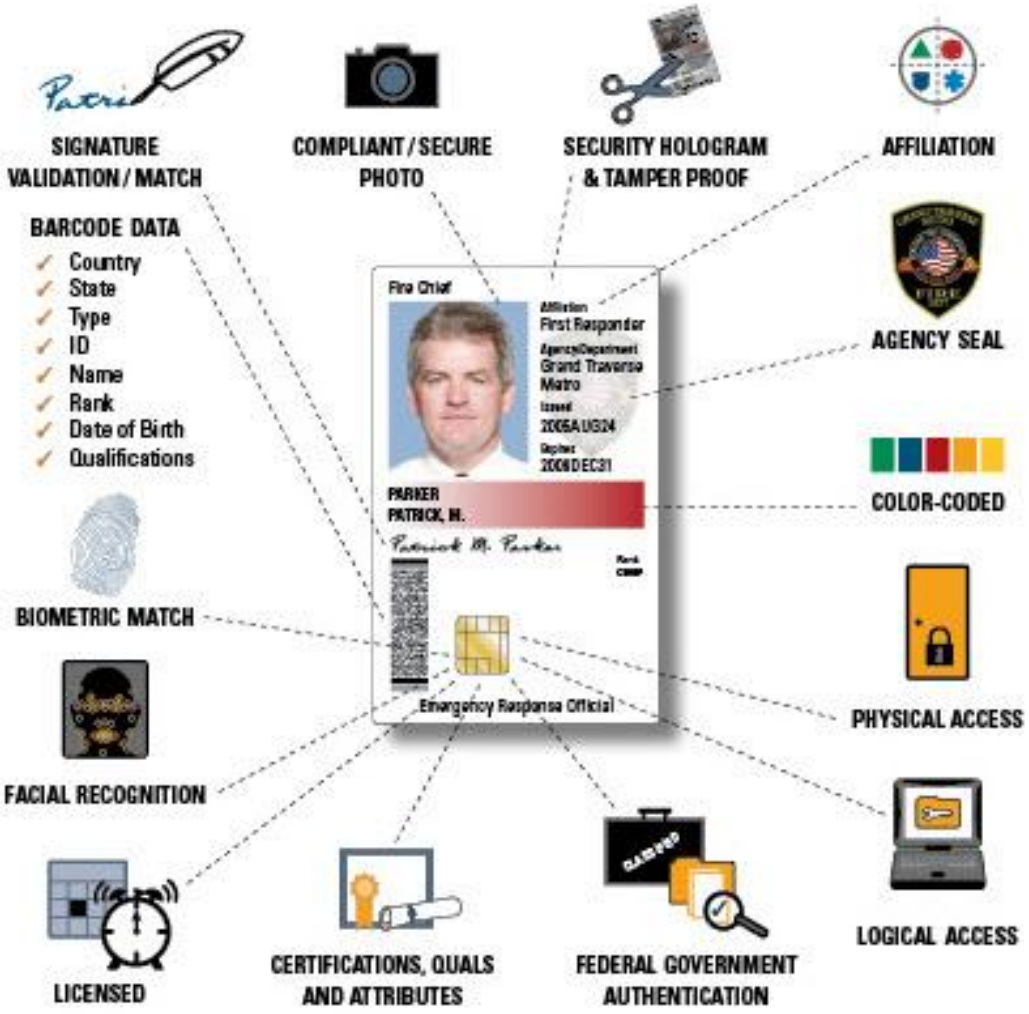
Enrolling with PIV and PIV-I

Velocity Enrollment Manager



Overview

The Homeland Security Presidential Directive 12 (HSPD-12) called for a common identification standard to be adopted by all Federal Government Agencies.
The Person Identity Verification (PIV) credential has been issued to over 8 million Federal employees (almost four million people). The PIV credential is a smart card operating at 13.56 MHz with a specific data module called End-Point. Certain data is available by a “free read”, while other personal data requires a personal (secret) PIN (personal identification number) to access (for example the required biometric fingerprint data).

PIV card users can utilize their cards in Physical Access Control Systems (PACS) in a number of ways based on the required level of assurance at the specific locations they are permitted to access. At the lowest level of assurance a “free read” of the Card Holder Unique Identifier (CHUID) data object, and at the highest level of assurance, a multi-factor authentication using Public Key Infrastructure (PKI).

The CHIUD contains a Federal Agency Smart Credential Number (FASC-N), which is used to enroll a user in Velocity, providing a unique credential number for use in the Physical Access Control System (PACS). In a PKI implementation, the FASC-N is used but the certificates on the card (the card certificate in the case of “contactless” CAK and the Person Certificate in the case of contact “PAK”) are used to validate the card and user.

For Government contractors, cards are issued with the same card data module, and the same CHUID, however the first three fields of the FASC-N contain only “9’s”. These cards are called PIV-I (interoperable). Correct implementation of these cards requires the PACS to utilize the Universal Unique Identification (UUID) number rather that the FASCN. PIV-I cards include the PKI certificates that enable the CAK/PAK schema.

Velocity provides the ability to enroll PIV cards on HIRSCH PACS with the appropriate read and MATCH custom settings.

