INCIDENTS

Version 01.00.01

The names of individuals displayed in this document have been removed from viewing clearly in accordance with security guidelines in protecting Personally Identifiable Information (PII)

Thursday, February 04, 2016

Table of Contents

Incidents Overview **4**
Add an Incident **5**
Add an Incident to Enterprise 5
Adding an Incident to Site 9
Adding a Site Database 9
Site Account Manager Setup 10
Completing the Incident Information in the Site Database 12
Adding Accounting Codes 12
Edit an Incident **15**
Deleting an Incident **18**
Restoring an Incident 19
Site 19
Enterprise 19
Adding User Accounts **20**
Site 20
Reset Password 20
Enterprise 20
Adding a User Account to an Incident in Enterprise 21
Removing a User Account from an Incident in Enterprise 22
Adding Users from User Group to a Single Incident 23
Reset Password in Enterprise 25
User Group Overview **26**
Adding User Groups in Enterprise **27**
Editing User Groups in Enterprise **30**
Deleting User Groups in Enterprise **32**
Reference Data Overview **34**
Non-Standard Reference Data 34
Agencies 35
Add a Non-Standard Agency 35
Edit a Non-Standard Agency 36
Delete a Non-Standard Agency 36
Unit ID's 37
Add a Non-Standard Unit ID 37
Edit a Non-Standard Unit ID 38
Delete a Non-Standard Unit ID 39
Jetports 39
Add a Non-Standard Jetport 39
Edit a Non-Standard Jetport 40
Delete a Non-Standard Jetport 41
Item Code 42
Add a Non-Standard Item Code 42
Edit a Non-Standard Item Code 43
Delete a Non-Standard Item Code 44

Incident Groups Overview **46**
Add Incident Groups **48**
Assigning Users to the Incident Group 51
Add Users from Group to an Incident Group 52
Remove Users from an Incident Group 53
Editing Incident Groups **56**
Deleting Incident Groups **58**
View/Hide Incidents **60**
Financial Export **62**
Create a Financial Export File 62
Uploading a Financial Export File 63
Index **64**

Incidents Overview

The e-ISuite system allows the user to manage all types of incidents. This section explains how to perform the following procedures for incidents in the e-ISuite system:

- Manually add an Incident
- Edit an Incident
- Delete an Incident
- View/Hide Incidents
- Financial Export

Add an Incident

NOTE: Only non-privileged user accounts with a Data Steward Role can create, edit, delete or manage Incidents.

NOTE: There are three ways in which to add an incident: Manually; through a ROSS import; or through the use of a Data Transfer file. See the appropriate sections for further information on the ROSS Import and Data Transfer processes.

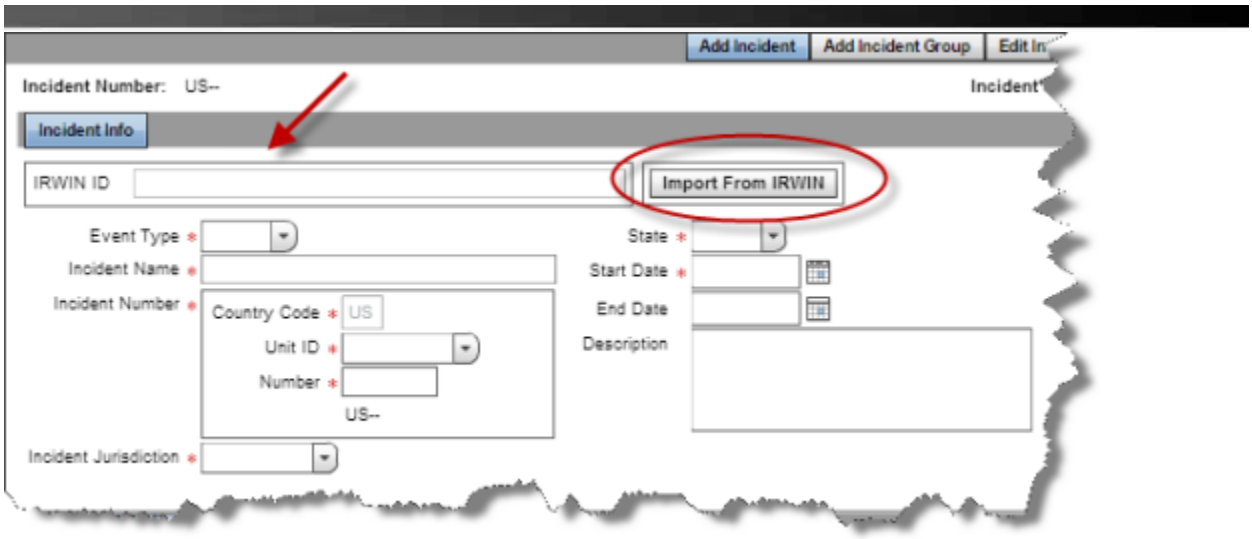
Add an Incident to Enterprise

Follow the steps in this section to manually add an incident to Enterprise:

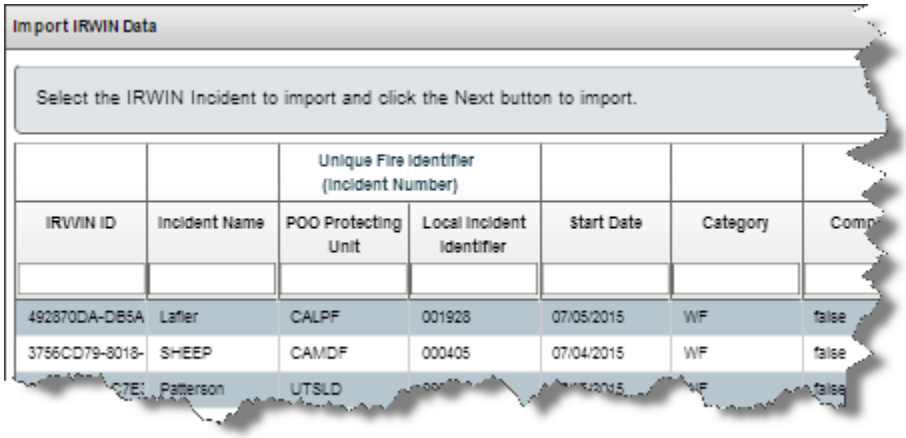
1. From the Home page click the **Incidents** button.

2. The Incidents grid will display.
3. Click **Add Incident**.

4. From the Incident Info tab, enter the Incident information.
5. If the incident is linked to IRWIN click the **Import From IRWIN** button. The Import IRWIN Data window displays.



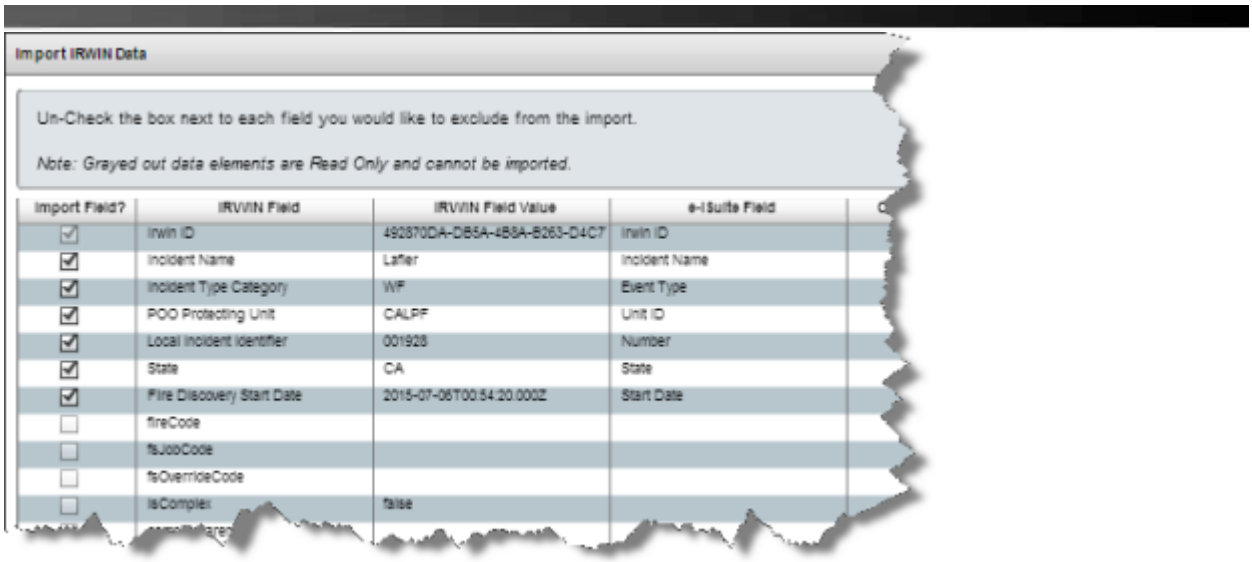
- To search for an Incident, enter the **Incident Name** or **Incident Number**.
- Enter the number of days for the system to return all incidents that started or have been updated within the number of days defined.
- Click the **Search** button to search for IRWIN incidents.



- Select an incident in the list of IRWIN incidents that displays and click the **Next** button.

NOTE: Only fields 2-7 can be selected. The IRWIN ID cannot be unchecked.

- Check to select the fields to include in the import data and click the **Complete** button. The user that add's the incident will automatically be added to the list of users in the **User Access List**.



Import IRWIN Data

Un-Check the box next to each field you would like to exclude from the import.

Note: Grayed out data elements are Read Only and cannot be imported.

Import Field?	IRWIN Field	IRWIN Field Value	e-ISuite Field
☑	Irwin ID	492870DA-DB5A-4B8A-B263-D4C7	Irwin ID
☑	Incident Name	Lafler	Incident Name
☑	Incident Type Category	WF	Event Type
☑	POO Protecting Unit	CALPF	Unit ID
☑	Local Incident Identifier	001928	Number
☑	State	CA	State
☑	Fire Discovery Start Date	2015-07-06T00:54:20.000Z	Start Date
☐	fireCode		
☐	fsJobCode		
☐	fsOverrideCode		
☐	isComplex	false	

NOTE: When the user manually enters an incident or imports an incident from ROSS that is also included in IRWIN, the system automatically matches the e-ISuite incident with the incident in IRWIN and populates the IRWIN ID field with the IRWIN number.

11. Select the **Event Type** from the drop-down list. Use the description that most closely describes the incident.

12. Enter the **Incident Name** as it appears on Resource Orders or as incident host unit directs. (Discuss with ITSS any issues with incident name not matching ROSS name for import purposes.)

13. Enter the **Incident Number**.

NOTE: The Incident Name, Incident Number and Start Date combined uniquely identify an incident. If there is another incident with the same name, number and year in the start date, an error message will display and the new incident record will not be saved.

14. Enter the **Country Code**, the default is US.

15. Select the **Unit ID** from the drop-down list. Ask the host unit personnel if uncertain.

16. Enter the **Number** as it appears on Resource Orders. Ask host unit personnel if uncertain. If the number entered is less than six characters, the system will fill in with leading zeroes in order to reflect six characters (e.g. 56 will be reflected as 000056).

17. Select the **Incident Jurisdiction** from the drop-down list.

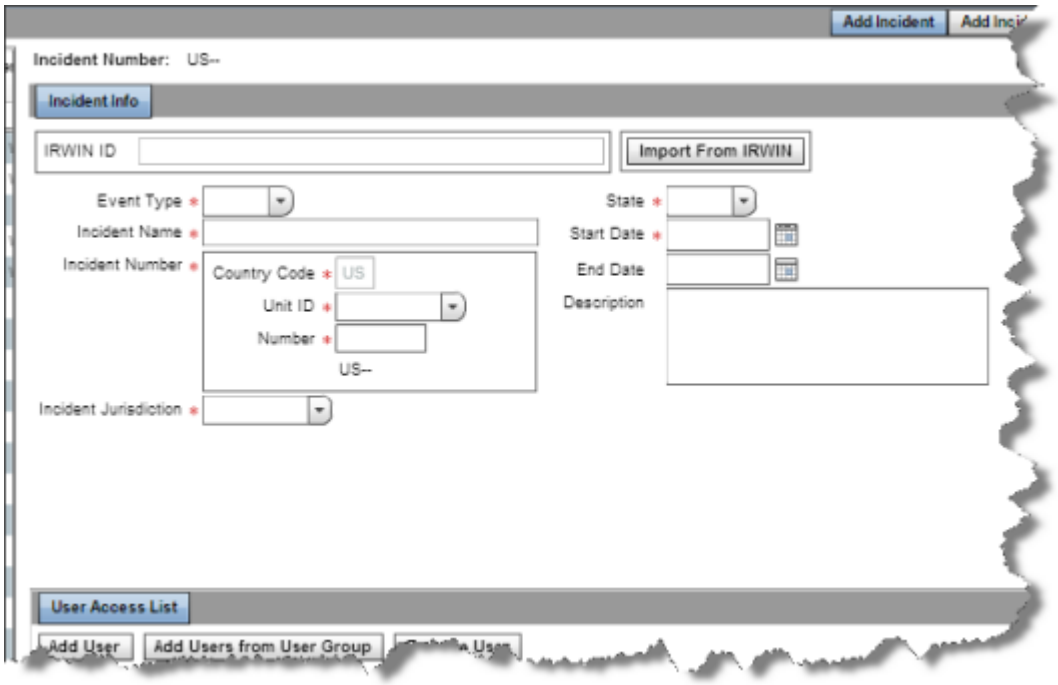
NOTE: The Incident Jurisdiction facilitates cost accrual category decisions.

