

WFDSS 3.8 Release Notes

(3.8 deployed December 16, 2009)

Version 3.8 of WFDSS was intended to address two primary areas – security requirements and the separation of analysis ignitions from incident perimeters. In addition, a ‘Feature Information’ link was added to the Information sub-panel on the maps, several minor UI enhancements were completed, and a number of defects were resolved.

I. Security Requirements

a. Password Policies

Two password policies are required – one for ‘privileged’ users and a second for the remainder of users. Within WFDSS, privileged users are defined based upon their roles within the application. Any user with a National Editor, Administrator, or Help Desk role is considered a privileged user. That is, the privileged password policy will be applied to any user with a National Editor, Administrator, or Help Desk role. The second password policy will be applied to the remaining roles within WFDSS (note that a user must have at least one role in order to be authorized within the system).

i. Password Policy Implementation Dates

WFDSS phased in the password policies to allow for testing within the training environment.

1. Training Site

- Privileged Policy (1 day expiration / Administrators only) – Dec 15, 2009
- Privileged Policy applied to ‘privileged’ users – Jan 5, 2010
- Default Policy – January 6, 2010

2. Production Site

- Privileged Policy – January 8, 2010
- Default Policy – January 8, 2010

ii. Password Policy Definitions

The default and ‘privileged’ password policies are identical with the exception of the password expiration timeframe. In the default password policy, passwords expire after 60 days. In the ‘privileged’ password policy, passwords expire after 30 days. The remainder of the password policy definition is as follows:

1. The minimum password length is 12 characters.
2. A password must contain a minimum of 2 alpha characters.
3. A password must contain a minimum of 2 non-alpha characters.
4. 24 passwords are maintained in the password history. A password cannot be re-used if it exists within a user’s password history.
5. System and Help Desk generated passwords must be changed upon login. Users will be directed to the ‘Change Password’ page when they log in with such a password and they will not be able to navigate from the ‘Change Password’ page until they successfully change their password.
6. An account will be locked out of WFDSS after five consecutive unsuccessful login attempts. Once a user is locked out of WFDSS, they can no longer make a request for the system to generate a password for their account. Instead, they

will need to contact the Help Desk. The following message will be displayed at the top of the login page when a 'locked out' user attempts to log into WFDSS:

FAILURE: Your account has been locked, please contact the Help Desk

iii. Unlocking a User Account

In order to unlock a user account, the user's password must be reset by the Help Desk or an Administrator. When a locked user's account is accessed from the Administrative perspective, the following message is displayed on the top of the page(s):

WARNING: User hans15 is locked. Resetting their password will unlock the account.

iv. Password Expiration Notification

1. The password expiration time is always displayed on the 'My Home Page' within WFDSS.
2. A password expiration message is displayed on the first page after a successful logon provided that the password will expire in less than 10 days.
3. A utility will be run as a scheduled task to notify users via email if their password will expire in 10 days, 3 days, or 1 day.

v. Changing a Password

WFDSS uses four different mechanisms for setting or resetting a user's password. They are as follows:

1. A random password is generated by the system for a new user account. The password is sent to the email address associated with the account.
2. A random password is generated by the system if a user requests a password reset. In order for a user to have WFDSS reset their password, they must correctly enter their WFDSS email address and their primary WFDSS phone number. In addition, they must correctly answer their security question. The generated password is sent to the email address associated with the account. This mechanism can be used regardless of whether or not the password has expired, but it cannot be used once the user is locked out of WFDSS.
3. A user can request that the Help Desk manually reset their password for them. In order to identify the individual prior to manually resetting the user's password, the Help Desk has access to the user's profile as well as the user's security question and answer. The manually reset password is sent to the primary email address associated with the user's account. Given the time sensitive nature of accessing WFDSS when a fire is burning (as well as the unreliable nature of email), this method was implemented so that the new password can be verbally communicated to the requestor.
4. A user can choose to reset their password after successfully logging into WFDSS. To do this, the user would navigate to the 'Change Password' page within the 'My Home' perspective.

Note that in the first three cases, the password is emailed to the user's primary email address. The WFDSS password policies only allow a password generated by the help desk or by the system to be used once. Upon logging on, the user is directed to the 'Change Password' page. They must successfully change their password prior to accessing any other page within WFDSS.

If a user or the Help Desk attempts to reset a password unsuccessfully, the failure message will display an explanation of why the password was unacceptable along with a short description of the password policy.

FAILURE:

Password in History

The new password does not meet the following standards:

1) Minimum Password Length = 12

2) Minimum Number of Alpha Characters = 2

3) Minimum Number of Non-Alpha Characters = 2

4) Passwords Stored in History = 24

5) Maximum Password Age is 30 days

- vi. Expired Passwords
Users may use an expired password to log into WFDSS provided that they are not locked out of the system. However, if the password has expired, the user will be re-directed to the 'Change Password' and will not be allowed to navigate within the application until they successfully change their password.
- b. Inactive Accounts
 - i. User accounts will be locked after 90 days of inactivity.
 - ii. Users will be notified via email 10 days, 3 days, and 1 day before their account is locked.
 - iii. Once an account is locked, the user will need to contact the Help Desk to unlock their account.

