National Fire Incident Reporting System (NFIRS 5.0)

System Administration Tool Users Guide

NFIRS 5.0 Software Version 5.6
1/7/2009

Department of Homeland Security
Federal Emergency Management Agency

United States Fire Administration

TABLE OF CONTENTS

1. Introduction

The System Administration Tool Guide provides comprehensive documentation to enable State NFIRS Program Managers to efficiently use the NFIRS System Administration Tool. The Guide is intended for new users as well as users familiar with the NFIRS system administration tasks. For a Rapid Startup Guide that outlines only the key steps for setting up groups and activating users refer to Section 10 of this document.

The System Administration Tool is a Graphical User Interface (GUI) developed for the administration of National Fire Incident Reporting System Database users and groups. With this tool the administrator may add and modify groups and users in a graphical environment.

State NFIRS Program Managers may assign system administration privileges to an individual (s) registered in the NFIRS community to assist with user account and group maintenance, if necessary.

System Administrators who access the System Administration Tool will be able to view the Group Hierarchy at their level and below. The System Administrator will be able to add, view, and modify groups and fire departments. **Note:** Groups can be modified but not deleted.

System Administrators will be able to add, view, delete, and modify user information in the User Maintenance Window. State NFIRS Program Managers may view all registered users, view administrators within the state, set users' permissions, reset passwords, view user activity status (inactive or no activity within 60 days) and number of bad logins.

State Program Managers and their System Administrators will use the System Admin Tool to assign necessary permissions to registered NFIRS 5.0 users who wish to access the new NFIRS 5.0 web-based tools. Permission for the Bulk Import Utility and the new web-based Summary Reports Output Tool can be assigned exclusively since they do not require the use of the USFA NFIRS 5.0 software.

NFIRS 5.0 Version 5.6

The NFIRS 5.0 Version 5.6 System Administration Tool is functionally equivalent to Version 5.5.

NFIRS 5.0 Version 5.5

The NFIRS 5.0 Version 5.5 provides the same functions as offered in previous versions 5.4 and 5.3. In addition to user account and group maintenance, the NFIRS 5.0 Version 5.5 System Administration Tool has three components formerly within the Program Administration Tool (as of version 5.3): the Codes Editor, the tool used to add and modify Plus One Codes; and the Special Studies Editor, used to add and modify Special Studies. The Chemical Editor enables the national level user to add and edit the chemicals information and codes in the National Database. The user must have the Program Admin permission to access these interfaces and to save changes made within them.

A user with the State Admin permission assigned to their account can assign the Bulk Import permission to users at their level and below, and access the Field Permission

(Field Perms) button. The Field Perms interface enables the State Program Manager to modify the default Field Level Security settings to prevent data from being released publicly at the federal level when to do so would conflict with state and local jurisdiction laws. The Design Documentation available at http://www.nfirs.fema.gov/documentation/design/ lists the default System Security Field Settings for the NFIRS 5.0 data fields, beginning on page 108.

The NFIRS 5.0 System Admin Tool Version 5.5 continues to automate password management and enforces password format to meet FEMA's guidelines established to ensure minimal risk to system and information access.

NFIRS 5.0 Version 5.4.2

The automatic deactivation of user accounts that have not had a login to the On-line system within 60 days continues to support the DHS/FEMA security standard. In Version 5.4.2, an adjustment was made which will assist State Program Managers in resetting Inactive status accounts: the 24 hour automatic deactivation has been removed. If an account is reset to Active status, the user will have 60 days to login. The adjustment allows the user longer than 24 hours to login with resets of these accounts. For complete information and recommendations, refer to Section 3, User Maintenance.

The release of NFIRS 5.0 Version 5.4.2 in August 2007 included a minor change which prevents users below the state level from creating groups. To create a group in the On-line system, a user must be assigned to the State level group and have the write incident Delete Group, which is a default permission. Also, in Version 5.4.2, the User maintenance Window's email address field has been lengthened to facilitate view.

Definition and Development of Groups

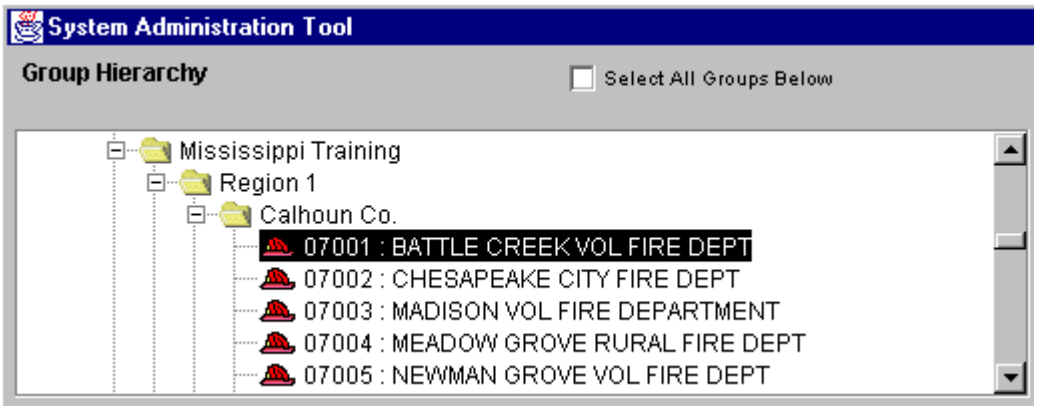
The hierarchical structure for group organization allows for ease in system administration maintenance, enforces security at group levels, and distributes administration privileges. The Group Hierarchy is in extended list form. Information in the Group Detail fields changes according to the highlighted group.

The extended list is analogous to a tree. The state is the trunk of the tree, the county or region is the branch, and the fire departments are the leaves (referred to as "nodes" throughout this document). Because of the hierarchical nature of Groups, all groups end at the FDID level. A group one level higher than another is referred to as a "parent" or "parent group." Parent groups are indicated by a yellow folder including a plus sign, and FDIDs are indicated with a red fire hat icon.

Note: The administrator can view, add, and modify a group and/or node at his or her level or below.

Fire Departments may be grouped several ways and should be created to facilitate the management of System Administrators and Fire Departments. One method of grouping Fire Departments is by region. Diagram 1.0 displays the Group Hierarchy for Mississippi Training with the groups defined by region, then defined by county, and ending with Fire Departments.

Diagram 1.0



Groups may be created for Congressional Districts, counties, cities, etc. It may be desirable to create a Group of Fire Departments for a large city and assign an Administrator to the Group. In this manner, the State level Administrator can share the workload of Groups and user maintenance through the sharing of administrative tasks and enforcing group level security. Users can be associated with individual Fire Departments and/or with Groups.

In order for a user to begin entering incident information with the NFIRS 5.0 software, the fire department must be created and saved by using the System Administration Tool. The administrator will need to create groups first, assign registered users to the appropriate group, then activate each user's status and set their permissions. Periodically the administrator should check for new registered users.

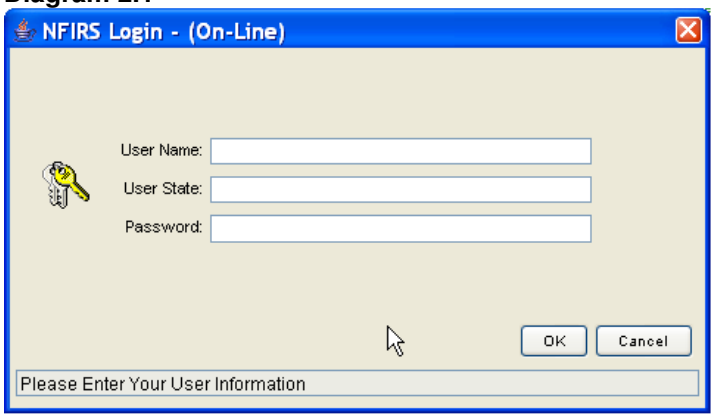
2. Starting the NFIRS System Administration Tool

The System Administrator may start the NFIRS System Administration Tool one of two ways: From the Start menu … Programs … NFIRSv56… System Admin Tool, or from within the NFIRS Data Entry Tool, click on the Tools Tab on the Menu Bar and then click on System Admin Tool.

When an administrator starts the NFIRS System Administration Tool, a pop-up window "Setting Database Connection" appears (diagram 2.0) followed by a login window (diagram 2.1). If the login window fails to come up, there is a configuration issue, which must be resolved. Please refer to the NFIRS Configuration Tool User's Guide Documentation to solve configuration issues can found at the NFIRS Web Site: http://www.nfirs.fema.gov/users/userdocs.shtm

Diagram 2.0

Diagram 2.1



At the login window, the Administrator must enter their User Name, State, and Password and then click on the **OK** button. **Note:** The Username, State and Password entered must be the same values as those entered during the registration process. If an Administrator registers under one name but tries to access the NFIRS System Administration Tool under a different name, an error will be generated. The **Cancel** button may be clicked to exit the System Admin Login Window.

The Administrator is allowed up to five consecutive failed login attempts after which the system locks the Administrator's account. Successful login after less than five failed attempts will reset the failed login counter. If the Administrator's account becomes locked, another Administrator at the Administrator's group level or higher will have to unlock the account using the NFIRS System Administration Tool.

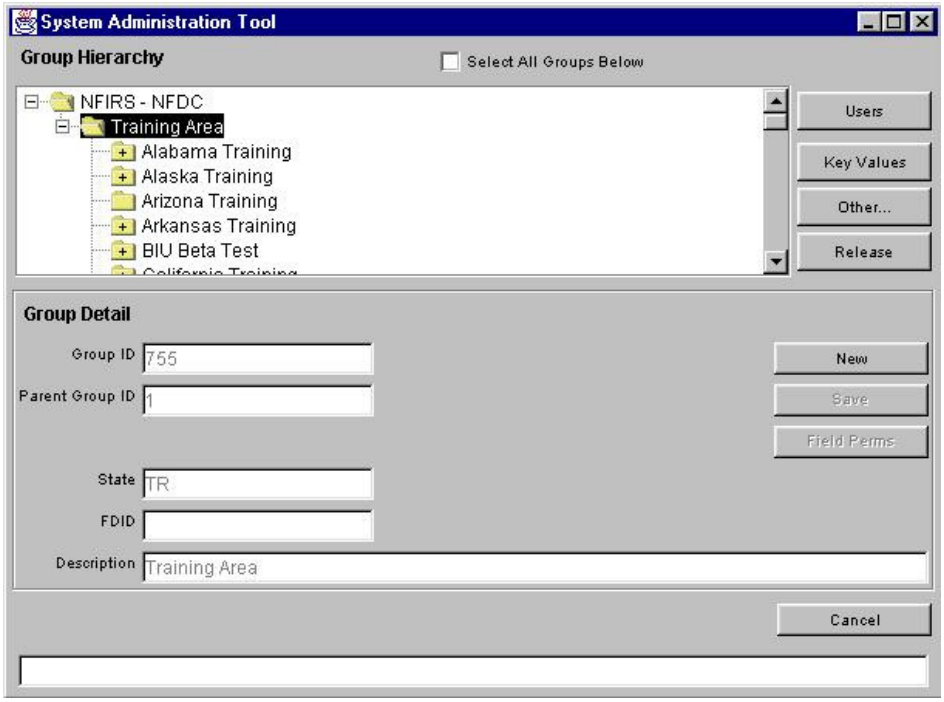
Upon successful login to the database, the first window that appears is the Group Hierarchy Window (diagram 2.3). Group maintenance is performed with the components of this window. Depending on the user's permissions, additional buttons will be displayed.