The following pages will assist in establishing the devices and Enrollment Manager Settings to enroll the PIV and PIV-I cards into the Velocity system.

To have the **PIV** read into the Velocity access control system the following setups need to be established.

1. **Create the following User Defined Fields in Enrollment Manager.**

- Name Parsing — Text
- Agency Code — Number
- System Code Credential Number — Number
- Credential Series — Number
- Individual Credential Issue — Number
- Person Identifier — Number
- Organizational Category — Number
- Organization Identifier — Number
- Person Org Assoc Category — Number
- Expiration Date — ***Date***

- *Locate under Enrollment Manager > Tools > User Defined Fields….*

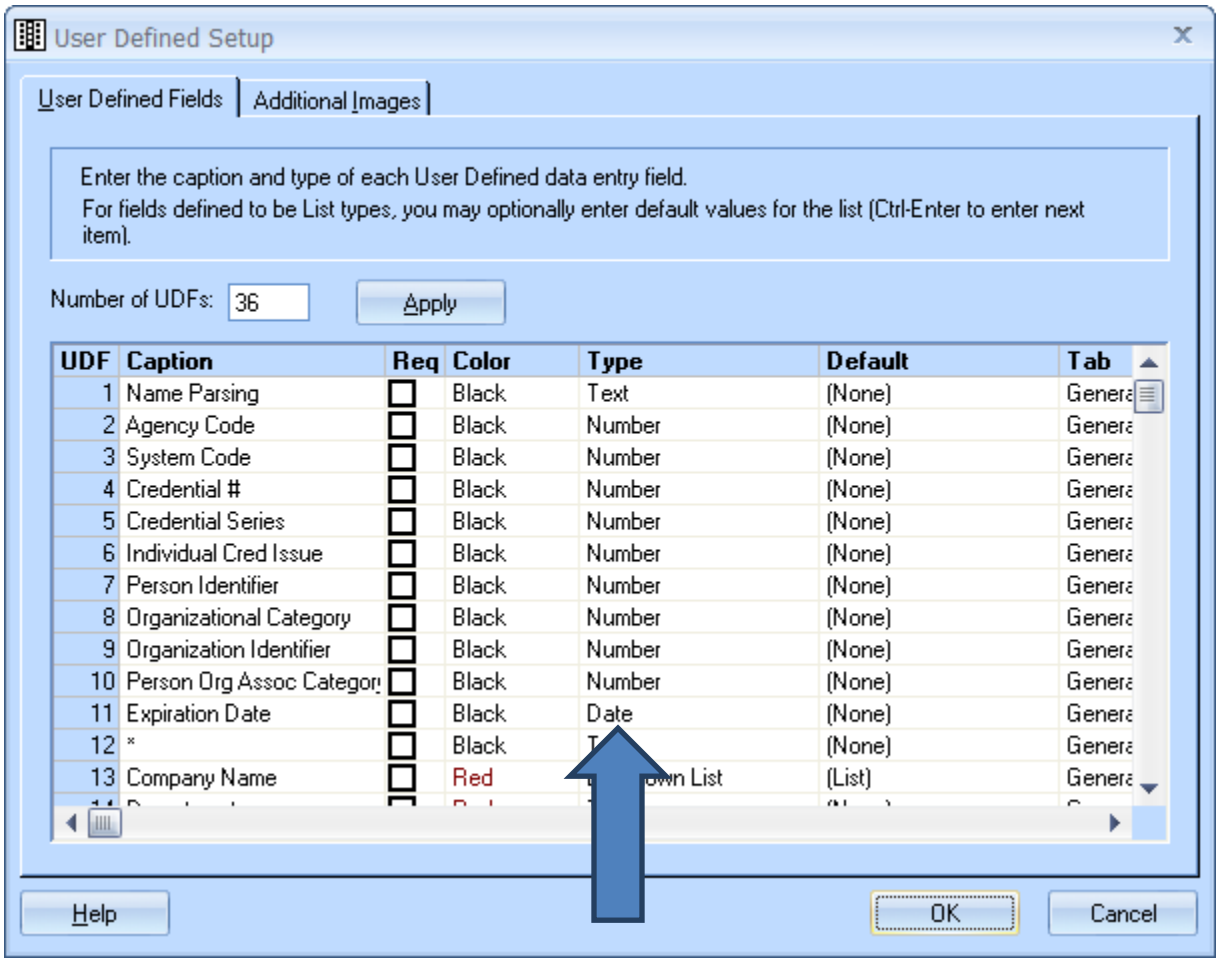


Figure 1 - User Defined Fields

2. **For PIV the Name field must be Parsed, split between First, Middle and Last Name.**

- Properties Enrollment Manager Tools > Preferences
- Change the UDF Name Parsing field to the UDF defined.