18. Select the **State** from the drop-down list.

19. Enter the **Start Date** or click the calendar icon to select a date. If uncertain, ask the host unit for date to be used.

20. The **End Date** should not be filled in until all costs and other activity associated with the incident have been entered. Enter the **End Date** or click the calendar icon to select a date. The host unit Fire Management Officer or Agency Administrator should specify the end date.

21. Enter any additional information about the incident in the **Description** box. This usually refers to the geographic location of the incident or incident base camp.



22. Go to the User Access list to add User Accounts to the incident.

23. Click **Save** to save the Incident. This will activate the Accounting Code tab. Accounting Code information is not required prior to saving an incident, but is required to generate payment documents.

NOTE: An Incident must be Saved to activate the Accounting Code tab.

Adding an Incident to Site

Adding a Site Database

NOTE: Once a Site database has been set up, incident data can be added manually, imported through a ROSS Import, or by using data from an existing Enterprise incident with a Data Transfer file copied to a portable media drive.

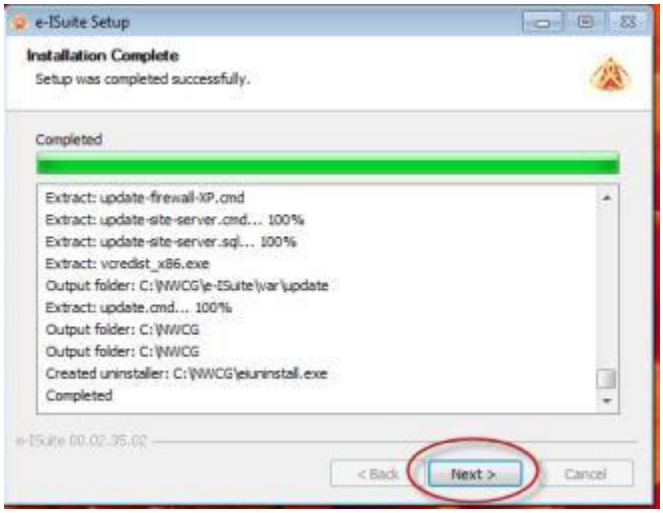
Follow these instructions for Site Installation and setup:

(These instructions are also included in *Getting Started*).

NOTE: e-ISuite Site only needs to be installed on the Site server. There is no need to install it on every computer at the site. All other computers will access the Site system by entering the appropriate URL into an Internet browser or double clicking on the e-ISuite Site icon that will display on the computer's desktop.

1. Go to the e-ISuite webpage (http://famit.nwcg.gov/applications/eISuite)
2. Click on the link for the e-ISuite Site download.
3. Download the Site database.
4. Save the file to the desktop.
5. When the download is complete, double click on the file on the desktop to begin the installation process.
6. Click the **Install** button.

7. When the installation is complete, click the **Next** button.



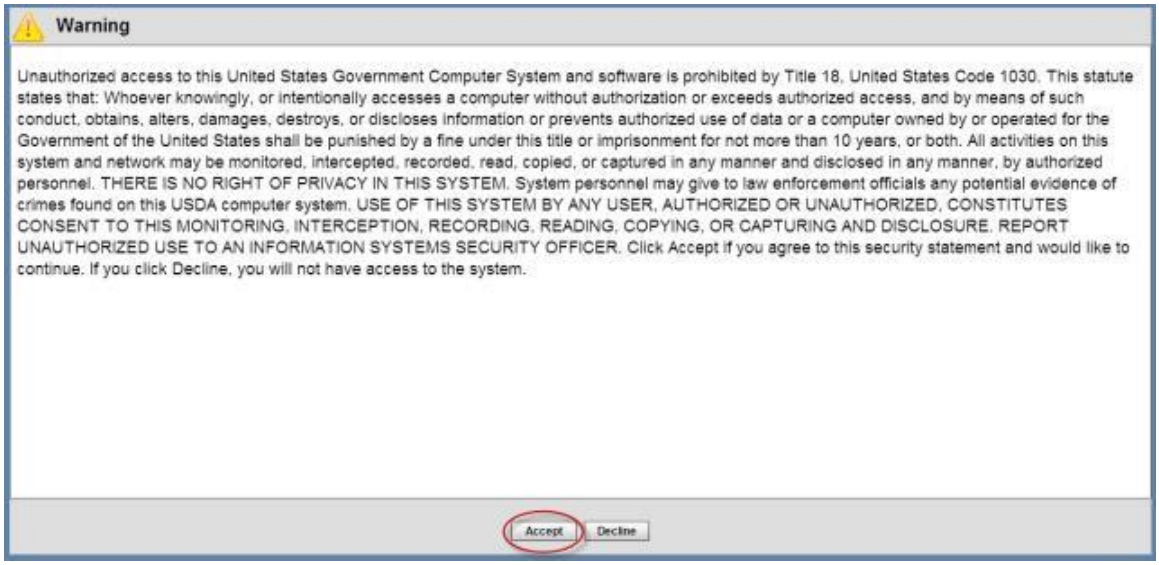
8. Click the **Finish** button when the message displays indicating that e-ISuite Site has been installed on the computer.

9. An e-ISuite Site icon will display on the computer's desktop.

Site Account Manager Setup

1. Double click on the e-ISuite Site icon on the desktop, or enter the web address for e-ISuite Site (received from the ITSS).

2. Accept the warning that displays. After accepting the warning a Create Account Manager User screen displays.



3. Enter a name for the new database that will be created in the **Database Name** box.

4. Enter a password for the new database in the **Database Password** field.

5. Confirm the **Database Password**.

6. Enter the **User Name** for the Account Manager account.

NOTE: The system will auto-populate "ad." at the beginning of the user name. The Account Manager account must contain the ad. prefix.

7. Enter the **First Name** for the user account.

8. Enter the **Last Name** for the user account.

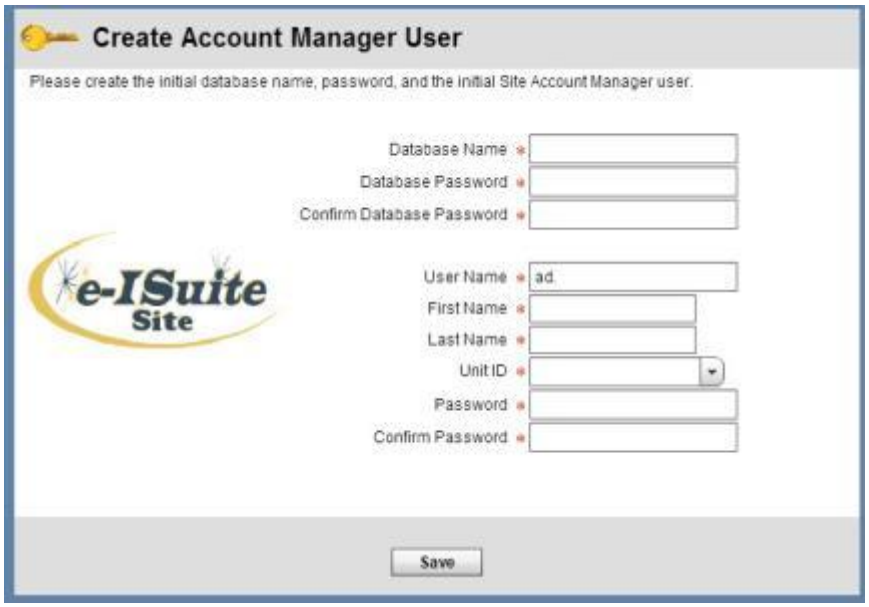
9. Select the **Unit ID** for the user account.

10. Enter a **Password** for the user account.

NOTE: Passwords must be 12 or more characters in length and must include at least one alpha, one numeric and one special character. Passwords cannot be a dictionary word and cannot match any of the previous 24 passwords that were used.

11. Enter the password a second time in the **Confirm Password** field.

12. Click the **Save** button.



Completing the Incident Information in the Site Database

Once the database has been set up and the Account Manager has created a user account with the role of Data Steward (see the section on Adding User Accounts), the Data Steward can log in to the Site database and complete the incident information.

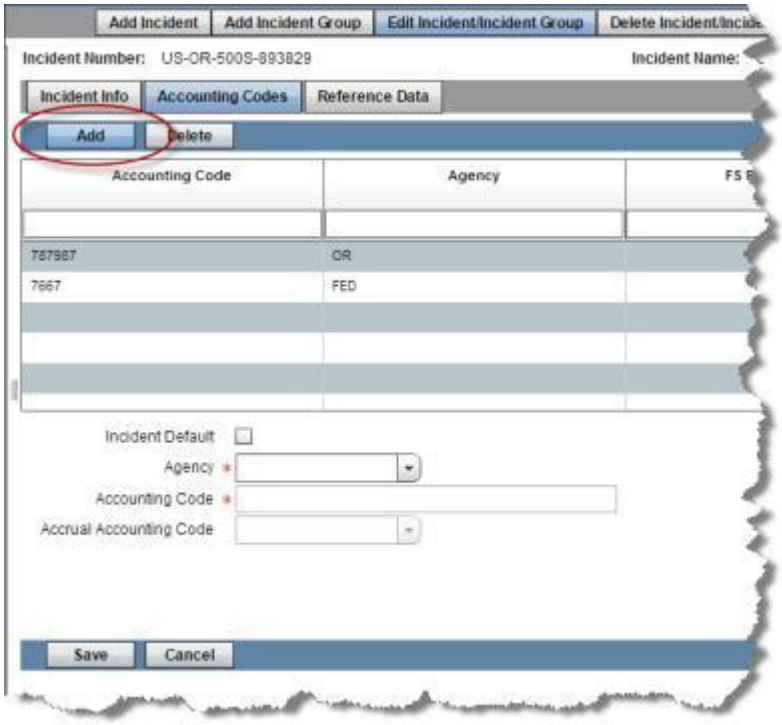
NOTE: There are three ways in which to complete the incident information: Manually; through a ROSS import; or through the use of a Data Transfer file. Follow the steps outlined in the section titled *Add an Incident to Enterprise* **to complete the manual process (this process is the same in Enterprise and Site). See the appropriate sections for further information on the ROSS Import and Data Transfer processes.**

Adding Accounting Codes

1. Select the **Accounting Codes** tab to add Accounting Codes to the Incident.

NOTE: Until the Incident information is saved, the Accounting Code tab will not display.

2. Click the **Add** button above the Accounting Code grid.



3. To set an accounting code as the incident default, click the checkbox to select the **Incident Default**.

4. Select the Agency from the **Agency** drop-down list.

NOTE: An Agency is required. An Accounting Code cannot be defined until an Agency is selected

5. Enter the Accounting Code.

6. To assign an accrual accounting code to the accounting code for Cost purposes, select the code from the Accrual Accounting Code drop-down list which is populated with all accounting codes entered for that incident.

7. If **USFS** or **FED** is selected in the Agency field, a Region/Unit drop-down list is available. Select the appropriate region or unit code from the list.

NOTE: The Region/Unit is NOT required. If a Region/Unit is selected, it prints on the OF-288 in Block 3.

8. Continue adding accounting codes until all accounting codes have been entered.

9. Click the **Save** button.

NOTE: All Accounting Codes entered for an incident will be available to assign to a resource, for use in posting time and recording costs appropriately. See *Check-in, Time and Cost* for further information.

NOTE:

- The first Accounting Code assigned to an incident is marked as the Default. A checkmark will display in the Accounting Codes grid under the Default column.
- The Incident Default cannot be unchecked and saved unless a new Accounting Code has been entered and designated as the default.
- The same Accounting Code can be the default code for multiple incidents.
- Agency has to be selected prior to entering an Accounting Code.
- The same Accounting Code cannot have different Agencies assigned.
- If there are no Accounting Codes defined for the Incident, the Accrual Accounting Codes drop down list will be blank.
- The User can still manually enter an Accounting Code even if it is in the drop down list.
- If an Accounting Code has been assigned to a Resource or used in any time postings, the system will prevent the user from deleting the Accounting Code.
- The same Accounting Code can be added to multiple incidents.
- If the Event Type selected is Fire - Wildfire Fire, the Agency list will only show FED and not individual fire agencies.
- The system will show a message if the accounting code for one incident is duplicated for other incidents. The system will not prevent use of the same accounting code, only issue a warning.

