Accountability & Compliance Tools

Overview

By creating solutions to quickly locate crucial data, DSX has developed reports to assist in data compilation for audits in high accountability situations. Contained in this document are Access Levels by Reader, Card Holder Management Reports, Access Level History & High Security Area (HSA) Logging.

Access Levels by Reader (Device)

When adding or editing an Access Level, a 3rd tab indicates which Access Levels contain a selected Device. Data is displayed in a text box that can be copied and pasted into other applications for storage, printing, or emailing. This View streamlines the ability to locate Access Levels that contain a specific reader/device.

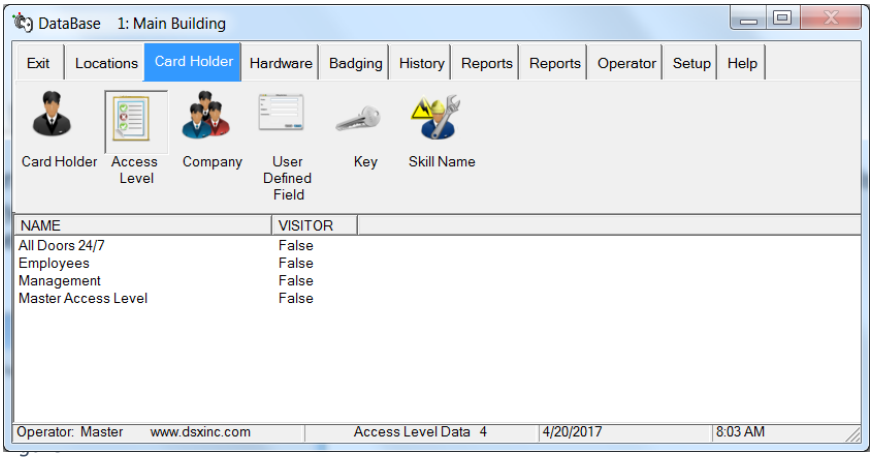


Figure 1: From DataBase
Select: Card Holder Tab
Select: Access Level
Then right click and select Add.

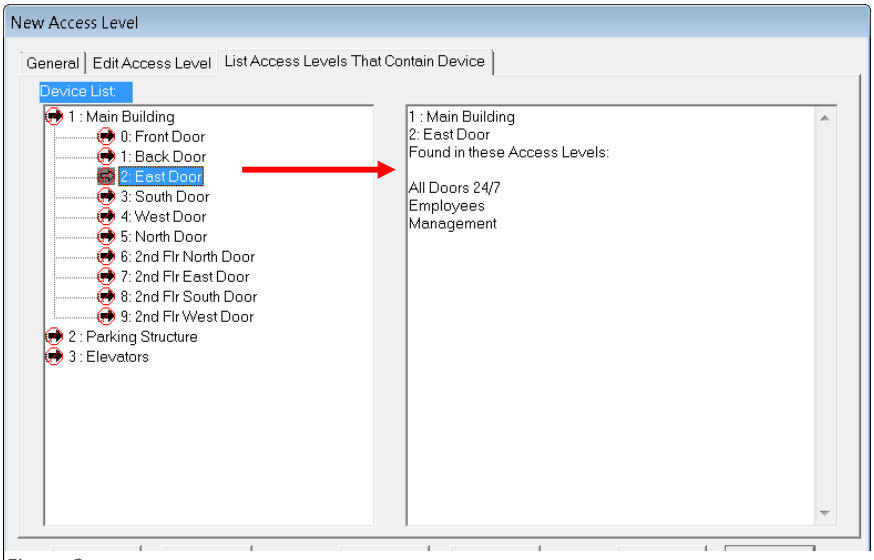


Figure 2

Figure 2: New Access Level Screen:
Tab: List Access Levels that Contain Device

The box on the left shows that Main Building Location Group has been expanded and Device 2 East Door is selected.

The box on the right shows the selections followed by all access levels that are active for this device:

All Doors 24/7
Employees
Management

Card Holder Reports: Management Reports

Card Holder data can be sorted by different criteria for audit and accountability purposes.

