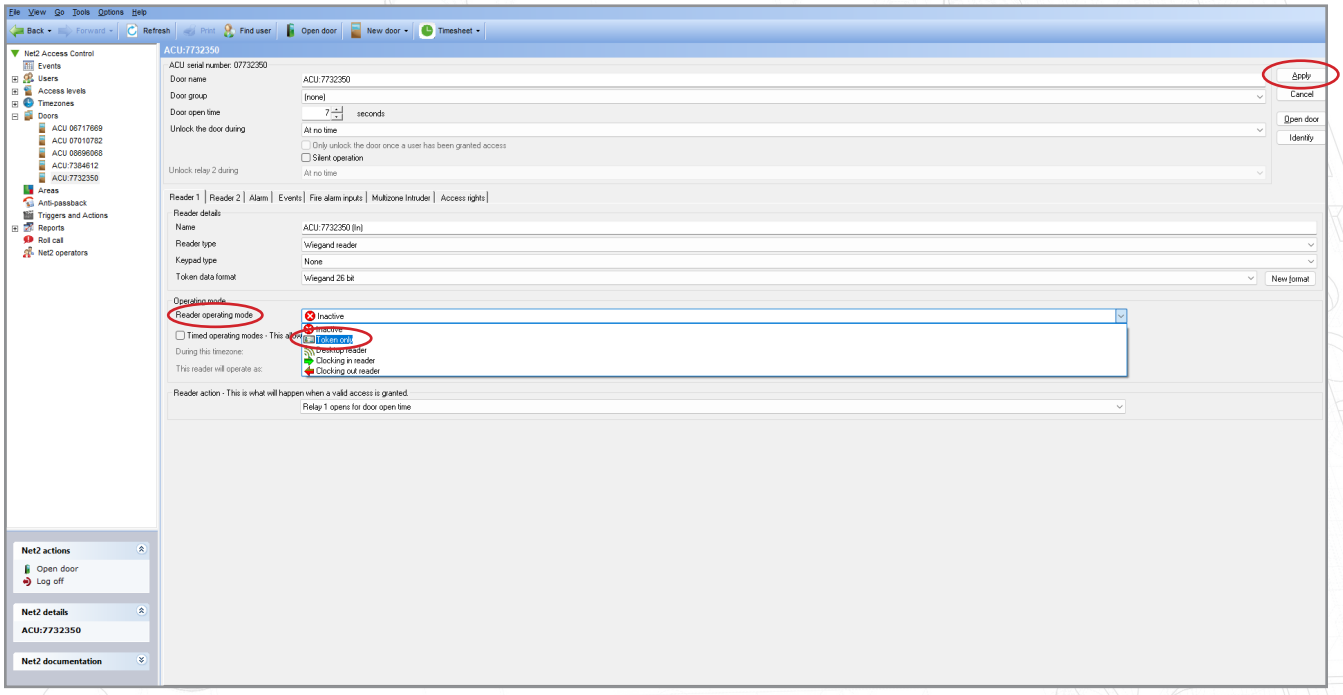
2. Change reader type to **'Wiegand reader'**