II. Separation of Incident Fire Perimeters and Analysis Ignition Shapes

Analysis ignition shapes have been separated from incident fire perimeters for a number of reasons, but primarily because they are fundamentally different entities. That is, although fire perimeters might be used as an analysis ignition, there are many instances when an analysis ignition shape is not a fire perimeter. Separating these shapes into two different layers enables WFDSS to eventually display the 'most recent' fire perimeter for an incident, to display fire perimeter progressions, to enable a 'most recent' fire perimeter layer for the current fire season, and to develop an interface for downloading a set of 'most recent' fire perimeters based upon various selection criteria. These enhancements have been discussed but have yet to be scheduled. The separation also allowed WFDSS to store the buffered point associated with an automated short term analysis. Consequently, it is now possible to view the analysis ignition point that was used in an automated short term analysis from the Analysis Results map.

At the time of the 3.8 deployment, existing perimeter shapes were copied into the new analysis ignition shape layer. This was necessary since many fire perimeters were used as analysis ignition shape files and it was not feasible to identify those shapes that were real perimeters, those that were only used for analyses, and those that were used for both purposes. Consequently, the separation of the shapes prior to the 3.8 release is at the application level only.

Application changes related to the separation of fire perimeters and analysis ignitions are detailed below:

a. Uploading Shapes

An 'Analysis Ignition' shape type was added to the Shape Type drop down list on the Shape Upload page. In addition, the 'Fire Barrier' shape type was renamed 'Barrier'.

Upload Shape File

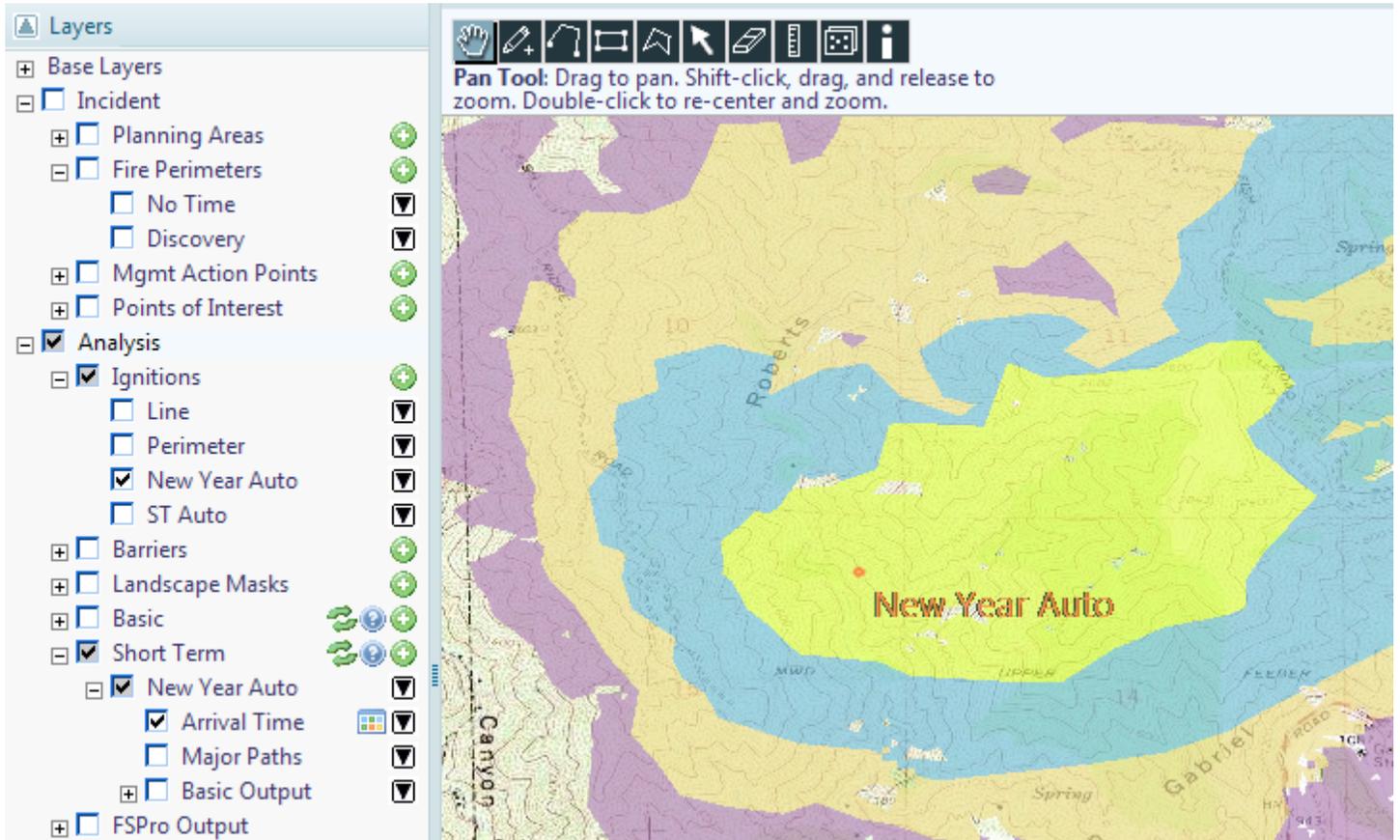
Select a zipped shape file and click the 'Upload' button to upload your shape. To successfully upload a shape file, it can only contain polygons. If you wish to include a point or a line, you should first buffer it to create a polygon.