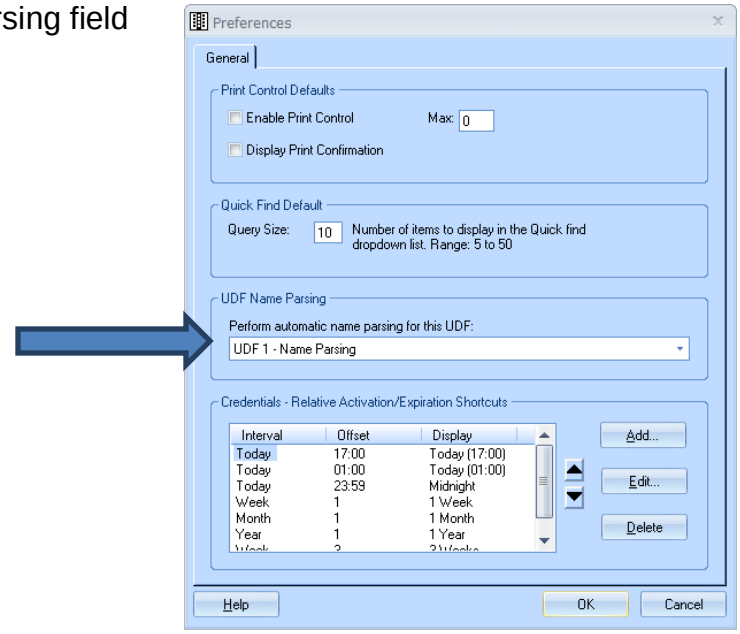


Figure 2 Enrollment Manager Preferences

3. **Establish the device for reading the card and install by USB. The driver for the device must be downloaded from the internet as Velocity does not supply the driver.**

   a. **SCR3310**
   b. **SCR3311**

Figure 3 - CRSCMCEUSB Card Reader

4. **The RUU device may also be used to enroll the PIV card. Be sure to have the correct firmware installed on the device using the Cogent software. This will allow for the addressing TCP/IP and will enable the choice for enrollment on the Device Configuration RUU tab.**

Figure 4 - RUU PIV version

5. **If an Enrollment Station is being used, the Special Handling needs to be established under Device Configuration. Enrollment Manager > Tools > Device Configuration > Credential Enrollment**

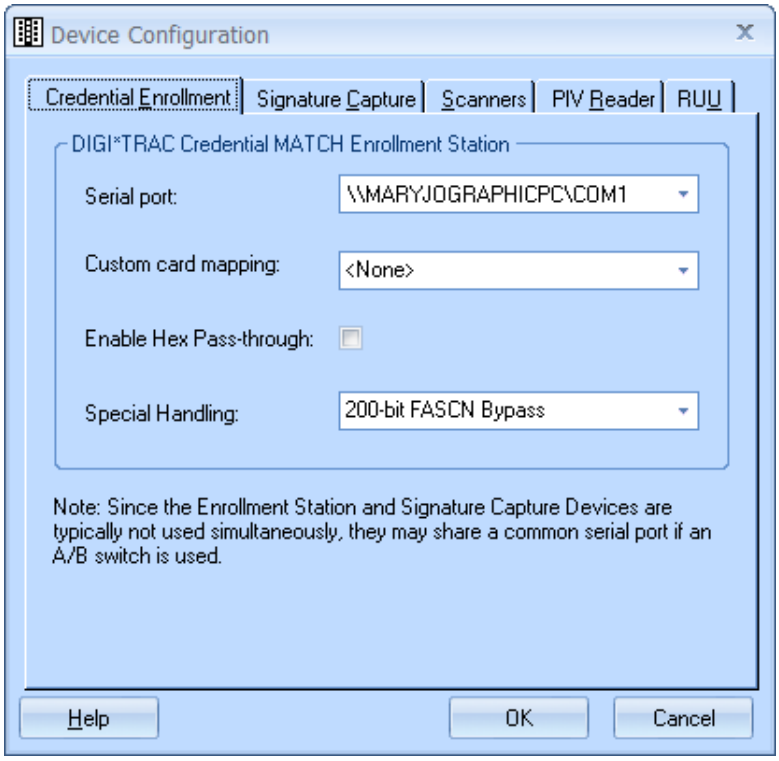


Figure 5 - Device Configuration Special Handling

Note: The reader used for the enrollment must have the MATCH custom settings as well as the correct firmware for the data to pass correctly into the Enrollment Manager Fields.

6. **Select Enrollment Manager Tools > Device Configuration and map the UDF fields to each device used for card reads.**

