

DataFetch Unilogger™ Users Manual

Revision 3.0x

DataFetch LLC
720 Washington Street, Liberty 1
Hanover, MA 02339
781-829-2022

Table of Contents

1	Installing the Unilogger™ Program	3
	1.1 Installation Checklist	3
2	Basic Operation	5
	2.1 Entering a student guest or host without ID	6
	2.2 Entering an outside guest without a license	6
3	Warnings and Exceptions	7
4	Restriction Warnings	8
	4.1 Student Restrictions	8
	4.2 Outside Guest Restrictions	8
5	The Display Button	9
6	Logging out guests	10
	6.1 Administrative vs. Verified Logouts	10
7	Options and Preferences	11
	7.1 Option: Administrative Password	11
	7.2 Option: Logging and Database Directories	12
	7.3 Option: Residence Hall Options	13
	7.4 Option: Msc'l Options	14
	7.5 Option: Mag Stripe Option	15
	7.6 Option: Security and Search	16
8	Working with Logs	18
	8.1 The Guest Log	19
	8.2 The Restricted Log	19
9	The Master File Log	20
	9.1 Accessing the Master Log	21

1.0 About This Manual

The DataFetch Unilogger program is specifically designed for universities, colleges, and similar institutions who need to maintain a log of visitors and guests to residence hall facilities or special events on campus. This program permits the user to associate students or members with their visitors or guests. Users who simply want to perform bulk scanning and logging for general events, without associating visitors or guests with students or other ID card holders, may want to use DataFetch's 'Event Log Recorder', instead.

1.0 Installing the Unilogger™

Prior to installing the software, users should first install the supplied Bluetooth adaptor, and then 'pair' the DF3D scanner to their PC or laptop. Instructions for accomplishing this are provided in a separate document, '**How to Pair the DF2D or DF3D.pdf**'.

Installation of the Unilogger™ program is straightforward. It is supplied as a self-installing executable (.exe) file which sets up the necessary files. The program is accompanied with additional information, including all reference manuals, as well as a sample student database, along with two sheets of test barcode targets which can be used for practice or familiarization purposes.

The executable file is installed in C:\Program Files\DataFetch\University Logger, and a shortcut is placed on the desktop, named '**DataFetch University Logger Version 3.0x**'.

If your institution will be using the optional magnetic stripe reader, please see the separate document entitled '**Installing the Mag Stripe Reader.pdf**'

Users of RFID cards (either low frequency proximity types, or higher frequency types) should consult DataFetch; we offer a configuration service which can make your RFID card format compatible with the Unilogger program.

Upon installation, the optional settings default to a condition which permits immediate testing with the sample barcode sheets included with the program. Administrators will want to alter the options to fit their particular institutional requirements, but we suggest working with the sample student database and sample barcode targets first, before making any options changes. After familiarization, please consult the separate document '**Installation for IT Staff Rev X.x.pdf**' supplied with the product.

1.1 Installation Checklist

1. Install the Bluetooth adaptor supplied with the product onto the laptop or PC
2. Install the batteries into the DF3D Scan & See scanner
3. Pair the scanner with the PC or laptop; see **'How to Pair the DF2D or DF3D.pdf'**.
4. Install the program by launching **'unilogger_setup_V3.x.exe'**
5. Familiarize and practice with the program, using the supplied sample student database, and the supplied sample target sheets (Print out the files **'sample guest license barcodes.pdf'** and **'sample student ID barcodes.pdf'**; we recommend that you print these using the best resolution your printer offers)
6. If your institution will be using the optional magnetic stripe card reader, install it; consult the file **'Installing the Mag Stripe Reader.pdf'**
7. Consult the document **'Installation for IT Staff Rev X.x.pdf'** before substituting your own student database, and setting the options.

2.0 Basic Operation

When the program is opened, the main screen will appear:



The center of the main form consists of four quadrants:

- The upper left quadrant displays the information on the student host, once the ID card is scanned or swiped.
- The lower left quadrant displays the information about the student guest whose ID was most recently scanned or swiped.
- The upper right quadrant displays the information about the outside guest whose ID was most recently scanned or swiped (or entered in manually)
- The lower right quadrant displays the names of the guests whose ID cards or licenses have been scanned, swiped, or manually entered.

The information displayed on the main form is not actually logged to disk until either the 'log' button is clicked, or the barcode next to the 'log' button is scanned.

The normal operating process works as follows:

1. **First**, the security guard scans or swipes the student ID card. Guest ID's may not be scanned until the host student ID has been entered.
2. **Next**, the guard scans or swipes the guest ID, which might be a student, or an outside guest. If an outside guest lacks a driver's license, their information may be entered by typing in the available fields and clicking on the 'manual entry' button.
3. **The guard can continue to swipe or scan additional guests**, up to the allowable limit of guests defined in the 'Options' menu item. If the number of guests of a particular student host exceeds the limit, a pop-up message will warn of this condition.
4. **Once the student host, and all the guests, have been entered**, the guard can either click on the 'log' button, or scan the bar code alongside the button, directly off the screen. Success will be indicated by all fields going blank. When the 'log' function is initiated, the relevant data is stored to disk.

2.1 Entering a Student Host or Guest without an ID card

If a student host presents, but is not in possession of their student ID card, the security personnel can manually enter as much information as desired, by first clicking on the 'name' field, and then filling out as many additional fields as desired, before clicking on the 'manual entry' button.

2.2 Entering Outside Guest Info without a Driver's License

If an outside guest is presented who has no driver's license, the information can be entered manually. Click on the 'Name' field in the outside guest section, and type in the information manually, using the TAB key to advance from one field to the next.

3.0 Warnings and Exceptions

Items in the 'options' menu, along with information in other files, can result in warnings being displayed when a scan or swipe is attempted.

The most common warning is when a host has exceeded his/her allowable number of guests. When the limit is reached, a pop-up window will warn the security guard of this condition.



It will not, however, prevent the scanning of additional guests; this allows for some flexibility in both the institutional policies, as well as the discretion of the guard, when other factors permit more than the usual number of guests.

