System Security

Setup

Table on Contents

Introduction

The manual describes how to setup the Security Management system. Only users with **Setup Security** rights will have access to the security system.

Access the security system by selecting the main menu choice **System**, then selecting the sub menu choice **Security**. The Security Setup screen will be displayed. There are several tabs in this module, each is explained in the following sections.

Security Report

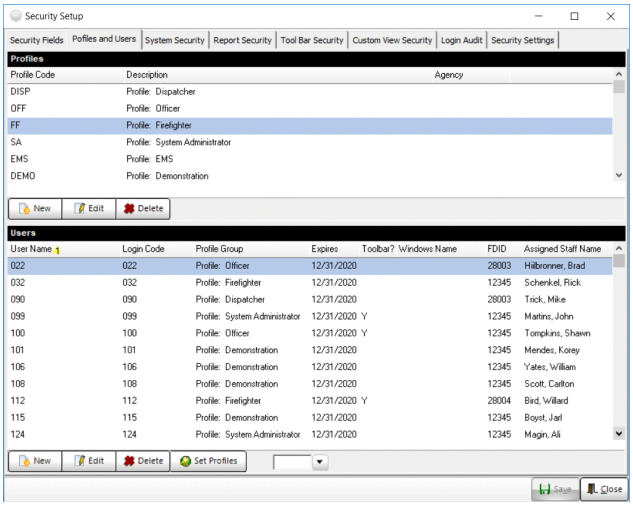
Included in the General Reports section of the Report Manager is a report called Security Fields. Access this report by clicking on the reports button from the main menu. The system defaults to displaying the list of reports under the General Reports Section, select the Security Fields report. This report prints out all of the possible security fields installed on your system. Included with each item is a brief description of each field.

Tab: Profiles and Users

The Security Module is broken up into two sections.

1. **Profiles.** Profiles represent a general level of security. Each user is assigned to a profile. Examples include:
   - A. ADM - Administrator Profile. Has access to everything like security, setup functions, and deletes.
   - B. OFF - Officer Profile. Access to most everything, but not able to get into setup functions and security.
   - C. FF - Firefighter. Can view most non confidential data, and can finish incident reports.

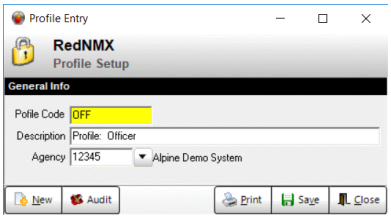
2. **Users.** Represents the entry made that a user selects to log in. It includes the user name, security settings, and password. **Users are assigned to Profiles.**



It is recommended that you enter profiles first, then assign users to profiles. This way you do not have to manage so many accounts.

Profiles

While in the security, select the Profile and Users tab. The profiles are listed in the Profile List.



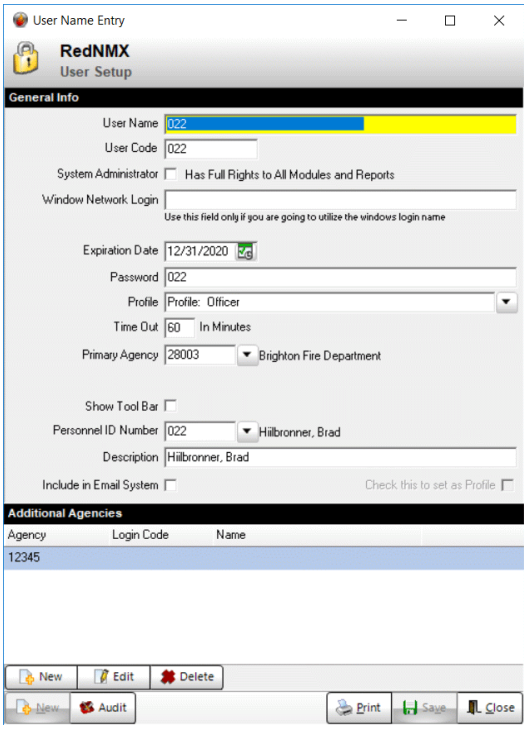
The following fields are entered in the Profile Section

Field	Description	Requirement	Comments	Example
Profile Code	Code that presents the Profile.	Yes	Enter something unique	OFF
Description	Description of the Profile	Yes	Keep it simple.	Profile: Officer
Agency	Agency profile applies to.	No	Only applies to multi agency systems	12345

Users

While in the security, select the Profile and Users tab. The User List is where all registered users of the system are maintained.

