DSX Access Systems, Inc.

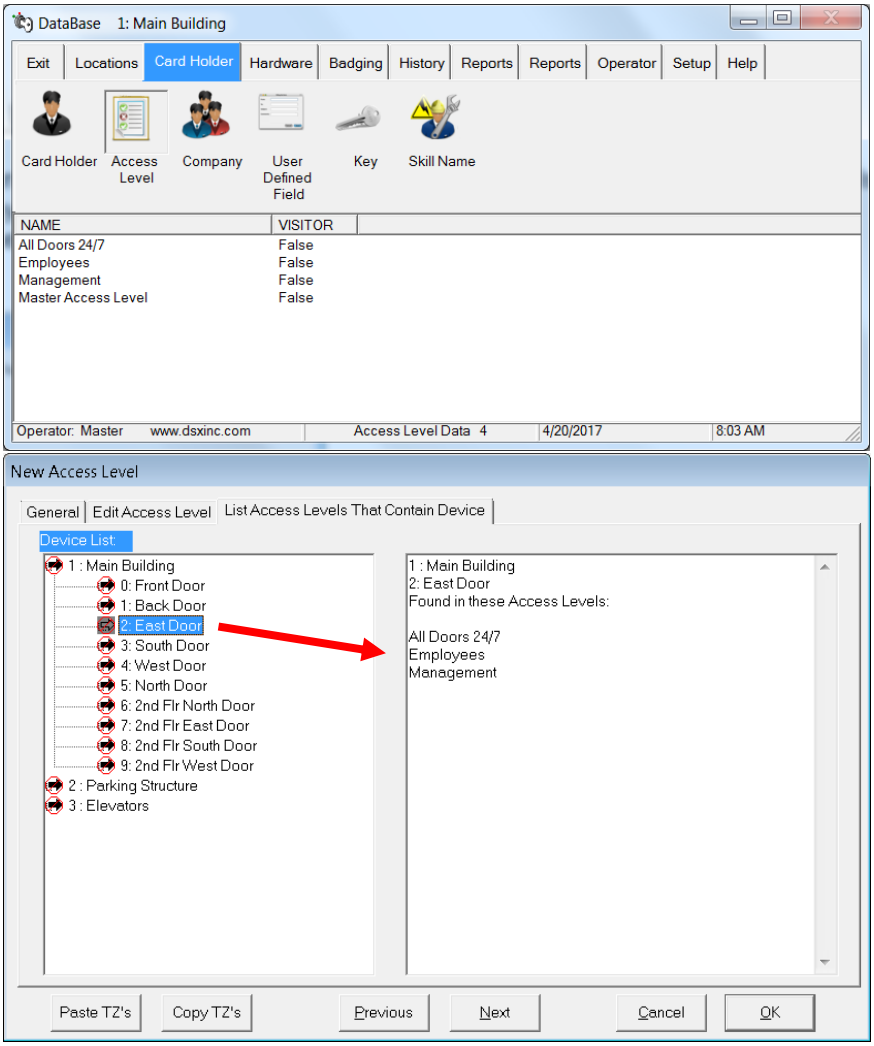
DSX Accountability Tools

DSX Accountability and Compliance Tools

At a time when Accountability and Reporting are an increasing requirement, DSX is creating solutions that will provide the information needed. Following are Reports that provide crucial data for audits in high accountability applications.