- The **Release** button will only be displayed if the user's Parent Group is 1 and the user has been assigned Release Incident permission. For more information on Releasing Incidents, refer to Section 5.
- The **Other…** button will only be displayed if the user has been assigned the Program Admin permission. The Codes, Chemicals, and Special Studies interfaces are accessed by clicking on the Other… button. For more information on these interfaces, refer to Sections 6-8.

- The **Field Perm** button will only be displayed if the user has been assigned the State Admin permission. For more information on the Field Perms interface, refer to Section 9.

Diagram 2.3 displays the main view of the System Admin Window, state of Training (TR).

Diagram 2.3



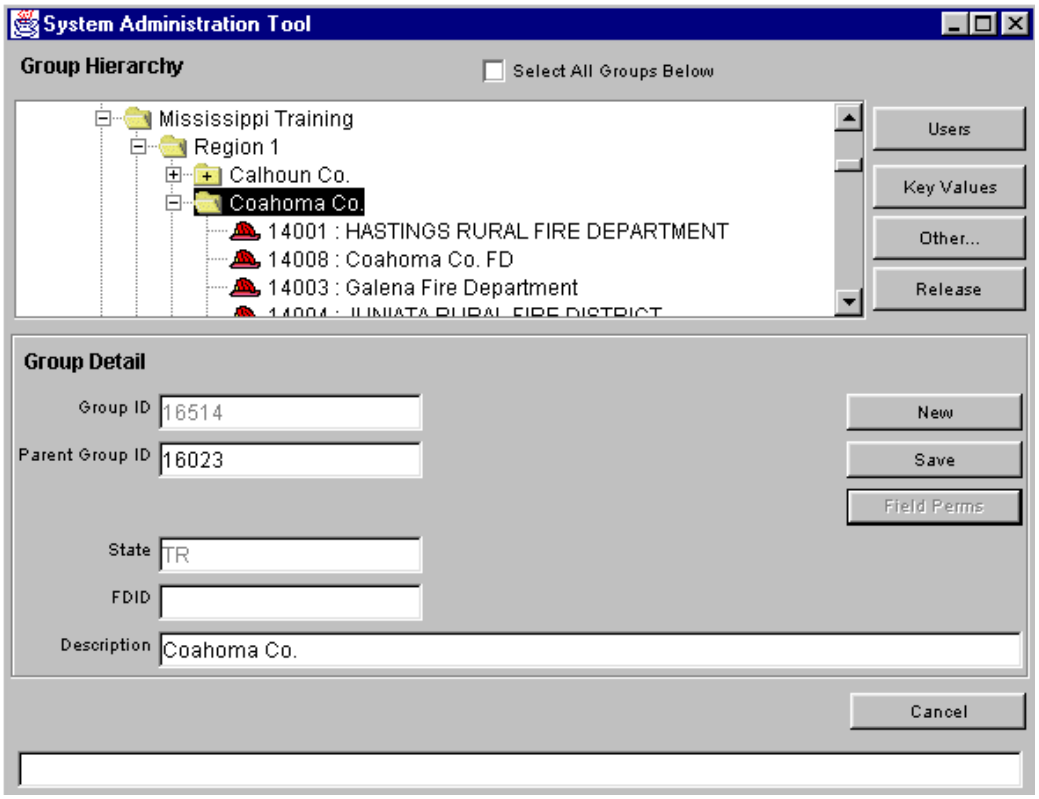
2.1 Creating a New Group

When the System Administrator first opens the Tool, he or she will see the Group Hierarchy Window (diagram 2.1.0). To create a new Group, the Administrator must click on the Parent of the new group to be inserted and then click the **New** push button. In the white message box at the bottom of the screen, Requesting New Group Number will be displayed. The system retrieves a new Group ID which will be displayed in the Group ID field. The description field clears.

The Administrator enters the description of the new group in the Description Field. If the new group is a Fire Department and will be an end node, enter the new group's FDID number. If the new group is not an end node, leave the FDID field blank.

Click on the **Save** push button to save the new group or node. A message will be displayed: "User Group Insert Successful." The System Administrator is returned to the Group Hierarchy in collapsed form. The System Administrator is then ready to begin assigning users to the group.

Diagram 2.1.0



The following table outlines the steps for adding a node to the Group Hierarchy.

To Add a Group to the Hierarchy:

Step	Action	Result
1	Click on the Parent group of the new group.	Parent Group becomes highlighted.
2	Click on the **New** push button.	The system retrieves next available Group ID number. The Description field clears.
3	Enter the Group's Descriptor in the Description field. **Note:** FDID is only entered if the node is a fire department and is to be the bottom the Group Hierarchy.	Group name is recorded.
4	Click the **Save** push button.	The Group Hierarchy collapses and the node is added.

2.2 Moving a Group

To move a group from one parent group to another, first note the Group ID for the *new* parent group. Click on the group to be moved. When the group is highlighted, the Parent Group field becomes editable. Enter the new Parent Group ID. Modify the Description field if desired. Click on Save. When the new information is saved, the message "User Group Changes Saved" will be displayed in the white message box at the bottom of the window. The System Administrator is returned to the Groups Hierarchy Window.

Note: A Parent group that has child groups within it should not be changed to an end node (FDID). Changing a parent group to an end node causes its original nodes to be removed from the hierarchy. These former end nodes will need to be manually deleted from the On-line System (contact the NFIRS Support Center).

2.3 The Group Detail Fields

Below the Group Hierarchy Pane, there are five fields for **Group Details**: the Group ID number, the Parent Group ID number, the State, FDID number, and a field for the description of the group. When the administrator highlights a group in the hierarchy, the corresponding information will appear in the fields.

2.3.1 Group ID

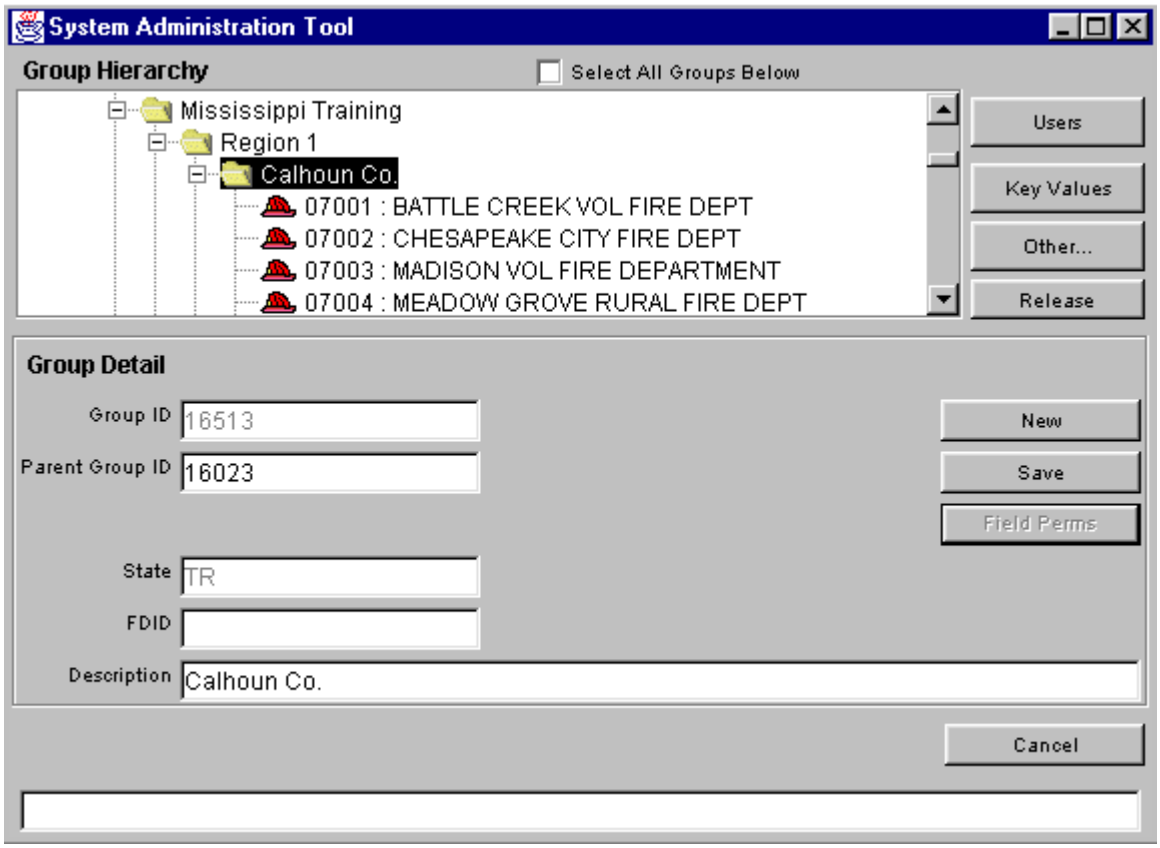
The **Group ID** is the number that distinguishes a group from all others in the hierarchy. The system assigns Group IDs when the administrator creates a new group. The Group ID field is not editable.

2.3.2 Parent Group

The Parent Group number will be displayed when the user highlights a group in the list. The Parent Group is the group one level above the highlighted group. For example, in diagram 2.3.2.0 the Parent ID for Region 1, when highlighted, is 6795, Mississippi Training. Region 1 is the parent for Calhoun Co., and Calhoun County's Parent Group ID is 16023. Calhoun Co. is the parent of Battle Creek Vol. Fire Dept., Chesapeake Vol. Fire Dept., Madison Vol. Fire Dept., and Meadow grove Rural Fire Dept. When highlighted, each of these group's Group IDs will display in the Group ID field.

A fire department cannot be a parent for another group, for example, a station.

Diagram 2.3.2.0



2.3.3 State

The standard, two-letter state abbreviation defaults in this field according to the administrator's state.

2.3.4 FDID

FDID is the Fire Department Identifier that is assigned by the state.
Note: Only the end node groups, Fire Departments, will have FDIDs assigned. Once created and saved, an FDID number cannot be edited.