Edit an Incident

Follow the steps in this section to edit an existing incident in Enterprise and Site:

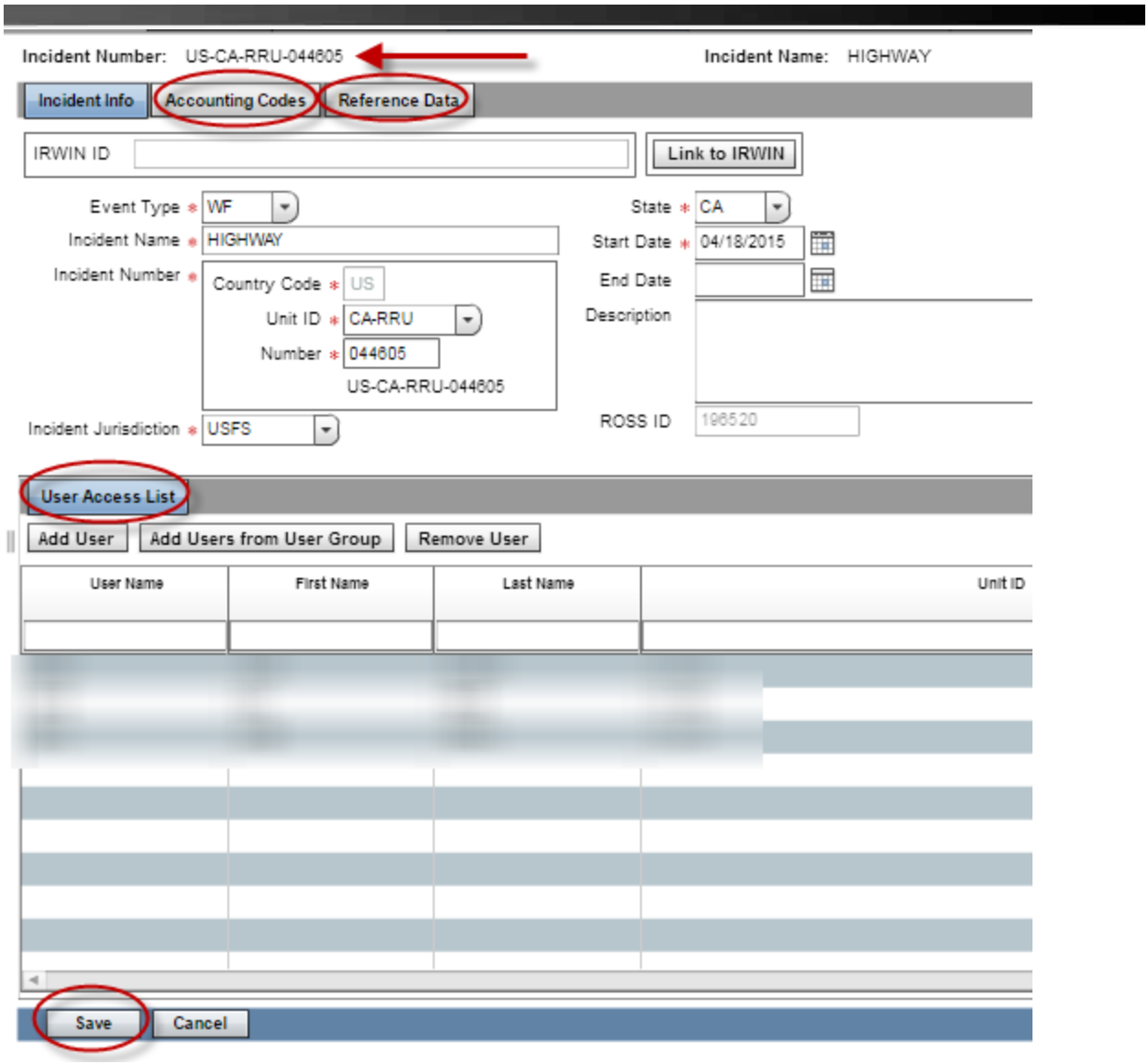
NOTE: Only users with a Data Steward Role can edit Incidents.

1. From the Home page click the **Incidents** button.

2. The Incidents grid will display.

3. Select the Incident to edit and click the **Edit Incident/Incident Group** button.

NOTE: In Enterprise if an Incident Group is selected instead of an Incident, the system will display the fields for editing an Incident Group. See the Manage Incident Groups section for more information about Incident Groups.



4. Edit the Incident data as desired.

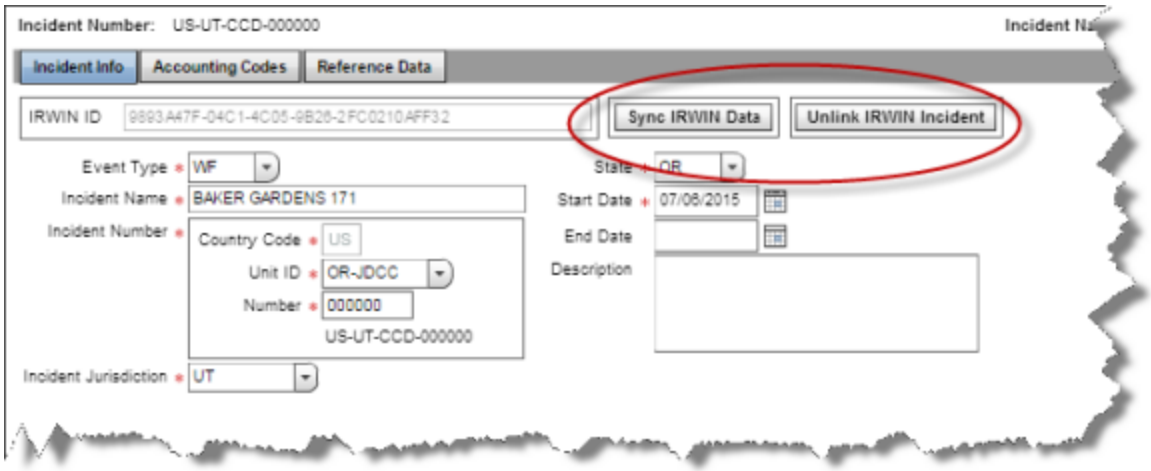
5. Optionally, if the incident is linked to IRWIN click the **Sync IRWIN Data** button to get the latest incident information from IRWIN.

    - The Sync IRWIN Incident window displays. Check the box next to each field to overwrite with the IRWIN value and click the **Complete** button.

    - Click the **Unlink IRWIN Incident** button to unlink the incident from IRWIN.

NOTE: Different messages will display when there is changed data.

* A message will display when the incident originally came from IRWIN, but the IRWIN incident no longer exists in IRWIN.
* A message will display when an incident was deactivated in IRWIN.



6. To edit the User Account List in Enterprise, select **Add User** or **Add Users from User Group** and make the appropriate changes to user's access to the Incident.

NOTE: To remove a User from the User Access List, select the User and click **Remove User**.

7. Select the **Accounting Codes** tab to edit Accounting Codes assigned to the Incident.

8. Select the **Reference Data** tab to edit Reference Data specific to this incident. (See *Reference Data for details*).

9. Click the **Save** button to save the incident.

Deleting an Incident

Follow the steps in this section to delete an incident from Enterprise:

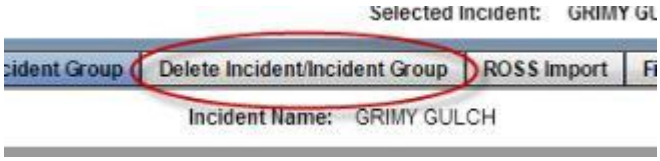
NOTE: Only users with a Data Steward Role can delete Incidents.

NOTE: The user can only delete incidents that do not have critical data associated with them (e.g., time postings).

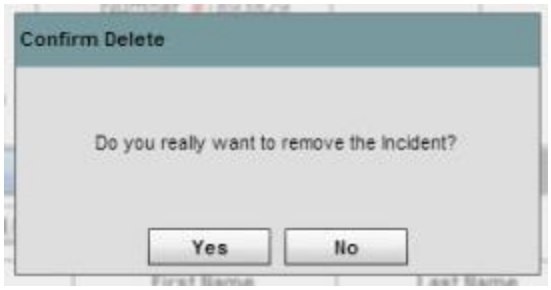
1. From the Home page click the **Incidents** button

2. The Incidents grid will display.

3. Select the Incident to delete and click the **Delete Incident/Incident Group** button. Only one Incident can be selected at a time for deletion.



4. A confirmation message will display.



5. Click **Yes** to delete the incident.

Restoring an Incident

Site

Ensure that either the auto back up option is selected, or the database is being backed up manually on a regular basis. If there is a problem with a database or it becomes corrupted for some reason, a back-up copy may be the only option to restore the database. The Account Manager role has access to Database Management options. Refer to that section in Site Account Manager.

Enterprise

Currently, there is no option to restore an Enterprise incident database. Call the IIA Helpdesk at 866-224-7677 if there is a problem with a particular incident that cannot be resolved.

Adding User Accounts

Site

After an Account Manager initially establishes an incident in Site, they can then create the user accounts. All user accounts created in a Site database have access to all of the incidents in the database.

See *Account Manager User Guide* **for further information on creating, editing and deleting user accounts.**

A user account must be created for each user in the Site database, even if that user already has a user account for Enterprise. A user account created in the Site database is not associated with any user account in Enterprise, and cannot be used to log into Enterprise.

A user account can be disabled or deleted, depending on whether the user has logged into the system using that account. If a user has logged into the system with a user account, that user account cannot be deleted, but it can be disabled by an Account Manager. If a User Account is disabled, the user can no longer log into that User Account until it is enabled by the Account Manager. A user account can only be deleted if a user has not used that account to log into the system.

Reset Password

See *Account Manager User Guide* for more detail on resetting passwords for Site user accounts.

Enterprise

NOTE: Only user accounts established and verified through the NAP can be added to the Access List for an incident in Enterprise. See the information in the Account Manager User Guide for further detail on how to request a NAP account.

See *Account Manager User Guide* for further detail on adding, editing and deleting user accounts in Enterprise.

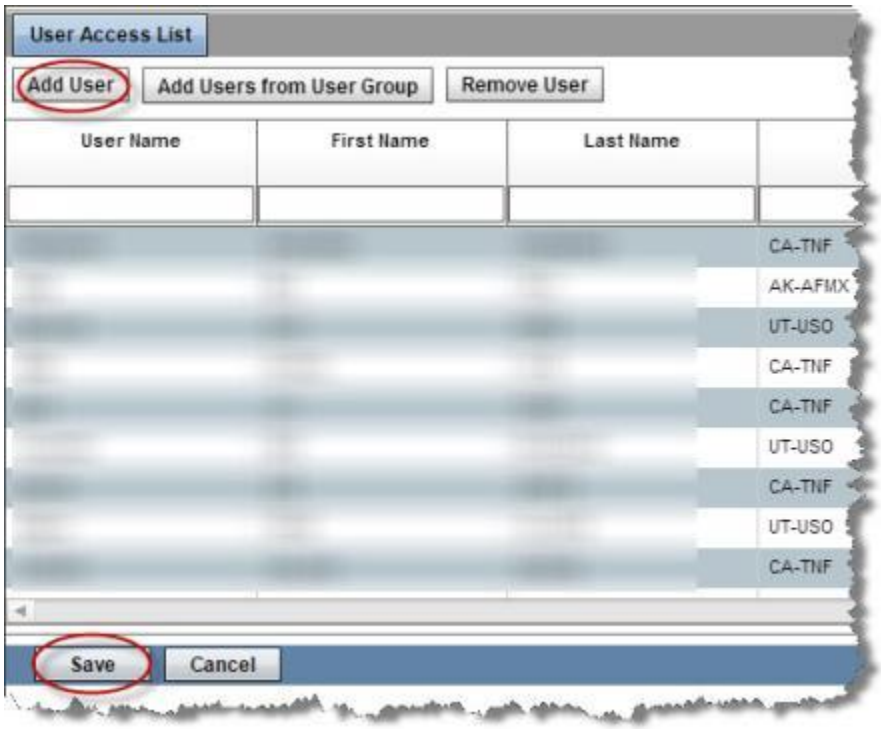
Adding a User Account to an Incident in Enterprise

After an Account Manager has added a user account(s) to the Enterprise system from NAP and assigned the necessary roles, a user with the Data Steward role can add the user account(s) to the User Access list for an incident. The User Access List screen only pertains to single incidents, not incident groups and only single users or an entire user group (not specific individuals within that group). See *Adding Users from User Group to a Single Incident*.