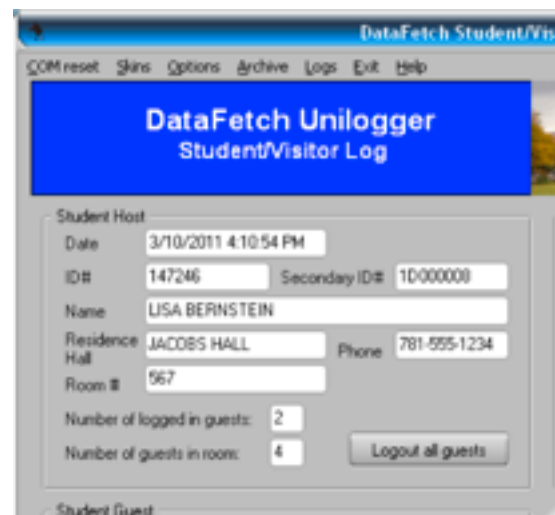
Additionally, when the student host is scanned or swiped, a summary of the student's current guest count, as well as the count of guests logged in who are being hosted by students occupying the residence hall room or suite, is displayed.

The 'number of logged-in guests' refers to the number of guests specifically logged in by this student host.

The 'number of guests in room' refers to the total number of all guests logged in by student hosts sharing the same room or suite.

The purpose of this feature is to advise the security guard of the number of total people who may be in one room or suite. Different institutions may have different rules about the limits of such an event; the guard is expected to apply any rules, or use his/her discretion when admitting additional guests.

The 'Logout all guests' button is a simple way to log out all guests of the student host. Normally, this could be used if a previous day's guests have left, but haven't yet been logged out. This type of logout is called an 'administrative' logout; see later sections on logout issues.

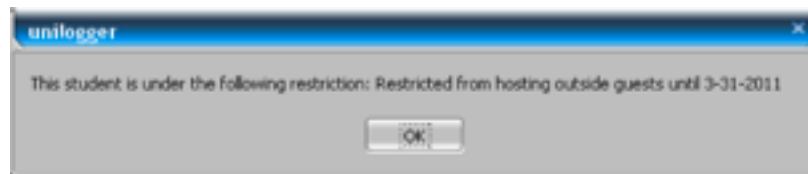


4.0 Restriction Warnings

The Unilogger™ program provides for establishing restrictions on specific students and/or outside guests.

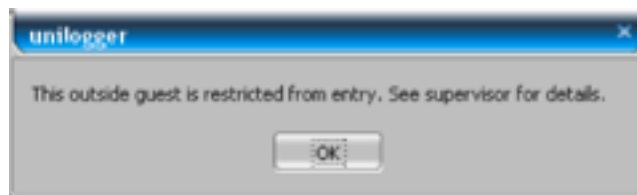
4.1 Student Restrictions

In the case of student restrictions, these are handled by an entry into the seventh column of the studentdb.xls file, or by the use of a separate 'studentrestrictions.xls' file. Since many institutions will have differing rules on restrictions, and may also employ multiple levels of restriction, the Unilogger™ program will display whatever text string is provided by the institutions' administration. It will not prevent a student under restriction from being logged in as a host or guest; this determination must be made by the security guard, in consideration of administration rules. When such a student is scanned or swiped, the restriction message will be displayed:



4.2 Outside Guest Restrictions

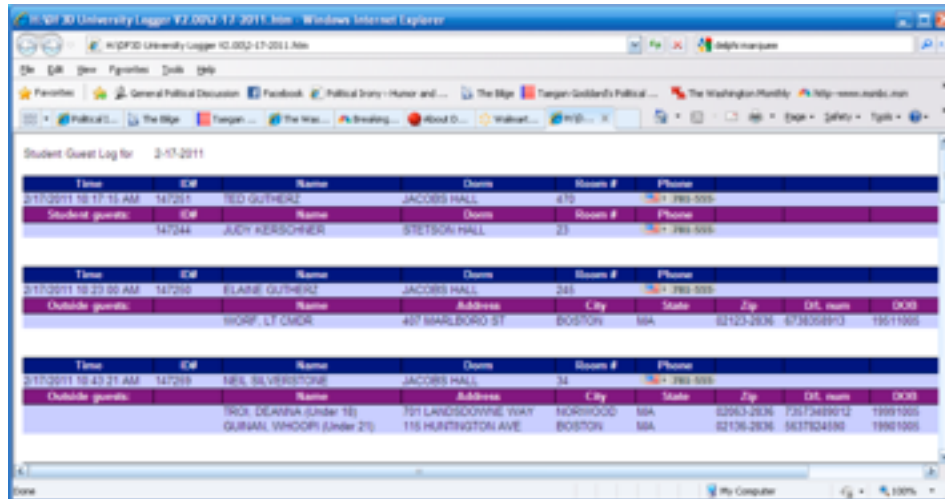
Restrictions on outside guests are handled differently. These restrictions are established by making an entry into a separate file, 'restricted.xls', which results in an absolute prohibition against being logged in.



The institution administrator can automatically transfer the information of any logged-in outside guest, to the restricted list, via a button in the 'guest log' display. Alternatively, the entry can be made by directly editing the restricted.xls file.

5.0 The Display Button

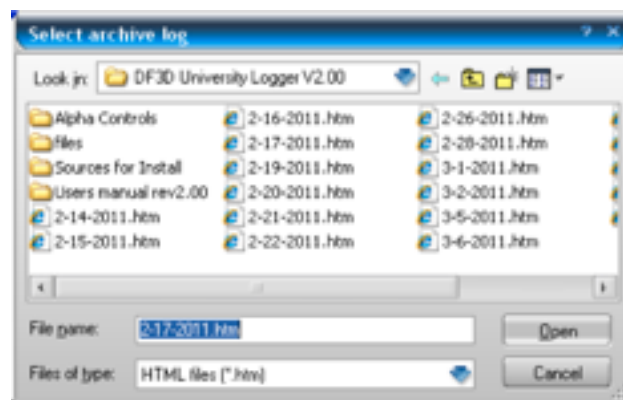
The 'display' button on the main form is provided as a very quick way of looking at the daily log. Clicking this button will launch the PC/laptop's default browser, and load it with the daily log, in HTML form. This log will show all log-ins since midnight of the previous evening, in event-sequential form. It does not include any log-outs.