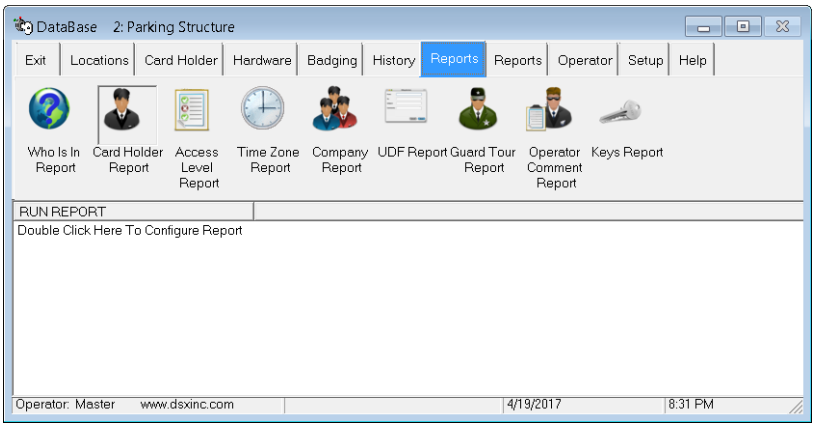


Figure 3 Selection of Card Holder Reports

From the Database program:

Select: Reports Tab

Select: Card Holder Report

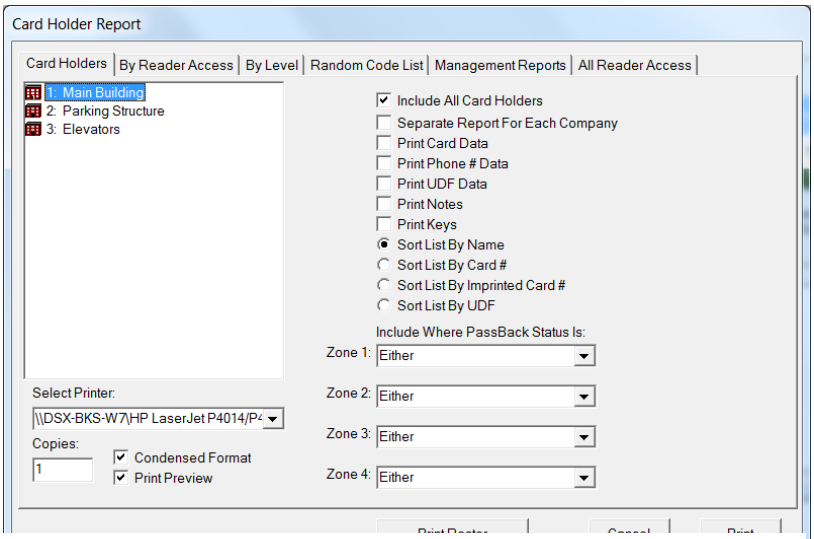


Figure 4 Card Holder Report Setup

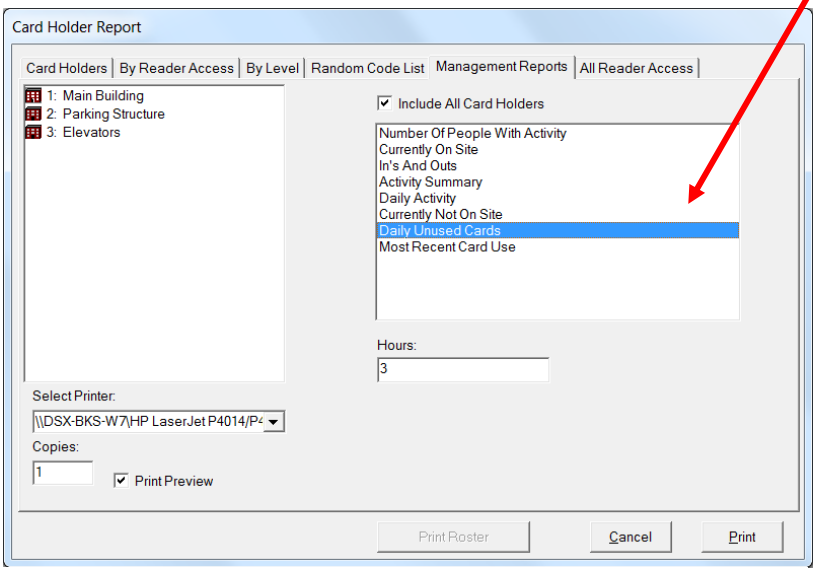


Figure 5 Daily Unused Cards Report Selection

Tabs Within Cardholder Reports:

Card Holder: Assembles Card Holders by Location with various search and sort criteria.

