DSX Access Systems, Inc.

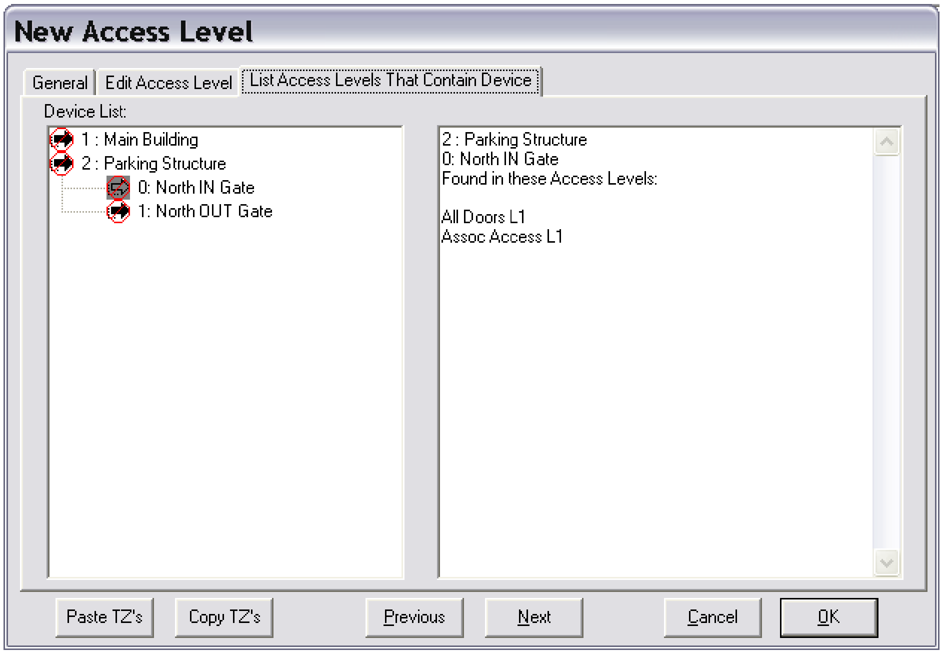
DSX Accountability Tools

DSX Accountability and Compliance Tools

At a time when Accountability and Reporting are an ever increasing requirement, DSX is creating solutions that will provide the information needed.

Reader (Device) Locator in Access Levels

When defining a new access level or editing an existing one there is a new tab that will show the user which access levels contain a selected device. This data is displayed in a text box that can be copied and pasted into any other application for storage, printing, or emailing. This new View streamlines the effort in locating all of the access levels that contain a specific reader.


New Access Level

Device List:

1 : Main Building
2 : Parking Structure
0: North IN Gate
1: North OUT Gate

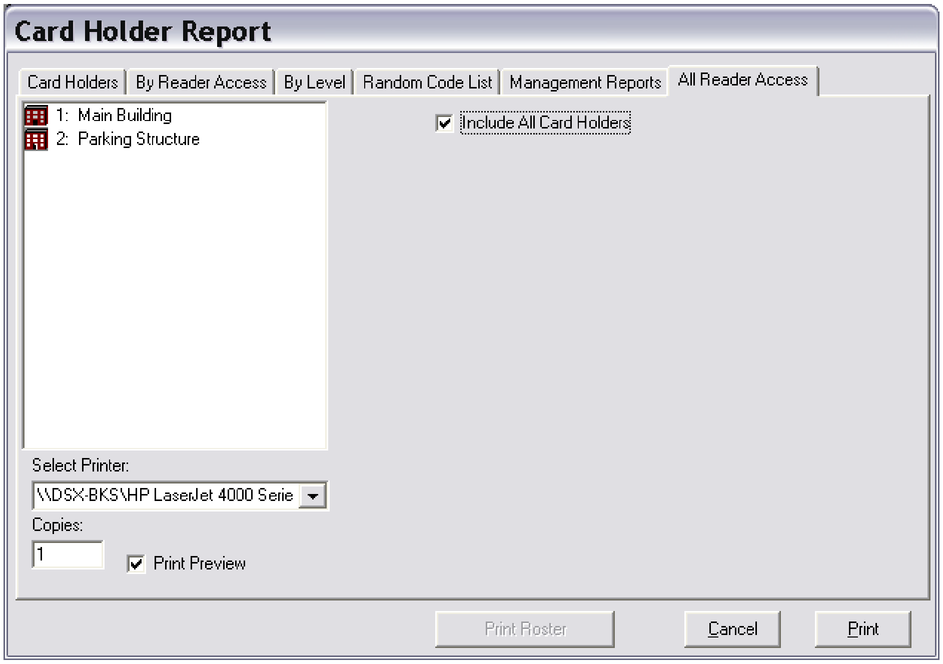
2 : Parking Structure
0: North IN Gate
Found in these Access Levels:

All Doors L1
Assoc Access L1

The example above shows a new access level that has no definition. Select the third tab - “List Access Levels That Contain Device”. In the “Device List” on the left you will see all of the Locations and Devices for the Location Group. Expand the Location of choice and click on the device/reader to be located. In the text box on the right you will see the Location and Device selected at the top followed by the name of every access level that contains that device/reader. In this example Location 2, Device 0, is part of the “All Doors L1” and “Assoc Access” levels. The contents of the text box on the right can be copied and pasted into a document or email.

Card Holder Reports

Card Holder Report can be used to obtain lists of card holders in the system sorted by different criteria. The First Tab "Card Holder" is used to report the card holders by Location. The Second Tab "By Reader Access" is used to report the card holders who have access to a particular reader. The Third Tab "By Level" is used to report card holders by who is assigned a particular access Level. The Sixth Tab "All Reader Access" will provide a report that lists every reader/device and time zone showing where and when a card has access. By default the report is set for everyone (Include All Card Holders) but can be changed to report just selected card holders. By de-selecting "Include All Card Holders" the card holder search engine is started so that you can search by company, name, UDF, or card number to define or narrow the scope of the report. The report includes each door the card holder has access to and includes the time zone that determines their access at those doors.



1: Main Building
2: Parking Structure

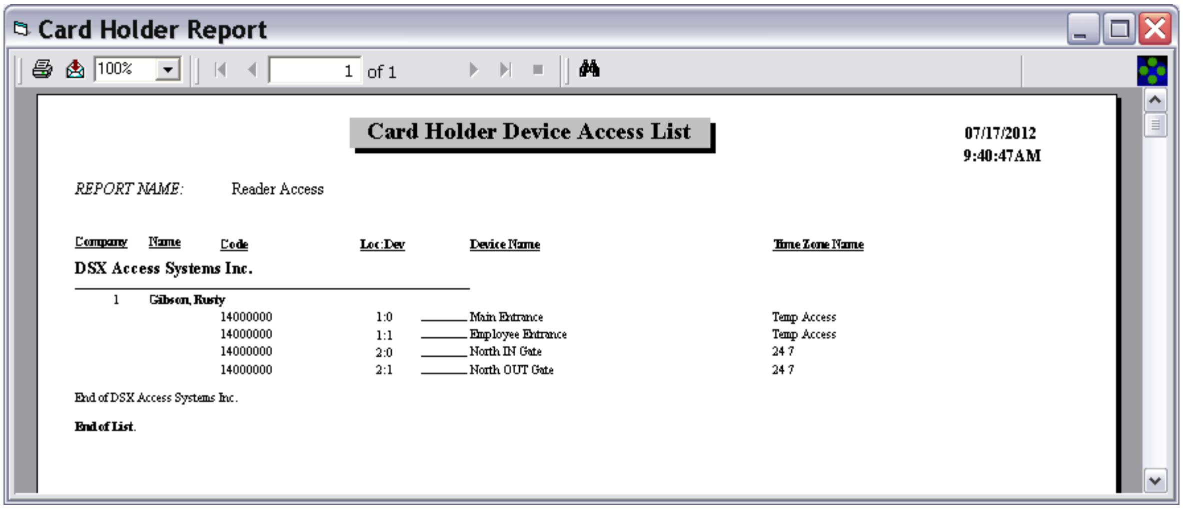
☑ Include All Card Holders

Select Printer: \\DSX-BKS\HP LaserJet 4000 Serie

Copies: 1

☑ Print Preview

Sample Device Access List for one Card Holder



Card Holder Device Access List

07/17/2012
9:40:47AM

REPORT NAME: Reader Access

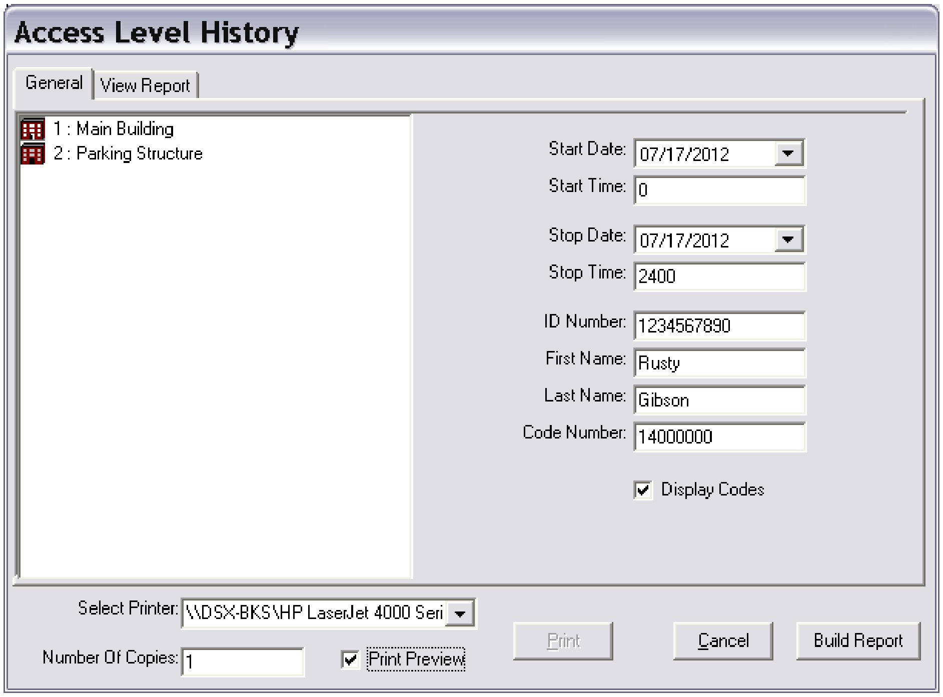
Company	Name	Code	Loc:Dev	Device Name	Time Zone Name
DSX Access Systems Inc.					
1	**Gibson, Rusty**				
		14000000	1:0	Main Entrance	Temp Access
		14000000	1:1	Employee Entrance	Temp Access
		14000000	2:0	North IN Gate	24 7
		14000000	2:1	North OUT Gate	24 7

End of DSX Access Systems Inc.

End of List.

Access Level History

When configured the WinDSX SQL software will create a database of all changes that are made to the card population's access level assignments. This ongoing accrual of changes provides sufficient data for the reporting of these changes. These changes can occur by adding or removing access levels from a card or by editing and changing the definition of an access level directly. This feature will create a log of all changes that can be searched and will produce reports. This is an optional feature that is enabled by the software features key. You must have the SQL version of WinDSX to enable this feature in your USB Key.



1 : Main Building
2 : Parking Structure

Start Date: 07/17/2012
Start Time: 0
Stop Date: 07/17/2012
Stop Time: 2400
ID Number: 1234567890
First Name: Rusty
Last Name: Gibson
Code Number: 14000000
☑ Display Codes

Select Printer: \\DSX-BKS\HP LaserJet 4000 Seri
Number Of Copies: 1
☑ Print Preview