- **User Accounts.** Each user is assigned a user account. Included with each account is a user name and password. ***User names must be unique, you cannot have duplicate user names.***

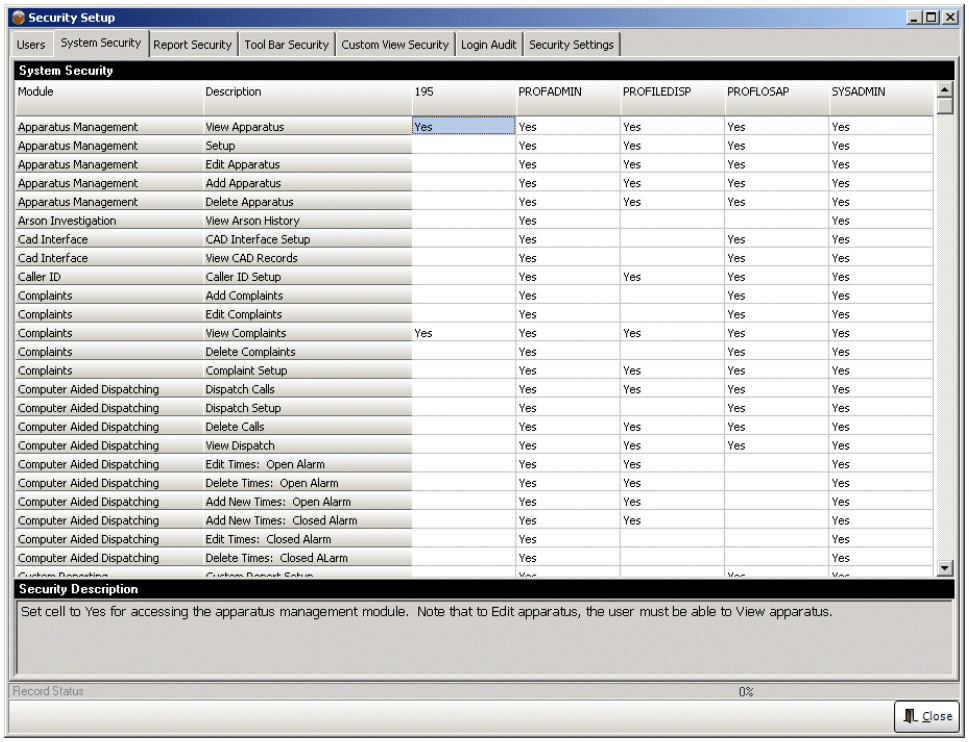


Field	Description	Requirement	Comments	Example
User Name	The user name that the user will enter to log in.	Required.	Must be unique. It is also recommended, but not required that you not have any spaces. Also user their staff ID if possible.	022
User Code	The user code that the user will enter to log in.	Required.	This is an additional field for departments that have coded users.	022
System Administrator	This overrides everything and makes the user a system administrator.	Not Required.	Checked or Unchecked.	N/A
Windows Network Login	User name for logging into the windows network. This works for Active Directory Security Settings.	Not Required.	Must be identical to users windows login. Used only when individual windows logins are used.	N/A
Expiration Date	The date the user account expires.	Required.	N/A	N/A
Password	Password used to verify the user is who they say they are.	Required	N/A	N/A
Profile	This represents the profile the user is assigned to.	Not Required.	If this is blank, the user becomes stand alone.	Profile: Officer

Time Out	Number of minutes till time out.	Not Required.	Leave this blank if this feature is not to be used.	10
Primary Agency	Agency user is assigned to. This only applies to Multi Agency Systems.	Not Required.	Leave this blank if the user can access all agencies. This only applies to Multi Agency systems.	12345
Show Tool Bar	Determines if the user account includes a floating tool bar.	Not Required.	Individual Tool Bars are setup in the Tool Bar Security section	N/A
Personnel ID Number	Personnel ID number of user in the personnel table.	Not Required, but highly recommended if this is active staff.	Enter the personnel ID number for use in several default for training and NFIRS reporting.	100
Description	Description of the User	Not Required.	Enter the description in the space provided.	N/A
Include in Email System	Include user in the email system.	Not Required	Applicable if you have the email system.	N/A

Tab: System Security

Select the System Security to access the following screen.



Please create users and profiles prior to completing this section.

This section allows for individual user rights to be toggled on or off. The first column references the module within RedNMX. The second column lists the items able to be secured within each module. The remaining columns show profile names and non profiled user names. Note that individual user names for users assigned to a profile are not displayed. This is because individual users assigned a profile, receive their security settings from the named profile. Therefore only profile names and non profiled user names will be displayed.