By Reader Access: Card Holders sorted by access to a specific reader.

By Level: Reports Card Holders assigned to a specific Access Level.

Random Code List: Generates Random Codes for keypad/ PIN applications.

Management Reports: A variety of Time & Attendance Reports. Daily Unused Cards & Most Recent Card Use require "Save Last Card Read" to be enabled in the DataBase program under Location on the "Yes/No Options Tab".

- **Daily Unused Cards**: *(Figure 5)* Cards not used within X Hours. Used to ascertain "Who is Not Here". In & Out readers are not required. Presented By Location and sorted by Company.

- **Most Recent Card Use:** Indicates last Card Use (time/date, location & Door) for each Active Card Holder selected. Presented by Location and sorted by Company.

ALL READER ACCESS REPORTS: Lists all Readers (Devices) accessible by Card Holder and the Time Zones that affect that access. By default, all Card Holders are included, *(Figure 6)* but by deselecting the box, the search engine allows search by Company, Name, UDF, or Card Number to narrow the results *(Figure 7)*. This could end up a Company or Department or an individual.

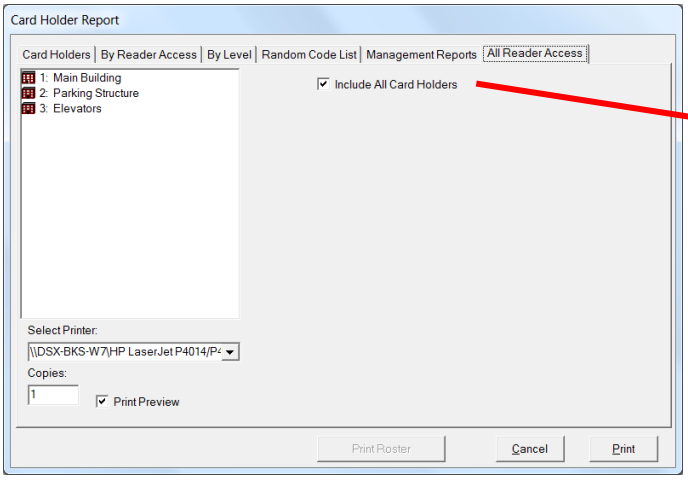


Figure 6 All Card Holders are included by default.