Time	ID#	Name	Doors	Rooms #	Phone		
2/17/2011 10:17:11 AM	147211	TED GUTHRIE	JACOBS HALL	412	388-955		
Student guests:							
	ID#	Name	Doors	Rooms #	Phone		
	147244	JUDY KERSCHNER	STETSON HALL	23	388-955		
Outside guests:							
Time	ID#	Name	Doors	Rooms #	Phone		
2/17/2011 10:23:00 AM	147260	ELANIE GUTHERZ	JACOBS HALL	245	388-955		
Outside guests:							
	Name	Address	City	State	Zip	Ext. num	DOB
	WONG, LI TAMAR	40 MARLBORO ST	BOSTON	MA	02102-2008	6173302713	19711005
Time	ID#	Name	Doors	Rooms #	Phone		
2/17/2011 10:43:21 AM	147269	MRS. SILVERSTEIN	JACOBS HALL	34	388-955		
Outside guests:							
		MR. DEANNA (Jinze 16)	721 LANGSCUYPER WAY	ROXBORO	MA	02673-2636	7261289972 19891001
		GURJAL WIKHORI (Jinze 27)	115 HUNTINGTON AVE	BOSTON	MA	02108-2838	6173044382 19861001

A new daily log will be created every day, and will be stored in 2 forms: as an HTML document (with the extension '.htm'), and as an Excel-compatible spreadsheet (with the extension '.xls'). The filename will have the date embedded; therefore, the file being displayed above shows that it covers February 17, 2011.

In addition, you can look at the daily log for any previous day stored on disk; simply select 'archive' from the menu, and you will be able to select any specific day you want to examine:



Selecting one of these files will result in the PC/laptop's browser being launched, with that specific day's log loaded.

6.0 Logging Out Guests

Unilogger™ provides for several ways to log out current guests.

Many institutions have different rules for logging out guests; some will want to automatically log out guests at the end of a security shift (such as midnight), others will want to actively require guests to log out, and still others will call the student host, or ask the student host to contact the guard station, when their guests leave.

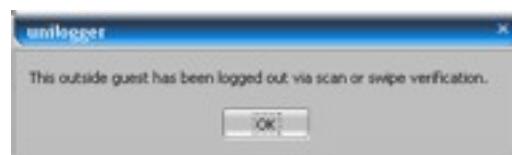
6.1 Administrative vs. Verified Logouts

Unilogger™ can perform two different types of 'logout' events. An **'administrative logout'** occurs when security personnel click on a button to log out a guest; a **'verified logout'** occurs when the ID of a guest is scanned or swiped a second time. The difference between a 'verified logout' and an 'administrative logout' is that the former is a guarantee that the guest passed the security desk and was personally seen by the guard, whereas the 'administrative logout' does not convey that level of verification, but is based on the testimony of the student host or an assumption on the part of the security guard.

Security personnel can perform an administrative logout in two different ways. The first way can be accomplished just after the student host is scanned or swiped; as shown in the section entitled 'Warnings and Exceptions', the result of a student host swipe will be the appearance of the guest count and the room count for this host, along with a button marked 'logout all guests'. The security guard can decide, based on questioning the student host, if previously logged-in guests have left, or not... and if so, he can click on the button to log out all guests that were logged in under the student's ID number.

The second way to perform an administrative logout is by launching the guest log window from the 'log' menu item. In this window, the list of current guests is provided (columns 9 and 10 will indicate who the student host of these guests are). The guard can select a particular guest by clicking on the line, and then log out that person by clicking on the 'log out selected' button, or he can log out all guests by clicking on the 'log out all' button.

A 'verified logout' is automatically accomplished by scanning or swiping the ID of a guest who is currently logged in. When this is done, a window will pop up to advise:



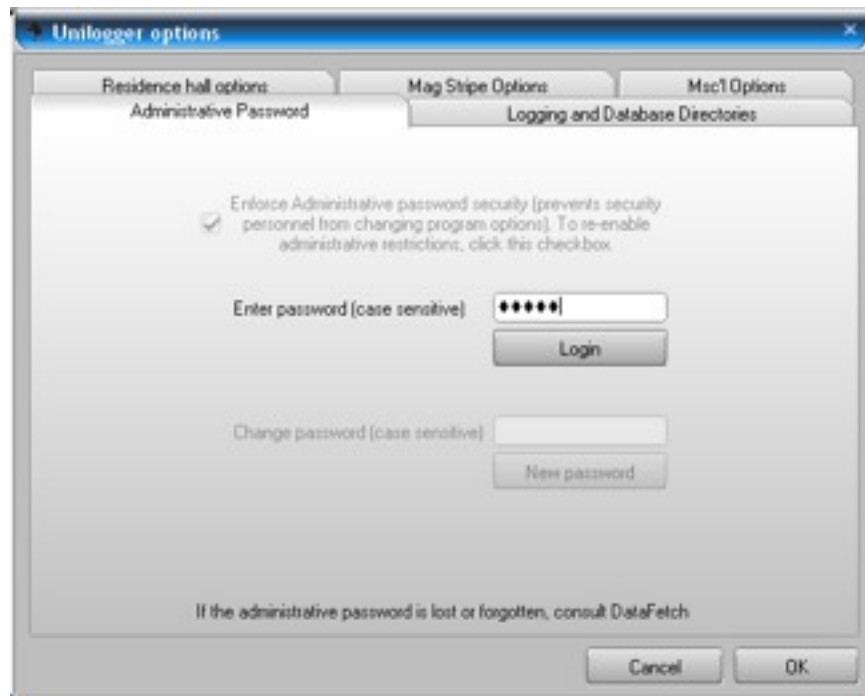
A verified logout may be performed at any time, even if the security guard is in the midst of logging in a student host and his/her guests; it will not affect the ongoing logging process.

7.0 Options and Preferences

The Unilogger™ can be configured for a variety of operating environments through the 'Options' menu at the top of the screen. These options are described below.

7.1 Option: Administrative Password

The program features an optional administrative password capability; when enabled, it prevents desk security personnel from changing any of the options or configuration information after the administration or IT personnel have installed the program.