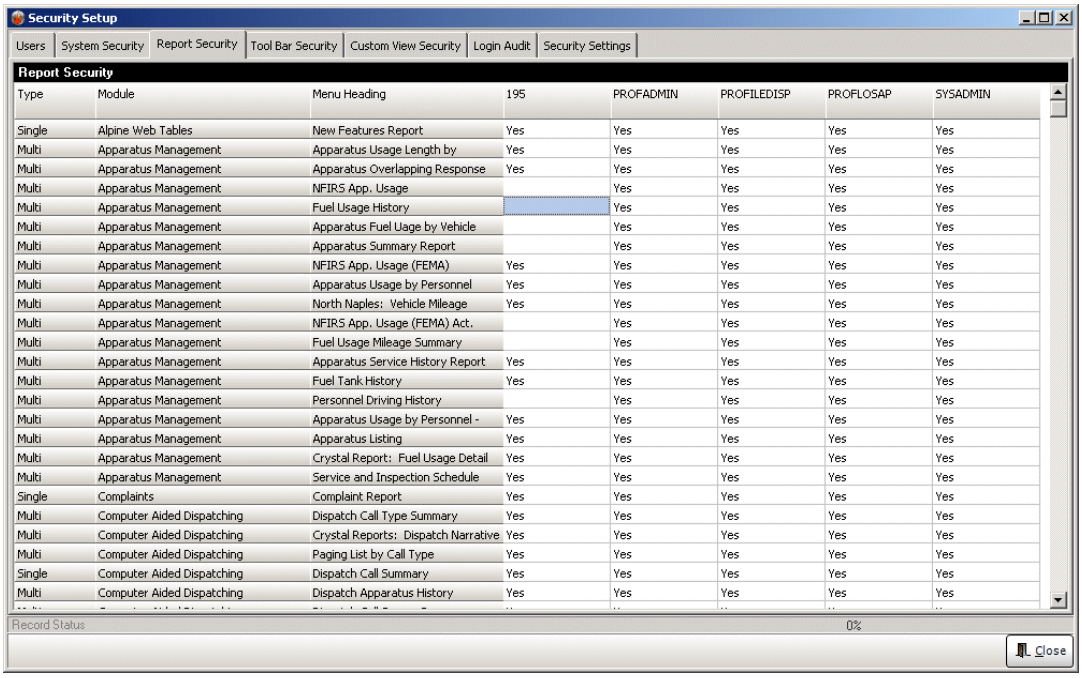
You can do any one of the following to grant or deny access to a particular item. “Yes” grants access, a blank cell denies access.

- Double Click on the cell.
- Press the Space Bar on the cell.
- Press the Enter button on the cell.

Anyone of the above keys will toggle the security entry. The security description field displays what the field does.

Tab: Report Security

Please create users and profiles prior to completing this section. Note that only profile names and non profiled user names are displayed. Select the Report Security tab to access the following screen

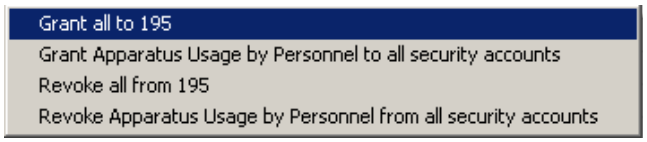


Type	Module	Menu Heading	195	PROFADMIN	PROFILEDISP	PROFLOSAP	SYSADMIN
Single	Alpine Web Tables	New Features Report	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	Apparatus Usage Length by	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	Apparatus Overlapping Response	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	NFIRS App. Usage		Yes	Yes	Yes	Yes
Multi	Apparatus Management	Fuel Usage History		Yes	Yes	Yes	Yes
Multi	Apparatus Management	Apparatus Fuel Uage by Vehicle		Yes	Yes	Yes	Yes
Multi	Apparatus Management	Apparatus Summary Report		Yes	Yes	Yes	Yes
Multi	Apparatus Management	NFIRS App. Usage (FEMA)	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	Apparatus Usage by Personnel	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	North Naples: Vehicle Mileage	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	NFIRS App. Usage (FEMA) Act.		Yes	Yes	Yes	Yes
Multi	Apparatus Management	Fuel Usage Mileage Summary		Yes	Yes	Yes	Yes
Multi	Apparatus Management	Apparatus Service History Report	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	Fuel Tank History	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	Personnel Driving History		Yes	Yes	Yes	Yes
Multi	Apparatus Management	Apparatus Usage by Personnel -	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	Apparatus Listing	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	Crystal Report: Fuel Usage Detail	Yes	Yes	Yes	Yes	Yes
Multi	Apparatus Management	Service and Inspection Schedule	Yes	Yes	Yes	Yes	Yes
Single	Complaints	Complaint Report	Yes	Yes	Yes	Yes	Yes
Multi	Computer Aided Dispatching	Dispatch Call Type Summary	Yes	Yes	Yes	Yes	Yes
Multi	Computer Aided Dispatching	Crystal Reports: Dispatch Narrative	Yes	Yes	Yes	Yes	Yes
Multi	Computer Aided Dispatching	Paging List by Call Type	Yes	Yes	Yes	Yes	Yes
Single	Computer Aided Dispatching	Dispatch Call Summary	Yes	Yes	Yes	Yes	Yes
Multi	Computer Aided Dispatching	Dispatch Apparatus History	Yes	Yes	Yes	Yes	Yes