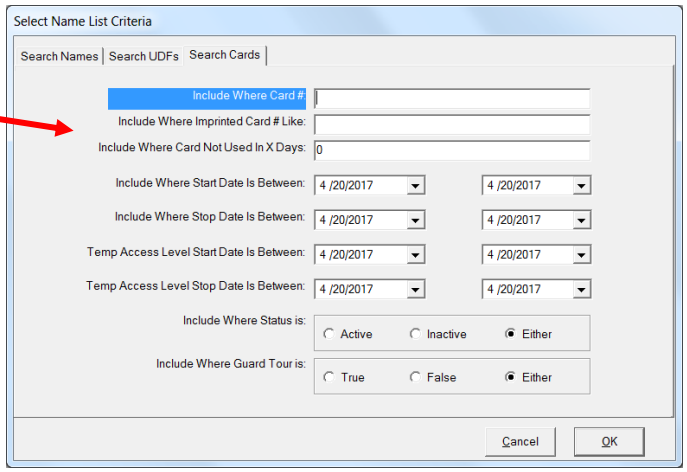


Figure 7 Search Engine Parameters

SAMPLE: DEVICE ACCESS REPORT FOR ONE CARD HOLDER

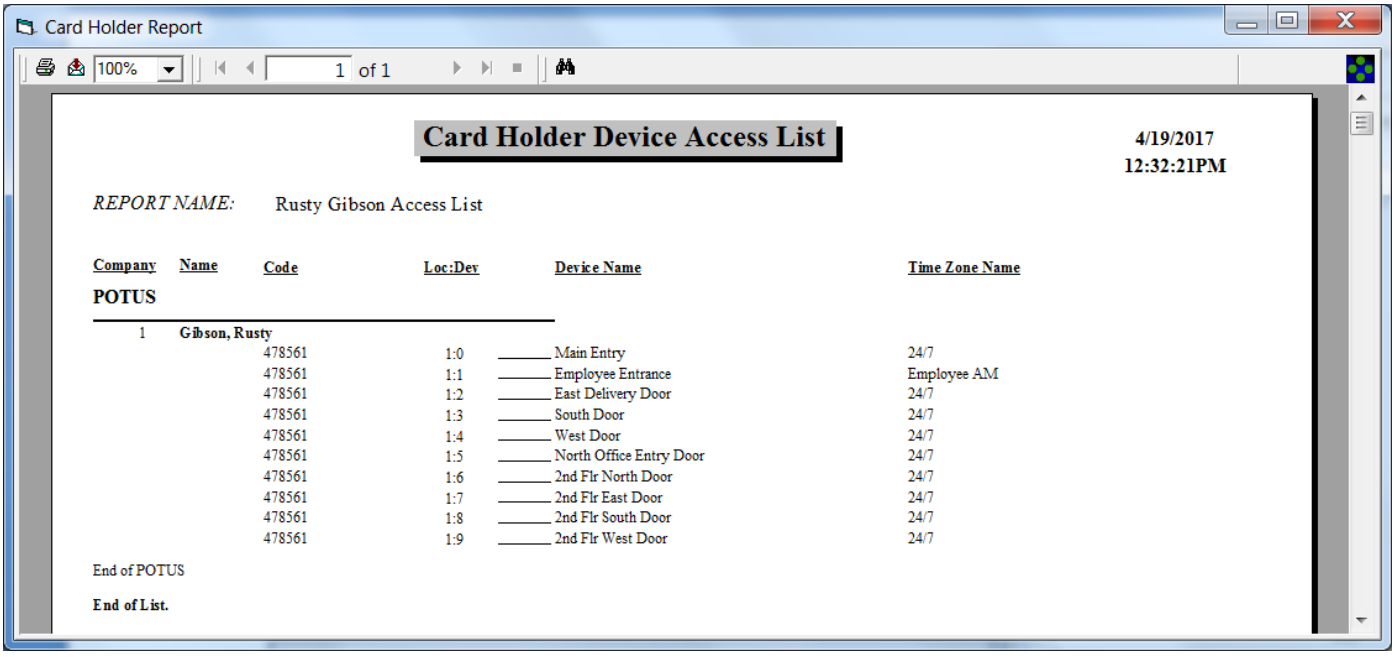


Figure 8 Sample Report

Access Level History

WinDSX SQL can create a log of all changes to Access Level assignments. Adding, removing, editing and changing definitions will create a log that can be searched and used for reports. This feature is optional and enabled by the DSX Softkey (dsxkeydata.xml).

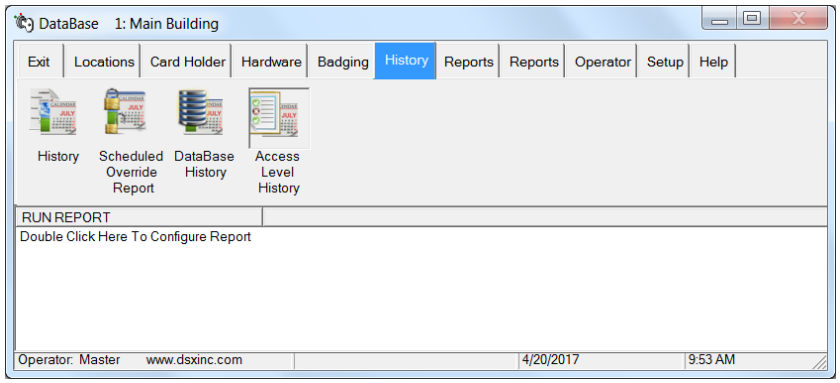


Figure 9: Access Level History is found on the History Tab in the DataBase program.