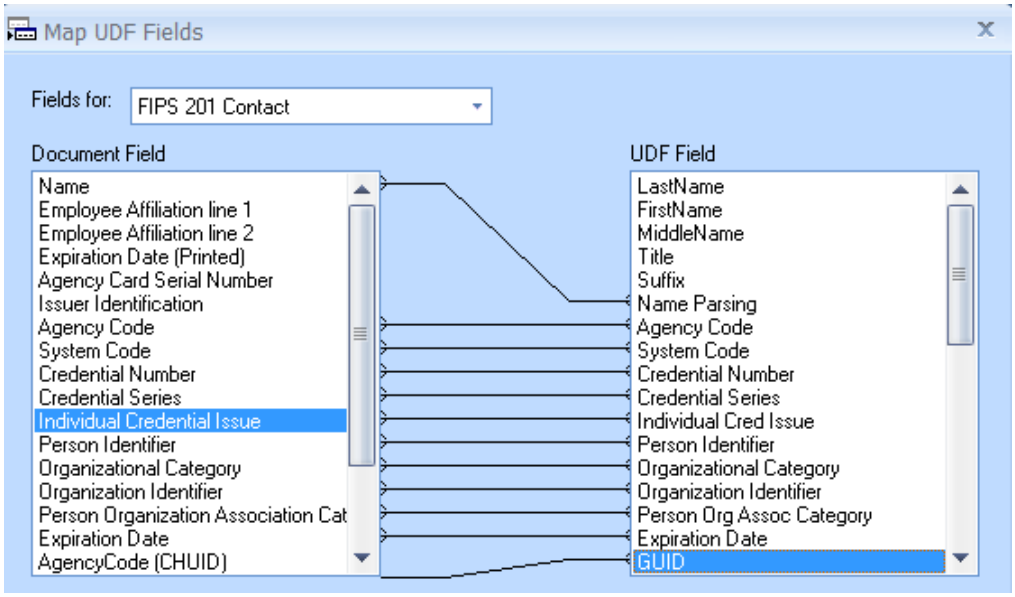


Figure 6 UDF Field Mapping for Enrollment – Click and Drag to UDF Field.

Note: For PIV-I cards, the UDF Field of UUID/GUID is the only field that is necessary to map for credentialing. This field will need to be added to the UDF Fields if both types of cards are being enrolled into Enrollment Manager if previously not added.

Enrollment Manager > Tools > User Defined Fields – be sure to select Unique Text as the UDF type.

7. **Close and reopen Enrollment Manager. There should now be a scan button**
8. **Select Add Person and select the scan button.**

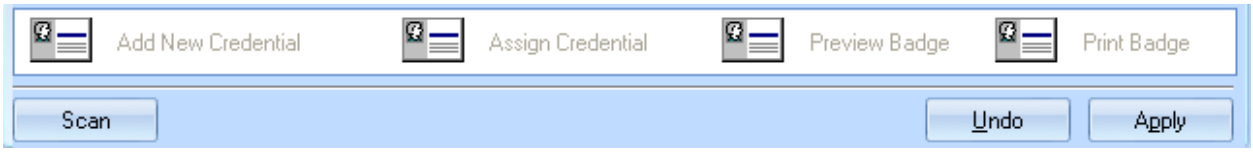
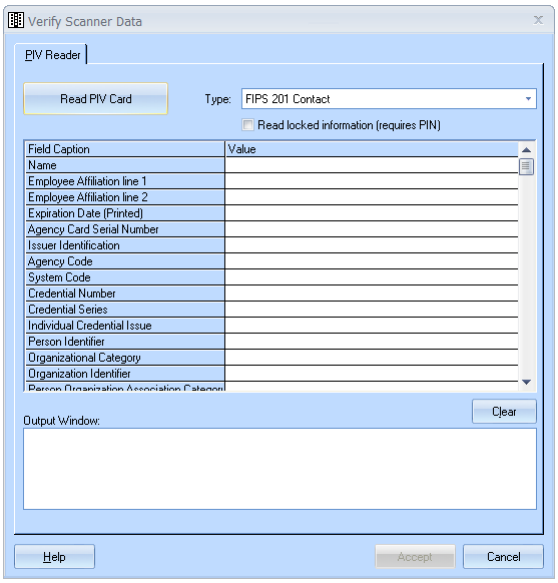


Figure 7 - Card Reader PIV

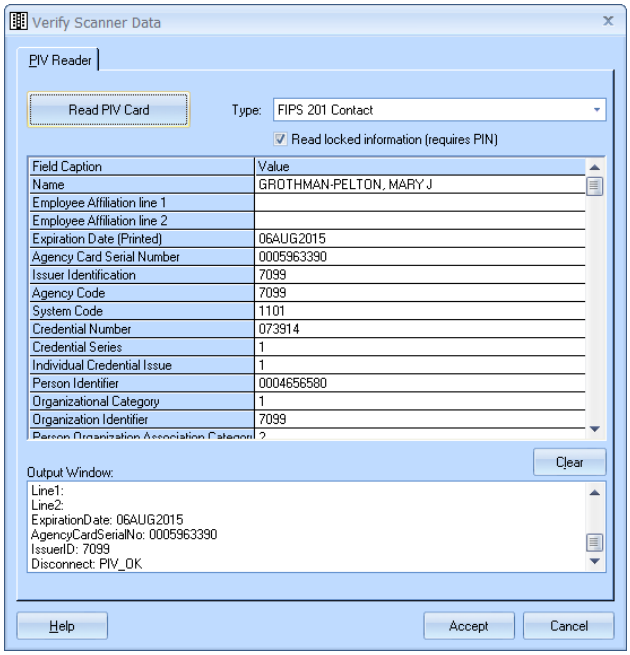
Figure 8 Users PIN code to unlock data.

9. **Select the device to read the card if multiple devices are being used.**



10. **To read all the fields, the card holder will need to enter their PIN to unlock the card. This applies to both PIV and PIV-I card. Once OK is selected, the card will read and the fields will show the data.**

[Give it a few seconds, and the data will fill in the fields above, and also the output window.]