3. Change Token data format to **'Wiegand Custom'**



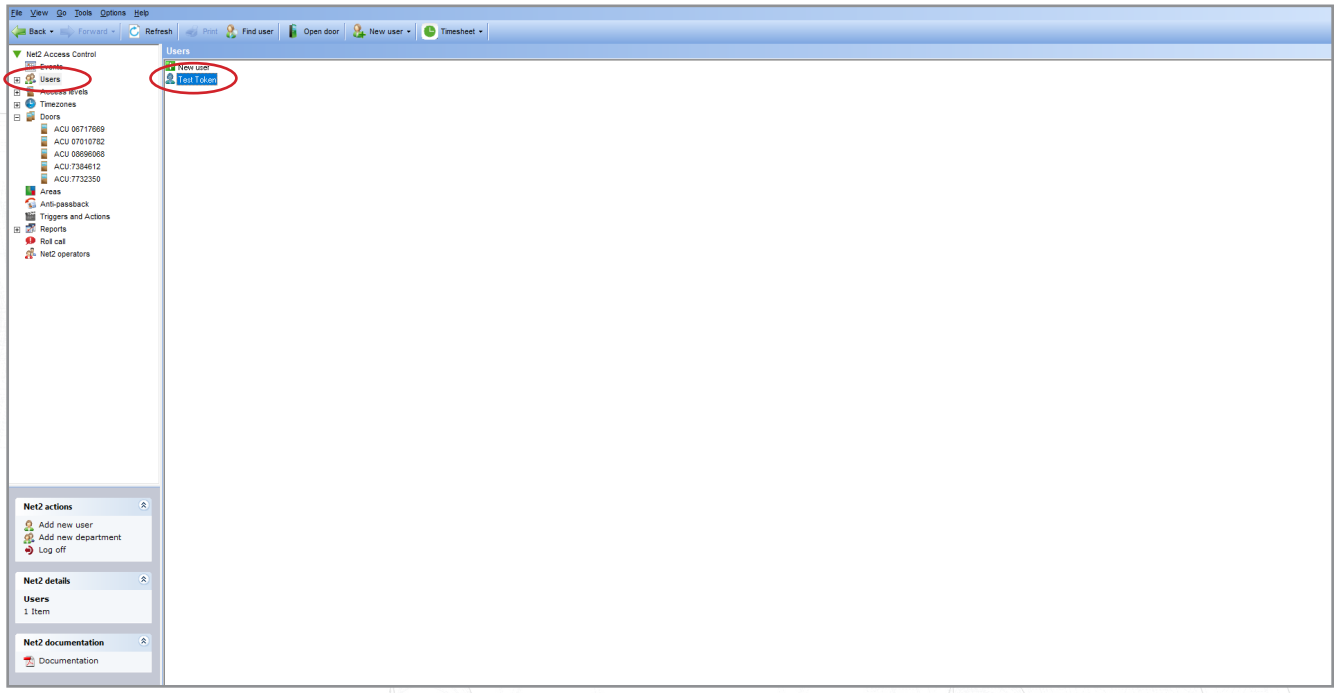
4. Change reader operating mode to **'Token only'** and click **'Apply'**



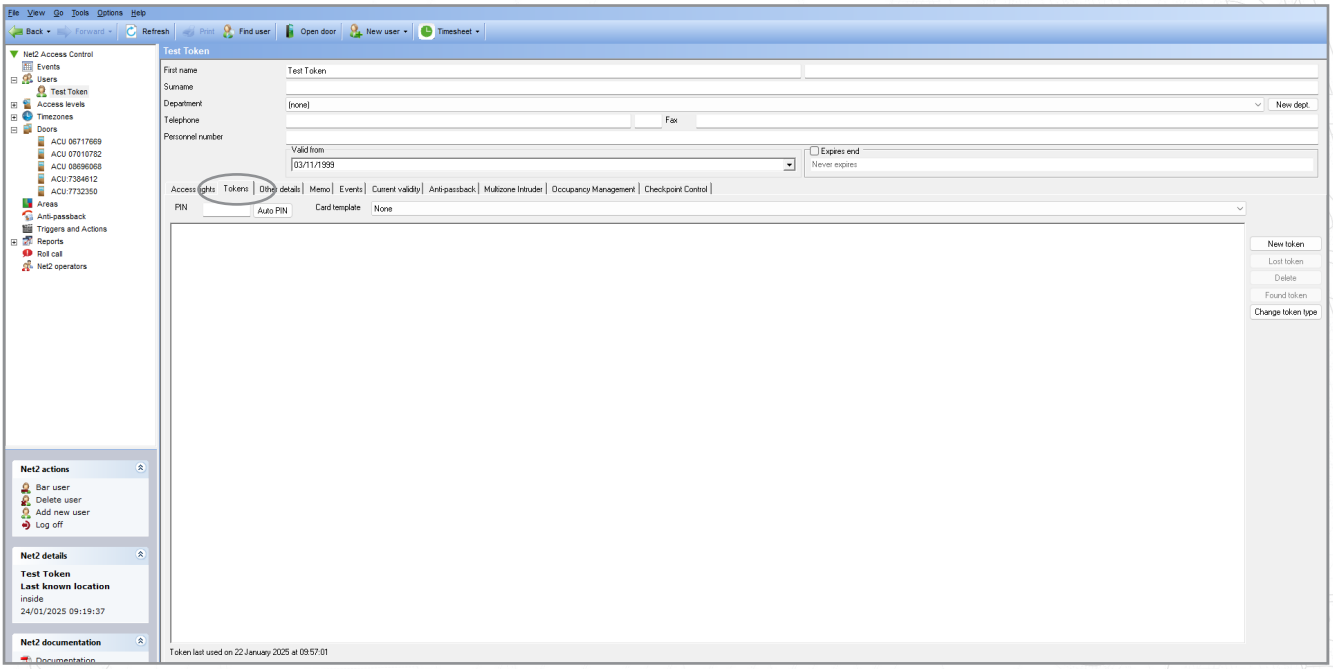
5. Repeat for all doors using HID® readers.