The Data Steward can access the User Access List tab by clicking the Add Incident button or selecting an incident in the incident grid, then clicking the Edit Incident/Incident Group button.

On the Incident screen under the **User Access List** tab:

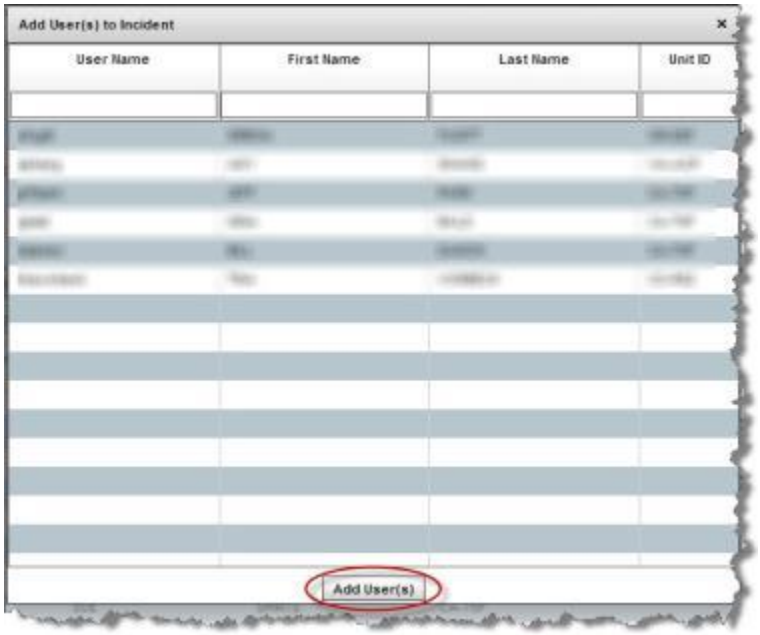
1. Select **Add User**.



2. A pop up window will display with a list of user accounts.
3. Select the user account(s) desired.
4. Click **Add User(s)**.
5. Click on the x in the upper right hand corner to close the window.

6. When the Data Steward adds user accounts from the pop-up window those accounts will display in the grid under the User Access List.

7. Click the **Save** button.



NOTE: A user account can be added to multiple Incidents in Enterprise.

NOTE: The creator of the incident is automatically attached to the incident as a user; however, any additional roles must be assigned by an Account Manager. The User that created an incident cannot be deleted from that incident.

Removing a User Account from an Incident in Enterprise

On the Incident screen under the **User Access List** tab:

1. In the grid highlight the user account to remove.

2. Select **Remove User**.

3. Click the **Save** button.

NOTE: A user account that has been removed from the Access List for an Incident in Enterprise is not removed or deleted from the NAP. The user account remains in the NAP, and if active, it can be added to other Incidents in Enterprise.

Adding Users from User Group to a Single Incident

Using the User Access List option, the Data Steward can add a pre-defined group of users to a single incident. The Data Steward cannot act on individuals within this pre-defined group of users, only the entire group. Once the "group" has been added to the User Access List, it will show all the individuals within the group. At that point the Data Steward can act on individual accounts.

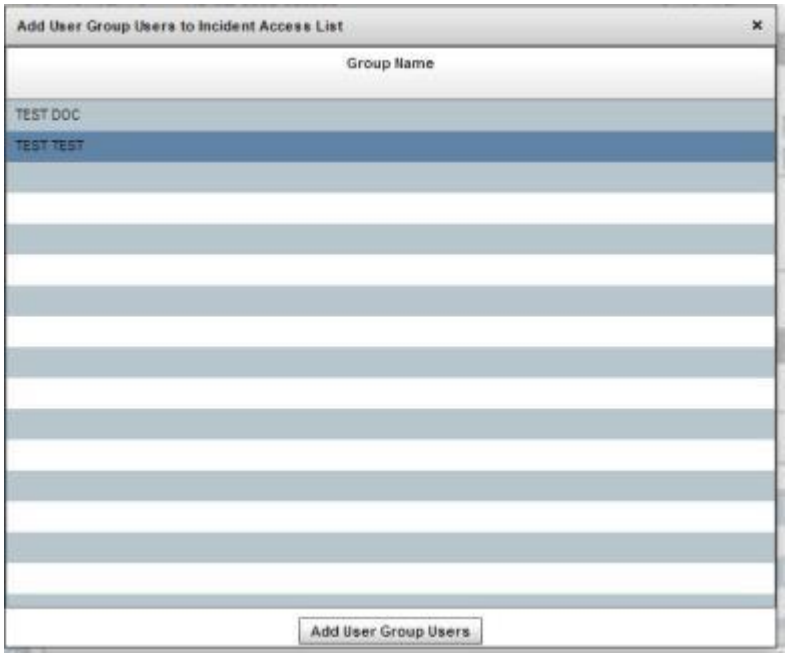
On the Incident screen under the **User Access List** tab:

1. Click **Add Users from User Group** tab.

2. Select a group(s) from the **Add User Group Users to Incident Access List** screen.

3. Click **Add User Group Users** button.

4. The group name will not appear in the User Access List grid. The list of individuals belonging to that group will be listed in the grid.



5. Click **Save**.

See *Adding User Groups section* for further details on creating a User Group.

Reset Password in Enterprise

Because the user accounts are created at the NAP, the password must be reset through the NAP web page: http://nap.nwcg.gov. The user must access the NAP web page and follow the process to change their password. Passwords cannot be reset in the Enterprise system.

User Group Overview

The purpose of a User Group is to provide quick and easy access to a set of User Accounts with associated roles. The User Accounts will be treated as individual accounts.

- Adding User Groups
- Editing User Groups
- Deleting User Groups

Adding User Groups in Enterprise

User/User Groups:

The Data Steward provides incident access to Users. The Data Steward can also create User Groups. These groups can be made up of users who consistently need access to specific incidents. This could be local dispatch office personnel, expanded dispatch personnel, incident management team members. Instead of adding each user individually to each incident, all those individuals can be grouped (e.g. dispatch group, IMT group, etc.) and added to an incident as a User Group.

NOTE:

- Non-Privileged Users can be added to User Groups.
- Privileged Users cannot be added to a User Group.
- The Name of a User Group must be unique.
- Users in a User Group cannot be duplicated.
- If a User Group is removed, the Users are not removed from the system, only from the Group.
- The Data Steward is automatically listed as a user under any incident or Incident Group they create.
- The Data Steward cannot be deleted.

Follow the steps in this section to add a user group to Enterprise:

NOTE: Only users with a Data Steward Role can manage User Groups.

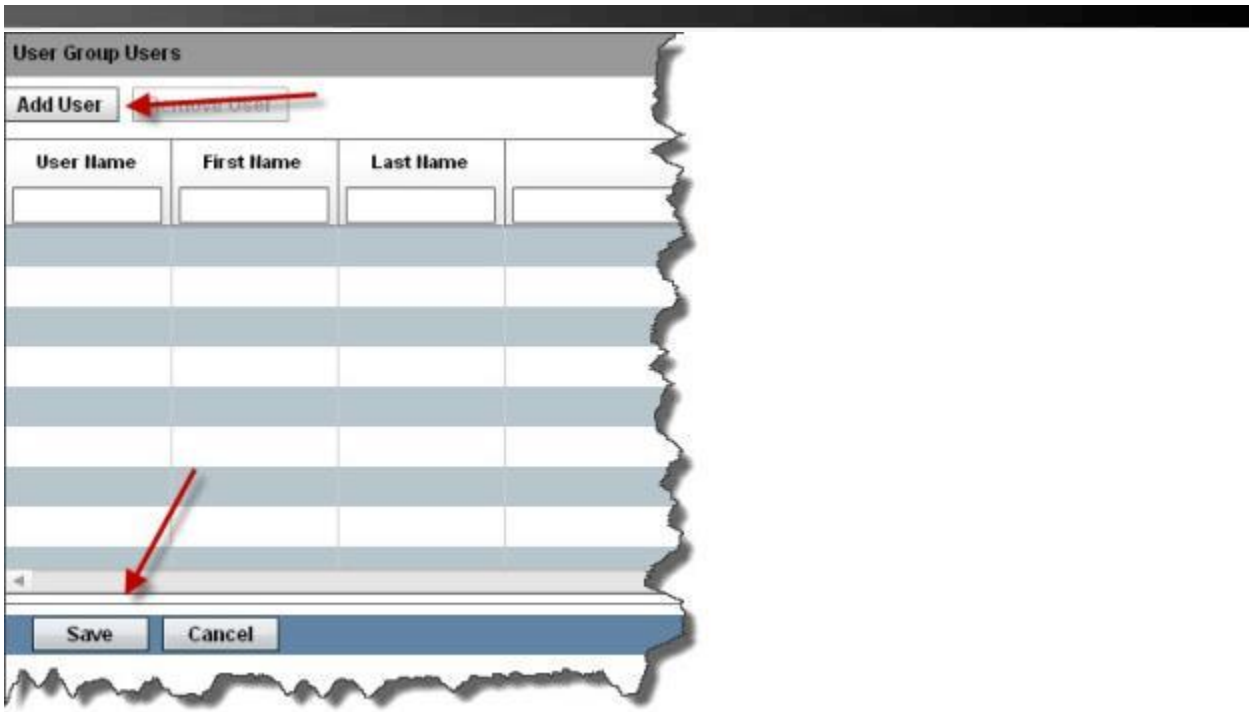
1. From the Home page click the **Incidents** button.

2. Click on the drop down arrow next to the Incidents menu button and select the User Groups option.

3. Click the **Add User Group** button.

4. Enter the **Group Name**.

5. Click the **Add User** button to view a dialogue box with a list of available users.



6. Select the user accounts to add to the user group from the grid that displays. Enter search criteria into the filters above the columns to easily find the user accounts.

7. Click the **Add** button on the **Add User(s) to User Group** window to add the selected user accounts to the user group. Multiple users can be added at the same time.

8. Click "x" to close the window.

9. Click the **Save** button on the User Group screen to save the User Group.

Editing User Groups in Enterprise

Follow the steps in this section to edit a user group in Enterprise:

NOTE: Only users with a Data Steward Role can manage User Groups.

1. From the Home page click the **Incidents** button.

2. Click the drop down arrow next to the **Incidents** menu button and select the **User Groups** option.

3. Select a User Group listed in the **Group Name** grid. This automatically activates the **Edit User Group** button and puts the user in Edit mode.

4. The User Group information displays in the detail area on the right of the screen.

5. If desired, change the User Group name by entering a new name into the **Group Name** field or editing the existing name.

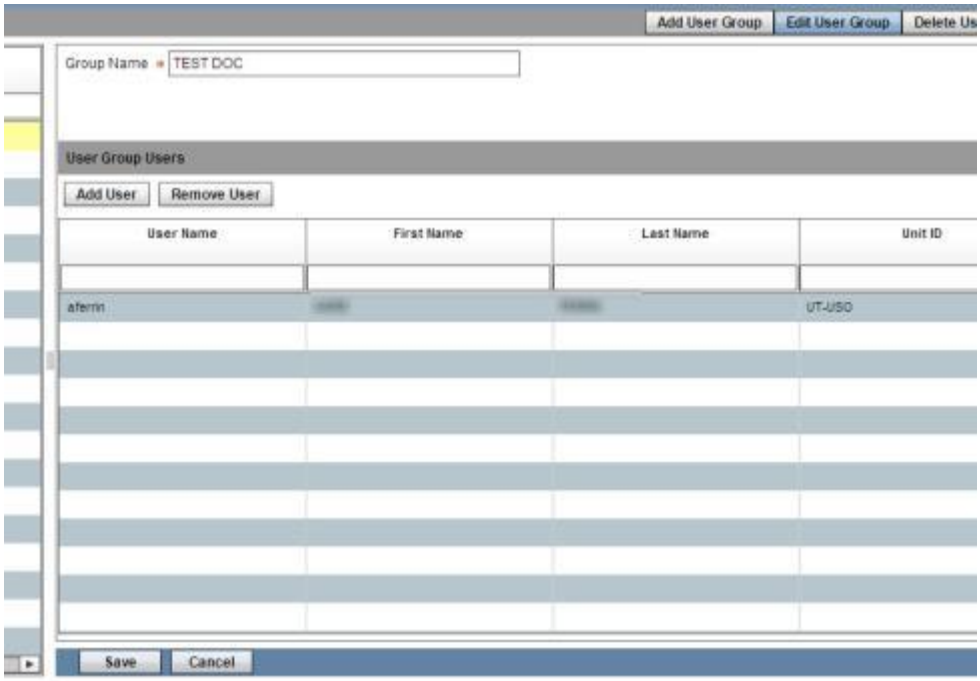
6. To add a new user account(s) to the user group, click on the **Add User** button. Highlight the user account(s) and click the **Add** button. This will add the user(s) to the User Group Users grid.