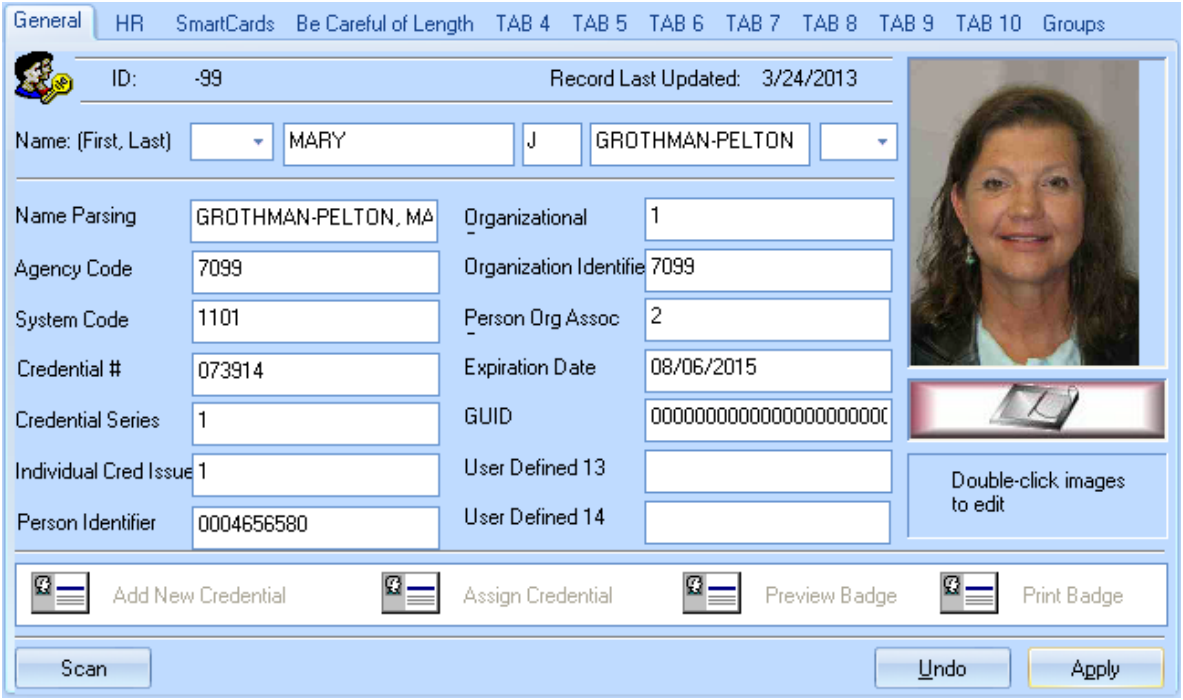


.

11. **Click Accept for the data to populate the UDF fields in Enrollment Manager.**

Figure 10 Scanned Data from PIV/TWIC Card

Figure 9 Enrolled TWIC from Scan Note the UUID/GUID is all zeros.



12. Click Apply to download. You are now ready to issue a credential.

For PIV Credentials - 200 bit FASCN

13. Add New Credential

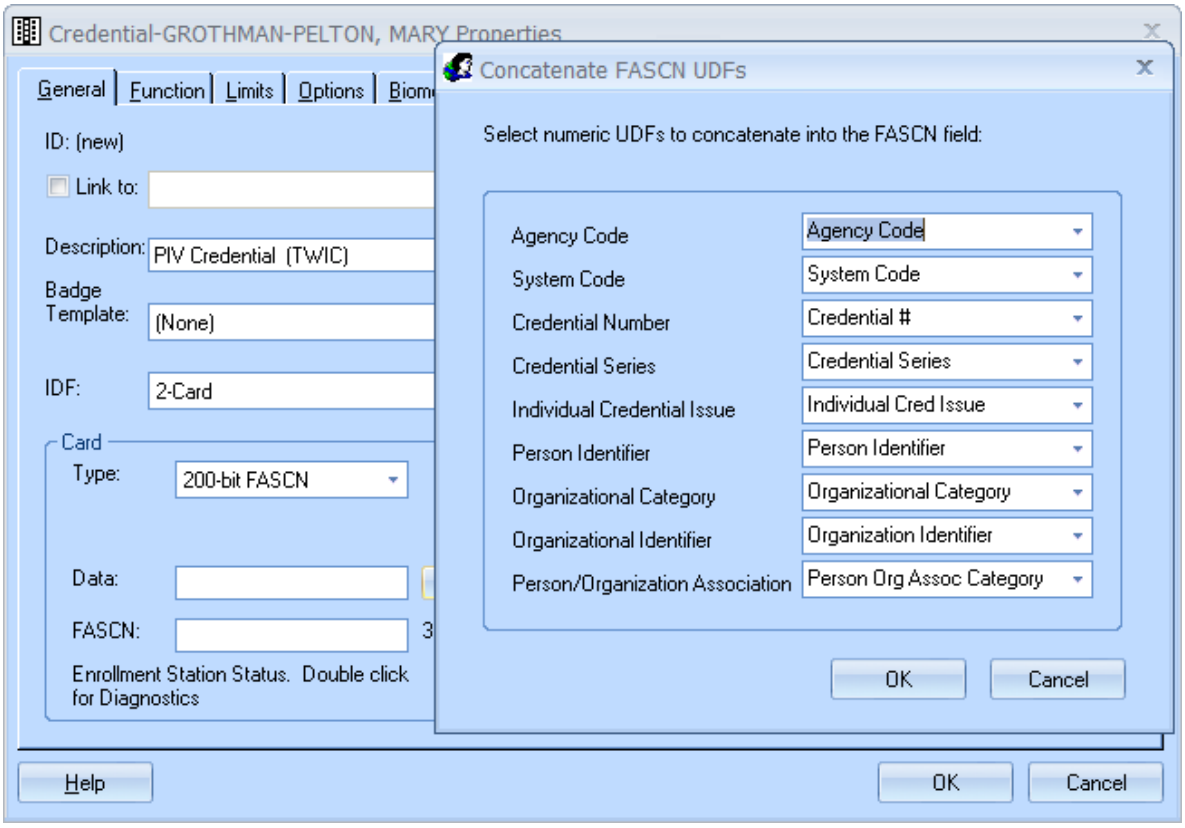
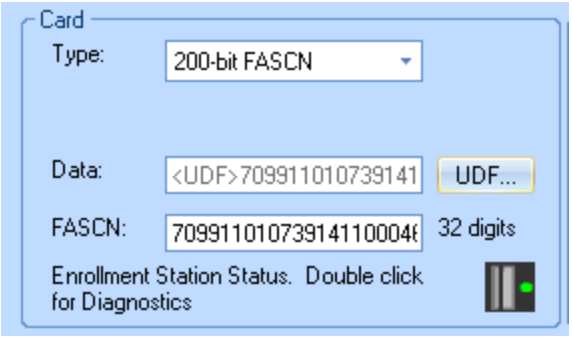