Enrolling tokens

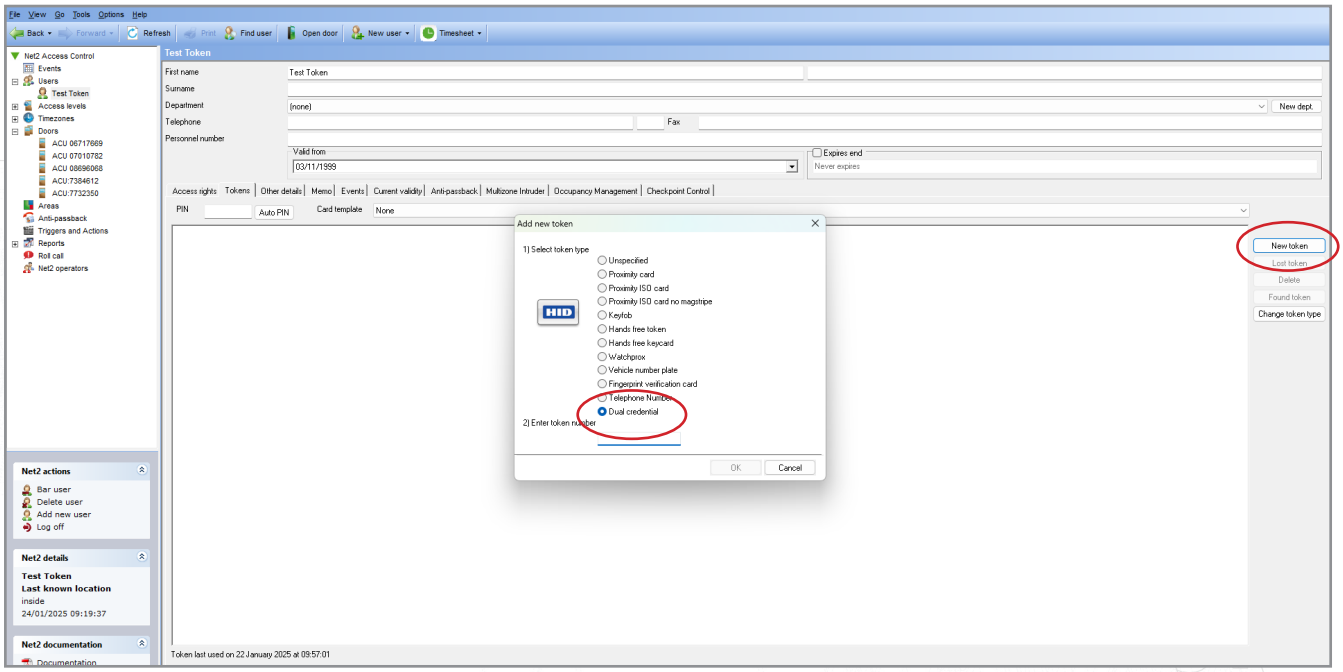
1. Select a **'User'** in Net2



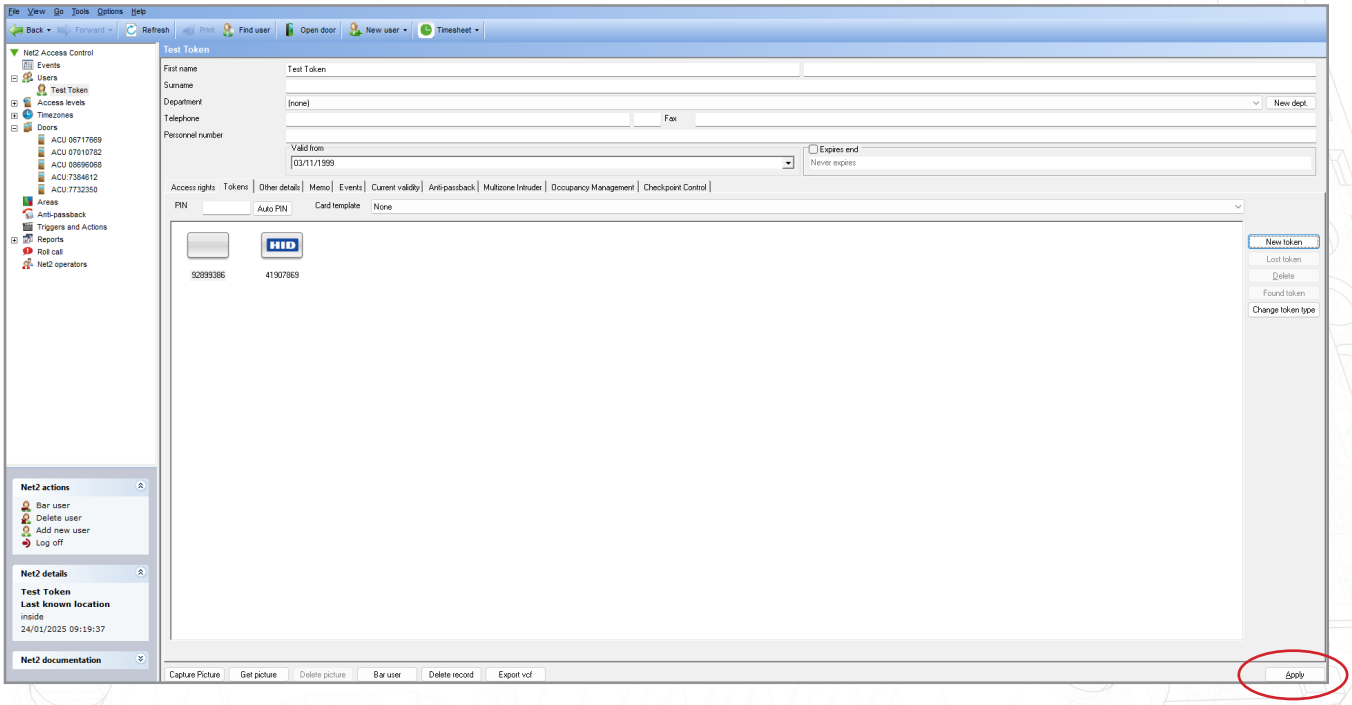
2. Click on the **'Tokens'** tab



3. Click **'New Token'** and select **'Dual credential'**



4. Present a HID® token to the desktop reader
5. Two tokens will be added to the user record. Click **'Apply'**.



Operation

When a credential is presented to an HID® Signo™ reader, the secure value is read from the token. When the same token is presented to a Paxlock the UID is read. As both values have been enrolled against the same user, access is granted in both cases.