Figure 9 History Tab contains Access Level History

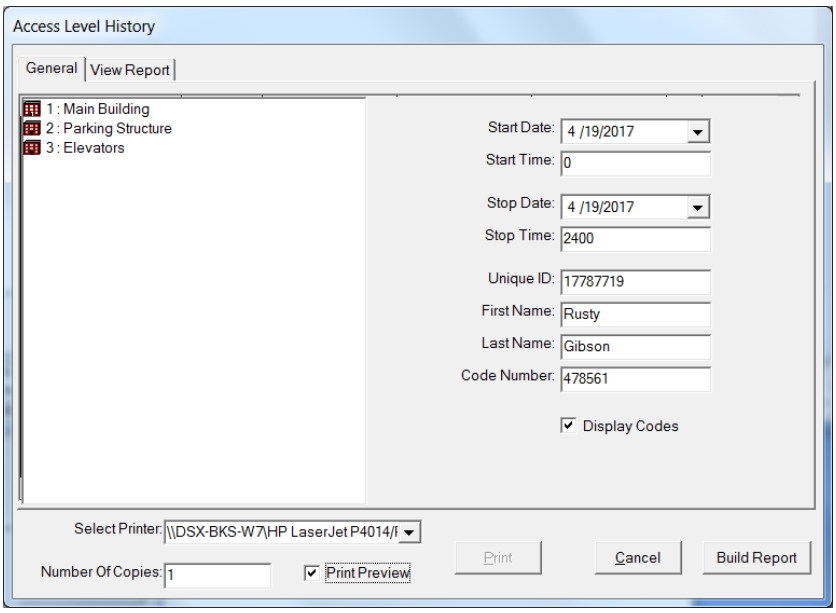


Figure 10: Parameters for the Reports:

- Card Holder- by name, card number or Unique ID (recommended). Using the Unique ID Number requires a UDF Field that has the Name ID attribute enabled.
- Start Date & Time
- Stop Date & Time

To configure the report:
-Enter Start Date & Time of audit period
-Enter Stop Date & Time of audit period
-Enter the Unique ID. Name or Card Number for the person of interest. If you want the card number to be displayed in the report, check the "Display Code" selection box.
-Select printer desired and number of copies.
Alternately, the report can be saved to a file.
-Select Print Preview to see the formatted report on screen
-Click Build Report.