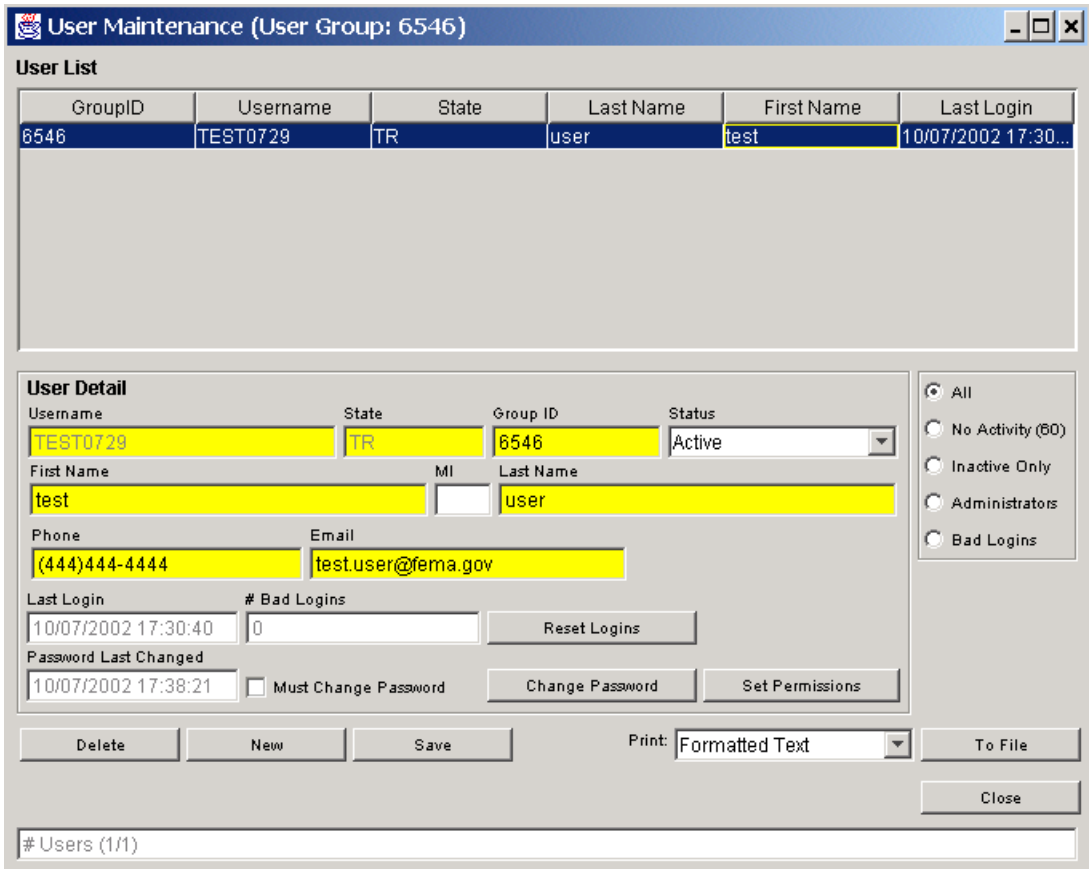
2.3.5 Description

The Description field is a free form text field in which the administrator enters the description of the group being defined or modified. The field is not case sensitive and has a maximum of twenty-five characters. The Description can be changed at any time by editing the field and clicking Save. Or, an FDID Information file can be imported to overwrite the existing Description.

3. The User Maintenance Window

The User Maintenance Window (diagram 3.0) is accessible by clicking the **Users** push button on the right of the Group Hierarchy Window. The Administrator can only access users that are at or below the group associated with the Administrator's login. For example, an Administrator associated at the State-level Group may administer, activate, or modify users at the State-level and below; an Administrator associated with a County-level Group may administer users at the County-level and below.

Diagram 3.0



To view all users within a specific group, highlight the group and check the **Select All Groups Below** check box (located on the Group Hierarchy Window). The User Maintenance Window will be displayed, and in the User List Pane will be the users for the specified group level. The list may further be defined by checking one of the five check boxes below the User List on the right: **All** (users), **No Activity** (60 days), **Inactive Only**, **Administrators**, **Bad Logins**.

The User Maintenance Window provides administrators the ability to view and modify user-specific information. The administrator can create, activate, and delete a user, modify user information, reset logins and passwords with the components of this window.

When the Administrator opens the User Maintenance Window, the users who have registered using the NFIRS Web Site will be listed with their State's level Group ID, with Inactive status.

A user must be moved to their appropriate group or Fire Department and activated before he or she can begin entering incidents. If a user has not registered through the NFIRS 5.0 Web Site, the administrator must obtain and manually enter the user-specific information in order to create the user in the system.

3.1 Creating Users

To create a user, click on the **New** button. All editable fields in the User Detail fields will be cleared and the Administrator can enter user-specific information. Yellow highlighted fields are required fields and must be filled out. Required fields include User Name, User State, Group ID, First name, Last name, Phone, Email (if user does not have an email address, enter NONE). Optional fields include Status (Active or Inactive), MI (middle initial), and Must Change Password.

The Administrator will enter the Group ID to which the user will be assigned. When all required fields are filled out, click the **Save** button. The new user information and group assignment will be saved.

To activate the user, click on the **Status** drop down box. Select **Active**. Click **Save**.

If a user is not active for sixty days, the user account will be automatically set to Inactive. The User List can be sorted by Active status users, Inactive status users, users with System Admin permissions (Administrators), and users with bad logins. It is recommended that State Program Managers or their System Administrators periodically review the list of Inactive users and delete unnecessary user accounts, or contact the user if necessary.

3.2 Adding Users to Groups

If the user registered through the NFIRS Web Site, his or her name and user specific information will appear in the Group List. To add or move the user to a group, highlight the user's name in the Group List. User-specific information populates the fields of the User Detail Pane. Highlight the **Group ID** field. Type in the Group ID to which the user will be assigned.

Click the **Save** button to save new user information.

To activate the user, click on the **Status** drop down box. Select **Active**. Click **Save**.

3.2.1 User Login Buttons

To view or change user login information, the Administrator must first highlight the desired user name in the User List Pane. When the user name is highlighted, the last login date will be displayed in the **Last**

Login field. The last login is recorded for all NFIRS 5.0 On-line or web based services: the On-Line client software, NFIRS 5.0 User login web page, login to the Bulk Import Utility, or to the NFIRS 5.0 Web Based Reporting site. Two push buttons, **# of Bad Logins** and **Reset Logins** provide the Administrator the capability to view the number of bad logins and to reset the login counter for the specified user.

After five unsuccessful login attempts, the user's account will become locked. The user must contact the Administrator to report and resolve the issue. The Administrator may reset the login counter by first highlighting the user's name in the User List Pane. Click the **Reset Login** button. The user will have five attempts at the next login before the account locks.

The accounts of users who have not logged in to the On-Line system in 60 days will be automatically deactivated. These users must contact a System Administrator or the NFIRS State Program Manager to have their account status reset. To re-activate their account, highlight their name in the User List Pane. Click the **Status** drop down box and select Active. Click Save. Or, if the account is no longer necessary, it can be deleted.

3.2.2 User Passwords and Password Management

When a new user registers through the NFIRS 5.0 web site, the password entered must comply with FEMA IT's Information Assurance guidelines, outlined below, which were established to minimize risk of access of critical IT systems and their information.

- All passwords must be at least eight (8) characters in length.
- All user-chosen passwords must contain at least one non-alphabetic character such as a numeral (0-9).
- All computer system users must choose passwords that cannot be easily guessed. Passwords must NOT be related to the user's job, personal life, for example, a car license plate number, a spouse's name, or an address. Passwords must not be a word found in the dictionary or some other part of speech; for example, proper names, places, and slang must not be used.
- Never store passwords online, or write them down and place them near the computer.
- Passwords and login IDs are not to be shared with anyone. It is the responsibility of the users to maintain the confidentially of their passwords. Users are responsible for actions and events resulting from the disclosure of personal passwords.
- Change your password every 6 months or sooner if the system permits (every 90 days is recommended).

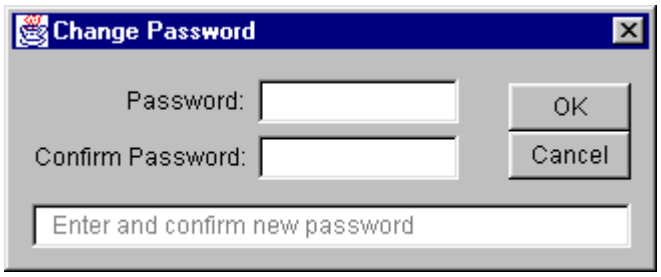
The NIRS 5.0 client software enforces a password change every 89 days. Also, users can change their passwords at any time from within the Data Entry Tool. In the Main View Screen under the Advanced Menu, there is a Change Passwords option for all users.

New NFIRS 5.0 Users

When a new user is manually created, the password will default to the user's Username. Upon initial login, the user will be required to change the password. The Administrator may change the default password by clicking on the **Change Password** push button. When the **Change Password** push button is pressed, a pop-up window (diagram 3.2.2.0) will appear providing the Administrator ability to change the user's password.
Note: The Administrator may only change a user's password after the user information has been saved.

To change a user's password, first select the desired user in the User List Pane. Type in the new password. Retype the password to confirm. Click the **OK** button. Click on **Change Password** button.

Diagram 3.2.2.0



When a new user registers through the NFIRS 5.0 User Registration Page, they must specify a password. If the password does not meet the necessary format, an error will be displayed and they will be prompted to enter another password.

Note: The Administrator cannot recover the initial password a user entered during NFIRS Web Site registration if the user misplaces it. The Administrator can only set or change a user's password.

3.2.3 Set Services Permissions

The **Set Permissions** push button provides the Administrator an interface to modify NFIRS Database users' permissions. Click once on the Set Permissions push button for the Services Permissions pop-up window to appear (diagram 3.2.3.0). A check box accompanies each of the eighteen permissions or services available.

Seven permissions will be checked by default, as shown in Diagram 3.2.3.0.

At this time, these four reporting permissions **Report Submit**, **Report Fetch**, **Report Templates**, and **Report Generate** are the necessary permissions for a user to access the web-based Summary Reports Output Tool. A user who does not have access to the USFA client software may be assigned the four reporting permissions and be restricted to the NFIRS 5.0 Web-based Reporting site. The reports can be generated on the data set available to the user, i.e., the data set at or below the user's Group assignment.