Figure 11 - Add New Credential - UDF MATCH

Note: The PIV and PIV-I cards may use IDF 2 for use with just the card presented at the reader. If any other IDF is selected, a PIN will be required. This should never be the secret PIN that the user has to unlock the data on the card.

The 200-bit FASCN will populate the UDF concatenate window. Select the corresponding UDF fields created and click OK. This will produce the FASCN that will be used for the card read.



To locate the UDF concatenate window, select the UDF…button on the Data field.

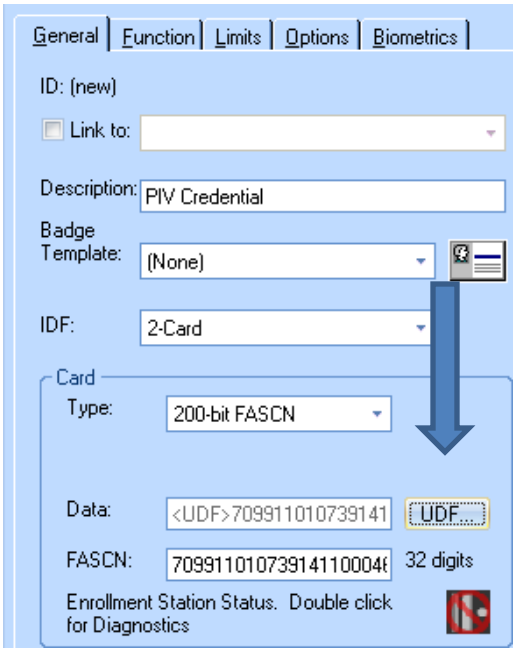


Figure 13- FASCN Assignment

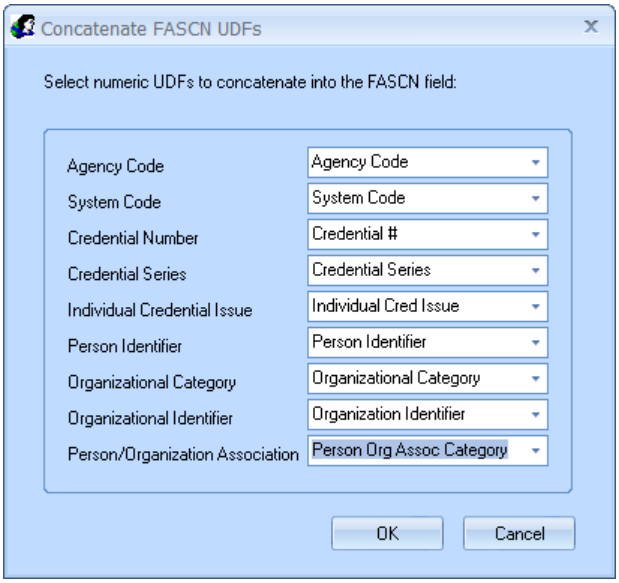


Figure 12 UDF button on Credential General Tab

This will supply a 32 digit number in both the Data field and the FASCN field.

Select the Function Tab and assign the appropriate Door Group for this individual.

- All Limits
  - Threat Authority and 2 –Person Rule may be assigned
- Options
  - Special Needs Access and Passback Executive Override may be assigned
- Click OK and the PIV credential has been issued.
- Verification of download may be seen in the Event Viewer.

For PIV-I Credentials

The UUID/GUID is the unique text that is used for the credential.

Using the contact reader, the card will be read just like the PIV card, with the addition of the UUID.

To read all the data the card holder will also need to enter their PIN number.

NOTE: The PIV-I card has 9999 instead of a Government Agency Code.

Assign a Door Group function and any Limits or Options for this credential.