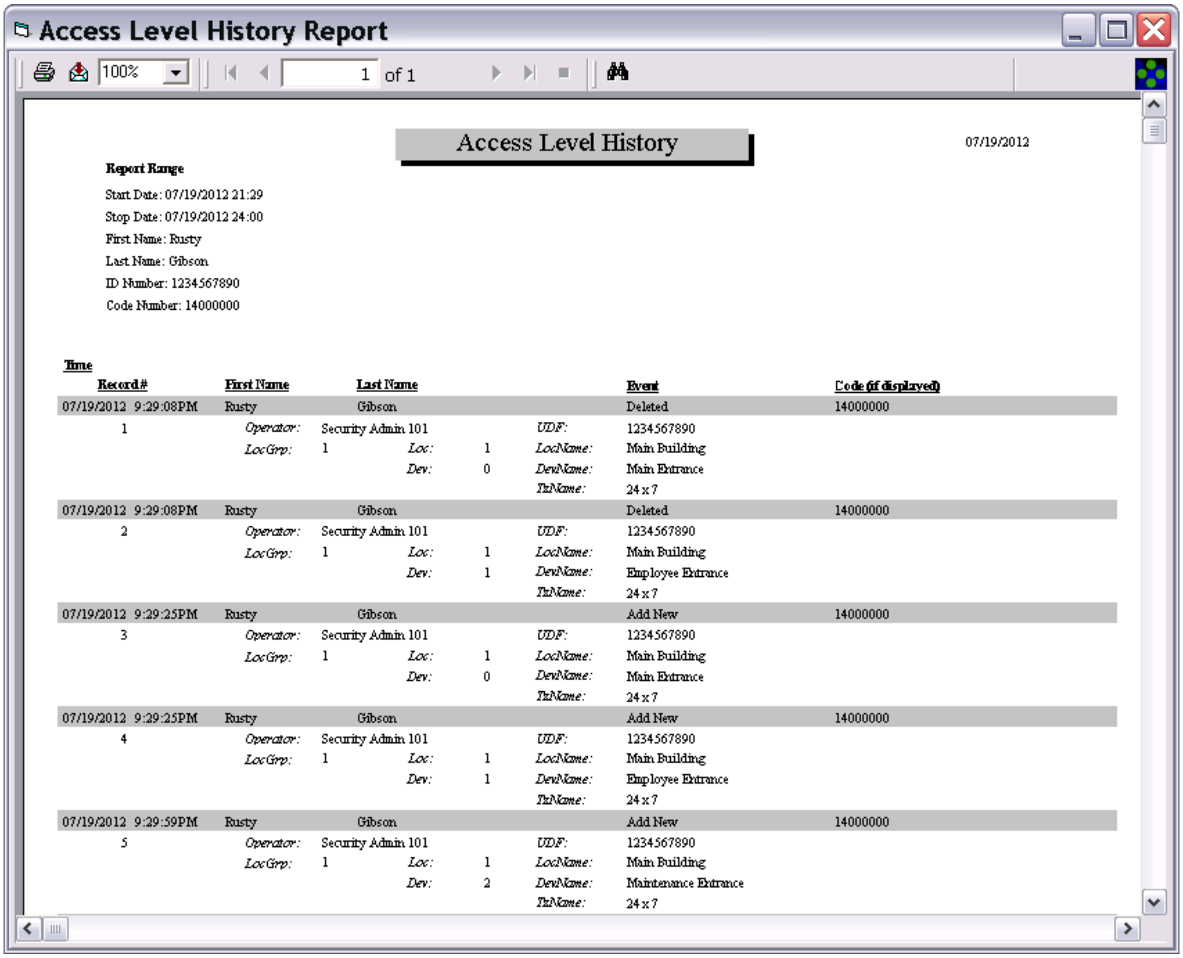
To use the ID Number field for identifying card holders you must have a UDF field that has the "Name ID" attribute enabled. To configure the report enter the Start Date and Time and the Stop Date and Time that encompasses the audit period. Next Enter the Name ID for the person of interest, or Name, or the Card Number. Any of these can be used but it is not necessary to use them all. If you want the card number to be displayed in the report check the "Display Code" selection box.

Set the printer the report should be sent to, set the number of copies desired, set Print PreView to see the formatted report on screen and then click on Build Report. The report can optionally be saved to a file.

The report displays the search criteria used at the beginning of the report. The report shows the location and device of the readers added or removed along with the Operator that made the changes.

Sample Access Level History Report for one Card Holder

In the sample below you will see a report for a card holder that shows access to 2 doors being removed from the card holder. Next the report shows the same 2 doors being reassigned to the card holder. Lastly the report shows access to a door being added to the card holder when a door was added to the card holder's access level. It doesn't matter how this card holder's access is changed it is recorded and reported here.



