

# Login Tracking Scripts by James Rudd

## Introduction

Often when managing a school network it is important to know who has been using a machine, who was at a certain IP address at a certain time and be able to show to school committees how resource are been utilised.

The following details an easy way to keep a login log of users that can be used for tracking and statistical purposes.

I have used this setup at a large high school for several years and it has worked well, providing quick lookup for info and allowing generation of usage statistics.

## Configuration

The setup consists of 3 items.

- A batch file that receives values from the login script and determines the machines IP then appends values to a log file.
- An item in the login script that echoes local values to a batch file.
- A batch script that is run weekly to rollover the file.

First we need to setup a location for login script and for stored logs. These must be on a mapped drive.

You can create the folders anywhere, but all users must have that location accessible through mapped drive letters. I created a folder on our Apps volume mapping to G: \LNScript, and a sub folder Logs. It is important to have the logs stored in sub folder for setting user rights as we will see.

Give your users container RF rights to the LNScript folder and RW to the Logs directory. You need to make sure that the same object is given rights, and that it does NOT have file scan rights to log directory. This means if anyone looks inside it appears empty.

In the LNScript directory, create a batch file track.bat contains as follows:

```
@set IP_Addr=
@for /f "tokens=1,15 skip=5" %%i in ('ipconfig') do @if "%%i"=="IP" if
"%IP_ADDR%"==" " set IP_ADDR=%%j
```

```
@echo %*, %IP_Addr% >>G:\LNScript\Logs\LNlog.csv
@exit
```

In the container's login script, after drive mappings have taken place, add the following line:

```
@G:\LNScript\Track.bat %<COMPUTERNAME>, %P_STATION, %<USERNAME>,
%LAST_NAME, %FULL_NAME, %YEAR%MONTH%DAY, %HOUR24:%MINUTE, %PLATFORM-
%OS_VERSION, %CN
```

```
Login Script:
MAP INS S1:=Server2/SYS:PUBLIC
MAP G:=Server2/APPS:
MAP ROOT H:=%HOME_DIRECTORY

@G:\LNScrpt\Track.bat %<COMPUTERNAME>, %P_STATION, %<USERNAME>, %LAST_NAME, %FULL_NAME,
%YEAR%MONTH%DAY, %HOUR24:%MINUTE, %PLATFORM-%OS_VERSION, %CN
```

Figure 1: Login Script from Console One

And finally on a windows machine that is always left on, (eg backup terminal), setup a scheduled task to run the following batch file once a week to rollover log file. I set it for midnight on Sunday but any time is fine. This batch file will make a copy of the file with the current time date in it and set the file as read only, delete inhibit and immediate compress. It will then clear the file and recreate the title row.

LoginLogReplace.cmd

```
set t2=%time:~0,5%
set Dy=%date:~10,4%
set Dm=%date:~7,2%
set Dd=%date:~4,2%
G:
copy "G:\LNScrpt\Logs\LNlog.csv" "G:\LNScrpt\Logs\LNlog %Dy%%Dm%%Dd%
%t2::='%'.csv"
echo Comp Name, Mac Address, Login, Surname, Full Name, Date, Time, OS
Ver, Nvl UserID, IP Addr >G:\LNScrpt\Logs\LNlog.csv
flag "G:\LNScrpt\Logs\LNlog %Dy%%Dm%%Dd% %t2::='%'.csv" Ro Sh Di Ic
```

### MS Active Directory Note

If you are only using Windows and not Novell you can modify Track.bat to grab only windows environmental variables to dump to the csv file. Just place the Track.bat file in the Group Policy Scripts folder for that user group.

## Uses

### Tracking

You can very easily look at the current log or previous one by browsing to it and double clicking the csv file. This should open it up in Excel (or Calc).

If you then click Data -> Autofilter and you easily can restrict the displayed information to a specific user, computer or date.

This makes it ideal for looking at all users who logged on to a machine on a certain date or determining where a student has logged in recently.

I have also used it to determine when staff accounts are compromised, by analysing where users are logging in. If a staff member is always logging into a student PC it is very suspicious.

## Statistics Generation

The log files can be used to generate statistics on computer usage and login patterns over the short and long term.