7. Click "x" to close the pop up window.

8. To remove a user account from the user group, select the user account and click the **Remove User** button. The user is removed.

NOTE: Removing a user account from the User Group does not remove the User Account from the e-ISuite system. This only removes the user account from the User Group. If the user account has logged into an incident in the group, it cannot be removed. Instead, the user account can be disabled by the Account Manager.

9. Click the **Save** button to save any changes made to the User Group.



Deleting User Groups in Enterprise

Follow the steps in this section to delete a user group in Enterprise:

NOTE: Only users with a Data Steward Role can manage User Groups.

1. From the Home page click the **Incidents** button.

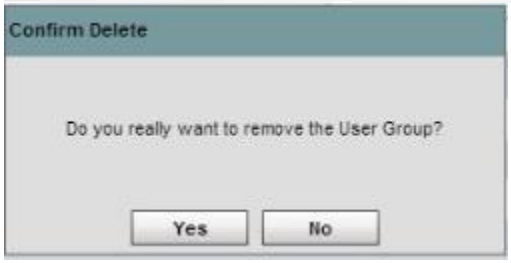
2. Click the drop down arrow next to the **Incident** menu button and select the **User Groups** option.

3. Select the User Group to delete.

4. Click the **Delete User Group** button.

5. A confirmation message will display.

6. Click **Yes** to remove the User Group.



NOTE: Deleting a User Group will delete the entire group. All the users are returned to the general user list. No users will be deleted from the system. The User Group name will be deleted from the system.

Reference Data Overview

NOTE: Until the Incident information is saved, the Reference Data tab will not display.

Non-Standard Reference Data

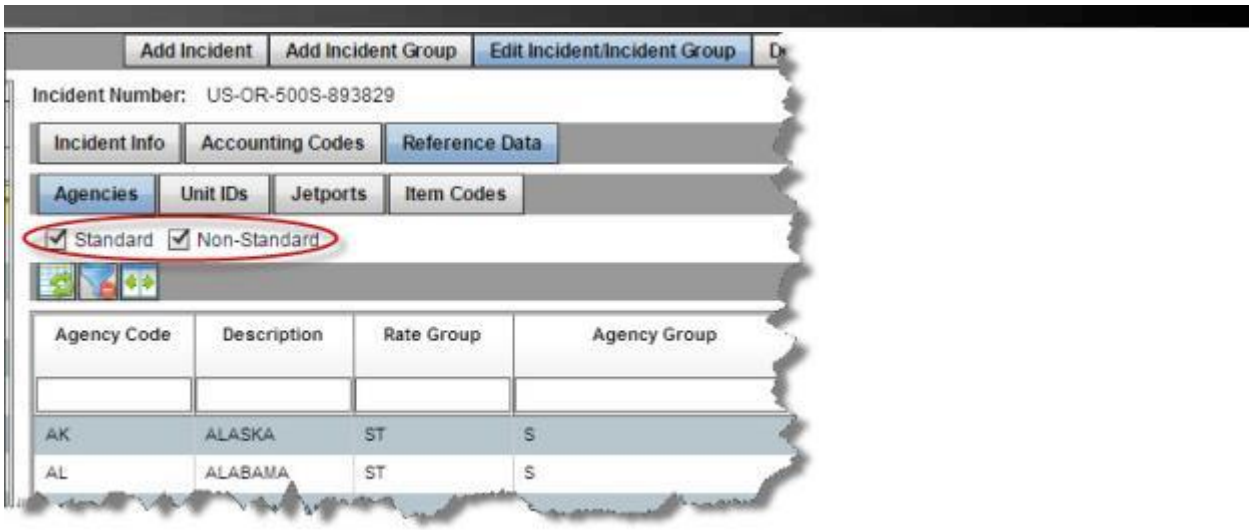
NOTE: **Standard Reference Data** for the e-ISuite application is the default data that applies to all incidents in Enterprise and Site. This data is managed by a privileged user account with the Global Reference Data role.

Non-Standard Reference Data is unique incident information for a single incident or a single incident within an Incident Group. A thorough search of the default Standard Reference Data should be completed before a decision is made to add Non-Standard Reference Data. The Data Steward role can add, edit and delete Non-Standard Reference Data.

NOTE: Reference Data is not a menu item available to Incident Groups. It is available to the individual incidents within an Incident Group.

Agencies, Unit IDs, Jetports and Item Codes can be added as Non-Standard Reference Data. When the user selects any of these tabs, a list of active, Standard Reference Data displays.

Above the grid, there are two checkboxes labeled Standard and Non-Standard. To view only Standard Reference Data, uncheck the Non-Standard checkbox. To view the Non-Standard Reference Data only, uncheck the Standard checkbox and make sure the Non-Standard checkbox is checked.



Non-Standard Reference data cannot duplicate a Standard Reference Data item. If a user enters a code that duplicates Standard Reference Data, the user will receive a message that the data they are trying to enter will not be saved.

Agencies

Add a Non-Standard Agency

1. Select an Incident (or continue adding information to an incident that is already selected).
2. Select the **Reference Data** tab and then select the **Agencies** tab.
3. The screen will default to **Add Agency**.
4. Enter the **Agency Code** (limit of 4 characters).
5. Enter a **Description** of the Agency.
6. Select the appropriate **Agency Group** from the drop down list.
7. Select the appropriate **Rate Group** from the drop down list.
8. Click the **Save** button.

Edit a Non-Standard Agency

1. Highlight an Agency in the grid to edit.
2. Click the **Edit Agency** button.
3. Edit the information as needed.
4. Click the **Save** button.

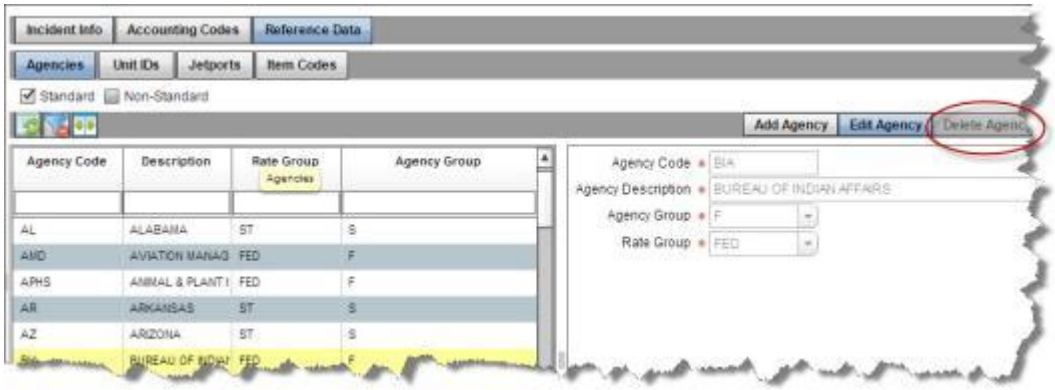
Delete a Non-Standard Agency

1. Highlight an Agency in the grid to delete. Only one code can be deleted at a time.
2. Click the **Delete Agency** button.

3. When the Confirmation message displays, click **Yes** to delete the Non-Standard Agency.

4. Click the **Save** button.

If a Non-Standard Agency is being used at an incident, the Agency cannot be deleted. The user will receive a notification that the code is in use.



Unit ID's

Add a Non-Standard Unit ID

1. Select an Incident (or continue adding information to an incident that is already selected).

2. Click the **Unit ID** button.

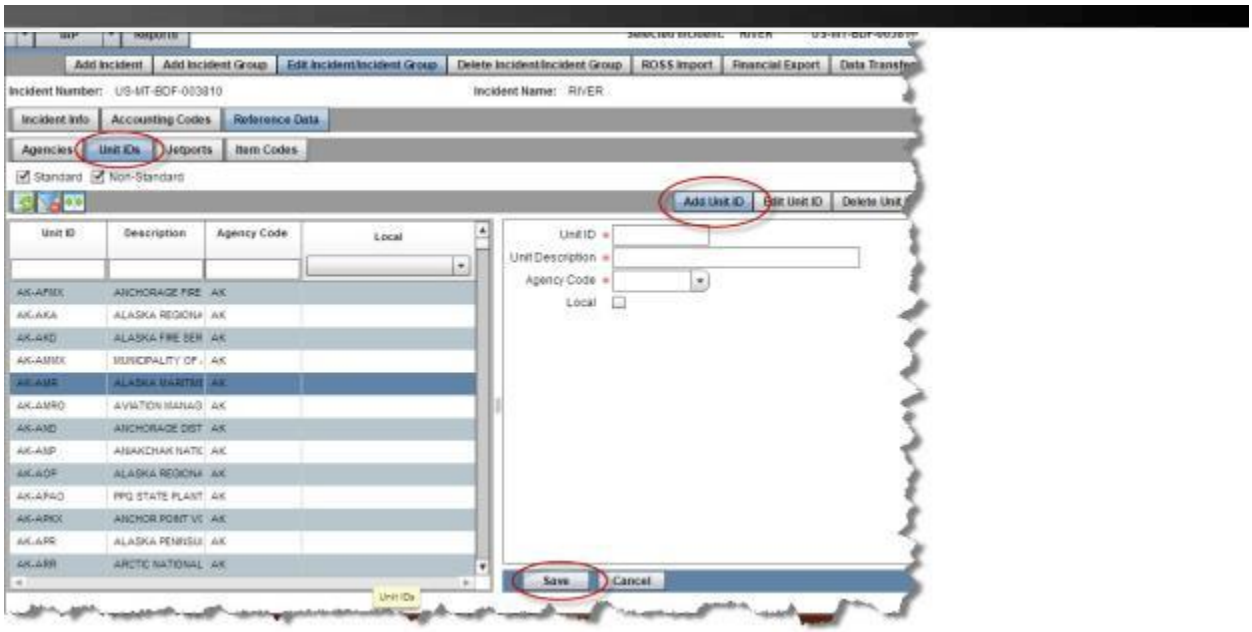
3. The screen will default to **Add Unit ID**.

4. Enter the **Unit ID**.

5. Enter a **Description**.

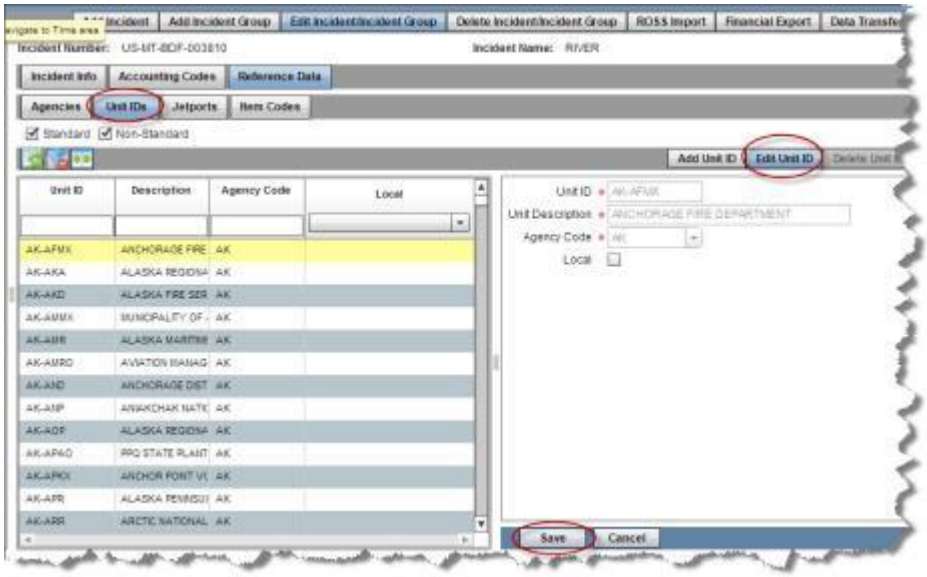
6. Select the **Agency Code** from the drop down list.