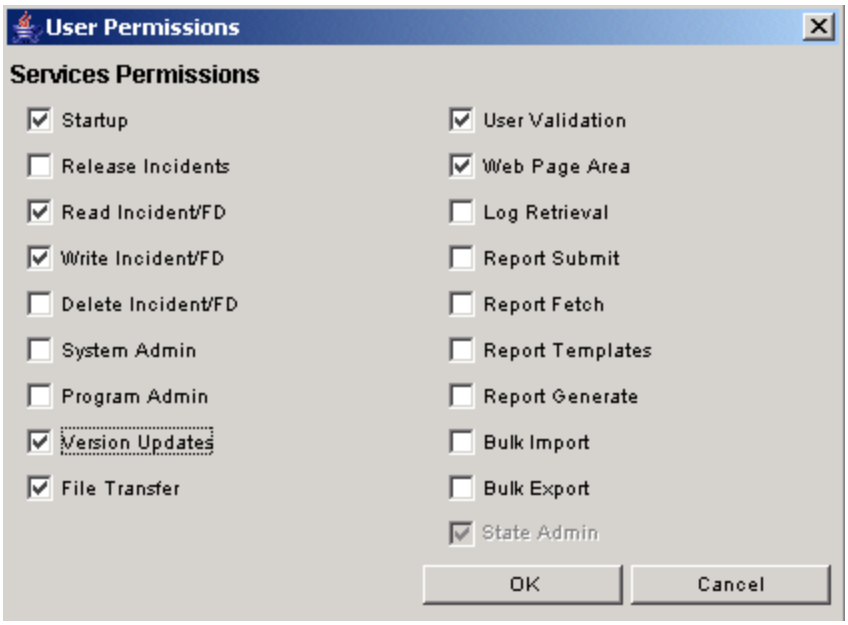
The permissions for **System Admin**, **Program Admin**, and **Release Incidents** should be reserved for users who will have system administration responsibilities, including user account maintenance at and below their group assignment, creation and maintenance of Plus One Codes and Special Studies.

The **Bulk Import** permission should be reserved for those users who will be sending files to the National Database via the Bulk Import web interface. The USFA Client software is not necessary to use the Bulk Import Utility. The **Bulk Export** permission should be reserved for those users who must access the incident data at their group level and below but do not have the USFA NFIRS 5.0 client software. A user can be assigned the Bulk Import Tool permission exclusively.

Note: If the user has access to the System Admin Tool, he or she has access to all available privileges of a System Administrator, including modifying permissions of other user at or below his level.

Diagram 3.2.3.0 on the next page shows the Services Permissions window with default permissions, with the exception of State Admin.

Diagram 3.2.3.0



Note: Diagram 3.2.3.0 shows the default permissions for a new user. The Administrator can change these permissions by removing the check from the desired box, or check the desired permission to add.

After the appropriate permissions have been checked, click the **OK** button to save the permissions to the user. Clicking the **Cancel** button returns the user to the User Maintenance screen without saving changes.

The services or permissions available for assignment to users are defined below. Following the list is a section explaining permissions that can be assigned to users who will not be using the USFA software.

Startup: provides the user the ability to connect to the National Fire Incident Reporting System Database only.

Read Incident/FD: provides the user the ability to query incidents and Fire Department Information from the NFIRS Database.

Write Incident/FD: provides the user the ability to enter or update incidents and Fire Department information into the NFIRS Database.

Delete Incident: provides the user the ability to delete incidents and Fire Department Information from the NFIRS Database.

System Administration: provides the user the ability to use the NFIRS 5.0 System Admin Tool.

Program Administration: provides the user the ability to use the NFIRS 5.0 Program Admin Tool, and save changes made with the Codes and Special Studies editors accessible from the System Admin Tool.

Version Updates: provides the user the ability to download NFIRS Client Tools updates from within the NFIRS Data Entry /Validation Tools menu. Users will be notified if this utility can be used for a particular update.

File Transfer: provides the user the ability to transfer Incidents from a flat file to the NFIRS Database.

Release Incidents: provides the state level user the mechanism to release incidents for National Trending by the USFA.

User Validation: provides the user the ability to revalidate user information and change passwords after 89 days when prompted.

Web Page Area: provides the user the ability to login on to the NFIRS 5.0 User login page on the NFIRS 5.0 web site, http://nfirs.fema.gov/

Log Retrieval: provides the user the ability to view the events, exceptions, and stats log files. These files can provide important information for troubleshooting.

Report Submit: provides the user the ability to access the web-based Summary Reports Output Tool on the NFIRS 5.0 web site.

Report Fetch: provides the user the ability to retrieve reports generated from web-based Summary Reports Output Tool on the NFIRS 5.0 web site.

Report Templates: provides the user the ability to create and save templates for reporting similar incidents within the group or department.

Report Generate: provides the user the ability to generate web-based Summary Reports Output Tool on the NFIRS 5.0 web site.

Bulk Import: provides the user the ability to login to the Bulk Import utility web page area and place files on the Bulk Import Utility server for processing without using the USFA Client software.

Bulk Export: In future versions, will provide the user the ability to login to the NFIRS web page area where the Mass Export will be located, and export at or below the group level to which the user is assigned.

State Admin: provides the user the ability to assign Bulk Import permission. This permission must be assigned by a National Level User.

View Only Permissions

A user without the need to report or modify a departments' incident data can be assigned the Start Up, Read Incident /FD to be able to login to the Data Entry Tool and view the Fire Departments and incidents available to the user's group. To generate reports using the web-based Summary Reports Output Tool on the NFIRS 5.0 web site, the user account must have the four reporting permissions assigned to it: Report Submit, Report Generate, Report Templates, Report Fetch. Refer also to section 3.4, *View Only Permissions* for information on creating a group for which a user can view only.

The Bulk Import permission, assigned exclusively, enables the user to access the Bulk Import Utility web page area and upload files to the National Database.

The Bulk Export permission, assigned exclusively, enables the user to access the Bulk Export in the Reporting web page area to create a flat file or Excel format file of the data in the National Database at their level and below.

3.3 Modifying Users

To modify user information, click on an existing user in the User List Pane. When the user is selected, the User Detail fields will be populated with the user's specific information. All values except for the username can be modified.

- To modify user information in a text field, highlight the text and type in new information. Click **Save**.
- To activate a user, highlight the user to be modified. In the User Detail Pane, click on the **Status** drop down box. Select **Active** to insert into the Status field. Click **Save**.
- To require the user to change passwords upon next login, check the **Must Change Password** check box.
- To reset the user's bad login count, click the **Reset Login** button.

System Administrators are urged to review the list of user account periodically and delete user accounts that have become Inactive, or contact the user and inquire about the status of reporting.

3.4 Moving a User

To move a user from one group to another group, in the Group Hierarchy Window the Administrator must highlight the group level or group the user is associated with; for example, the State. Check **Select All Groups Below** box. Click the **Users** button. In the User List Pane, all users (active and inactive status) will be displayed. Highlight the desired user to be moved. User-specific data populates the fields of the User Detail Pane. Highlight the user's Group ID and type in the desired new Group ID. Click **Save**. **Note:** Both the Group Hierarchy Window and the User Maintenance Window can be opened and arranged to view concurrently for accuracy.

View Only Permissions

Occasionally a user may request the ability to view a county or several departments that already exist in the hierarchy without the need to report or modify those departments' incident data. A separate folder can be created on the tree and the desired departments can be added to the folder. The FDID and Departments' Descriptions must be named exactly as they appear in their original location in the hierarchy. The user will need an separate account assigned to that folder, *without* the permissions System Admin, Delete Incident, Write Incident,

File Transfer, or Bulk Import. The incident counts will not be duplicated when generating statistical reports.

3.5 Deleting a User

To delete a user, highlight the user in the User List and click on the **Delete** button. A pop up box will appear which shows the user's name and state. Click **Yes** to delete the user permanently from the list. Click **No** or **Cancel** to return to the User Maintenance Window without deleting the user.

The administrator may periodically see a duplicate registration. In the event that a user makes a duplicate registration, the administrator can delete the duplicate from the User List. Users need to be notified which Username is active.

After sixty consecutive days without a login to the On-Line system, active user accounts are reset to Inactive status. The user must contact their State Program Manager or System Administrator and request the account be re-activated. It is recommended that the State Program Manager review the Inactive list periodically and delete unnecessary user accounts.

Note: The administrator cannot delete groups, only users.

3.6 Miscellaneous Components

Several components of the User Maintenance Window facilitate user maintenance and user list organization. Five check boxes (diagram 3.6.0) control how the User List is sorted and displayed. The System Administrator can choose to display the list of **All** users, users with **No Activity (60 days)**, users with the status **Inactive Only**, users at the **Administrators** level, or users with **Bad Logins**.

Diagram 3.6.0

The **Delete**, **New**, and **Save** buttons (diagram 3.6.1) are used to delete a user from the list (an irreversible action), to add a new user manually to the User List, and to save user specific information.

The **Print** drop down box allows the administrator the ability to save the User List in Formatted Text or Excel file format. **Note:** Files formatted for Excel will require Excel on the user's PC to open and view.

The **To File** button allows the Administrator to save the user list to a specified location. When the **To File** button is pressed, the **Save User List To** pop up window appears. The administrator chooses a location to save the file. The default location is in the NFIRS root directory. Name the file and click **Save**. The files may be opened with NotePad or WordPad as well as any word processing program. They may also be imported to an Excel spreadsheet.

Diagram 3.6.1

The **Close** button when pressed closes the User List Window and returns the user to the Group Hierarchy Window. The white rectangular box at the bottom of the screen displays messages pertaining to the display and actions taking place in the User List Window.

4. The Release Incidents Window

By releasing a 5.0 incident or incidents, a state (or fire department) is allowing the USFA to use the incidents' data in National Trending reports and statistical information. Once an incident is Released, the incident can be accessed and viewed in the On-line database, however, the Released incident is not editable.

If a user wishes to edit a Released 5.0 incident, a State level user or System Administrator at the state level assigned the Release Incident permission must "Unrelease" the incident to allow editing. After the incident has been modified, the incident must be released again.

Valid, 4.1 Data incidents are automatically Released when sent to the National Database. To update or modify a 4.1 incident, the Program Manager or user with Release Incident permissions import the updated incident with Overwrite Incidents specified. **Note:** The 4.1 incident that is Un-released, opened, and saved will be validated against 5.0 rules.

4.1 Release Incidents Permissions

A user at the US level must assign the State Program Manager the Release Incident Permission and assign the Program Manager to a level whose Parent Group ID is 1. Program Managers may request the Release Incident permission to be assigned a user(s) who will assist in releasing incidents. When a Program Manager or System Administrator with the Release Incident Permission opens the System Admin Tool, the Release button will be available on the interface.

Note: the File Transfer permission, which is assigned by default at the time of a user's account activation, allows users to send a flat file to the National Database in order to report incident data. The Release Incident permission is not assigned to any user by default.

