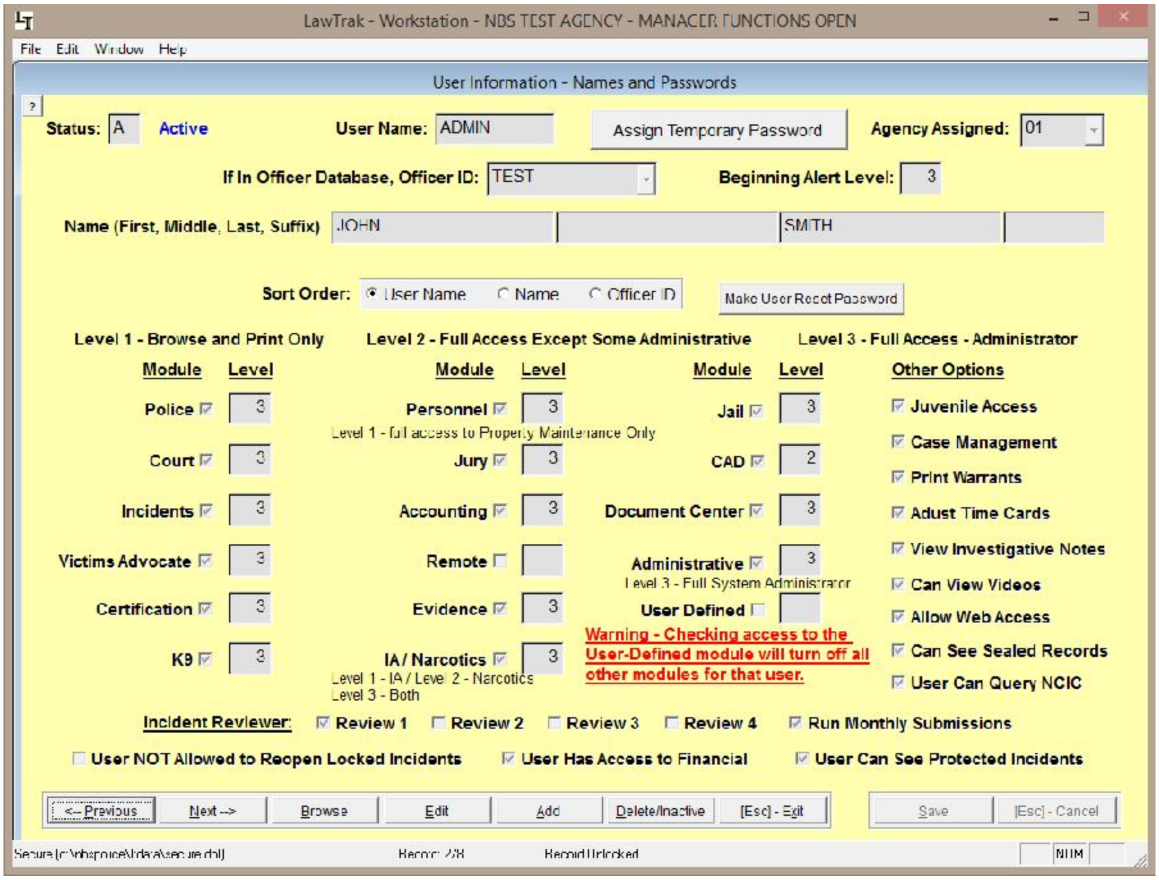
# User Information – Names and Passwords

Top Section: Administrative
Side Button: Lookups


LawTrak - Workstation - NBS TEST AGENCY - MANAGER FUNCTIONS OPEN
File Edit Window Help
User Information - Names and Passwords
Assign Temporary Password
Make User Reset Password
<-- Previous
Next -->
Browse
Edit
Add
Delete/Inactive
[Esc] - Exit
Save
[Esc] - Cancel

Status: A Active
User Name: ADMIN
Agency Assigned: 01
If In Officer Database, Officer ID: TEST
Beginning Alert Level: 3
Name (First, Middle, Last, Suffix) JOHN SMITH
Sort Order: ● User Name ○ Name ○ Officer ID