Reader (Device) Locator in Access Levels

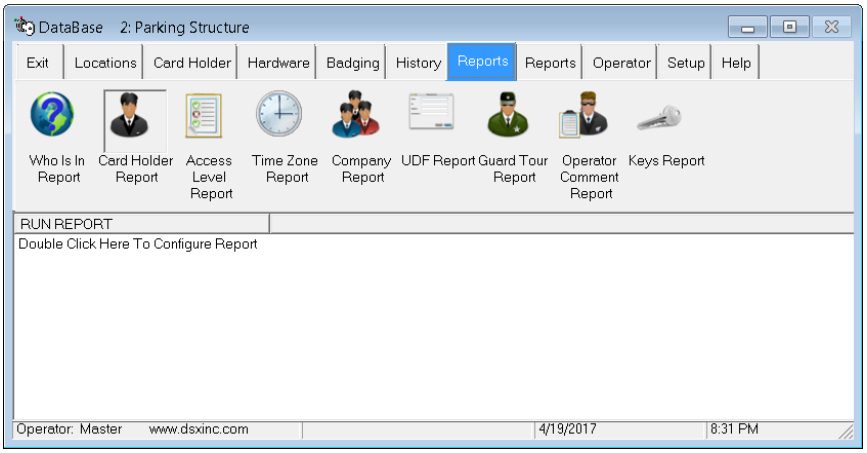
When adding a new Access Level or editing an existing one you will see a 3rd tab that shows the user which Access Levels contain a selected Device. This data is displayed in a text box that can be copied and pasted into any other applications for storage, printing, or emailing. This new View streamlines the effort in locating the Access Levels that contain a specific reader.

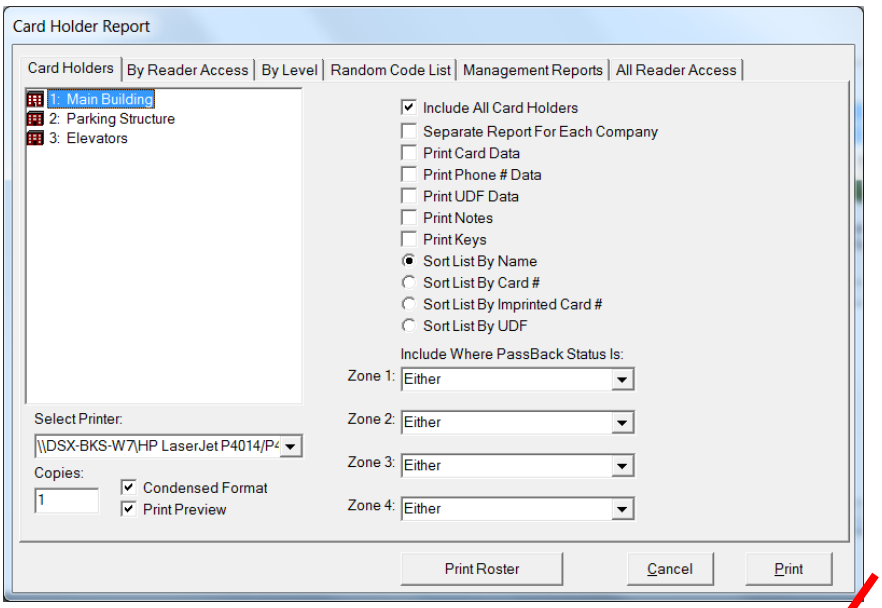


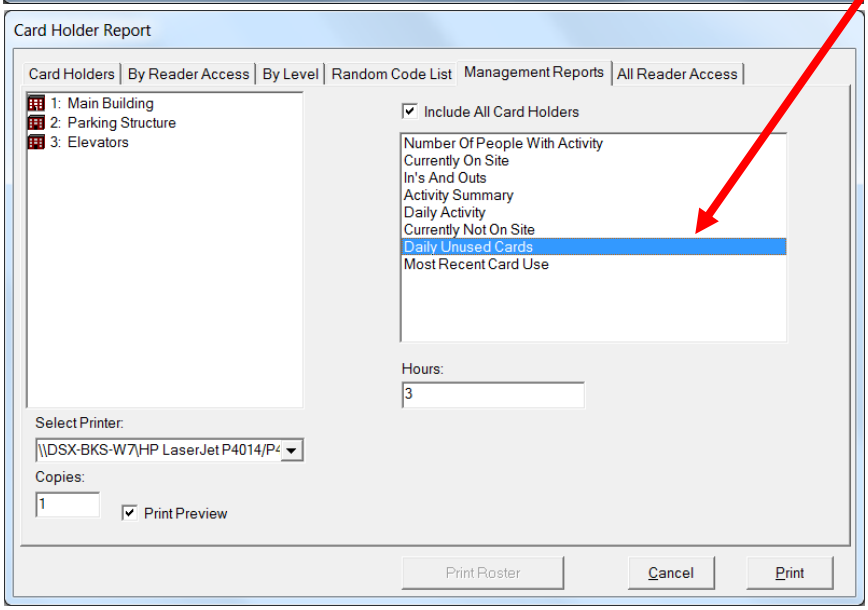
This example shows a new Access Level, just added, that has no definition. Select the third tab - **"List Access Levels That Contain Device"**. In the "Device List" on the left you will see the Locations and Devices for the Location Group. Expand the Location of choice and click on the Device/Reader 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 1, Device 2, is part of the "All Doors 24/7", "Employees", and the "Management" Access Levels. The contents of the text box on the right can be copied and pasted into a document or email.