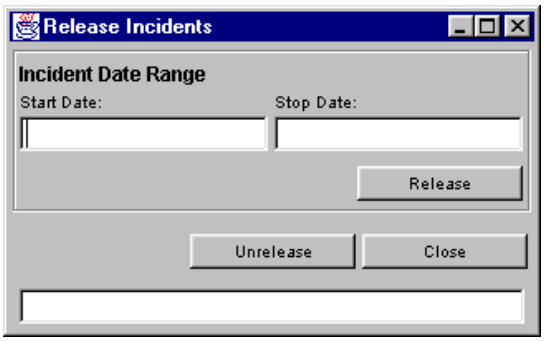
A specific level of security has been assigned to each field in all modules to ensure that sensitive information is not released. The security level is the highest level at which the data in the field may be released from the national system. The list of security levels is in the Data Dictionary in the Design Documentation, http://www.nfirs.fema.gov/documentation/design/ beginning on page 108. States do have the option to change the security level of a field if necessary to meet specific state laws

4.2 To Release an Incident:

The following section refers to the client software Release mechanism. To release and unreleased incidents using the Web-based NFIRS System Admin Tool, refer to: http://www.nfirs.fema.gov/webtools/

When a Program Manager or System Administrator with the Release Incident Permission opens the System Admin Tool, the Release button will be available on the interface. After clicking on the Release button, an Incident Date Range window will be displayed (diagram 4.2.0). Specify a date range for which all incidents will be released, or the range in which to search for incidents to be released. Note: When releasing a large quantity of incidents, the return message occurs after the setting for each incident has been updated in the database, so the return message may not immediately be displayed.

Diagram 4.2.0



The Incident Date refers to the date in the incident's Key Information - Section A. For example, if the Program Manager specifies the range: Start Date 06/01/05 and Stop Date 09/01/05 and clicks the Release button, all incidents with a Key Information date from June 1, 2005 to September 1, 2005 will be released.

In order to update a released 4.1 or 5.0 incident, an Add transaction must be imported with Overwrite Existing Incidents specified in the Configuration Tool or Bulk Import Tool. Or, to manually edit a released 5.0 incident using the Data Entry Tool, the Program Manager must "unrelease" the incident. **Note:** 4.1 incidents are validated against 4.1 rules, converted to 5.0 format, and flagged in the database as 4.1 incident data. If a 4.1 incident is unreleased, opened and saved, it will be validated against 5.0 rules.

4.3 To Unrelease an Incident:

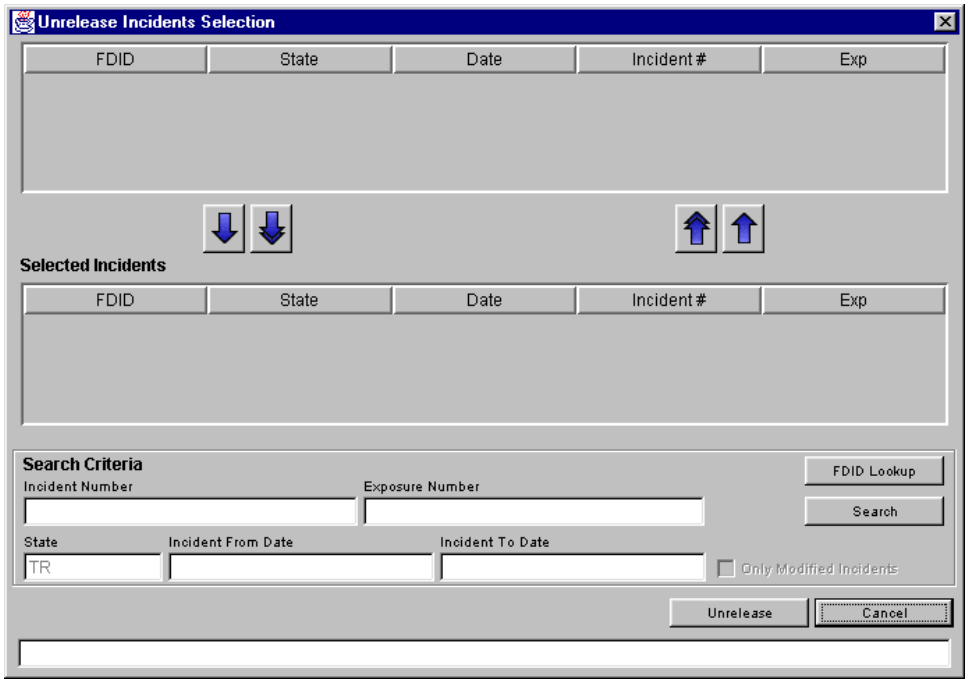
In the System Admin Tool, click on the Release button. Specify the incident's date or a range of dates for several incidents. Click on the Unrelease button. The Unrelease Incident Window will be displayed (diagram 4.3.0). Select (highlight) the desired incidents to be Unreleased and click on the blue down arrow to move the selected incidents to the lower portion of the window. Click the Unrelease button. The status of the incidents will be changed and they can be edited using the Data Entry Tool.

A maximum of 1000 incidents can be Un-released at one time.

Note: A released 4.1 incident that is opened will be validated against 5.0 rules when saved and closed.

The Program Manager can verify an incident has been released by opening the Data Entry Tool and retrieving a released incident and opening it. The data will be displayed in the modules' fields but will be grayed out. The incident cannot be edited.

Diagram 4.3.0



5. The Codes Window

The Codes Window is accessed by Clicking on the **Other…** button in the System Admin Tool main view.

The Codes Window enables the National level user to create, modify, and delete code categories from the National Database, and enables State Program Managers and their System Administrators to implement Plus One Codes within their state. The Program Admin permission is necessary for the user to save changes made when making code categories and Plus One codes.

Plus One Codes

The fields that support a Plus One code have a fixed maximum size which allows the potential extra digit of the new code. A Plus One code may be implemented to allow many additional, more specific values to be defined by local departments or states for their own uses. When a plus one code is imported to the USFA National Database, only the national length code is used for analysis.

For complete information on the Plus One Code requirement for NFIRS 5.0 transaction file fields, refer to page 131 under "Coded Fields" and "Multiple Choice Fields" in the Flat File Transfer Format section of the Design Documentation, available at: http://www.nfirs.fema.gov/documentation/design/

For example, a state or Fire Department may wish to further define the national length description for a Mobile Property Type to specify when an electric vehicle is involved in fires. In the Mobile Property Type codes, the national length code (10) Passenger Road Vehicle, Other, could have a Plus One Code added for (101) Electric Vehicle. Or, the national length code (13) Off-road Recreational Vehicle could have a Plus One Code added for (131) Golf Cart.

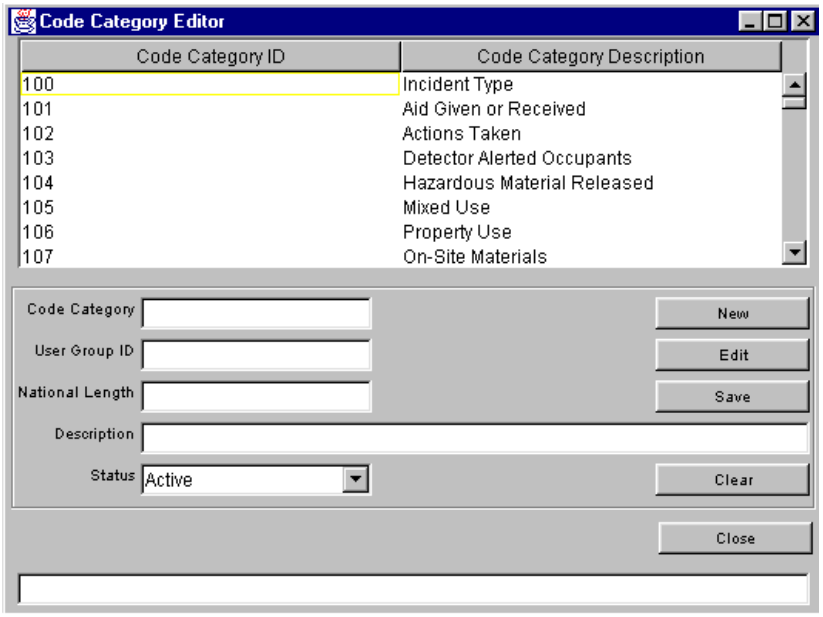
When the new plus code is first created, it may take fifteen to twenty minutes to be re-cached and appear in the Data Entry Tool.

Off-Line users must perform User Injection to obtain new codes that are implemented and saved to the National Database.

5.1 Creating a Plus One Code

To create a Plus One code, Click on the **Other...** button the click on the **Codes** button. The Codes Category Editor will appear. The national level code categories are assigned a standardized, numeric number, which are displayed in the left side of the window, and their descriptions will be displayed in the right side (diagram 5.1.0). A scroll bar on the right of the window enables the view of all available codes for the category.

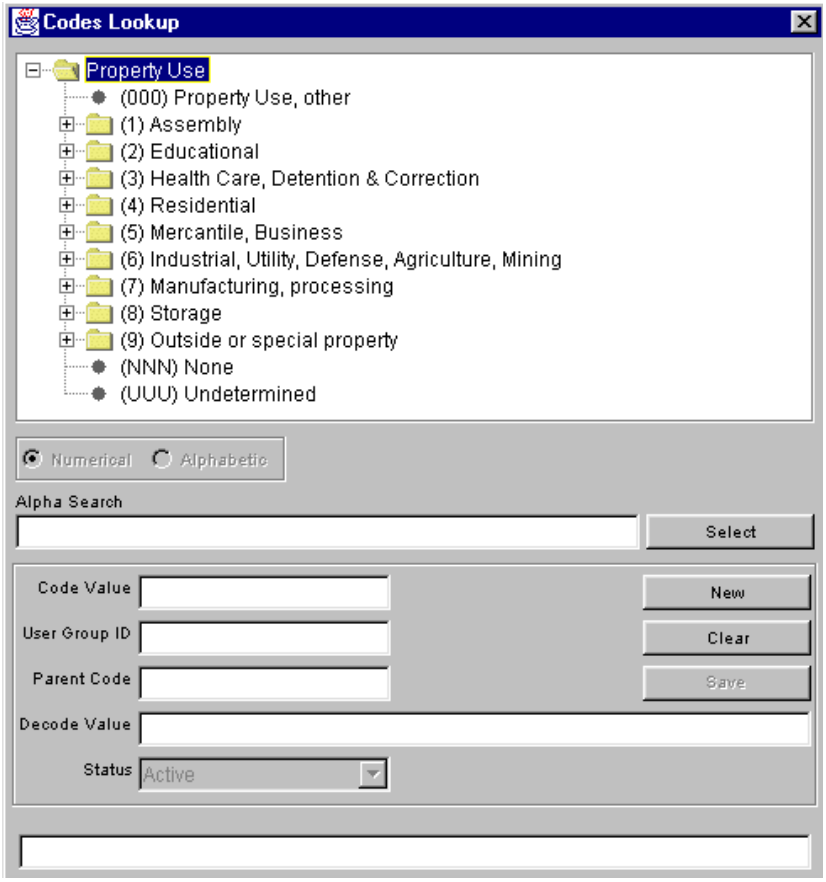
Diagram 5.1.0



Select the parent code group in which the new Plus One code will be created, for example, Property Use. System information for the highlighted code category will be displayed in the Details fields. For example, the system information for Property Use that will be displayed is: national Code Category ID (106), the User Group ID (defaults to the user's system assigned group ID), National Length (3), which states the specified length for the code category, and the code's Description as it appears in the code look up information (Property Use). The Status box displays whether the code category is Active or Inactive.