Figure 10 Report Parameters

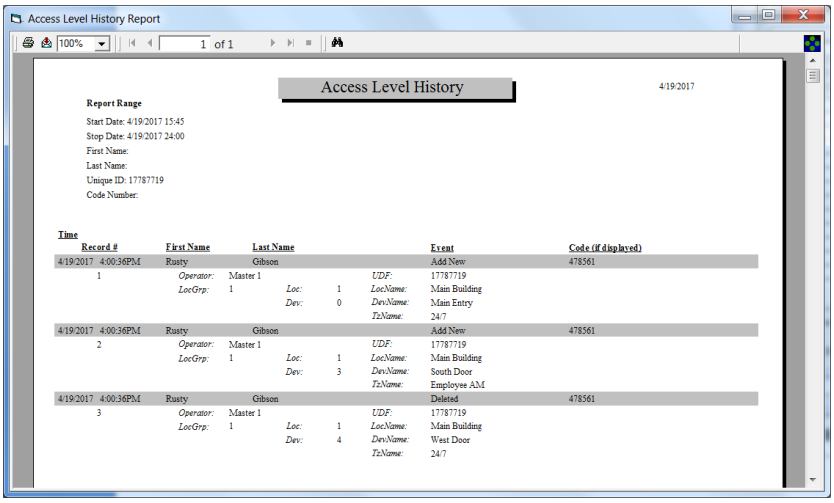


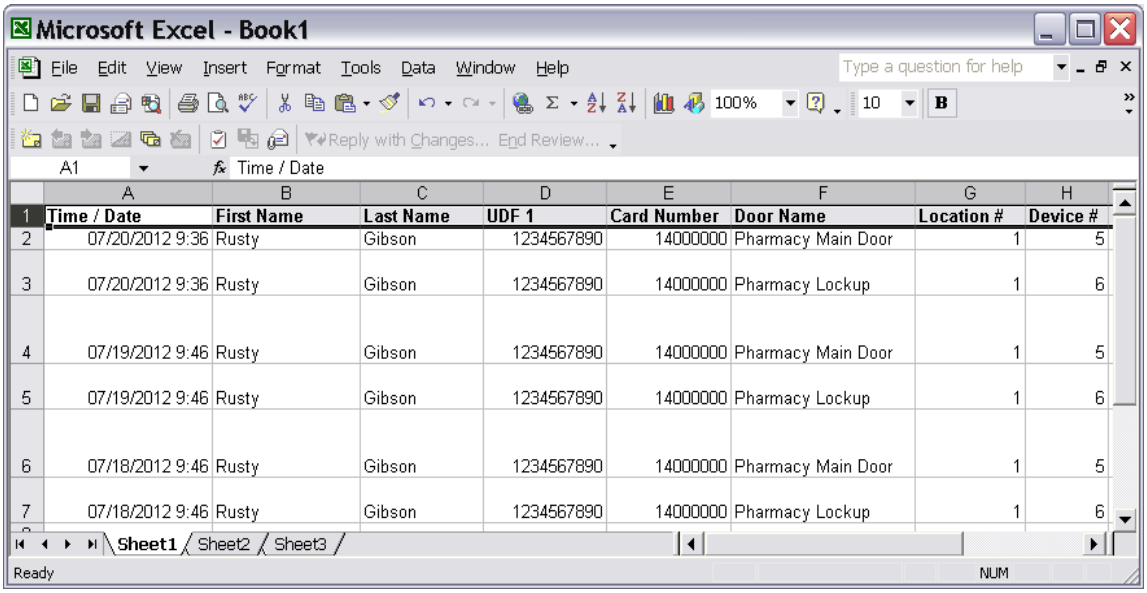
Figure 11: Report includes search criteria, Location & Device of readers added or removed as well as the identity of the Operator making the changes.

Sample Report shows Card Holder access to 2 doors being added and 1 door being removed from the Card Holder. All changes to Access Levels are recorded here.

Figure 11 Sample of Access Level History Report for one Card Holder

High Security Area Logging

Activity at Readers (Devices) with a High Security Area (HSA) designation is recorded into the DataBase automatically. During Daily Ops, a log of all Card Holders and Cards with access is recorded and provides a daily snapshot of activity at each HSA reader. Any or all readers may be designated as HSA. The data contained in this report may be queried or exported according to User requirements.



Microsoft Excel - Book1

Time / Date	First Name	Last Name	UDF 1	Card Number	Door Name	Location #	Device #
07/20/2012 9:36	Rusty	Gibson	1234567890	14000000	Pharmacy Main Door	1	5
07/20/2012 9:36	Rusty	Gibson	1234567890	14000000	Pharmacy Lockup	1	6
07/19/2012 9:46	Rusty	Gibson	1234567890	14000000	Pharmacy Main Door	1	5
07/19/2012 9:46	Rusty	Gibson	1234567890	14000000	Pharmacy Lockup	1	6
07/18/2012 9:46	Rusty	Gibson	1234567890	14000000	Pharmacy Main Door	1	5
07/18/2012 9:46	Rusty	Gibson	1234567890	14000000	Pharmacy Lockup	1	6

This example shows
-Two entries each day
-Cardholder Name
-One User Defined Field
-Card Number
-HSA Name, Location & Device number.