Card Holder Reports / Management Reports

Card Holder Report can be used to obtain lists of Card Holders in the system sorted by different criteria. This document will cover the sections of Card Holder Report that pertain to audits and accountability.







The First Tab "**Card Holder**" is used to report the Card Holders by Location with various search and sort criteria.

The Second Tab "**By Reader Access**" is used to report the Card Holders who have access to a specific Reader.

The Third Tab "**By Level**" is used to report Card Holders by who are assigned a specific Access Level.

The Fourth Tab "**Random Code List**" is a random code generator.

The Fifth Tab "**Management Reports**" holds a list of Reports that mainly have to do with Time and Attendance. There are two of these reports that could be considered Accountability Reports. Discussed below.

The Sixth Tab "**All Reader Access**" will provide a report that lists every Reader/Device a Card Holder has access to. This report is discussed on the next page.

Daily Unused Cards

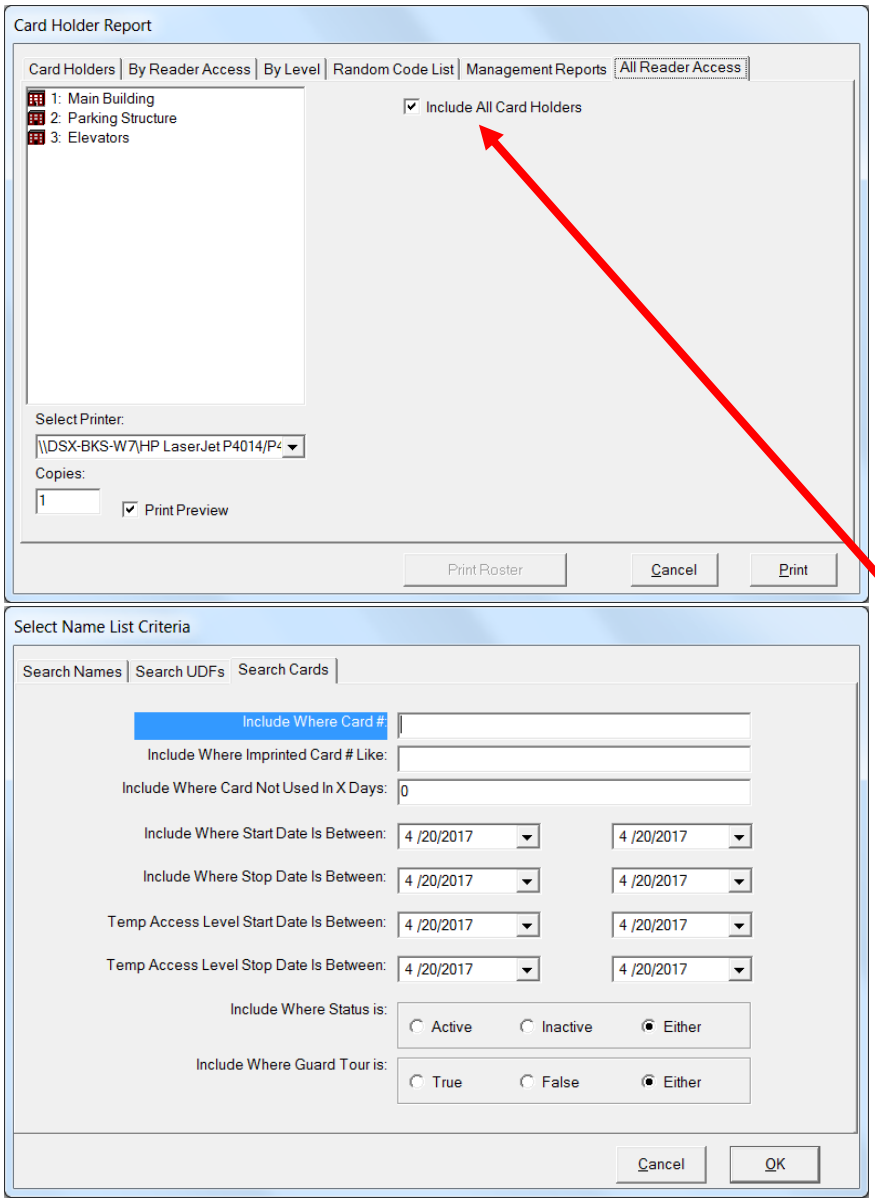
Daily Unused Cards shows Card Holders that have not used their Card in X Hours – This could be used to quickly ascertain "Who is Not Here" or has not used their code in x hours. This report does not require In and Out readers. This report is presented by Location and sorted by Company.