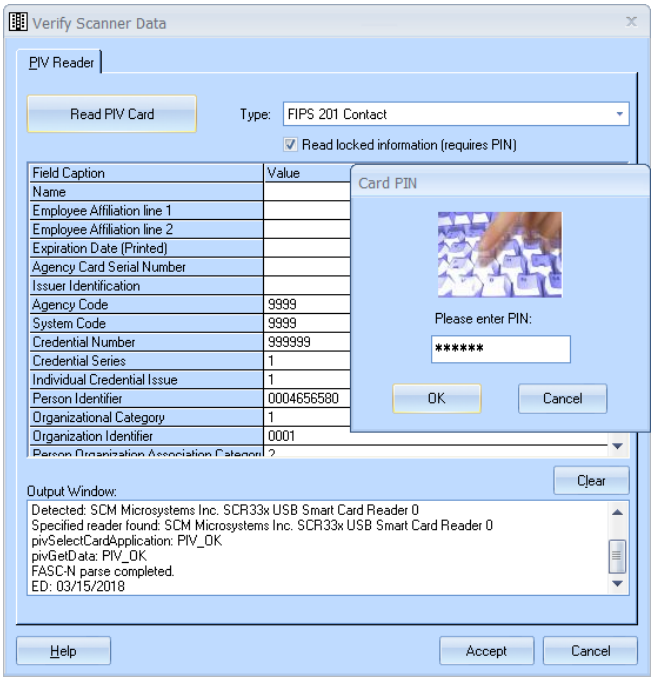
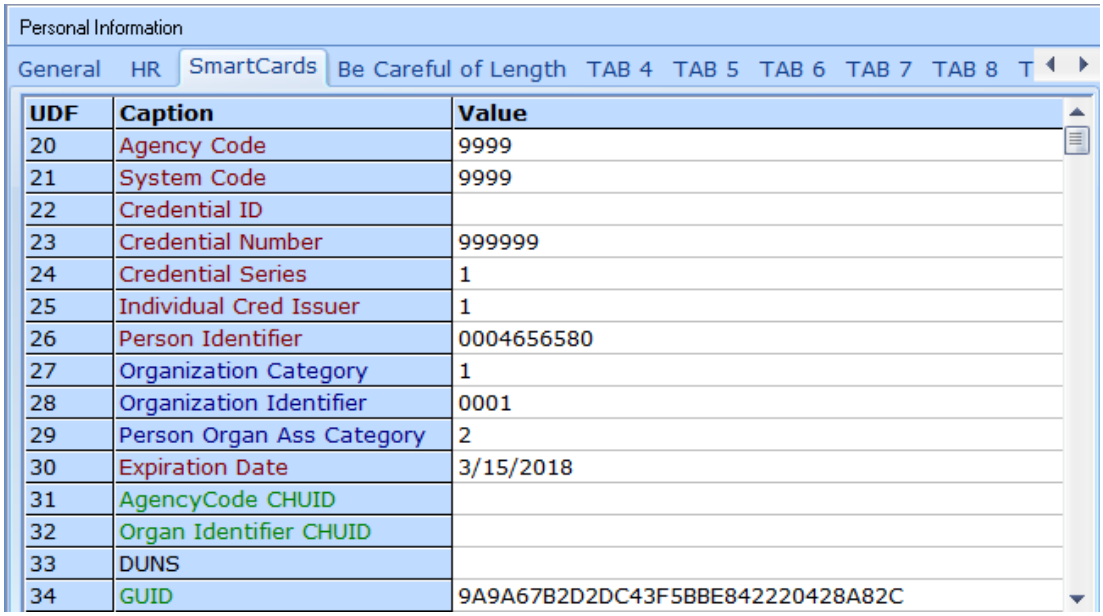


Figure 14 - PIV-I card with PIN



UDF	Caption	Value
20	Agency Code	9999
21	System Code	9999
22	Credential ID	
23	Credential Number	999999
24	Credential Series	1
25	Individual Cred Issuer	1
26	Person Identifier	0004656580
27	Organization Category	1
28	Organization Identifier	0001
29	Person Organ Ass Category	2
30	Expiration Date	3/15/2018
31	AgencyCode CHUID	
32	Organ Identifier CHUID	
33	DUNS	
34	GUID	9A9A67B2D2DC43F5BBE842220428A82C

Figure 15 The UUID/ GUID will have numbers and letters.

.Door Properties - PIV

- **HID iCLASS reader with 200 bit firmware** – using a MATCH2 set with Custom 27-28 - 29
- Entry Reader Setup Tab – Special Handling- 200 bit FASCN Bypass

- Present PIV card and access granted.