7. If this is a local Unit ID, click the **Local** checkbox to display a check mark.



Edit a Non-Standard Unit ID

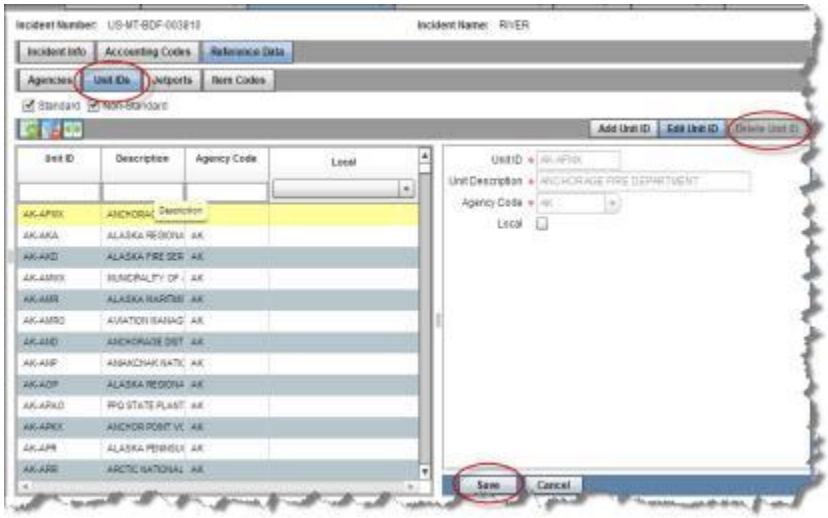
1. Highlight a Unit ID in the grid to edit.
2. Click the **Edit Unit ID** button.
3. Edit the desired information.
4. Click the **Save** button.



Delete a Non-Standard Unit ID

1. Highlight a Unit ID in the grid to delete.
2. Click the **Delete Unit ID** button. Only one Unit ID can be deleted at a time.
3. When the Confirmation message displays, click **Yes** or **No** to delete the Non-Standard Unit ID.
4. Click the **Save** button.

If the Non-Standard Unit ID is being used at an incident, the Unit ID cannot be deleted. The user will receive a notification that the Unit ID is in use.



Jetports

Add a Non-Standard Jetport

1. Select an Incident (or continue adding information to an incident that is already selected).
2. Click the **Jetport** button.

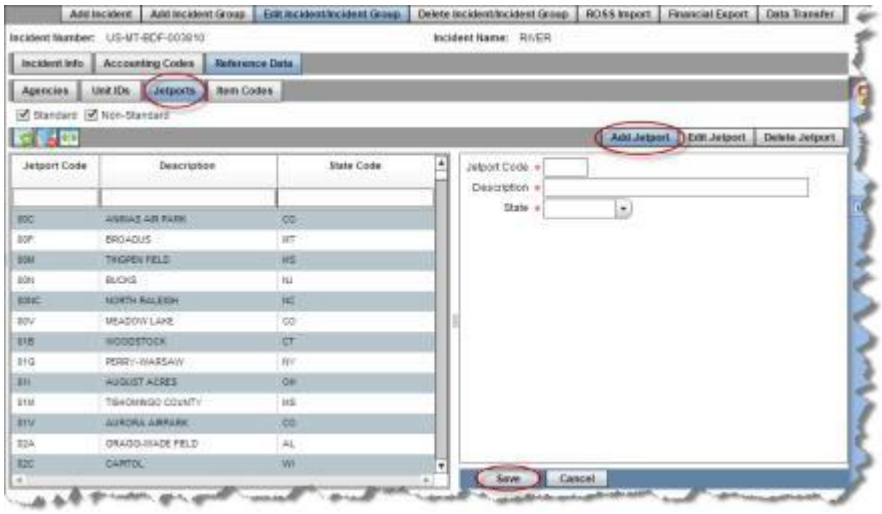
3. The screen will default to **Add Jetport**.

4. Enter the **Jetport Code**.

5. Enter a **Description**.

6. Select the **State** in which the jetport is located from the drop-down list.

7. Click the **Save** button.



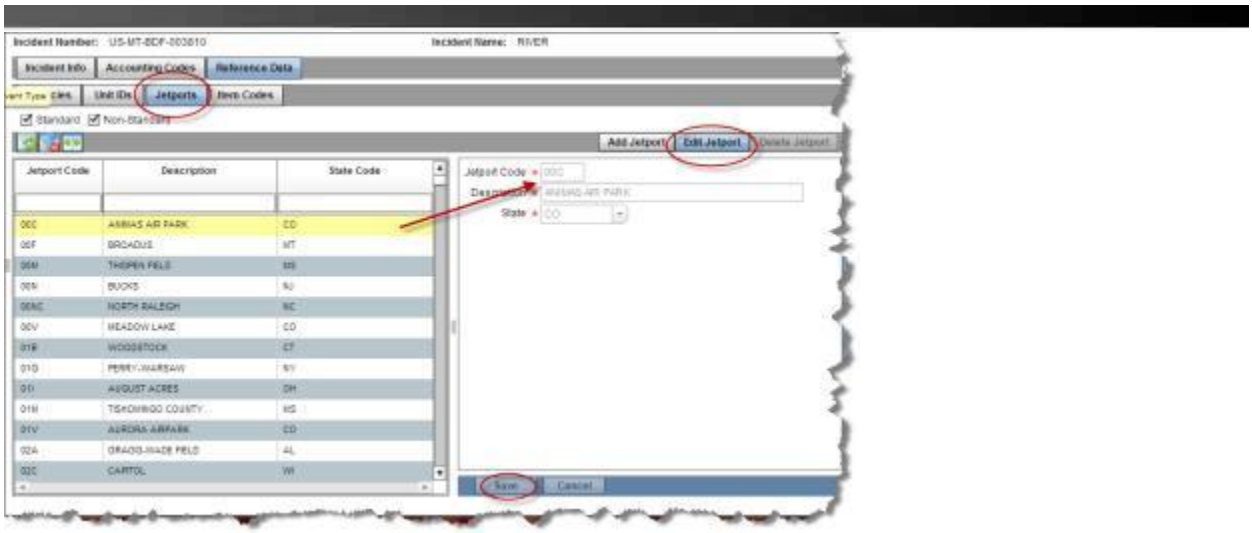
Edit a Non-Standard Jetport

1. Highlight a Jetport in the grid to edit.

2. Click the **Edit Jetport** button.

3. Edit the desired information.

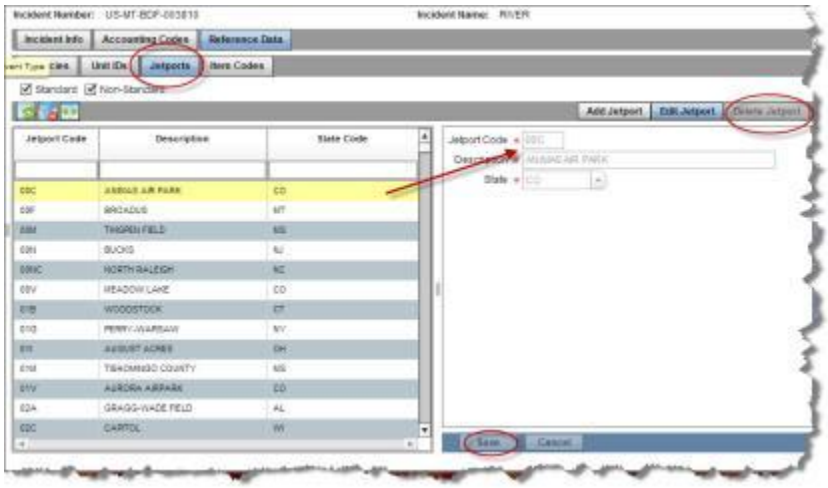
4. Click the **Save** button.



Delete a Non-Standard Jetport

1. Highlight a Jetport in the grid to delete.
2. Click the **Delete Jetport** button. Only one Jetport can be deleted at a time.
3. When the confirmation message displays, click **Yes** to delete the Non-Standard Jetport.
4. Click the **Save** button.

If the Non-Standard Jetport is being used at an incident, the Jetport cannot be deleted. The user will receive a notification that the Jetport is in use.



Item Code

Add a Non-Standard Item Code

NOTE: Non-Standard Item Codes cannot be duplicated within a single incident. An Incident within an Incident Group can have duplicate Non-Standard Item Codes. This occurs when single incidents already have a Non-Standard Item Code that is the same as another incident, then those incidents are combined in an Incident Group. The duplicates will remain in the Incident Group because they originated from different incidents.

Example of Non-Standard Item Codes:

- Incident #1 has Item Code ABCD - animal counter
- Incident #2 has Item Code ABCD - bird counter
- These 2 incidents are combined in an Incident Group. Each Item Code remains within its incident.
- No additional Item Code ABCD can be added to either of these incidents.
- Incident #3 is added to this Incident Group. Incident #3 can add Item Code ABCD - fish counter because it relates only to Incident #3.

NOTE: Item Code data impacts several ICS 209 and Finance calculations.

1. Select an Incident (or continue adding information to an incident that is already selected).

2. Click the **Item Code** button.

3. The screen will default to **Add Item Code**.

4. Enter the **Item Code**.

5. Enter a **Description** of the Item Code.

6. Select the appropriate **Section Code** from the drop-down list.

7. Select the appropriate **209 Code** from the drop-down list. If this field is left blank, it will be marked as NR (Non-Reportable) and will not be included in the 209 Report.

8. Select the appropriate **Request Category Code** from the drop-down list.

9. If this Item Code is involved in Direct suppression activities, check the **Direct** checkbox, otherwise leave the checkbox blank.

10. Select the appropriate **Daily Form Code** from the drop-down list. This code allows the proper Daily Cost screen view to display - Aircraft or All Others.

11. Enter the number of **Units**.

12. Enter the number of **People** associated with this Item Code.

13. Select a **Cost Sub-Group Category** from the drop down list.

14. Select the **Cost Group Category** from the drop down list.

15. Check the **Line Overhead** box if appropriate.

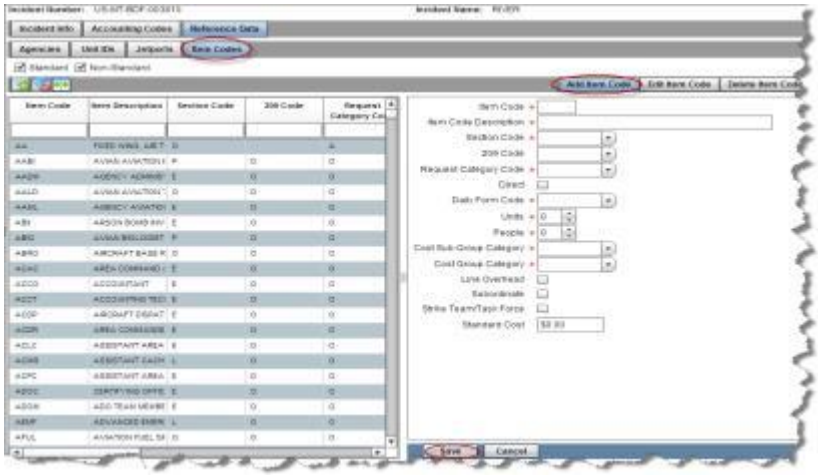
16. Check the **Subordinate** box if this Item Code is a subordinate to another Item Code.

17. Check the **Strike Team/Task Force** box if this Item Code is a Strike Team or Task Force.

18. Enter a **Standard Cost**.

19. Click the **Save** button.

NOTE: After adding an Item Code, add a cost rate to the Item Code on the Cost Rates screen. If the user does not add a rate to the Item Code, the rate will default to 0.00.



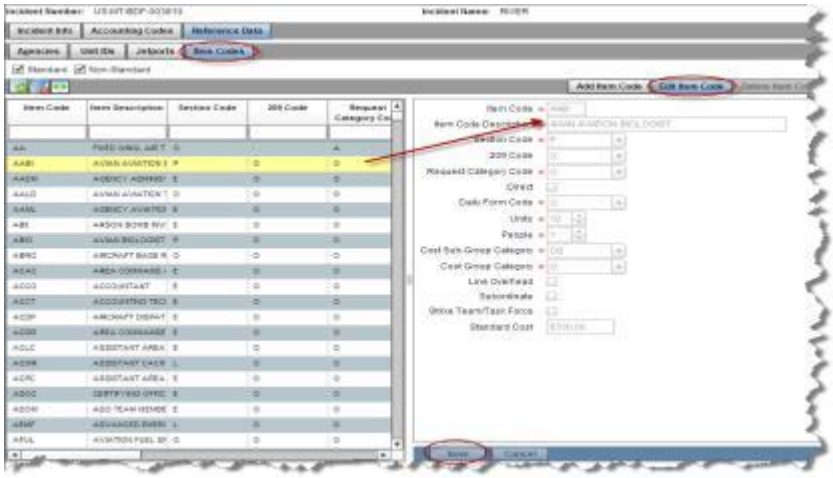
Edit a Non-Standard Item Code

1. Highlight an Item Code in the grid to edit.

2. Click the **Edit Item Code** button.

3. Edit the information as needed.

4. Click the **Save** button.



Delete a Non-Standard Item Code

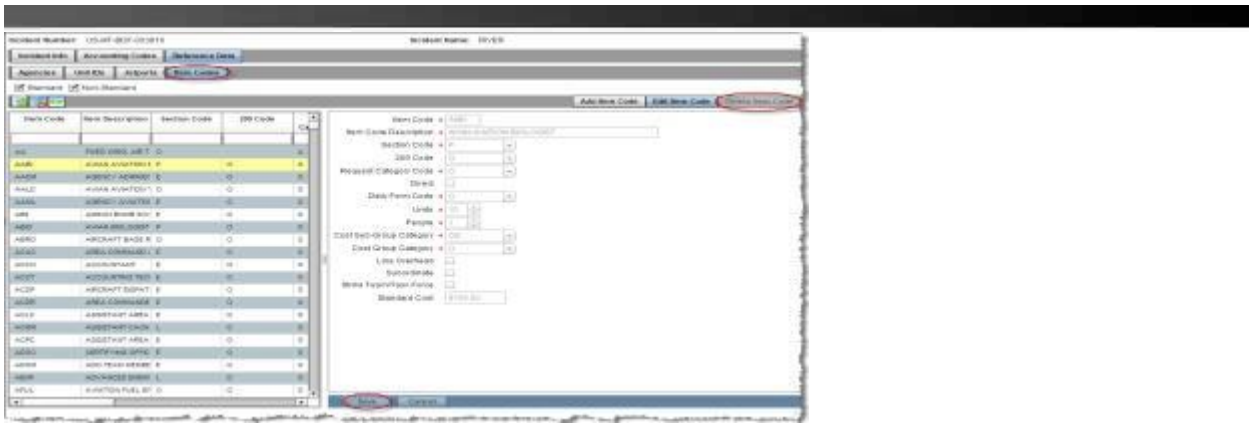
1. Highlight an Item Code in the grid to delete. Only one code may be deleted at a time.