Click the **Edit** button (not the New button). The Codes Lookup window will display the existing codes for the selected category .For example, diagram 6.1.1 on the following page shows the Property Use category.

Diagram 5.1.1



In the Code Lookup window, click on the plus sign to extend the view of all codes for the category. Or, use the selection feature: select the **Numerical** radio button, enter a code, and click the **Select** button. If the desired code is not numeric, select the **Alphabetic** radio button, type in the Decode Value (description) and click the Select push button.

Click on the desired national length code from which a new code will be assigned (example: 111, Bowling Alley). The selected code's system-assigned information will populate the fields in the lower portion of the window.

Click on the **New** button. The information fields will clear. Enter the **Code Value**. This will be the new, numeric code (or alpha, alpha numeric depending on the parent code's format). Enter the **Parent Code**. Enter the **Decode Value**, which is the description the user will view. There is a fifty character maximum length for the Decode Value. Set the Status to **Active** to implement the code. Click **Save** to save the new information. The message window in the lower left will display: Updating code information…. Information saved successfully. The code hierarchy will collapse and when extended, the new code will appear under the parent code value. The new Code will be saved and you will be returned to the Code Category Editor.

To Delete a code, highlight the code and set its status to **Inactive**. The user will be prompted to confirm the delete action, which is not reversible. To clear the information from the fields, click **Clear.** Click **Close** to close and exit the Code Category Editor.

Note: On-Line Users may not view the new code until the next day when the system has re-cached the new information. Off-line users must perform User Injection to update their local Codes Lookup information.

The steps to create a Plus One code are outlined below.

Step	Action	Result
1	Log into the System Admin Tool. Highlight the group for which the Plus one code will be visible.	The System Admin Tool opens The desired group level is specified.
2	Click on the **Codes** push button.	The Codes Category Editor window is displayed.
3	Select a Code Category in which the plus one code will be created.	The desired code will be highlighted and its information will be displayed in the fields below.
4	Click the **Edit** push button.	The Codes Lookup window will be displayed.
5	Highlight the parent for the Plus One code about to be created.	The parent code information will populate the fields,
6.	Click the **New** push button.	The fields will clear, and the user Group ID will be entered automatically. Users at this group level will view and have access to the code..
7	Enter a Code Value	The numeric or alpha numeric code will be established for the new code.
8	Enter a Parent Code Value	The parent code will be specified.
9	Enter a Decode Value	The new code Description will be specified.
10	Click Save	The hierarchy view will collapse and the new Plus One code will be saved.

5.2 Deleting a Plus One Code

Locate and highlight the desired Plus One code. When the Plus One code's information has populated the fields, set the Status to Inactive. A message box will appear confirming if you wish to set the status to Inactive, which will delete the code. Click Yes. This action is not reversible.

6. The Chemicals Window

The Chemicals Editor enables the national level user to add, modify and delete chemicals and their associated information from the National Database. The Chemicals window is accessible by clicking on the button named: **Other…** the table of chemicals will be displayed when the user enters a letter or two into the Chemical String Search field.

7. The Special Studies Window

The Special Studies Window enables the State Program Manager or System Administrator to create, modify, and delete a Special Study and its codes from the National Database.

The Special Study codes information must be created and saved to the On-Line system in order to make the codes selection available to the USFA client software user in the Basic Module's Special Studies Tab, E3 fields. Having the code saved in the National database also allows third party transaction files containing the Special Studies information to be validated at the National level. The Special Study code, if present in a 5.0 transaction file, is contained in the record Type 1060 with the Basic module Information. This record must contain the unique system-assigned Special Study ID number for the record and the codes it contains to be validated upon import to the National Database.

Special Studies may be created for state-wide use, a county or region, or a single FDID. When the Special Study is created, a date range is specified which determines the availability of the Special Studies selection according to the Incident Date.

Each login level has a Key Value assigned to and can be identified by the system-assigned User Group ID in the Key Values Window of the System Admin Tool. The Key Value assignment ensures no duplicate Special Studies IDs are created and no Special Studies IDs are overwritten. Key Values may be viewed and edited by clicking on the Key Values button from the System Admin Tool.

If a user attempts to create a Special Study and receives the following error: "Your user group is not set up to add Special Studies, contact your System Administrator to request assistance, " the key value must be established for the user's group. State Program Managers or System Administrators with state level login and Program Admin permission can establish the key value, or contact NFIRS support.

Examples of Special Studies

Two examples of Special Studies are as follows: a study to collect information on a particular type of sprinkler system: its brand and if it operated successfully or unsuccessfully. Another example is a study to collect information on historical properties involved in fires: the type of property: residential, commercial, or other type; and if the property was operating or vacant.

The following sections provide complete instructions on creating a Special Study. Users creating a Special Study are recommended to plan the group level for which the study will be available, the name of the Special Study, the date range the special study will be effect, and the descriptions for the selectable codes the user will see in the Codes Lookup box. For example:

- The name of the Special Study will be "Historical Properties Involved in Fires".
- It will be available state wide (all departments may view and select its codes in the Basic Module)
- The study will be conducted for the current year (Start Date: 01/01/2006, Stop Date: 12/31/2006)
- The selectable codes will be: (1) Residential and inhabited, (2) Residential and uninhabited, (3) Commercial and operating, (4) Commercial and operating, (5) Other space or other structure type.

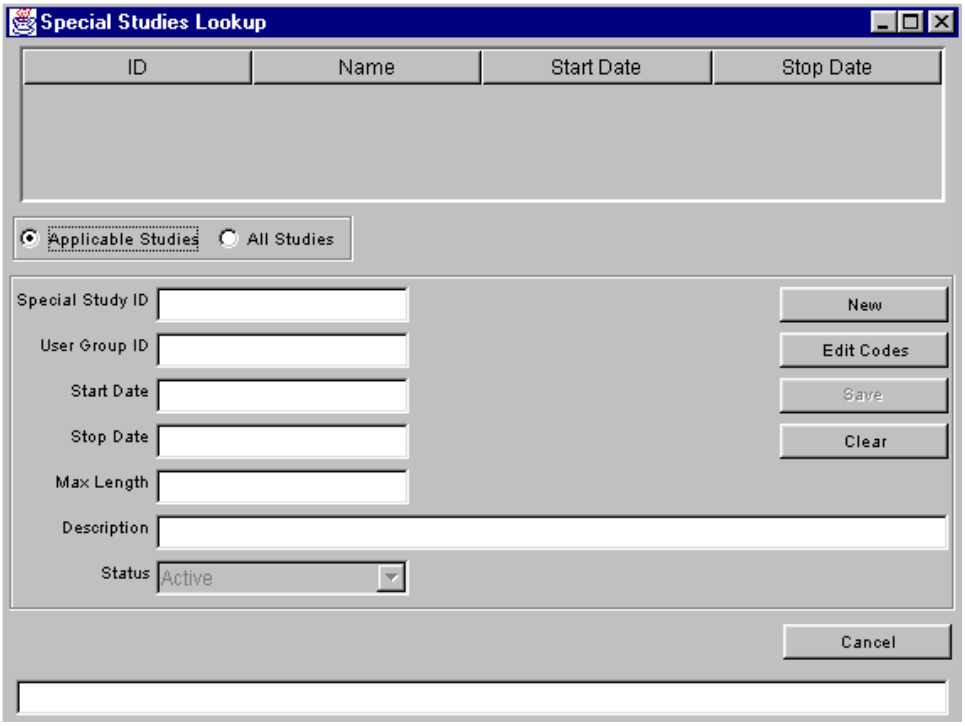
The System Administrator will first create the Special Study, and then create the codes that users will select to represent applicable data.

7.1 Creating a Special Study and its Codes

Open the System Admin Tool and click on the **Other…** button. Click on the Special Studies button. The Special Studies Lookup window will appear (diagram 7.1.0).

The upper portion of the window displays the Special Studies ID, Name, and date range for the study for Special Studies saved in the National Database. Two radio buttons, **Applicable Studies** and **All Studies** enable the user to retrieve the Special Studies that are applicable only those studies that are Active status or all studies available to the user's group. The fields on the lower left portion will display information for a selected study. Buttons on the right of the window enable the user to create a **New** study, **Edit Code** values (by accessing the Codes Lookup utility), **Save** new codes or modifications, and **Clear** the information fields. The **Cancel** button will close the window without saving changes.

Diagram 7.1.0

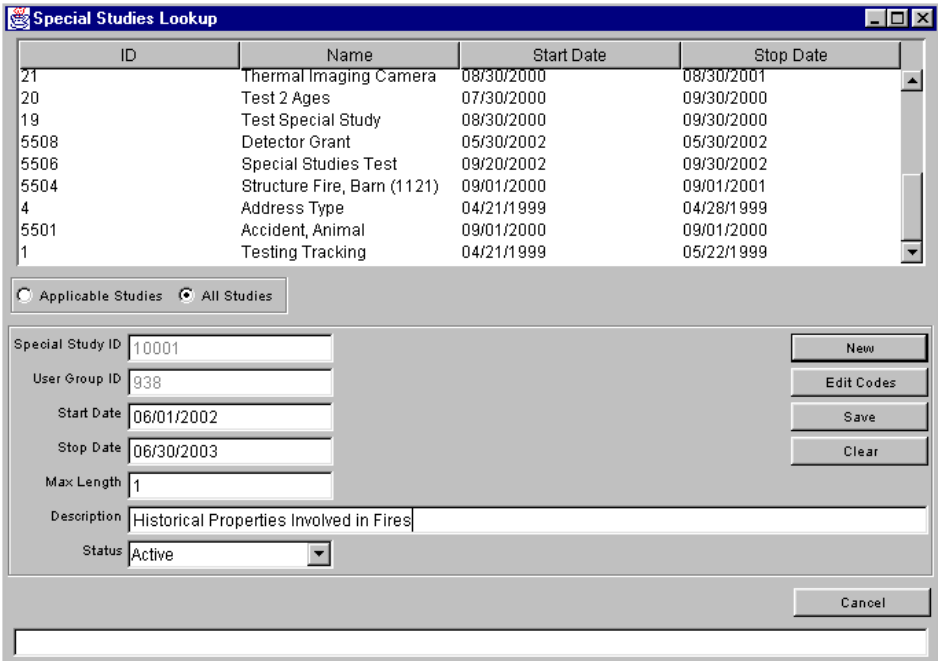


To create a Special Study, click the **New** button. The system assigned ID for the study will be entered automatically in the **Special Study ID** field. The **User Group ID** will be entered automatically in the User Group ID field (as shown in diagram 8.1.1). **Note:** each login level has a Key Value assigned to it to ensure no duplicate IDs are created and no IDs are overwritten.