Most Recent Card Use

Shows the last Card Use (time/date, location and door) for each Active Card Holder selected. Reports are presented by Location and sorted by Company.

These two new reports require "Save Last Card Read" to be enabled in the DataBase program under Location on the "Yes/No Options Tab".

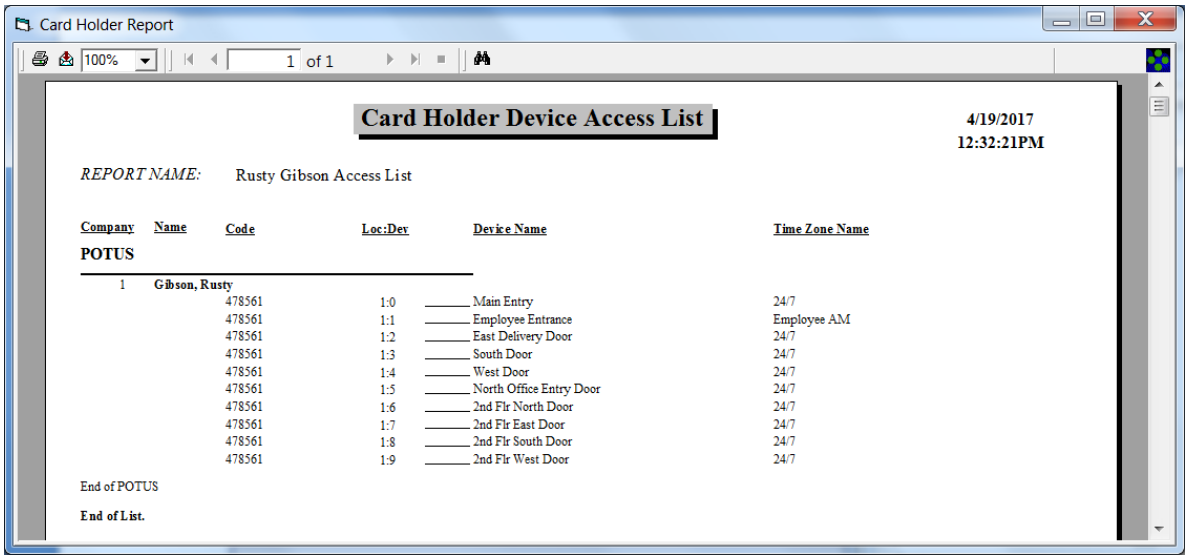
Card Holder Reports / All Reader Access Reports



The **All Reader Access Report** provides a list of every Reader/Device a Card Holder has access to. The report includes each door the Card Holder has access to and includes the Time Zone that determines their access at each door.