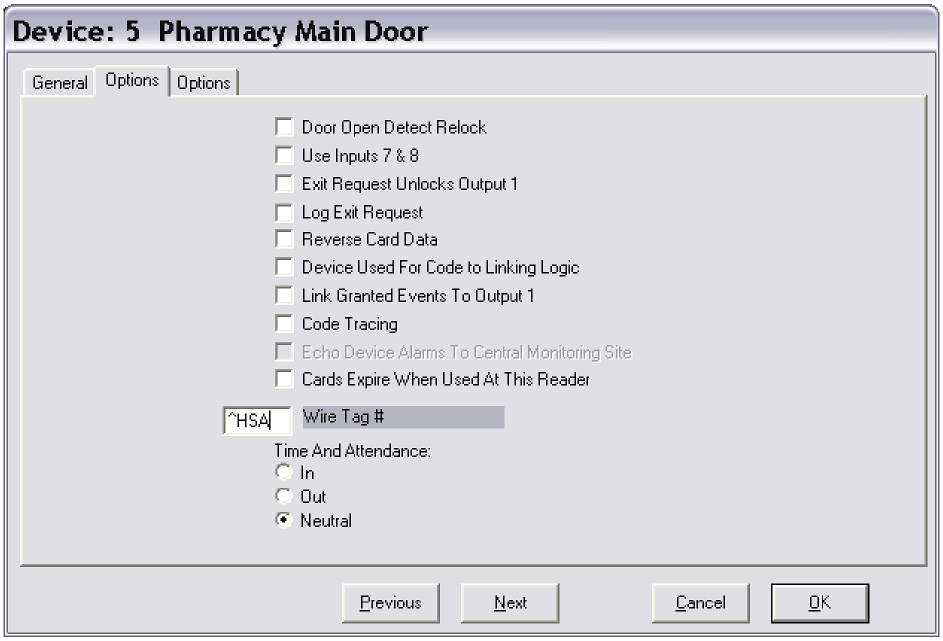
```
                              Access Level History                          07/19/2012
      Report Range
      Start Date: 07/19/2012 21:29
      Stop Date: 07/19/2012 24:00
      First Name: Rusty
      Last Name: Gibson
      ID Number: 1234567890
      Code Number: 14000000

Time
   Record#          First Name      Last Name                   Event            Code (if displayed)
07/19/2012  9:29:08PM  Rusty        Gibson                      Deleted          14000000
      1             Operator:  Security Admin 101      UDF:      1234567890
                    LocGrp:    1        Loc:    1      LocName:  Main Building
                                        Dev:    0      DevName:  Main Entrance
                                                       TzName:   24 x 7
07/19/2012  9:29:08PM  Rusty        Gibson                      Deleted          14000000
      2             Operator:  Security Admin 101      UDF:      1234567890
                    LocGrp:    1        Loc:    1      LocName:  Main Building
                                        Dev:    1      DevName:  Employee Entrance
                                                       TzName:   24 x 7
07/19/2012  9:29:25PM  Rusty        Gibson                      Add New          14000000
      3             Operator:  Security Admin 101      UDF:      1234567890
                    LocGrp:    1        Loc:    1      LocName:  Main Building
                                        Dev:    0      DevName:  Main Entrance
                                                       TzName:   24 x 7
07/19/2012  9:29:25PM  Rusty        Gibson                      Add New          14000000
      4             Operator:  Security Admin 101      UDF:      1234567890
                    LocGrp:    1        Loc:    1      LocName:  Main Building
                                        Dev:    1      DevName:  Employee Entrance
                                                       TzName:   24 x 7
07/19/2012  9:29:59PM  Rusty        Gibson                      Add New          14000000
      5             Operator:  Security Admin 101      UDF:      1234567890
                    LocGrp:    1        Loc:    1      LocName:  Main Building
                                        Dev:    2      DevName:  Maintenance Entrance
                                                       TzName:   24 x 7
```

High Security Area Logging

The High Security Area logging feature will automatically create a daily log of all card holders and cards that have access to readers that are marked as High Security Areas (HSA) readers. The function runs at daily-ops each day and will record Current Date, First Name, Last Name, One Selected UDF, Card Number, Reader Name, Reader Location, and Reader Device Number into the specified database for every HSA reader. In Short it will build a database with a daily snapshot of Card Holders that have access to the HSA Readers. HSA Readers can be readers located in the Pharmacy or other volatile areas or it could be every reader.