Level 1 - Browse and Print Only
Level 2 - Full Access Except Some Administrative
Level 3 - Full Access - Administrator

| Module | Level | Module | Level | Module | Level | Other Options |
|---|---|---|---|---|---|---|
| Police ☑ | 3 | Personnel ☑<br>Level 1 - full access to Property Maintenance Only | 3 | Jail ☑ | 3 | ☑ Juvenile Access |
| Court ☑ | 3 | Jury ☑ | 3 | CAD ☑ | 2 | ☑ Case Management |
| | | | | | | ☑ Print Warrants |
| Incidents ☑ | 3 | Accounting ☑ | 3 | Document Center ☑ | 3 | ☑ Adust Time Cards |
| Victims Advocate ☑ | 3 | Remote □ | | Administrative ☑<br>Level 3 - Full System Administrator | 3 | ☑ View Investigative Notes |
| | | | | | | ☑ Can View Videos |
| Certification ☑ | 3 | Evidence ☑ | 3 | User Defined □ | | ☑ Allow Web Access |
| K9 ☑ | 3 | IA / Narcotics ☑<br>Level 1 - IA / Level 2 - Narcotics<br>Level 3 - Both | 3 | Warning - Checking access to the User-Defined module will turn off all other modules for that user. | | ☑ Can See Sealed Records |
| | | | | | | ☑ User Can Query NCIC |

Incident Reviewer: ☑ Review 1 □ Review 2 □ Review 3 □ Review 4 ☑ Run Monthly Submissions

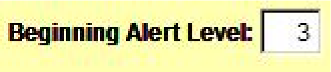
□ User NOT Allowed to Reopen Locked Incidents ☑ User Has Access to Financial ☑ User Can See Protected Incidents

Secure (c:\nbspolice\ltdata\secure.dbf) Record: 2/8 Record Unlocked NUM

This file contains information about User Names and Passwords allowed into LawTrak, and what level of access the user will have. **Every person accessing LawTrak should have their own User Name and Password.** This will allow the program to track what users are doing. Only someone with Administrative Level 3 can access this screen.

Every entry must have a unique User Name. This can be up to 10 characters/numbers. Every user name must have a Password.

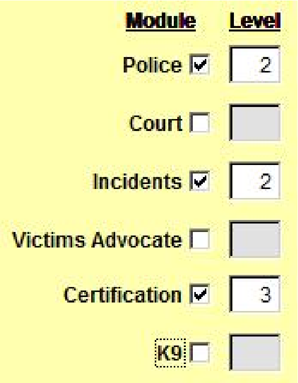
**Delete/Inactivate Users:** When a user is no longer allowed into LawTrak, he should be deleted off this screen. If a user is temporarily barred from the system (i.e. password not reset before time limit expires), he can be temporarily inactivated. Pressing the Delete/Inactive button once will Inactivate the user. Pressing it again will mark the user for Deletion. Pressing it a third time will bring the user back active.



Beginning Alert Level: 3

The Beginning Alert Level will determine which alerts/warnings the user can see when he first logs onto LawTrak. An Alert Level of 3 will show most warnings.

## Setting Access to Modules and Levels



| Module | Level |
|---|---|
| Police ☑ | 2 |
| Court □ | |
| Incidents ☑ | 2 |
| Victims Advocate □ | |
| Certification ☑ | 3 |
| K9 □ | |

A user can be assigned to specific modules within LawTrak, and kept out of other modules. Each module has a Level associated with it. The Levels basically correspond as follows:

**Level 1** – can Browse some records and print some reports. No data entry is allowed.

**Level 2** – can Add, Edit and mark some records for Deletion. This is the basic level set for most individuals using the program.

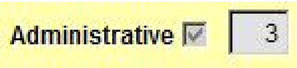
**Level 3** – can access any part of the module and run most administrative functions for the areas they are allowed in. Can delete most things.

As seen above, you can mix the levels to different parts of LawTrak. For example, if this user is allowed to enter tickets and incidents as a normal user, but is in charge of keeping track of Certification, he can have Level 2 in most areas and Level 3 in Certification.

There are a couple of modules that do not follow this basic rule:

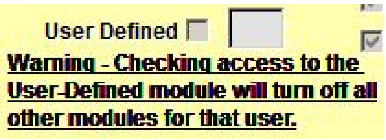
**Personnel** – Level 1 has full access to the Property Maintenance, but cannot see the Complaints and Disciplinary Actions.

**Evidence** – Level 1 can put in the initial evidence entry (i.e. collecting it in the field), but cannot edit or move the evidence once it has been entered.



Administrative ☑ 3

**WARNING:** Allowing someone access to the Administrative module may give that user more influence in the program than you want. A Level 3 Administrator can change his own level in any module, and can add or change the access of other users. This should be given to as few users as possible. Administrative Level 2 has the ability to do some maintenance (i.e. Reindex files), but cannot reset access levels for anyone.