The type column shows either Multi or Single. Multi reports are found in the main report manager, where as Single types are found in the individual record report managers.

The Report Security section provides the system administrator with the ability to control access to specific reporting functions throughout the system. Double click the appropriate cell on the grid to grant or deny access to a particular report. “Yes” grants access, a blank cell denies access. You can also use the space bar to grant or deny.

In addition, right click on a column to bring up the following menu:



These menu choices allow you

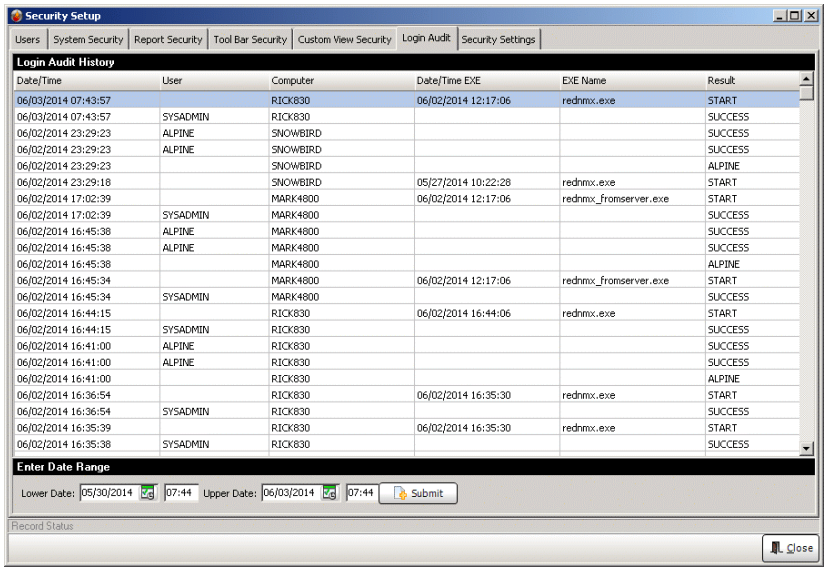
- Grant or revoke access to all users for one report.
- Grant or revoke access for one user for all reports.

Tab: Tool Bar Security

The items in the first column are setup by Alpine personnel. The administrator can control which quick pick functions are available for each profile and non profiled user.

Tab: Login Audit

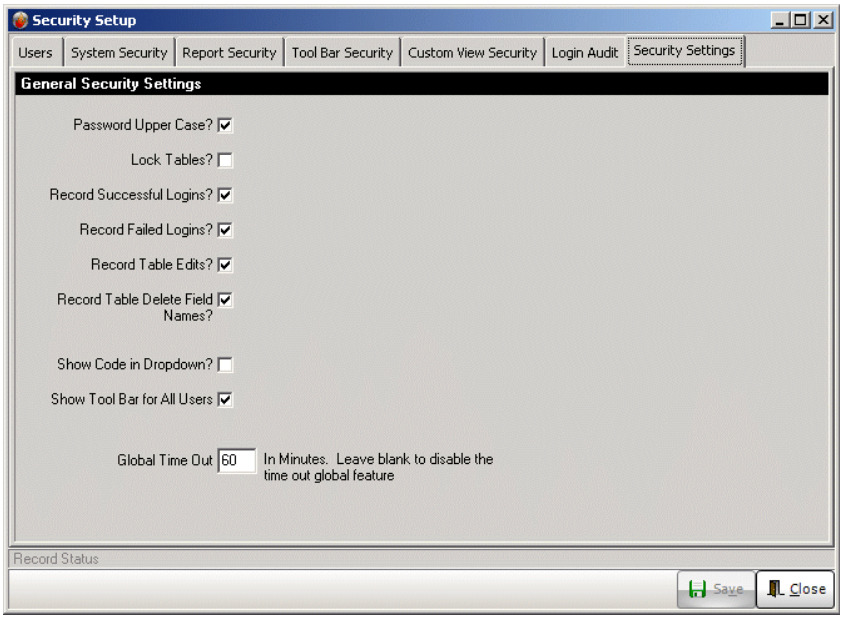
This section lists all logins from all users during the time period entered at the bottom of the window. This time frame is configurable by any user with access to this window.