2. Click the **Delete Item Code** button.

3. When the confirmation message displays, click **Yes** to delete the Non-Standard Item Code.

4. Click the **Save** button.

If a Non-Standard Item Code is being used at an incident, the Item Code cannot be deleted. The user will receive a notification that the Item Code is in use.



Incident Groups Overview

An Incident Group allows multiple Incidents to be grouped together in Enterprise in order to manage those Incidents as if they were a single Incident. Creating an Incident Group allows a user to share data between the different incidents for resources (e.g., posting time to an accounting code for an incident to which the resource is not assigned). These multiple incidents can be managed quickly and easily from a single point of reference.

When an Incident Group is selected, the user can either choose to manage the incidents separately or manage them as a group. To manage the incidents as a group, check the Manage as Group checkbox (upper right hand corner). This will provide a "flattened" view of all resources assigned to all incidents within the Group. To manage the incidents separately, uncheck the Manage as Group checkbox and select an incident from the drop-down list that displays next to the Manage as Group checkbox. This will cause the system to display only the resources assigned to the selected incident.

When Manage as Group checkbox is selected, the following will occur within the system:

- A Select Incident field is added to the Common Data area when adding or editing a resource. This field allows the user to select the incident to which the resource is assigned.
- The accounting codes for all incidents in the Incident Group will display in the Accounting Codes drop-down list in both the Common Data area and the Time Posting area.
- All resources for all of the incidents in the Incident Group will display in all resource lists.

NOTE: Only those users with User Accounts in the Users Assigned to Group list can select the Incident Group in Enterprise.

The following buttons become active:

- Adding Incident Groups
- Editing Incident Groups
- Deleting Incident Groups

Add Incident Groups

Follow the steps in this section to add an Incident Group to Enterprise:

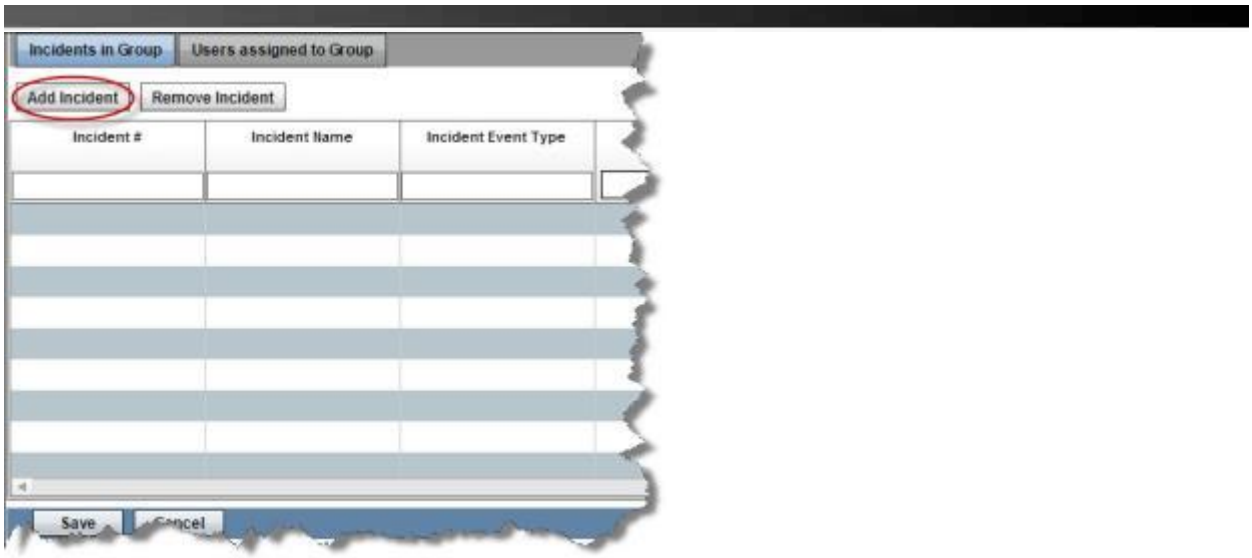
1. On the Home page, click the **Incidents** button.

2. Select the **Add Incident Group** button.

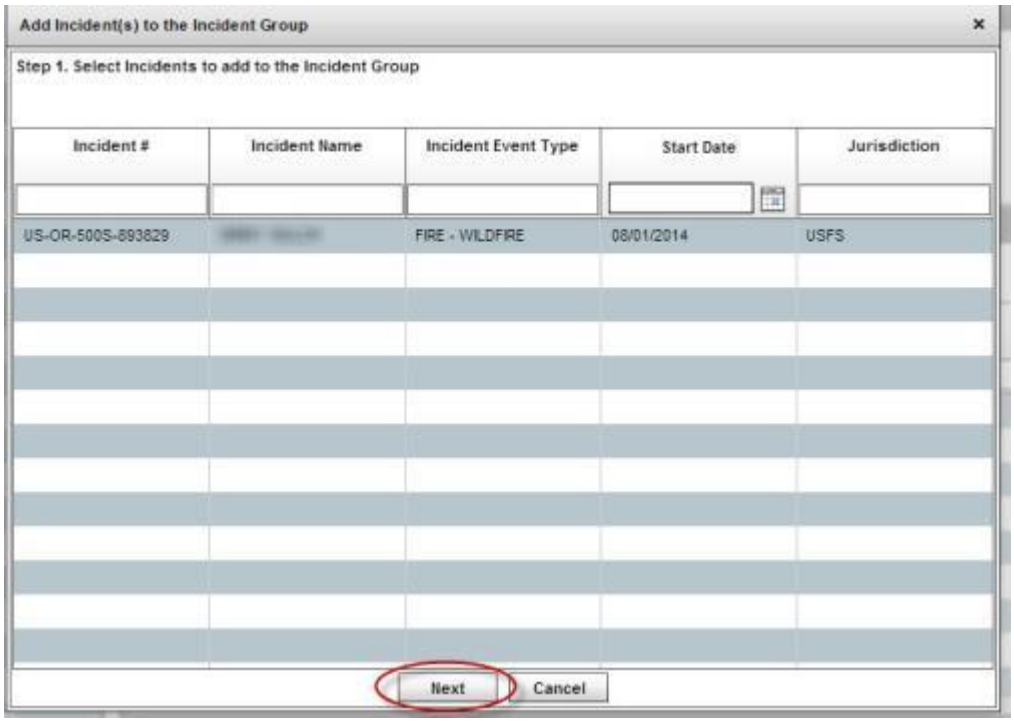
3. The Incident Group Info screen will display.

4. Enter a **Group Name** for the Incident Group.

5. Click the **Incidents in Group** tab, click the **Add Incident** button.

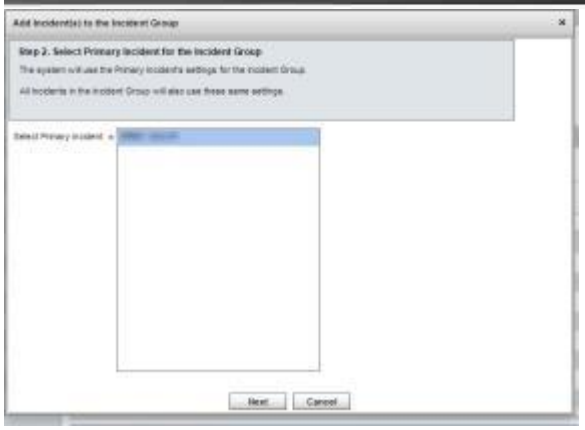


6. Select the Incidents to include in the Incident Group.



7. Click the **Next** button.

8. Select the **Primary Incident** for the Incident Group. The Primary Incident settings will be used on all other incidents in the group.



9. Click the **Next** button.

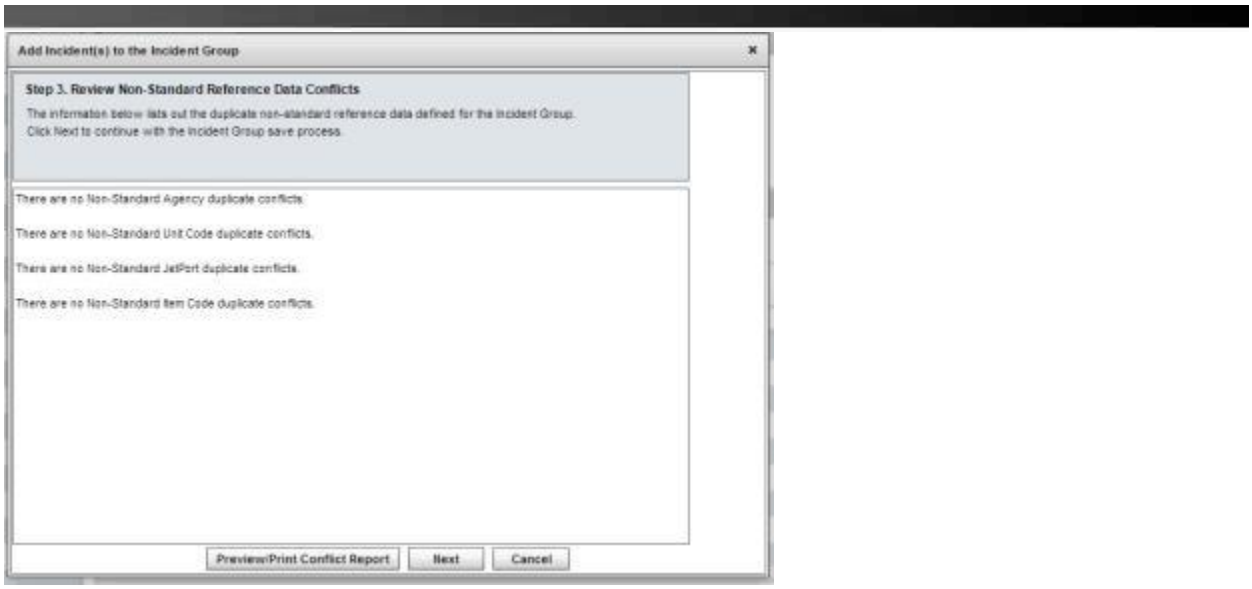
10. Review the **Non-Standard Reference Data Conflicts**.

NOTE: When adding two or more incidents to a group, it is possible there will be conflicting information in the Non-Standard Reference Data. These conflicts will be identified on the Non-Standard Reference Data report. If there are duplicate Non-Standard Codes, the system will display both codes in all lists that include the Non-Standard Codes. For example if the Valley incident has a Comp1 code that is defined as Laptop and the Rocky Mountain Incident has a Comp1 code that is defined as Compresses, the system would display both codes, with the description next to the codes. The user can either cancel the process of adding incidents to the incident group and fix the issues or continue with the process and fix the issues after the incidents are added to the incident group.