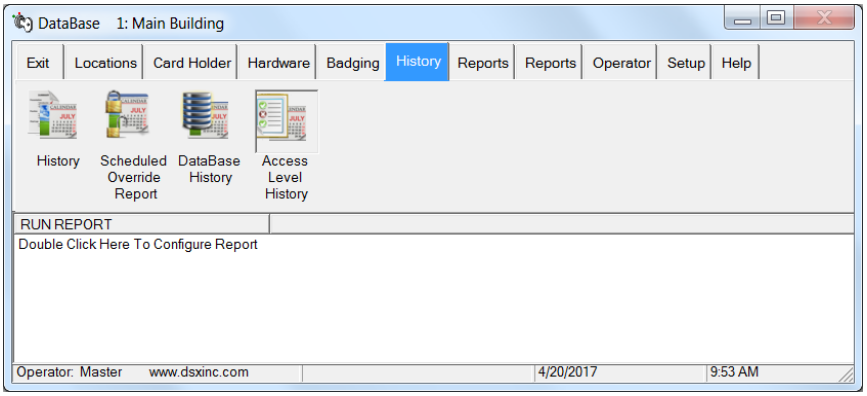
By default, the report is set for everyone (Include All Card Holders) but can be changed to report just selected Card Holders. By de-selecting “Include All Card Holders” the Card Holder search engine is started so that you can search by Company, Name, UDF, or Card Number to define or narrow the scope of the report.

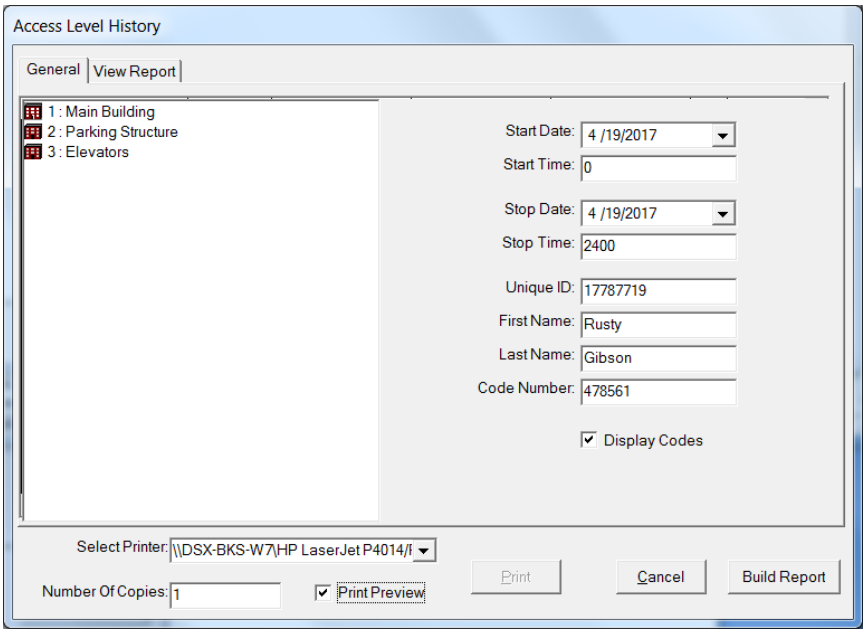
Sample Device Access Report for one Card Holder