User Defined □

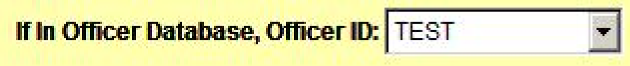
**Warning - Checking access to the User-Defined module will turn off all other modules for that user.**

There is an option to set a user as User Defined. This will allow you to assign up to 13 very specific buttons to that user. Example: A user is responsible only for writing Parking Tickets. He can be assigned the Parking Ticket menu button, and some of the Report buttons. He will not be able to get into any other parts of the program.

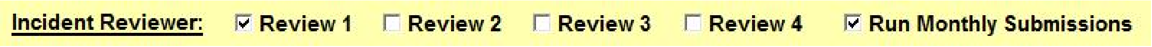
Once you get the user entered, you must Assign a Temporary Password. When the individual logs in for the first time, he must change his password to something more permanent.

All passwords have a 90-day expiration, and you must use 10 passwords before you can re-use any old ones. You can change the user password as often as you want.

## Attaching Users to Officer Database

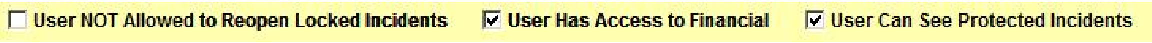

If In Officer Database, Officer ID: TEST

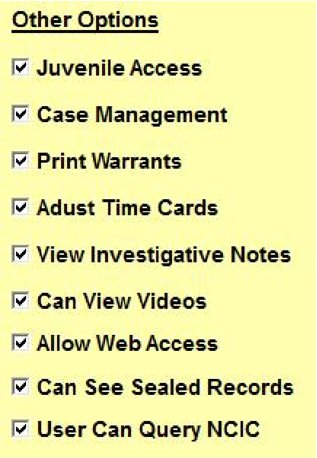
If the user is also in the Officer Database, you can attach the Officer ID to the user. This will allow parts of the program to access the Logon Name as well as the Officer ID number if needed. For example, there are certain places in LawTrak that will send LawTrak Mail to officers, but must have the Logon Name attached since the LawTrak Mail works on the User Name.


Incident Reviewer: ☑ Review 1 □ Review 2 □ Review 3 □ Review 4 ☑ Run Monthly Submissions

The **NIBRS Reviewer** options should be assigned to those users Reviewing Incident Reports, and those doing the NIBRS submissions.

## Other Options


□ User NOT Allowed to Reopen Locked Incidents ☑ User Has Access to Financial ☑ User Can See Protected Incidents


Other Options

- ☑ Juvenile Access
- ☑ Case Management
- ☑ Print Warrants
- ☑ Adust Time Cards
- ☑ View Investigative Notes
- ☑ Can View Videos
- ☑ Allow Web Access
- ☑ Can See Sealed Records
- ☑ User Can Query NCIC

These options allow for some specific access to parts of the program, or keeps the user from accessing some sections.

**User NOT Allowed to Reopen Locked Incidents** – This option is normally turned off, and users are generally allowed to unlock reports to make necessary edits. An Incident Report is locked when it is either Reviewed or Submitted. Turning this option on for a user will keep him from editing a report once it has been reviewed.

**User Has Access to Financial** – This will allow the user to enter receipts and run money collection reports.

**User Can See Protected Incidents** – Normally if an Incident Report is Protected, only the user who protected it can see any information. If a user is responsible for reviewing Incident Reports, he may need to see the protected report.

**Juvenile Access** – A user can override the Juvenile settings on printing reports.

**Case Management** – Allows a user to assign investigators and close cases in-house.

**Print Warrants** – If this option is checked, the user will be allowed to Add, Edit and Print Warrants.

**Adjust Time Cards** – The user can make corrections to Time Cards.

**View Investigative Notes** – Investigative Notes access should only be given to Investigators or those reviewing the cases. These notes normally do not print out with the regular Incident Reports. Only someone with this option checked will be allowed to view, create, or print incident reports.

**Can View Videos** – This will allow the user to view videos attached to Incident Reports.

**Allow Web Access** – There are a couple of places in LawTrak where the user can have an Internet Page displayed. Normally this is not used.

**Can See Sealed Records** – This option allows the user to see the Sealed Records which contain expunged Incidents and Court Cases.

**User Can Query NCIC** – This allows the user to do LawTrak Quick Queries that can tie into several NCIC systems that we work with.