The **Start Date** and **Stop Date** will default to the current day. Modify the Start Date and Stop Date fields as desired to establish the date range for which the Special Studies will be available to the user for reporting.

Enter a **Description** (50 character maximum length value). Click **Save**. The message bar will state the status: "Changes are being saved…," "the Display is updating…" and finally, "Special Study Information Saved Successfully." After Special Study has been saved in the National Database, and follow the steps to create the supporting codes for user selection.

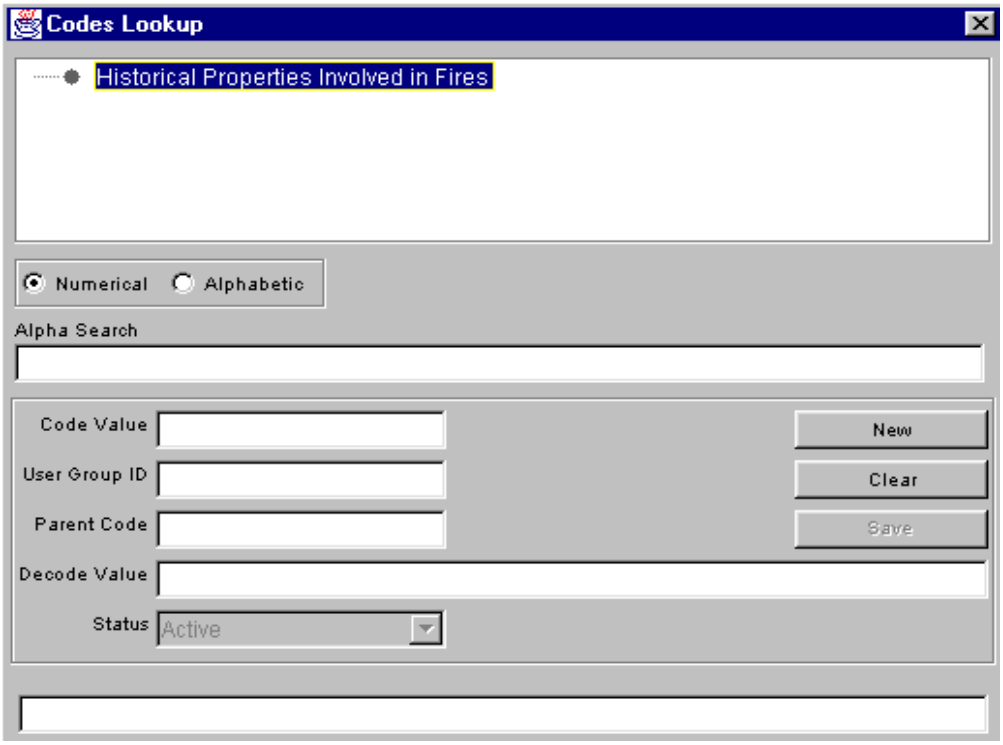
Diagram 8.1.1



Creating the Code Values

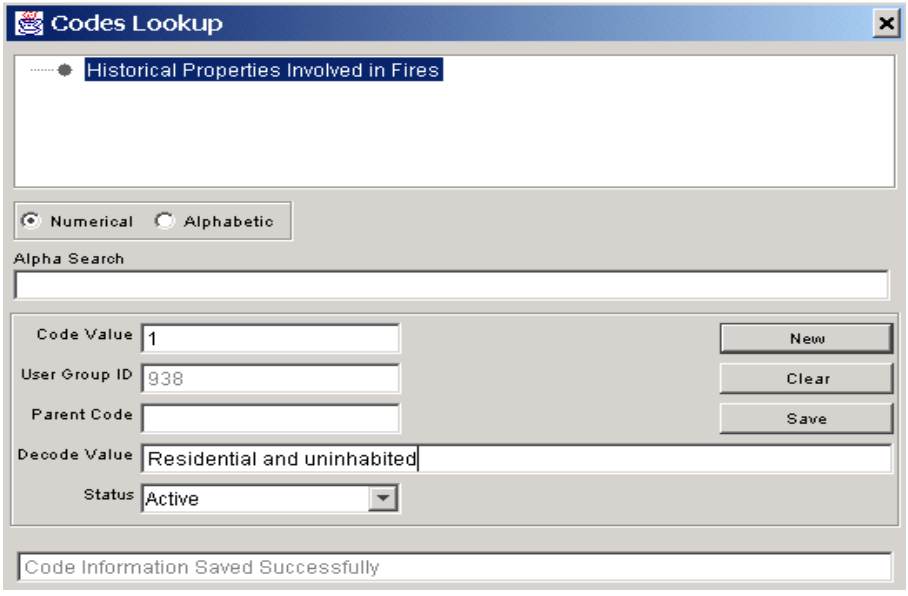
Locate the new Special Study in the list and click once on it to select it. Click on the **Edit Codes** button. The Code Look up window will be displayed and in the pane will be the Special Study that was just created, as shown in the example in diagram 7.1.2.

Diagram 7.1.2



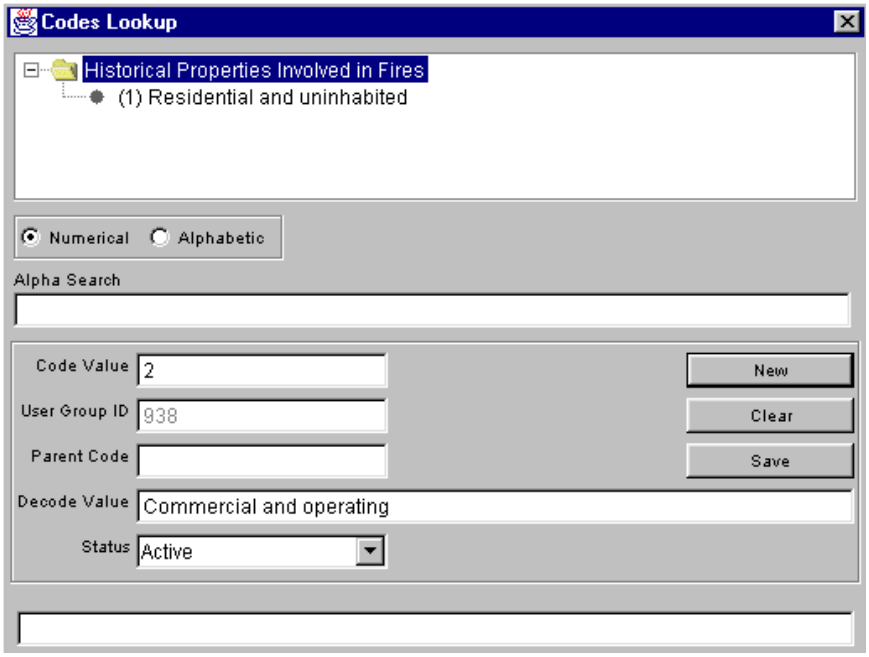
Highlight the Special Study name in the Codes Lookup window and click the **New** button. The User Group ID will be entered automatically. Enter a **Code Value**, This will be the numeric or alpha numeric code that is associated with the code value, and it must be length specified when the Special Study was created. Leave the **Parent Code** field Blank. Enter the **Decode Value,** which is the description the user will see in the Special Studies Lookup box. Click **Save**. Diagram 7.1.3 shows the Code Lookup window with a defining code (1) Residential and uninhabited that has been created and is ready to be saved.

Diagram 7.1.3



To create an additional code to define the study, repeat the steps taken in the Code Lookup window: highlight the Special Study, click Edit Codes button, enter the code value and Decode Value, and click Save. Diagram 8.1.4 shows the Code Lookup window with an additional code, (2) Commercial and Operating, that has been created and is ready to be saved.

Diagram 7.1.4



An outline of the steps necessary to create a Special Study and its codes follow Section 7.2 .

7.2 Modifying Codes in an Existing Special Study

To modify a Special Studies code, open the System Admin Tool and click on the **Other…**button, then click on the Special Studies button. The Special Studies Lookup window will appear. Select the **All Studies** radio button to display all available Special Studies. A scroll bar on the right of the window enables the view of all available Special Studies.

Select (highlight) the desired Special Study. Click on the **Edit Codes** button. The Code Lookup window will be displayed and list the existing codes for the selected study. **Note**: if an error message displays in the lower left message bar: "exception during Special studiesLookupViewActionEvent null, " verify the desired Special Study is highlighted.

To modify a code, in the Code Lookup window, highlight the desired code. The details for selected code will populate the fields (the Parent Code field may be blank). Place the cursor in the field that needs to be edited and type in the correction. Click **Save**.

To add a code an additional code to for the selected Special Study, in the Code Lookup window highlight the name of the special study. Click the **New** button. The detail fields

will be cleared. Enter the criteria for the new code. The Code Value is the actual numeric (or alpha-numeric) code the user will select and enter in the named Special Studies Value field in the Basic module. The User Group ID will be entered automatically, and a parent code entry is not necessary. Enter a Description (maximum 50 characters). Click Save. The New code will be added to the Codes Lookup list for the selected Special Study.

The following table outlines the steps to create a Special Study.

Creating a New Special Study and its Codes

Step	Action	Result
1	Open the System Admin Tool and click on the Other… button, then click on the Special Studies button	The System Admin Tool's Special Studies Lookup window will be displayed.
2	Click on the **New** push button.	The Special Study ID and User Group ID field will default to system assigned values.
3	Enter a Start Date and a Stop Date for which the Special Study will be applicable.	The date range will be specified. The Special Study will be available and validated for incidents that have an Incident Alarm Date within this range.
4	Enter a Decode Value.	Enter a description that defines the code value.
5	Leave the Parent Code field blank.	
6	Enter a Code Value	A code value will be created for display in the Special Studies Look up box.
7	Click the **Save** push button.	The Special Study will be saved.
8	Highlight the Special Study where it appears in the Lookup list	The Special Study will be selected in order to continue creating its codes.
9	Click the **Edit Codes** push button.	The Codes Lookup window will be displayed.
7	Highlight the new Special Study (it will appear as the single bullet item)	The New Special Study will be selected.
8	Click the **New** button.	The detail fields will clear.
9	Enter a Decode Value	Enter a description that defines the code value.
10	Leave the Parent Code field blank.	
11	Enter a Code Value	The numeric or alpha numeric code value will be established.
12	Click Save	The code to define the Special Studies will be saved.
	Repeat steps 8 – 12 if an alternative code is necessary.	