11. To preview and then print the conflict report, select the **Preview/Print Conflict Report** button.

12. Click the **Next** button to add the incidents to the Incident Group.

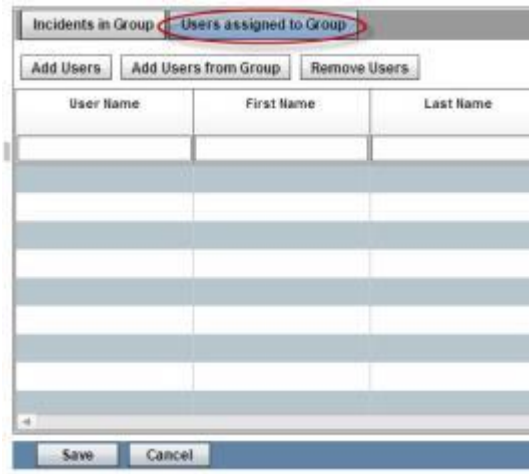
13. Click the **Save** button to save the Incident Group.



Assigning Users to the Incident Group

1. To assign users to an Incident Group, select the Incident Group from the Incident grid.

2. Select the **Users assigned to Group** tab.



3. Click the **Add Users** button to add individual users to the Incident Group from the Add User(s) to Incident Group screen.

4. Select one or more User Accounts to add to the Incident group list.

5. Click the **Add** button.

6. Once all users have been added, click **x** to close the pop-up window.

NOTE: If User Groups are defined in the system, they can be added to the user list by clicking the **Add Users from Group** button, selecting the User Group and then clicking the **Add User Group Users** button in the pop up window that displays.

7. Click **Save** to save the changes.

Add Users from Group to an Incident Group

1. To assign users from a user group to an incident group, select the Incident Group from the Incident grid.

2. Click **Edit Incident/Incident Group**.

3. Select the **Users assigned to Group** tab.

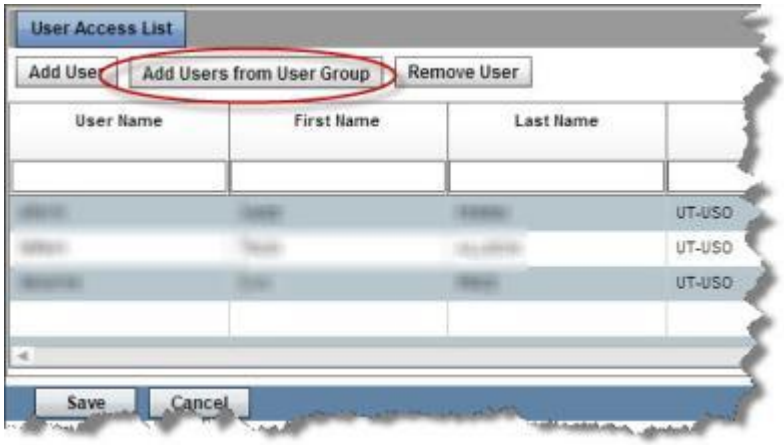
4. Select **Add Users from User Group** tab.

5. Select a group(s) from the **Add User(s) from User Group** to Incident Group screen.

6. Click the **Add user Group Users** button when group(s) has been selected.

7. Click the **Save** button.

NOTE: Individual users from the group(s) will be listed in the user grid. The User Group name will not appear. Action can now be taken on individual users by the Data Steward.



Remove Users from an Incident Group

1. Highlight the users(s) to remove from the grid list.

2. Click **Remove Users**.

3. Users are removed from the list.

Notes on Incident Groups:

- The same incident cannot be added to multiple incident groups.
- Only user accounts in the incident group User Access list can access the incident group and incidents within the group.
- When an incident is added to the incident group, the user access list for the individual incident is no longer valid and will be overwritten by the access list for the incident group. Users from the Incident will automatically be added to the access list for the incident group.
- When an incident is removed from an incident group, that incident remains in the system as an individual incident. It is no longer part of the incident

group.

- An incident can only be removed from the incident group if that incident has no cross-over data with the other incidents in the incident group (e.g., time postings to an accounting code for another incident in the group).

- When an incident is removed from an incident group, the user access list for the removed incident is the same as for the incident group. Once removed, the access list can be edited for that incident.

- Settings for all incident financial documents (e.g., reports, non-standard reference data, etc.) are appended to the group.

- Only Non-Privileged Users can be added to Incident Groups.

- When a new Incident Group is created, one of the incidents in the new group must be identified as the Primary Incident:

    - A Primary Incident must be selected when a group of incidents is saved as an incident group.

    - Settings menus for several functions (Check-In, Demob, etc.) can only be set for single incidents, therefore in an incident group - one incident must be selected as the Primary Incident. The Primary Incident settings will be used on all other incidents in the group.

    - To remove a Primary Incident from the group, all other incidents in the incident group must first be removed. The group will, in essence, be de-grouped.

    - The integrity of any data used in the IAP program forms for any incident in an incident group will be maintained if any of the group incidents are removed.

- If there are Non-Standard Reference Data conflicts with an incident that is added to an incident group, a screen will display that lists all the Non-Standard Reference Data Conflicts. Print a conflict report or save the report prior to resolving all conflicts.

- Once an incident group is created, the name of the Incident Group will display in the top right-hand corner of the screen. When the group is being managed as one, the **Manage as Group** checkbox will be checked. When Manage as Group is checked, all resources for all incidents in the group will display in the resources grid.

- When a user checks the **Manage as Group** checkbox, the system adds a field to the Common Data area that allows the user to assign a specific Incident to the Resource.

Editing Incident Groups

Follow the steps in this section to edit an Incident Group in Enterprise:

1. On the Home page, click the **Incidents** button.

2. Select the Incident Group to edit.
3. Select the **Edit Incident/Incident Group** button.

NOTE: To see the incidents in an Incident Group, click on the arrow next to the Incident Group name in the Incident grid. This will open a tree view of the incidents.

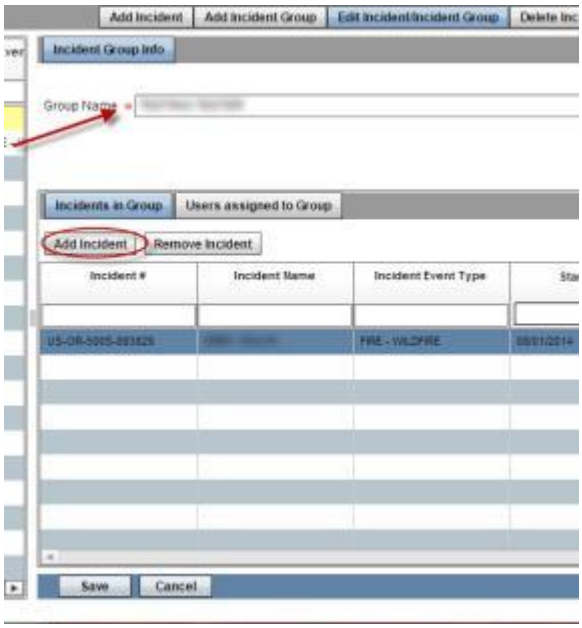
NOTE: If the user selects an incident in the incident group and clicks the Edit Incident/Incident Group button, the system will open the Edit Incident screen, rather than the Edit incident Group screen. The user must have the actual group selected to edit the group.

4. Edit the Incident Group Name if desired.
5. When needed, add Incidents to the Incident Group by clicking on the **Incidents in Group** tab.
6. Click the **Add Incident** tab.
7. Select the incident(s) to add.
8. Click the **Add** button.
9. Click the "**x**" to close the window.
10. Click **Save**.

11. To remove incidents from the Incident Group, click on the **Incidents in Group** tab.

12. Select **Remove Incident**.

13. Click **Save**.



Users Assigned to Group tab
See *Add Incident Group, Users assigned to Group* for more information.

NOTE: Incidents can only be removed from the incident group if that incident has no cross-over data (e.g., time postings to an accounting code for another incident in the group). If there is cross-over data, the system will not allow the user to remove the incident from the group.

NOTE: If the user removes an incident from the incident group, that incident will remain in the system, but is no longer part of the incident group.

14. Click **Save** to save the changes to the Incident Group.

Deleting Incident Groups

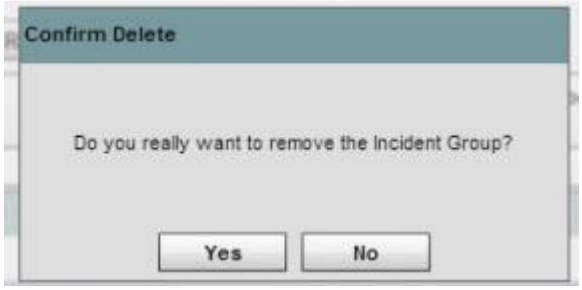
Follow the steps in this section to delete an Incident Group in Enterprise:

NOTE: A user must first remove all incidents from the incident group prior to deleting the incident group. Incidents can only be removed from the incident group if that incident has no cross-over data (e.g., time postings to an accounting code for another incident in the group). If there is cross-over data, the system will not allow the user to remove the incident from the group.

NOTE: When an Incident Group is deleted, only the group is deleted, the incidents that had been included in the group will remain unchanged in the system.

1. On the Home page, click the **Incidents** button.

2. Select the Incident Group to delete.
3. Select the **Incidents in Group** tab.
4. Remove all incidents from the incident group by highlighting them and selecting **Remove**. Only one incident can be removed at a time.
5. After all of the incidents are removed from the incident group, click the **Delete Incident/Incident Group** button.
6. A confirmation message will display.
7. Click **Yes** to delete the Incident Group.


Confirm Delete
Do you really want to remove the Incident Group?
Yes
No

View/Hide Incidents

Follow the steps in this section to View/Hide Incidents in Enterprise:

1. From the Home page click the **Incidents** button.

2. The Incidents grid will display.

3. Under the Incidents button on the toolbar click the **Customize Data View** icon.

4. The Customize User Data window displays.

NOTE: Incidents that will display on the Incidents screen are listed in the Included List grid.

5. To hide an Incident:

   a. Select an incident in the Incidents List.

   b. Click the **>** button to move the incident to the Excluded list.

   c. Click the **Save** button.

6. To display a hidden incident:

   a. Select an incident in the Excluded List.

b. Click the **<** button to move the incident to the Incidents List.

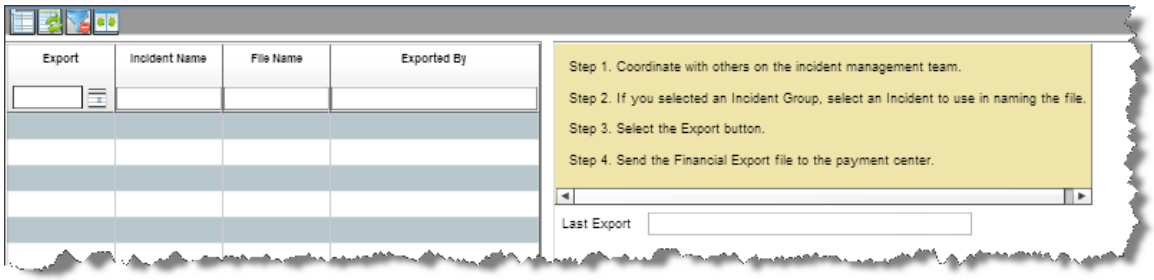
c. Click the **Save** button.

Financial Export

This topic contains information about exporting Financial Data from the e-ISuite system. Follow the steps in this section to create a Financial Export file that includes payment and cost accrual information.

Create a Financial Export File

1. From the Home page click the **Incidents** button.
2. Select an Incident or Incident Group.
3. Select the **Financial Export** button on the Incidents page.
4. If an Incident Group is selected, select an **Incident** from the drop-down list.
5. Click the **Export** button.
6. When the **Warning** message displays, read the message and click the **Yes** button to continue.
7. The financial export file will be generated and a **Save As** window will open.
8. Browse to the location where the Financial Export file should be saved.



TIPS

- Only one financial export file can be created per calendar day.
- When creating a financial export, all data for all incidents in an Incident Group/Site Database will be included regardless of what incident is selected during the Financial Export file creation process.

- To access the data repository, the user must have a DMS username and password.

Uploading a Financial Export File

1. Open an Internet browser.
2. In the **Address** bar, enter **http://famit.nwcg.gov/applications/eISuite**.
3. On the e-ISuite website, click the **Data Repository** button.
4. On the **Enter Network Password** dialog box, type the **DMS User Name** and **DMS Password**, and then click **OK**.
5. On the **Data Repository page**, select the file to upload by clicking to **Browse** button next to the File box.
6. To upload the file, click the **Upload** button.

Index

A

Add Incident
- manually add an incident, 4

E

Edit
- incident, 14

F

Financial Export
- creating, 57
- uploading, 58

I

Incident
- deleting an incident, 17
- edit an incident, 14
- manually add an incident, 4

Incident Groups, 44
- adding, 45
- assigning users to incident groups, 48
- deleting, 54
- editing, 52

Incidents
- view/hide, 55

IRWIN
- import from, 4
- sync, 15
- unlink, 15

U

User Groups
- adding, 26
- deleting, 31
- editing, 29
- overview, 25