Figure 12 Sample HSA Logging DataBase Created by Daily Ops

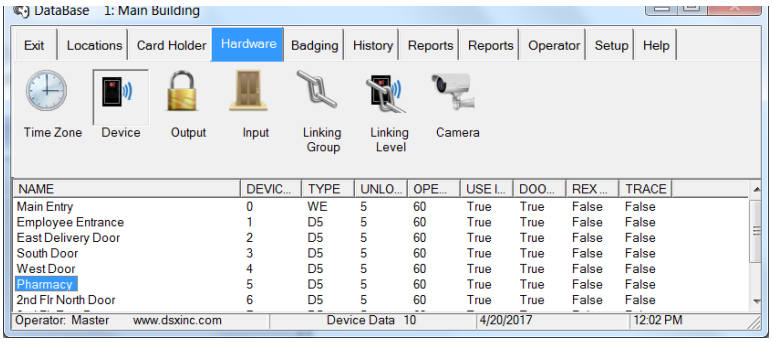


Figure 13 Selection of Reader to Designate as High Security Area (HAS) Reader

Figure 13: To designate a Reader as HSA:
From DataBase

1. Select the Hardware Tab
2. Select the reader to designate
3. Enter " ^HSA " into the Wire Tag # field
4. Repeat for all other readers to be designated as HSA
5. Create a new DataBase in SQL
6. Name the database CaAccessLog
7. Locate the SQL script file named HighSecurityAreaLog.sql located in the WinDSX\MdbStruc\ folder and run the script against the new database.
8. Close the program. Next in the Shared folder edit the C:\WinDSX\RunData\gDB_Settings.txt file and locate the keys shown on the **next page**. Make entries on the lines marked Value: Save the file and restart the program.

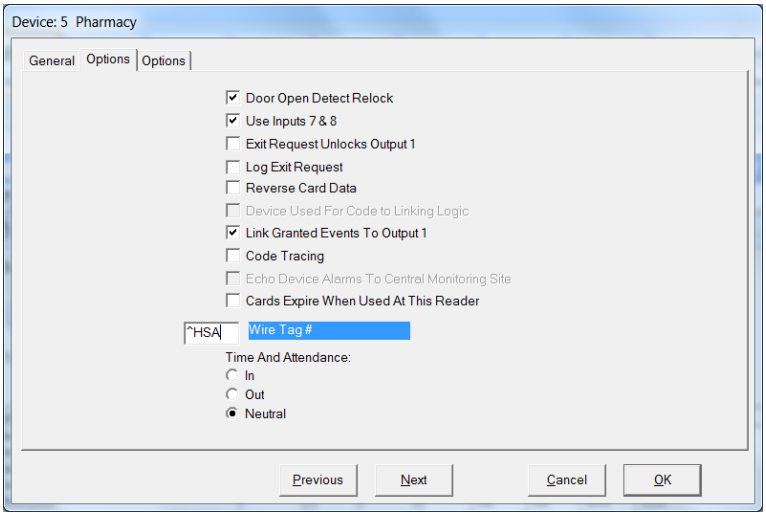


Figure 14 Designation of Pharmacy Reader as High Security Area (HSA)

C:\WinDSX\RunData\gDB_Settings.txt

Name: HsAlSql
Value:
Default:
Desc: Name of SQL Server for High Security Area Log

Name: HsAlDb
Value:
Default:
Desc: Name of Database on SQL Server for High Security Area Log
---
Name: HsAlUdf
Value:
Default:
Desc: UDF number stored with High Security Area Log. Unique ID.

This defines the name of the SQL Server where the data will be stored, the database name the data will be stored in (CaAccessLog), and the UDF Number that indicates which UDF data will be stored with the name. The UDF data selection is optional, and if used, should be a unique identifier for a person (Name ID). This will make it easier to differentiate between two people with the same name.

Example:
c:\WinDSX\RunData\gDB_Settings.txt

Name: HsAlSql
Value: DSX-SQL2
Default:
Desc: Name of SQL Server for High Security Area Log

Name: HsAlDb
Value: CaAccessLog
Default:
Desc: Name of Database on SQL Server for High Security Area Log
---
Name: HsAlUdf
Value: 1
Default:
Desc: UDF number stored with High Security Area Log. Unique ID.

The above specifies a SQL Server named DSX-SQL2, a database file within the DSX-SQL2 server named CaAccessLog, and UDF 1. The software will connect to DSX-SQL2 using Windows Authentication and store the data in the CaAccessLog database. The data contained in UDF 1 will be stored with each Card Holders name to help provide a positive ID.