7.2.1 Sample Special Study: Collecting Data on Fires Involving Meth-amphetamine Labs

The steps below outline how to create a new Special Study and its codes that describe fires where the Property Use may involve a meth-amphetamine lab on site.

Step	Action	Result
1	Open the System Admin Tool and click on the Other… button, then click on the Special Studies button	The System Admin Tool's Special Studies Lookup window will be displayed.
2	Click on the **New** push button.	The Special Study ID and User Group ID field will default to system assigned values.
3	Enter a Start Date and a Stop Date for which the Special Study will be applicable.	The date range will be specified. The Special Study will be available and validated for incidents that have an Incident Alarm Date within this range.
4	Enter a Decode Value (this is the Description the user will view)	Enter: Meth-amphetamine Lab Presence
5	Leave the Parent Code field blank.	
6	Click the **Save** push button.	The Special Study will be saved. Proceed to create its codes.
Continue with the following steps to create the supporting codes.		
7	in the Lookup list, locate and highlight the Special Study "Meth-amphetamine Lab Presence"	The Special Study will be selected.
8	Click the **Edit Codes** push button.	The Codes Lookup window will be displayed.
9	Highlight¨ Meth-amphetamine Lab Presence (it appears as the single bullet item)	The Special Study will be selected.
10	Click the **New** button.	The detail fields will clear.
11	In the Decode Value field, enter a description to define the code.	Enter: No Meth Lab materials found on site
12	Leave the Parent Code field blank.	
13	In the Code Value field, enter value to represent the code	Enter: 0
14	Click Save	The code to define the Special Studies will be saved.
Repeat steps 8 – 14 if an alternative code is necessary.		
15	Highlight¨ Meth-amphetamine Lab Presence (it appears as an open directory folder, with a bullet item for code 1 underneath it.)	The Special Study will be selected.
16	Click the **New** button.	The detail fields will clear.
17	In the Decode Value field, enter a description to define the code.	Enter: Meth Lab materials found on site
18	Leave the Parent Code field blank.	
19	In the Code Value field, enter value to represent the code	Enter: 1

20	Click Save	The code to define the Special Studies will be saved.

8. The Field Perms Window

State Program Managers assigned the State Level permission will have the ability to modify the field security levels of data fields in the NFIRS 5.0 system for their state and fire departments by using the components of the Field Permissions window. The purpose of these settings is to prevent data from being released in the public data format if this would conflict with state or local jurisdiction privacy laws. The Design Documentation (page 108 - 125), available at http://www.nfirs.fema.gov/documentation/design/ contains a list of default security levels for each field in the NFIRS 5.0 system.

The data security settings are in effect once the data is transmitted to the National Database via transaction file or entry with the USFA client software. Data fields marked "State" and “FDID” are collected and stored in the National database, but may not be released publicly without the State’s permission or originating Fire Department's permission.

8.1 Changing a Field's Security Level

To modify an existing default field security setting, open the System Admin Tool. To modify a field's security setting for the entire state, highlight the State in the hierarchy and click the **Field Perms** button. A confirmation window will appear which states: Since you have not selected a specific FDID, you will be setting preferences for the entire State. Do you wish to continue? Click Yes to modify a field level's security for the entire state. Click No or Cancel to return to the hierarchy and select a FDID.

To modify a field's security setting for an FDID, locate the desired FDID in the hierarchy. Click on the **Field Perms** button. The Field Level Perms window will open.

When the Field Perms button is clicked, the Field Level Perms window will be displayed. In this window, the list of fields in the NFIRS 5.0 System will be displayed. Select (highlight) the desired field. The selected field's info will appear in bottom pane, including the default level security for the selected field.

There are three checkboxes in the Visibility section where the field permissions are specified: and National, State, Fire Department. Make the desired change for the selected field by un-checking or checking the box next to the level. Example, to specify the selected fields' data should not be included in release at the public level, uncheck the National box. Click the Save button.

To verify a field's security level setting has been saved, close and reopen the System Admin Tool. Locate the desired field and verify the visibility is set as was specified in the previous session.

9. The System Administration Tool Rapid Start-up Guide

The Rapid Start-Up Guide for the System Administration Tool outlines the key steps necessary for the System Administrator to begin using the Tool as quickly as possible. Only key points are described below. In-depth information on the System Administration Tool can be found beginning on Page 3 of this document.

9.1 Starting the System Administration Tool

1. Go to Start…Programs…NFIRSv56…System Admin Tool.
2. A screen will appear: "Login On-Line." Enter User Name, State and Password. Click **OK**.

9.2 To Create a New Group

1. Click once on the Group in which the County or Fire Department is to be added.
2. Click on **New** push button.
3. The System will assign a Group ID, and the Parent Group will become the Group to which you are adding.
4. Enter an FDID number and description of the Group you are adding. For a County or Region, enter the description; for a Fire Department, enter the description and FDID.
5. Click on **Save**.
6. The Group Hierarchy will collapse.
7. Click on the + sign to display the hierarchy tree.

Note: When the System Administrator exits the System Administration Tool after any changes were made to the Groups, these changes will not be seen for about 20 minutes.

9.3 To View Users

1. Go to Start…Programs…NFIRSv56…System Administration Tool.
2. The On-Line login screen appears. Enter Username, State and Password. Click **OK**.
3. At the Group Hierarchy Window, click on the desired Group to view its users' list.
4. Click on the **Users** push button.

5. The User Maintenance Window will be displayed and the users associated with the Group will be displayed.

9.4 To View All Users in the State

1. In the Group Hierarchy Window, click on your state to highlight.
2. Check the box next to **Select All Groups Below**.
3. Click on the **Users** push button.
4. The User Maintenance Window will be displayed and all users in selected state will be listed.

9.5 To View All Inactive Users in the State or Group

1. In the Group Hierarchy Window, click on your state to highlight.
2. Check the box next to **Select All Groups Below**.
3. Click on the **Users** push button.
4. The User Maintenance Window will be displayed and all users in selected state will be listed.
5. Click on the **Inactive - 60 Days** radio button (located on the right side of the window). The list displayed lists only those users whose accounts Status is Inactive.

9.6 To Activate a User

1. At the Group Hierarchy Window, click on your state.
2. Click on the **User** push button.
3. Users will be displayed.
4. Highlight the user to be activated.
5. Enter the system assigned **Group ID** the user is to be associated with (not the FDID).
6. Click on **Status**…select **Active**.
7. Click on the **Set Permissions** button.
8. Check the box next to the permissions to be assigned. Note: The Bulk Import Permission enables users to access the Bulk Import Web interface. The Bulk Export Permission allows the user to access the Bulk Export.

9. Click **OK** to close the Permissions window.

10. Click **Save** on the User Maintenance window before closing. .

Note: When a user registers using the User Registration Form from the NFIRS 5.0 Web Site, their default Group ID is the Group ID of the state they registered in. The user's accounts are inactive until the System Administrator activates them. Additional permissions may be assigned at the time of activation or at a later date.

9.7 To Create A Plus One Code

1. Click on the **Other…** button, and then click on the **Codes** button.
2. Select (highlight) the Code Category for which the Plus One code will be created.
3. Click on the **Edit** button.
4. The Codes Lookup window will be displayed, and contain the existing codes for the selected category.
5. Highlight the parent code for the new Plus One code.
6. Enter the **Parent Code** value.
7. Enter the **Code Value**. This is the numeric or alpha numeric value that signifies the code.
8. Enter the **Decode Value,** This is the description users will see in the Code Lookup window.
9. Verify the **Status** is **Active**.
10. Click **Save.**

9.8 To Create A Special Studies

1. Click on the **Other…** button, and then click on the **Special Studies** button.
2. Select (highlight) the Code Category for which the Plus One code will be created.
3. Click on the **New** button.
4. A system assigned number will fill the Special Study ID field. The User Group ID will default to the System Administrator who is logged in.
5. Modify the Start and Stop dates as desired.
6. Enter the Max Length for the codes that will define the Special Study (1 is adequate for most codes).
7. Enter a Description for the Special Study.

8. Verify the Status is Active (if it is to be implemented immediately).

9. Click **Save.**

10. Locate the newly created Special Study in the list and click the **Edit Codes** button.

11. In the Codes Look up window, highlight the Special Study where it appears as a bullet item and click the **New** button.

12. Enter a **Decode Value** (the description).

13. Leave the **Parent Code** field blank.

14. Enter a **Code Value** (the numeric or alpha code to represent the Special Study details).

15. Click Save.

10. Troubleshooting

- A user contacted me to report he forgot his password. How do I reset his password?

  An Administrator cannot recover a lost or forgotten password. Change the user's password.

  In the User List Pane, highlight the user. In the User Detail field, click the **Change Password** button. A pop up window appears. The administrator enters a new password, then reenters the password to confirm. Click **OK**. Report the password to the user.

- When a user opens the Data Entry Tool, "**FDID Not Found" message** displays instead of the Fire Department name.

  The Header Record has not been created for the group. The user must create the Header Record.

  To create a Header Record, the user selects **Fire Dept** from the Menu Bar (in the Data Entry Tool Main View Screen). Click on **New Fire Dept**. In the Fire Department Screen, the user will see the FDID number. The user enters the Fire Department Name. All other information is optional. When the user clicks **OK**, the information will be saved and the user is returned to the Data Entry Main View Screen. An import of Fire Department information will also create the header record.

- A user trying to register reports an error message: **Failed to Register User: 10477** (or **9999**).

  The Username is already been taken by another registrant in the state. The user must choose a new username. Advise the user to alter a character in the name and submit the registration again.

Note: The Username is not case sensitive, but is space sensitive. It may be an alpha-numeric value. Punctuation or other characters is not recommended in the Username

- A user trying to login reports an error message: **You have not been activated** or, **Failed to Register User: 10468**

  The user account status is Inactive. In the System Admin Tool User Maintenance window, locate the user account and reset his or her status to Active. Click Save. Advise the user to login the same day, or their account will deactivated upon the daily reboot of the system.

- How long does it take to activate a Group?

  When an administrator creates or adds a group, it takes approximately twenty minutes for the information to be processed in the National Database. After this period, the group will display in the hierarchy. When an administrator activates a user or changes the user's status, the change takes place immediately.

- How long does it take to activate and View a Plus One Code?

  When an administrator creates or adds a Plus One Code, it takes approximately twenty minutes for the information to be processed in the National Database. After this period, the Plus One Code will display in the On-Line User's View of the Code Lookup box. Off-Line users must perform User Injection to obtain the added Plus One codes in the Code Lookup box.

11. Index