Enter the date range in the fields and then press the Submit button.

Tab: Security Settings

Description of each security setting.



Field	Description	Comments
Password Upper Case	Determines if the user name and password are converted to upper case.	This is determined by the system administrator.
Lock Tables	Determines if viewing a table will lock it.	This is entered by Alpine tech personnel. This is not active at this time.
Record Successful Logins	Records when a user logins in successfully	This is determined by the system administrator.
Record Failed Logins	Records when a user fails to login.	This is determined by the system administrator.
Record Table Edits and Views.	Records every time a user edits or view a record in the table. You can access t his history from the	This is determined by your system administrator.
Show Code in Dropdown	Show the user code in the user name pick list.	This is determined by your system administrator. Many departments use the code instead windows name.
Show Tool Bar for All Users	Show the tool bar for all users.	This is determined by your system administrator.
Global Time Out	Number of minutes of inactivity until the program will exit out of the system.	This is determined by your system administrator.

Security Management Methods and Configuration

This section describes two primary methods of security set up configuration. These can be used in combination with each other.

1 to Many Profile Method

This method is typically utilized for larger departments where a large number of users all receive the same access privileges. It is based on creating and maintaining one master profile for a larger number of individual users. Each individual user has a unique User-name and Password. The System Administrator controls the access from the Profile.

Most agencies utilize 3 or 4 different profiles. Examples include

- **View Only Profile.** This type of profile can only view records. No editing or deleting can take place.
- **Line Officer Profile.** This type of profile can only view, add, edit and delete records. User assigned to this profile cannot change modules settings.
- **Administrator Profile.** This type of profile can access any part of the system.

To set up a profile

1. Go to the **Users** tab of the Security Setup and select the **New** button on the bottom left.
2. Fill in the **User Name** field with the title of the Profile (ie: Department X, Department Y, Chiefs, Officers, etc.)
3. **Windows Network Login** is not utilized for Profile setup.
4. **Expiration Date** is not utilized for Profile setup.
5. Leave the **Password** field blank for Profile configuration.
6. Select an **FDID** number from the drop down to isolate access to one particular agency. Leave blank for all agencies.

To set up a new user with Profile configured Access

1. Go to the **Users** tab of the Security Setup and select the **New** button on the bottom left.
2. Fill in the **User Name** field. Note: it is common to use a persons system ID number for this purpose.
3. (Optional) **Windows Network Login** can be utilized if desired. Enter the user's Windows Username exactly if desired.
4. Enter an **Expiration Date** for the user account. Leave the **Expiration Date** field blank for Profile configuration.
5. Enter a **Password** for the user.
6. Select the **Profile** you want to link the user account with.
7. Select an **FDID** number from the drop down to isolate access to one particular agency (multi-agency systems only).
8. Test the user configuration.

1 to 1 Method

This method involves granting security access to each user. This is a more labor intensive method that requires individual management of each user. Use this method for allowing an individual specific access not shared with any other user.

To set up an individual unique user

1. Go to the **Users** tab of the Security Setup and select the **New** button on the bottom left.
2. Fill in the **User Name** field. Note: it is common to use a persons system ID number for this purpose.
3. (Optional) **Windows Network Login** can be utilized if desired. Enter the user's Windows Username if desired.
4. Enter an **Expiration Date** for the user account. Leave the **Expiration Date** field blank if no expiration is desired.
5. Enter a **Password** for the user. Leave the Password field blank for Profile configuration.
6. Select an **FDID** number from the drop down to isolate access to one particular agency (multi-agency systems only).
7. Test the user configuration.

Multi FDID Systems

The RedNMX System supports multi agency systems. Only Alpine personnel can turn on the Multi Agency flag. The following changes will be visible when the system runs in the Multi Fdid mode.

1. All primary views will have the Agency field visible. These include
   - NFIRS History
   - EMS History
   - Personnel
   - Dispatch Locations
   - General Inventory, Hose, SCBA and Apparatus
   - Non Incident History

2. The RedNMX View System will include an agency check list. The following rules apply:
   - If the agency field found in the user security setup is blank, this user can view data for all agencies.
   - If the agency field is filled in with an agency, this user can only view records that match the agency.

3. The Agency field will be visible on the data entry screens for all of the primary tables. These include
   - NFIRS Incident Entry
   - EMS Incident Entry
   - Personnel Record
   - Dispatch Location Entry
   - General Inventory, Hose, SCBA and Apparatus Entry
   - Non Incident Entry