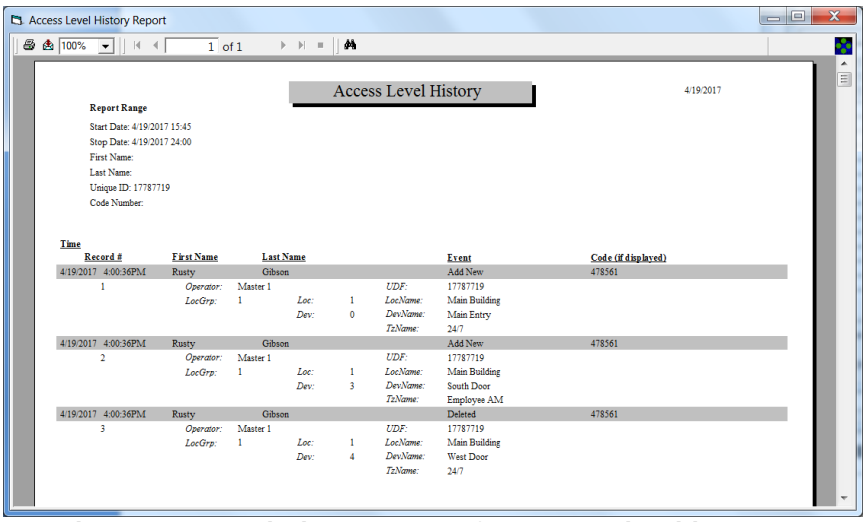


Access Level History

When configured the WinDSX SQL software will create a database of all changes that are made to the card population's Access Level assignments. 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.







Sample Access Level History Report for one Card Holder

This is an optional feature that is enabled by the DSX Softkey. You must have the SQL version of WinDSX to enable this feature in your SoftKey (dsxkeydata.xml). Access Level History is found on the History Tab in the DataBase program.

Reports are run by Card Holder for a Time and Date range. Card Holders can be reported by name, card number or the Unique ID (recommended). To use the Unique 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 Unique "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.

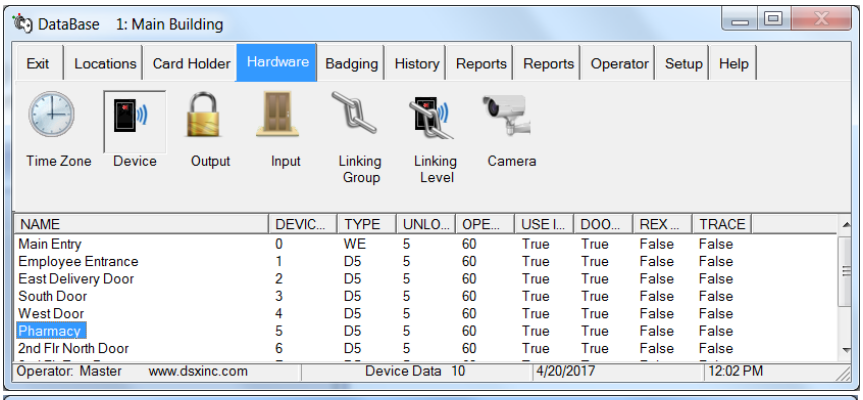
The report displays the search criteria used at the beginning of the report. The report shows the Location and Device of the readers added or removed along with the Operator that made the changes.

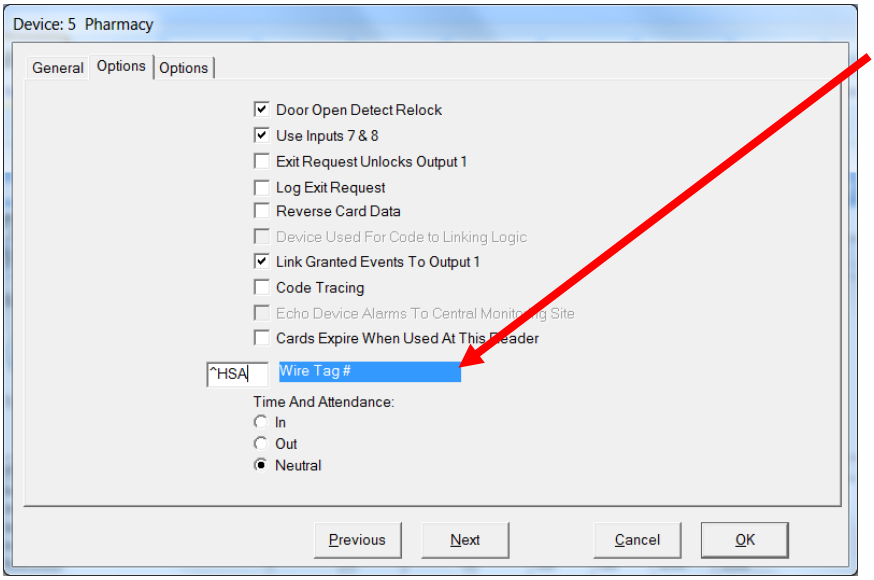
In this sample you will see a report for a Card Holder that shows access to 2 doors being added and 1 door being removed from the Card Holder.