### Short Term

Weekly login statistics can be quickly generated using Excel Pivot Tables.

1. Open a log file in Excel
2. Select all the columns with data and Insert -> PivotTable
3. Drag the data around to show what details you want

Some Ideas:

- Show users who logged in the most
- Find which computers are frequently used
- You can also do extra processing to data:
  - Round times to the nearest hour or have it display day of week to see login distributions.
  - Strip of the individual machine identifier to extract just the location of PC and see which labs are used the most. I use a strip and vlookup approach to categorise each entry.

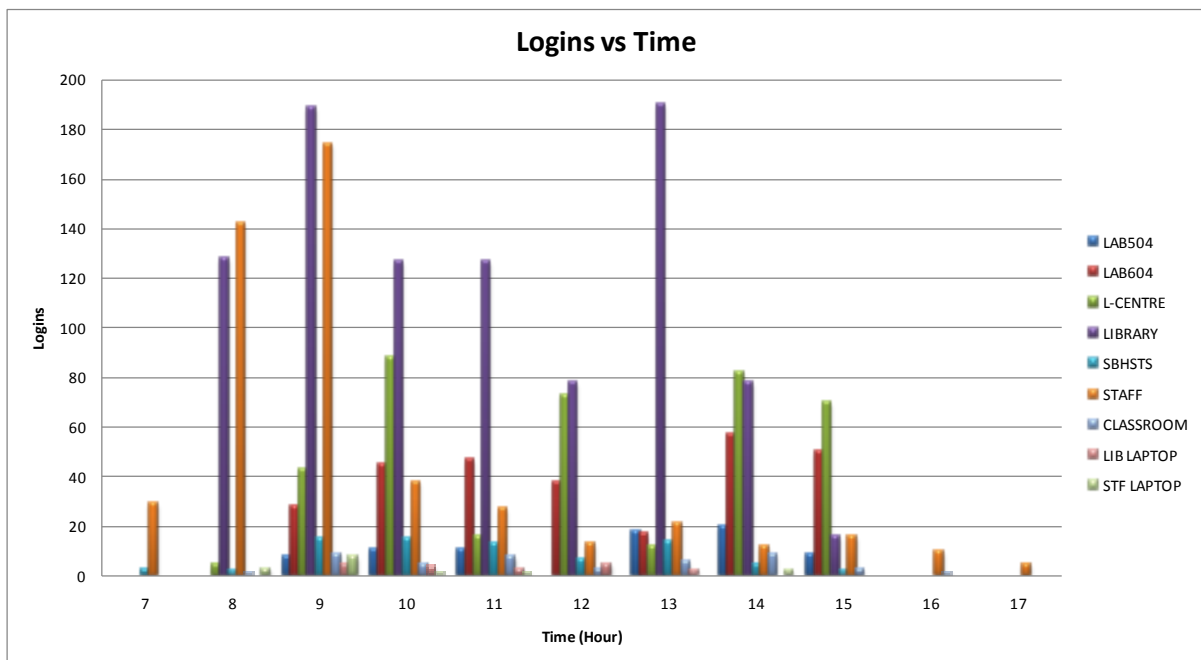


Figure 2: Shows hourly login profile over week

### Long Term

Statistics can be generated over a longer period of time by using Access or Base and importing all the log files. This is required because of the maximum row limit in Excel.

Access is a powerful program and once data is imported it can be manipulated in many ways. The following only provides an overview of one way to import data.

1. Open a command prompt and browse to the logs directory
2. Merge all the files by typing "copy Inlog\*.csv logGen.csv" or similar (eg 'copy "Inlog 2007\*.csv" logGen.csv').
3. Import the merged file into Access (or Base) and configure the import to recognise yyyyymmdd dates. As well as making date field useful it forces the DB to ignore the duplicate column headers that occurred from merging the logs.
4. Run some queries against the logs, eg Use the aggregation functions to count the top users, use similar matching to find most used labs or most used PCs

Examples:

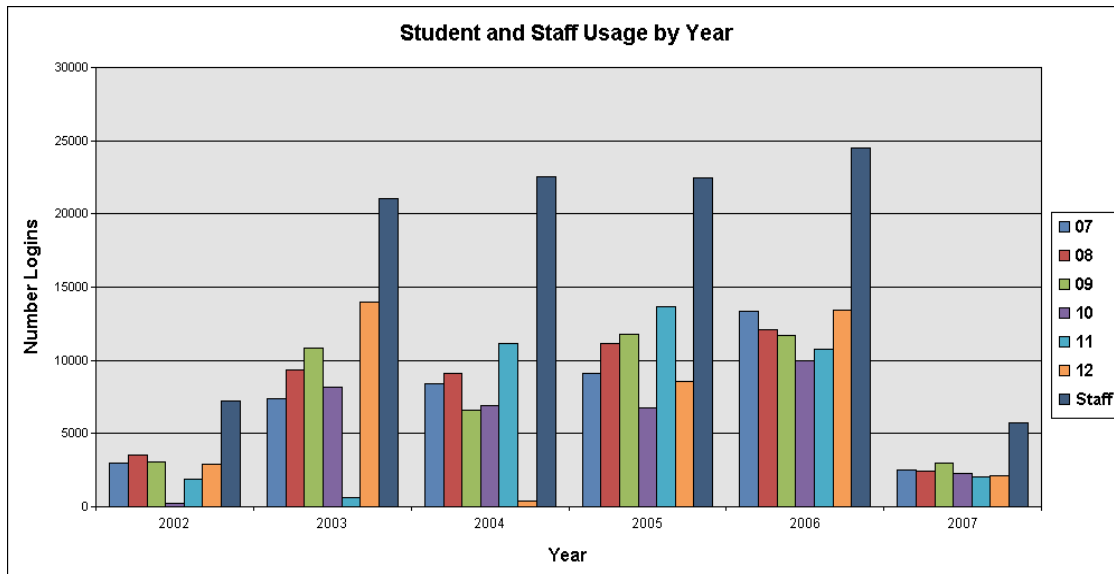


Figure 3: Shows how much each year group has used computers. (This required having a table that matched users to year to calculate what form they were in when login records were made.)

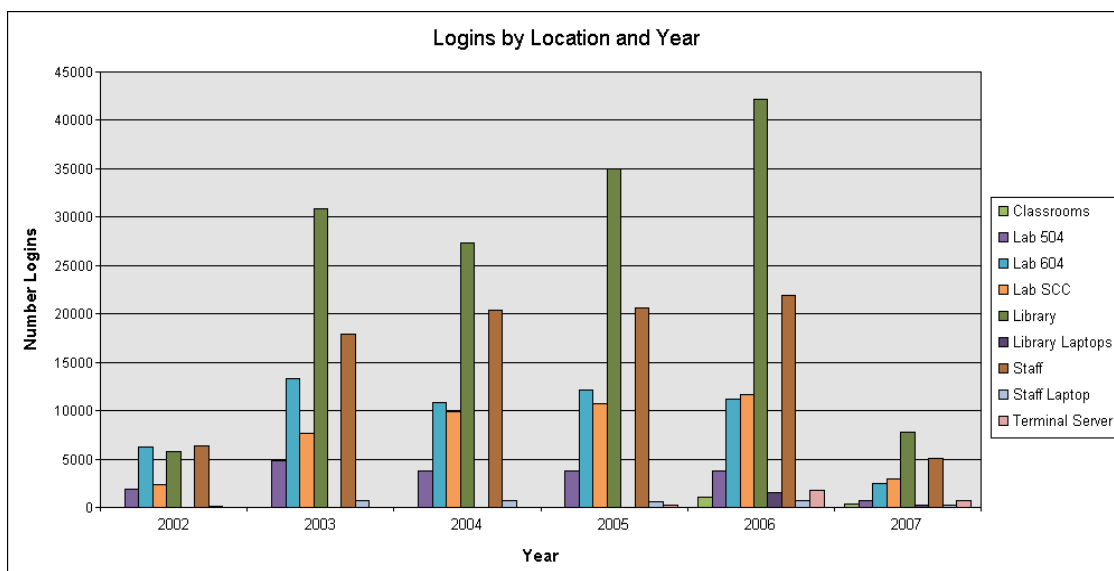


Figure 4: Shows location usage by year. Similar technique to Excel.

The IP Address batch code is by Herb Martin from <http://tinyurl.com/yup57g>