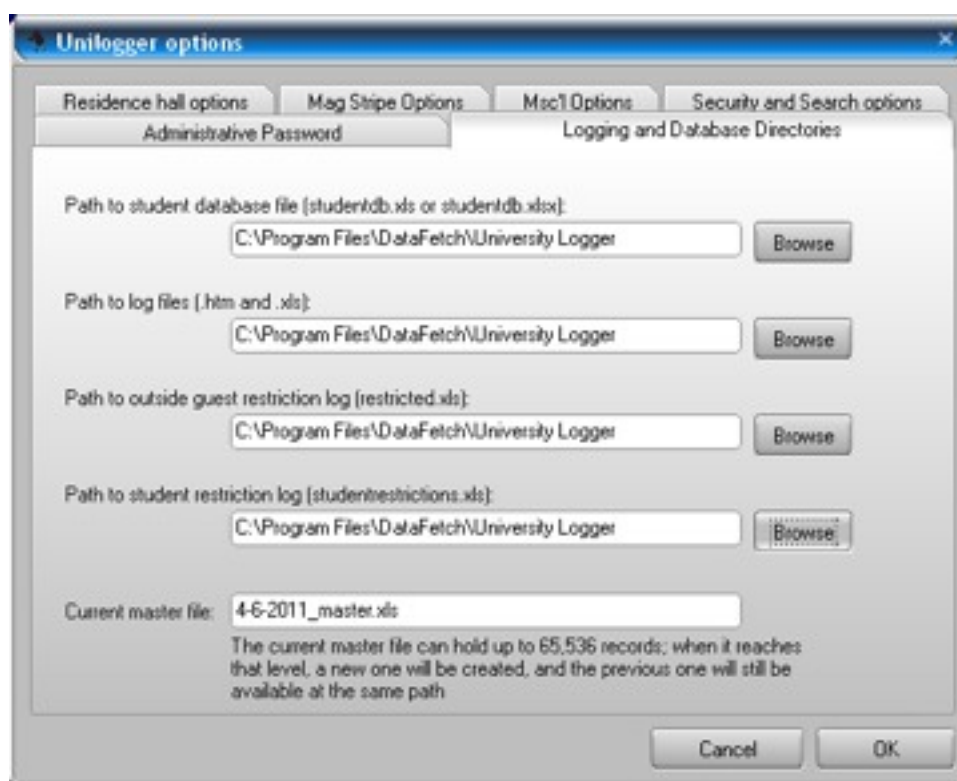


When the option is clicked, all other options within the options menu are disabled, and can only be enabled after the password is entered. The default password (case sensitive) is 'admin'. Once the options are enabled with the correct password, the administrator may change the password. To re-establish the security lockout, the option must then be clicked again.

In the event of a lost or forgotten password, contact DataFetch.

7.2 Option: Logging and database directories

The Unilogger™ provides for setting the path to the directories where log information, as well as daily logs and the student and restriction databases are stored. The default paths are set for the same directory as where the program is installed, but most users will want to create separate directories, either on the local PC or laptop, or on a networked server.



The first path defines the location of the student database (see ‘The Student Database’). This is the database of all students, containing their ID number, name, residence hall, room number, telephone number, and (optionally) any administrative restrictions which may be noted. The file is named ‘studentdb.xls’ or ‘studentdb.xlsx’, depending on the security and search options selected (See ‘Security and Search Options’ later in this manual).

The second path defines the location where the logs will be stored. The program will generate two daily logs, whose name contains the date of the log. One is formatted for display using the PC/laptop’s standard browser (such as Internet Explorer), and has a .htm extension; the other is the same thing, but in .xls format. In addition to the daily log files, the program will generate and maintain a master log of all events and transactions, named by the date when it was started, and with the word ‘master’ in its file name (e.g., ‘2-16-2011_master.xls’). This file is a continuous log; after it reaches

approximately 65,000 events, a new log will be created, but any older ones will still be in the same directory. Finally, this path will also contain a 'guestlog.xls', which is a continuously updated log of all guests currently logged in.

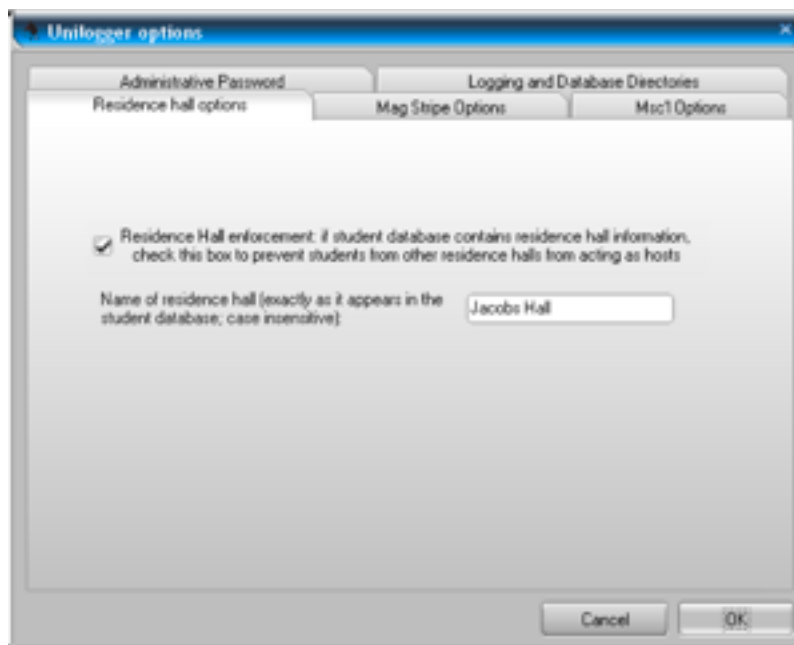
The third path contains a log of outside guests who are restricted, named 'restricted.xls'. Each guest logged in is checked against this log, and will not be admitted as a guest.

The fourth path defines the location where an optional studentrestrictions.xls file may be found. In Revision 3.00 and up, this is an optional alternative to recording student restrictions in the studentdb.xls or studentdb.xlsx file, and may make it easier to maintain and update.

The first two paths are specific to the location (normally, the residence hall) where the Unilogger™ is being used, and should ordinarily be set for a path or folder specific to the residence hall. The third and fourth paths should be accessible to all Unilogger™ installations, so restricted students and outside guests can be detected in all locations.

7.3 Options: Residence Hall Options

In most installations, the Unilogger™ will be used in each residence hall. In this application, the program can restrict the ability to host a guest or visitor to only those students who reside in the particular residence hall, as defined in the student database file.