It doesn't matter how this Card Holder's access is changed, it can be reported here. Any doors added, deleted or changed to any Card Holder directly by Access Level assignments or by redefining the Access Levels that are already assigned is recorded here. The changes are recorded for each Card Holder and listed by Door/Device.

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.





1. 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.

2. Create a new database in the SQL Server and name the database CaAccessLog.

3. Locate the SQL script file named HighSecurityAreaLog.sql located in the WinDSX\MdbStruc\ folder and run the script against the new database.

4. 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.

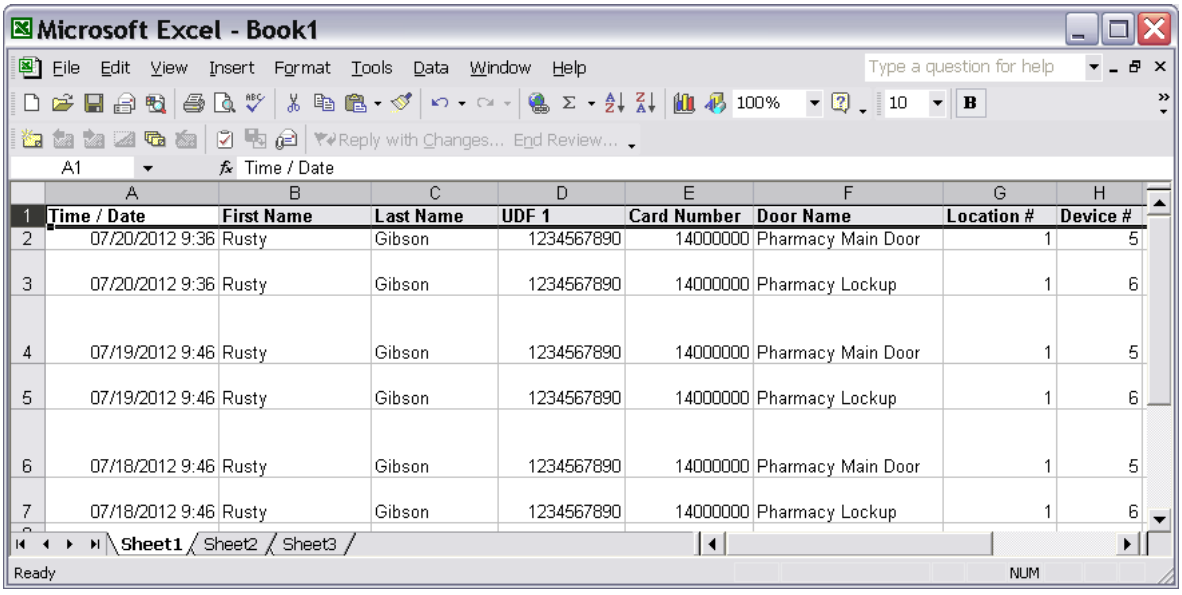
Example:
c:\WinDSX\RunData\gDB_Settings.txt

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



	A	B	C	D	E	F	G	H
1	Time / Date	First Name	Last Name	UDF 1	Card Number	Door Name	Location #	Device #
2	07/20/2012 9:36	Rusty	Gibson	1234567890	14000000	Pharmacy Main Door	1	5
3	07/20/2012 9:36	Rusty	Gibson	1234567890	14000000	Pharmacy Lockup	1	6
4	07/19/2012 9:46	Rusty	Gibson	1234567890	14000000	Pharmacy Main Door	1	5
5	07/19/2012 9:46	Rusty	Gibson	1234567890	14000000	Pharmacy Lockup	1	6
6	07/18/2012 9:46	Rusty	Gibson	1234567890	14000000	Pharmacy Main Door	1	5
7	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. There is no predefined report in WinDSX for this database. The data can be exported or queried against however the User requires.