To Mark a Reader as a HSA (High Security Area) device, edit the device and select the first options tab. Enter the letters ^HSA into the Wire Tag # field. Do this for all doors required to be tracked.



Device: 5 Pharmacy Main Door

□ Door Open Detect Relock
□ Use Inputs 7 & 8
□ Exit Request Unlocks Output 1
□ Log Exit Request
□ Reverse Card Data
□ Device Used For Code to Linking Logic
□ Link Granted Events To Output 1
□ Code Tracing
□ Echo Device Alarms To Central Monitoring Site
□ Cards Expire When Used At This Reader

^HSA Wire Tag #

Time And Attendance:
○ In
○ Out
● Neutral

To enable this feature you must first create a new database in the SQL Server. Create a new database and Name the database CaAccessLog. Locate the SQL script file named HighSecurityAreaLog.sql located in the WinDSX\MdbStruc\ folder and run the script against the new database.

Close the program. Next in the Shared folder edit the C:\WinDSX\RunData\gDB_Settings.txt file and locate the keys shown below. Make entries on the lines marked **Value:** Save the file and restart the program.

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.

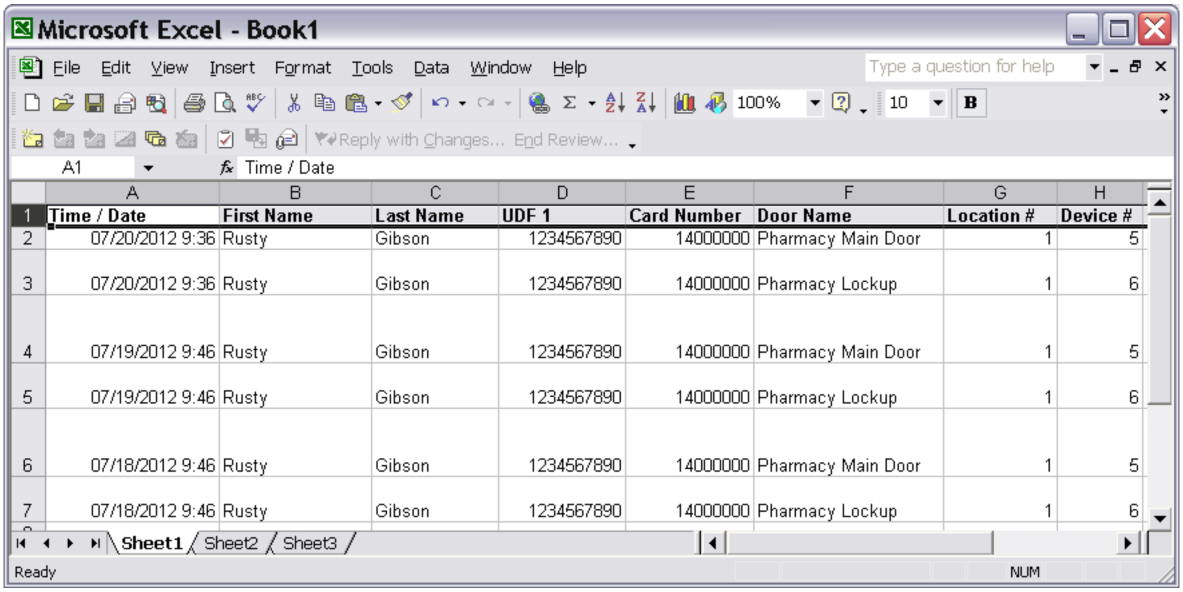
This defines the name of the SQL Server where the data will be stored, the database name the data will be stored in (CaAccessLog), and the UDF Number that indicates which UDF data will be stored with the name. The UDF data selection is optional, and if used, should be a unique identifier for a person (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.

Sample of HSA Logging DataBase



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

The HSA database will have a record for each day of everyone that has access to a Reader/Device in WinDSX that is marked as ^HSA. The sample above shows two entries each day for a card holder that has access to Device 5 and 6 which happens to be for the Pharmacy in this example.