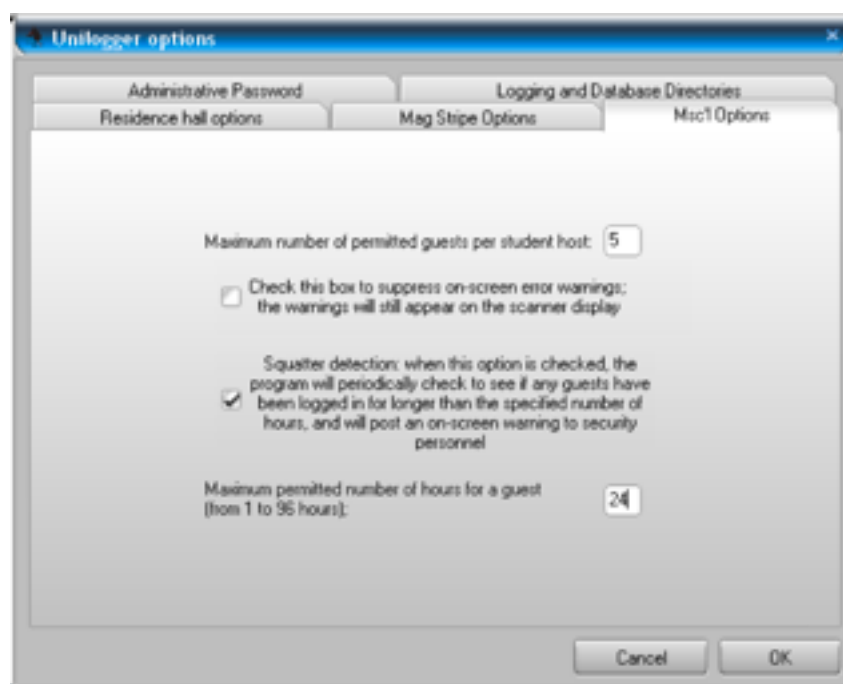


When this option is enabled, only students who are residence of the residence hall named in the option window are permitted to host any guests.

In some other applications, such as where the Unilogger™ might be used at a guard shack or front gate, the admission of guests might not be based on any specific residence hall. In applications like that, the option can be disabled.

7.4 Options: Msc'l Options

This options tab provides for several different capabilities:



Maximum number of student guests: this can be set for from 1 to 5 guests per student

Suppression of on-screen warnings: In normal operation, using the DF3D Scan & See™ bar code scanner, the scanner display will show any warnings associated with a host or guest entry. Clicking on this option will eliminate duplicate warnings displayed on the screen of the PC or laptop, and will eliminate the need to click 'OK' on many on-screen warnings that may pop up. This is provided for users who may be using the DF3D scanner at some distance from the associated laptop or PC.

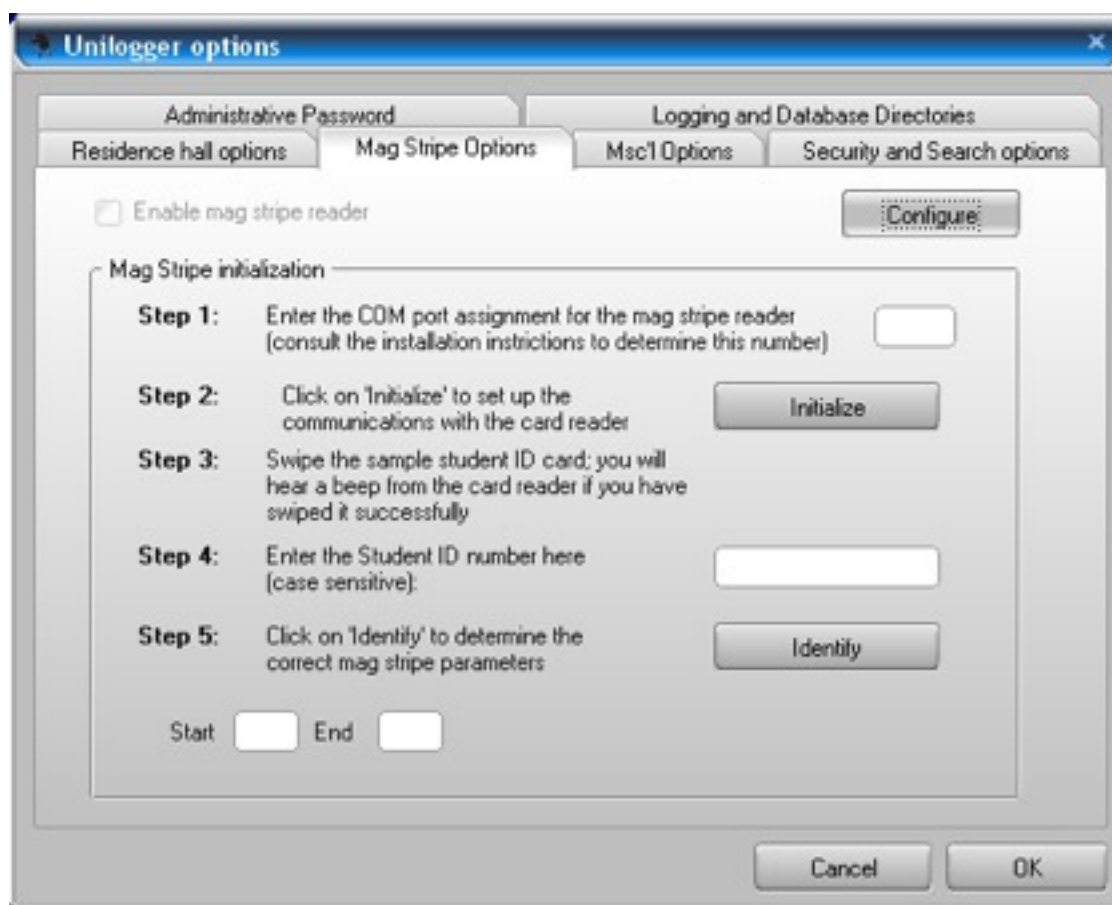
In the case of operations using the optional mag stripe reader, the on-screen warnings will not be suppressed. Also, warnings associated with manual operations requiring the mouse or keyboard will not be suppressed, regardless of the selection or de-selection of this option.

Squatter detection: Some institutions permit guests to be logged in for only a limited time period. Selecting this option will generate a warning on the main screen if any guests have been logged in for more than the specified number of hours (which can be set for anywhere from 1 to 96 hours).

7.5 Option: Mag Stripe Options

This option refers to the optional magnetic stripe reader, supplied by DataFetch, for use in institutions where the ID card uses a magnetic stripe instead of a bar code.

When this option tab is selected for the first time, the following screen appears:



Mag Stripe initialization is a one-time process which automatically adapts the Unillogger program to the mag stripe format being used by the institution. To use this capability, you need to have a sample student ID card available.

Before using this initialization process, the mag stripe reader must be installed first, and the COM port number associated with the mag stripe reader must be determined (See 'installing the Mag Stripe reader').

To perform the initialization, enter the COM port number in the box provided. Next, click on the 'Initialize' button, which will confirm and establish the COM port availability for the mag stripe reader. Next, swipe the sample ID card. Finally, enter the ID number for the sample student ID card, and click on 'Identify'. The mag stripe data

will be analyzed, and the screen will indicate that the ID card has been successfully analyzed, and the important parameters stored.