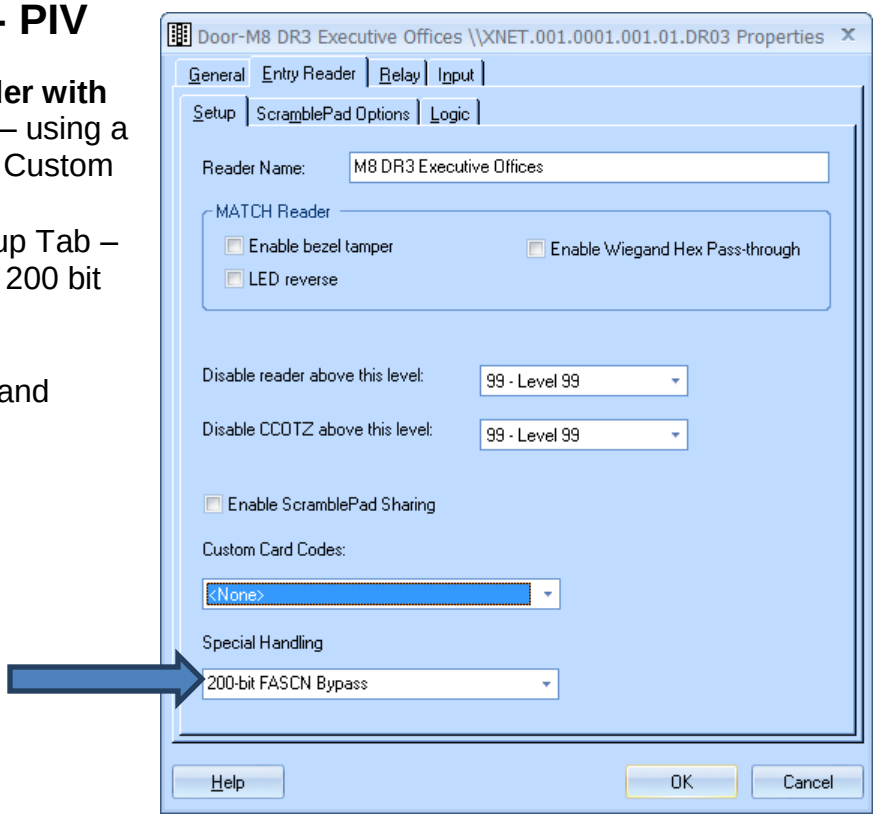


Figure 16 - Entry Reader Settings

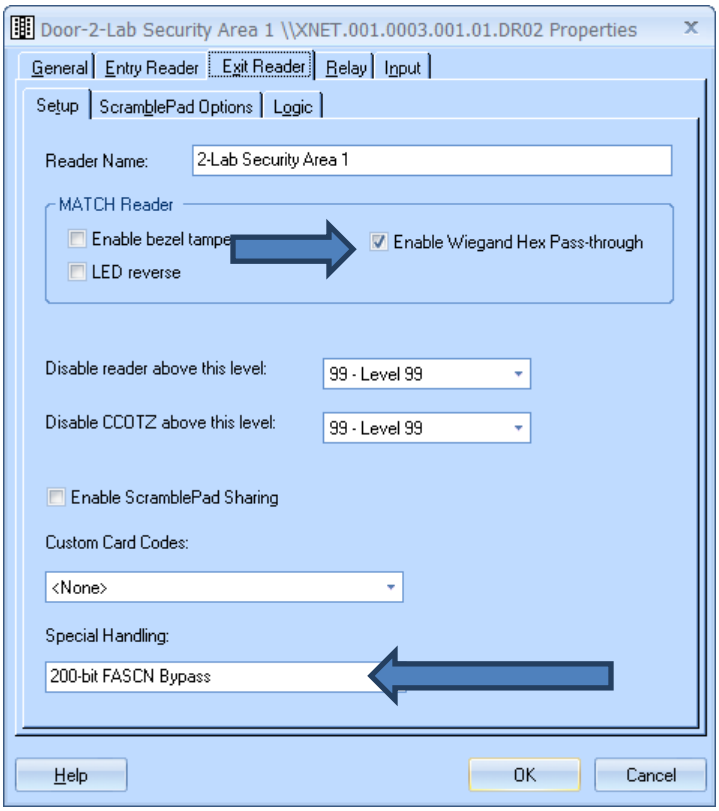
Note: MATCH special settings for the corresponding bit formats

- **64 bits – Custom 24,25,or 26**
- **75 bits – Custom 18, 20 or 21**
- **128 bits –Custom 18,20,21,24,25,26,27,28,and 29[PIV only]**
- **200 bits –Custom 27,28,or 29**

Note: Along with the MATCH custom settings, the firmware on the reader must also correspond to the bit format.

For PIV-I cards

- **HID iCLASS with 128 bit firmware** and MATCH2 with Custom 27-29
- The PIV-I card uses the FASCN Bypass to allow the UUID to be used
- Along with the Wiegand HEX Pass-through, the card reads the same at the door
- **The Door Properties** is different, using the **Enable Wiegand Hex Pass-Through** to enable the UUID/GUID to pass through
- Presented to the reader, the PIV-I card will issue an access grant
- If the reader has the ability to read both formats, then the cards enrolled will read by presenting the card
    - If the Agency Code is all “9s” the reader will pass through the UUID



Velocity Enrollment Manager has all the ability to read both PIV and PIV-I cards. The trick is to make sure all the corresponding devices are established with the correct formats.

- Enrollment Station
    - MATCH Custom settings
    - Reader firmware
- Device Configuration
    - User Defined Fields to map the data
    - Name Parsing is PIV cards are being read
- Scanning the card
    - PIN needed for name field
- Door Properties
    - Reader settings