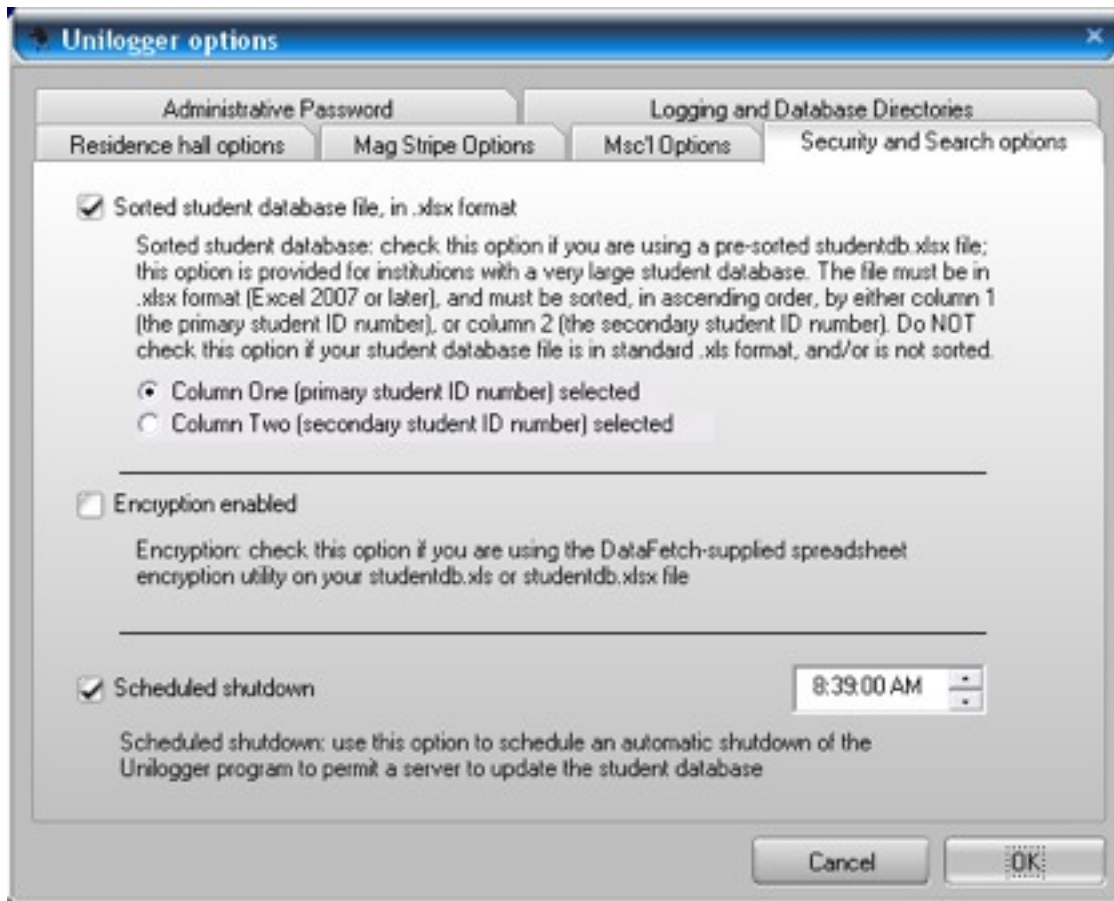
At this point, you can click on 'Enable mag stripe reader', and the Mag Stripe Initialization box will disappear. The mag stripe reader is now configured for your particular mag stripe card data format.

In the event of error, or a change to the ID card data format, the initialization process can be repeated by simply disabling the mag stripe reader, and clicking on the 'configure' button.

7.6 Option: Security and Search Options

This option page permits the user to optionally employ several features new to Version 3.00, including:

- Encryption for the student database file
- Fast searching for large student databases
- A programmable timeout which will automatically terminate the program to permit a server to access and update the student database, or restriction files



Sorted student database file, in .xlsx format: this option is provided primarily for users with very large student database files (>65,536 students, faculty, and employees). With student database files this large, the time required to search for student information can be very long, unless a 'fast search' algorithm is used; however, the algorithm requires that the database be sorted, in ascending order, using either column 1 (the primary student ID), or column 2 (the secondary student ID) as the sort key. The sort is easily done in Excel. The file must be in .xlsx format (Excel 2007 or later).

Instructions for preparing the studentdb.xlsx file can be found in the document '**Installation for IT Staff Rev X.x.pdf**', provided with the software.

Smaller student databases can avoid the sort requirement, and can be supplied in standard .xls format (Excel 2003 or earlier). The delay in accessing student info is insignificant for student databases smaller than 10,000 students.

Encryption enabled: Unilogger provides a capability for encrypting the studentdb.xls or studentdb.xlsx file, in order to keep it confidential. A utility program, 'DFencrypt.exe', is provided, and can be found in the installation directory. This encryption system uses a cell-by-cell algorithm, rather than encrypting the entire file; once encrypted, the spreadsheet file looks like it is filled with hexadecimally-encoded strings. The algorithm is highly secure, and proprietary to DataFetch; it is a progressive encryption algorithm in which equivalent data appears to be different, even though the underlying original data may be the same. The encryption utility also provides for a decryption function, for use in checking the integrity of the data.

The encryption utility requires approximately 90 seconds to encrypt a 130,000 line student database file, on a reasonably fast PC. Once encrypted, access to each student is very quick, and the combination of encryption and use of the 'fast search' option results in little perceptible delay when scanning or swiping a student ID card.

While the encrypted studentdb.xls or .xlsx file may be hosted on a server, it will be faster, in many applications, to simply download the file to the workstation; the encryption will keep the data secure.

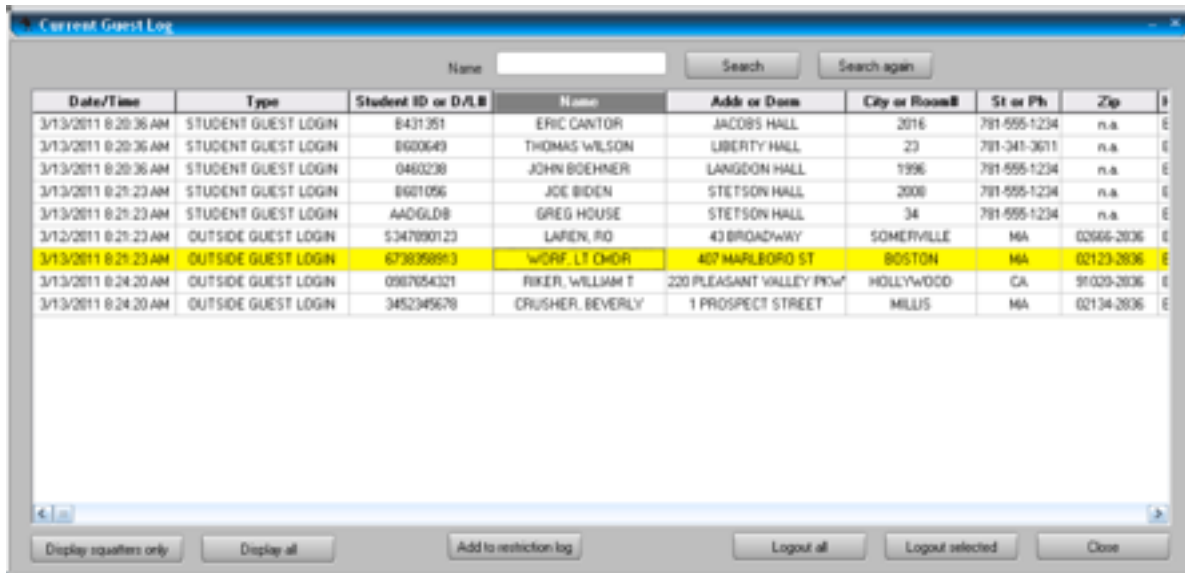
Scheduled shutdown: The Unilogger program 'opens' the student database file upon startup. Since opening a large file takes considerable time, this means that the file remains 'opened' until Unilogger is shut down. During this time, the file may not be updated.

The scheduled shutdown feature is provided to insure that the Unilogger program, if it is running continuously, will automatically shut down at a specified time so that a server may update the file.

8.0 Working with Logs

8.1 The Guest Log

A log of all guests currently logged in is available by clicking on 'Logs' in the top menu, and selecting 'Guest Log', which will bring up a new window similar to this one:



The screenshot shows a window titled "Current Guest Log" with a search bar and "Search" and "Search again" buttons. Below is a table with columns: Date/Time, Type, Student ID or D/A/B, Name, Add or Dorm, City or Room#, St or Ph, Zip, and a small icon column. The table contains several rows of guest login data, with one row highlighted in yellow.

Date/Time	Type	Student ID or D/A/B	Name	Add or Dorm	City or Room#	St or Ph	Zip	
3/13/2011 8:20:36 AM	STUDENT GUEST LOGIN	8431351	ERIC CANTOR	JACOBS HALL	2016	781-555-1234	n.a.	E
3/13/2011 8:20:36 AM	STUDENT GUEST LOGIN	8600649	THOMAS WILSON	LIBERTY HALL	23	781-341-3611	n.a.	E
3/13/2011 8:20:36 AM	STUDENT GUEST LOGIN	0460238	JOHN BOEHNER	LANGDON HALL	1996	781-555-1234	n.a.	E
3/13/2011 8:21:23 AM	STUDENT GUEST LOGIN	8601056	JOE BIDEN	STETSON HALL	2000	781-555-1234	n.a.	E
3/13/2011 8:21:23 AM	STUDENT GUEST LOGIN	A40GLD8	GREG HOUSE	STETSON HALL	34	781-555-1234	n.a.	E
3/12/2011 8:21:23 AM	OUTSIDE GUEST LOGIN	5347890123	LAFEN, RO	43 BROADWAY	SOMERVILLE	MA	02666-2036	E
3/13/2011 8:21:23 AM	OUTSIDE GUEST LOGIN	6738358513	WDRF, LT OMR	407 MARLBORO ST	BOSTON	MA	02123-2836	E
3/13/2011 8:24:20 AM	OUTSIDE GUEST LOGIN	0987654321	RIKER, WILLIAM T	220 PLEASANT VALLEY PKWY	HOLLYWOOD	CA	91023-2836	E
3/13/2011 8:24:20 AM	OUTSIDE GUEST LOGIN	3452345678	CRUSHER, BEVERLY	1 PROSPECT STREET	MILLIS	MA	02134-2836	E

At the bottom of the window are buttons: "Display squatters only", "Display all", "Add to restriction log", "Logout all", "Logout selected", and "Close".

This log shows all guests currently logged in at this particular security location. The log will show both student guests, as well as outside guests (signified by the guest type column). Scrolling the grid to the right will reveal additional columns, which include the name and student ID number of the student host, as well as any notes about outside guests.

When the size of the guest log becomes large, it may be desired to search for a specific guest, by name. This can be achieved by entering the name in the box provided above the 'name' column, and clicking on 'search'. This is a substring search: entering the name 'John' will result in the window highlighting the first occurrence on the substring 'John'. It is advisable to search on a surname, which is far more likely to be unique. If the person sought is not the person highlighted by the first search, the button 'Search again' will repeat the search and find the next matching entry.

When first opened, this window will display all guests; clicking on 'Display squatters only' will result in only those guests who have been logged in for more than the allowable number of hours (as defined in the options menu). Clicking on 'Display all' will restore the list to all guests.

Any outside guest can be simultaneously logged out as a guest, and added to the outside guest restriction log ('restricted.xls') by clicking on 'Add to restriction log'.

Security personnel can also administratively log out a single guest, or log out all guests, by clicking on the 'Logout Selected' or 'Logout all' buttons, respectively.

8.2 The Restricted Log

This log contains the information about outside guests whose behavior (or any other reason) requires that they be prohibited from being logged in as guests.

Date/Time	Type	D/L #	Name	Address	City	State	Zip
3/13/2011 8:22:19 AM	ADMIN RESTRICTION	5967890123	LAFORGE, GEORGE	1776 AVENUE E	PROVINCETON	RI	02942-2606
3/13/2011 9:48:02 AM	ADMIN RESTRICTION	678058913	WOLF, LT. CMDR	407 MARLBORO ST	BOSTON	MA	02123-2806

Whenever an outside guest is entered into the system, the restricted log is first checked to see if this person is restricted from being admitted as a guest. The criteria used is the driver's license number and the state of issue, so only outside guests whose full information had been scanned before eventually being transferred to the restricted list will be flagged.

It is advisable for security personnel using this system to manually check the restricted list for any outside guest who is unable to produce a driver's license. The restricted list can be edited using Excel, to add any names which might not have been logged in via a scan.

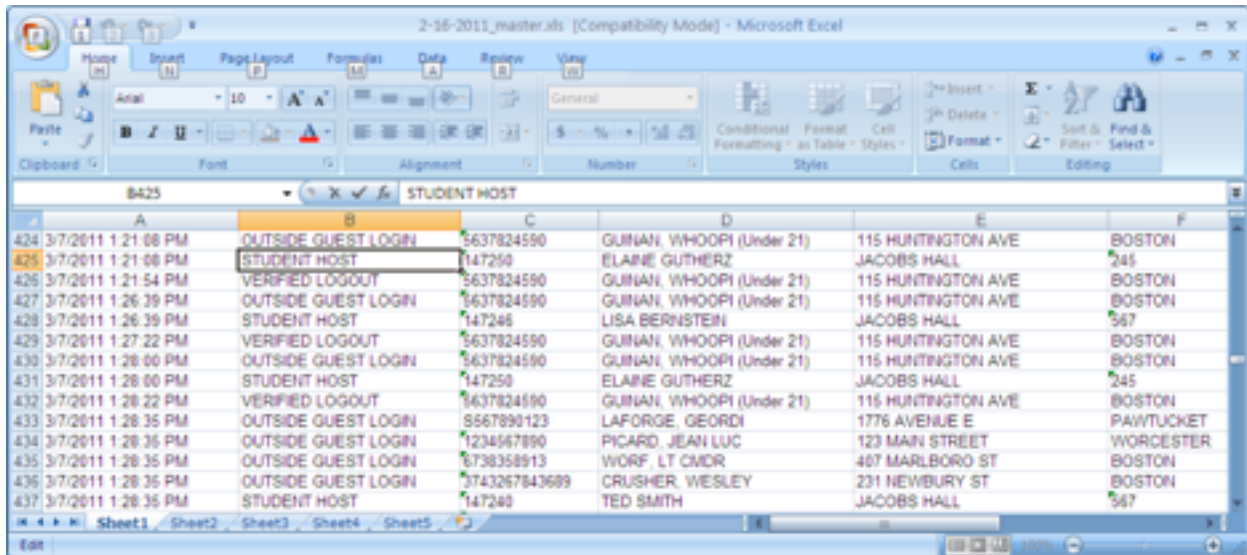
The search capability in this window works similarly to the one in the guest log window; you can specify a surname, or a fragment of a name, and find the closest match.

A person can be removed from the restricted list by clicking the 'delete' button.

9.0 The Master Log File

Unilogger maintains a master log file of all events recorded. The log starts after the program is installed and used for the first time, and is continued until approximately 65,000 entries have been appended; at that point, a new log is started. The logs are named for the date at which they are started; therefore, '2-16-2011_master.xls' was started on February 16th, and '4-30-2011_master.xls' was started on April 4th, and so on. This log is stored in the same path as the daily logs. The logs are in standard Excel compatible format, and can be read, sorted, searched, or edited, by any Excel-compatible program, such as Excel itself, or OpenOffice.

The master log file contains a record of every event, in sequence of occurrence. Each record is denoted by a record type tag in the second column:



	A	B	C	D	E	F
424	3/7/2011 1:21:08 PM	OUTSIDE GUEST LOGIN	5637824590	GUNAN, WHOOP! (Under 21)	115 HUNTINGTON AVE	BOSTON
425	3/7/2011 1:21:08 PM	STUDENT HOST	147250	ELAINE GUTHERZ	JACOBS HALL	567
426	3/7/2011 1:21:54 PM	VERIFIED LOGOUT	5637824590	GUNAN, WHOOP! (Under 21)	115 HUNTINGTON AVE	BOSTON
427	3/7/2011 1:26:39 PM	OUTSIDE GUEST LOGIN	5637824590	GUNAN, WHOOP! (Under 21)	115 HUNTINGTON AVE	BOSTON
428	3/7/2011 1:26:39 PM	STUDENT HOST	147245	LISA BERNSTEIN	JACOBS HALL	567
429	3/7/2011 1:27:22 PM	VERIFIED LOGOUT	5637824590	GUNAN, WHOOP! (Under 21)	115 HUNTINGTON AVE	BOSTON
430	3/7/2011 1:28:00 PM	OUTSIDE GUEST LOGIN	5637824590	GUNAN, WHOOP! (Under 21)	115 HUNTINGTON AVE	BOSTON
431	3/7/2011 1:28:00 PM	STUDENT HOST	147250	ELAINE GUTHERZ	JACOBS HALL	567
432	3/7/2011 1:28:22 PM	VERIFIED LOGOUT	5637824590	GUNAN, WHOOP! (Under 21)	115 HUNTINGTON AVE	BOSTON
433	3/7/2011 1:28:35 PM	OUTSIDE GUEST LOGIN	5567890123	LAFORGE, GEORDI	1776 AVENUE E	PAWTUCKET
434	3/7/2011 1:28:35 PM	OUTSIDE GUEST LOGIN	1234567890	PICARD, JEAN LUC	123 MAIN STREET	WORCESTER
435	3/7/2011 1:28:35 PM	OUTSIDE GUEST LOGIN	5738358913	WORF, LT CMDR	487 MARLBORO ST	BOSTON
436	3/7/2011 1:28:35 PM	OUTSIDE GUEST LOGIN	3743267843689	CRUSHER, WESLEY	231 NEWBURY ST	BOSTON
437	3/7/2011 1:28:35 PM	STUDENT HOST	147240	TED SMITH	JACOBS HALL	567

The record types are as follows:

- **STUDENT HOST:** this is a record of the scan of a student host ID
- **STUDENT GUEST LOGIN:** this is the record of the admission of a student guest
- **OUTSIDE GUEST LOGIN:** this is the record of the admission of an outside guest
- **ADMINISTRATIVE LOGOUT:** this record shows that a guest was logged out by the action of a security guard, without an absolute verification of the guest ID
- **VERIFIED LOGOUT:** this record shows that a guest was logged out by a repeat swipe or scan of the guest ID

Although not shown in the screen capture above, scrolling to the right will show the same sort of information (such as the name and ID number of the host) as is shown in the guest log.

This spreadsheet may be used by administrative personnel for audit purposes, and can be sorted or searched using standard Excel tools. The Unilogger™ program itself does not have a means of displaying this log, or creating reports from it; those functions can readily be done by administrative staff.

9.1 Accessing the master log

The master log (as well as the guest log and restricted log) must be online and available for use by Unilogger at any time. If any of these logs are opened by another user on the network, the logs will not reflect events which occur while another user has them opened.

Therefore, it is advisable, if administrative personnel wish to examine or work with these logs, to first copy the log, and work with the copy, rather than the log itself.