*Shape Label

Shape Date
01/07/2010

Shape Type
Fire Perimeter
Fire Perimeter
Analysis Ignition
Barrier
Landscape Mask
Mgmt Action Points
Final Fire

b. Situation Assessment Map

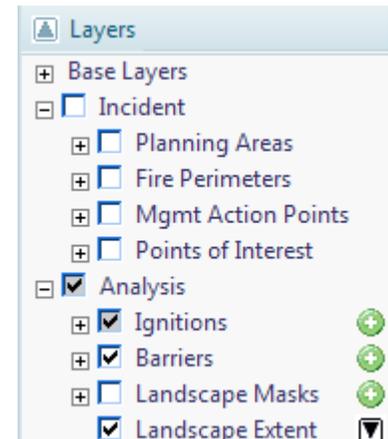


i. Ignitions were added to the Analysis sub-tree of the Layer Switcher.

- ii. 'Fire Barriers' was changed to 'Barriers' and moved from the Incident sub-tree into the Analysis sub-tree.
- iii. Landscape Masks were moved from the Incident sub-tree into the Analysis sub-tree.
- iv. Users with incident editing privileges are allowed to create analysis ignitions from the Situation Assessment map even though analysis ignitions are only used when an analysis is run. The rationale for this is that personnel at the fire generally have a better idea of where the fire is currently burning than a fire behavior specialist who is not at the incident.
- v. The ignition shapes used for automated short term analyses can be displayed. In this instance, the name of the ignition shape is the same as that used for the short term analysis.

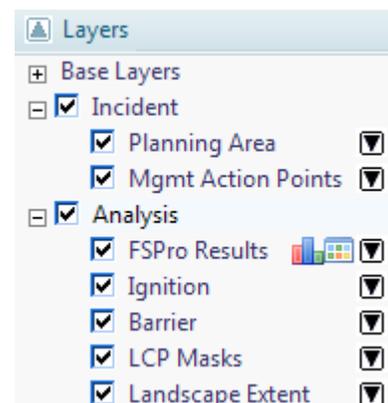
c. Analysis Map

- i. An Analysis sub-tree was added to the Layer switcher to accommodate analysis specific shapes.
- ii. Ignitions were added to the Analysis sub-tree of the Layer Switcher.
- iii. 'Fire Barriers' was changed to 'Barriers' and moved from the Incident sub-tree into the Analysis sub-tree.
- iv. Landscape Masks were moved from the Incident sub-tree into the Analysis sub-tree.
- v. 'Extent' was changed to 'Landscape Extent' and moved from the top level of the tree into the Analysis sub-tree.
- vi. Planning Areas, Fire Perimeters, Management Action Points, and Points of Interest are still displayed in the Incident sub-tree, but they cannot be created from the Analysis Map.
- vii. Ignitions, Barriers, and Landscape Masks can only be created by users with analysis editing privileges.
- viii. To create an analysis ignition from a fire perimeter, you can use the following steps:
 1. Expand the Fire Perimeters sub-tree and click on the checkbox in front of the desired perimeter. This will cause the perimeter to be displayed on the map.
 2. Click on the expand button (☐) to the right of the perimeter name.
 3. Use the shape selection tool (☒) to select the perimeter on the map (the perimeter will be highlighted in yellow when it is selected). Note that if other selected or drawn shapes are also highlighted in yellow, they will be combined with the perimeter you just selected. If you do not want this to occur, 'de-select' the unwanted shapes so that they are not highlighted in yellow.
 4. Click on the 'Create New Shape' icon (⊕) to the right of Ignitions.
 5. Enter the desired name for the analysis ignition and click the Save button.



d. Analysis Results and Landscape Maps

- i. The Results sub-tree was renamed to Analysis.
- ii. Ignitions were added to the Analysis sub-tree of the Layer Switcher.
- iii. 'Fire Barriers' was changed to 'Barriers' and moved from the Incident sub-tree into the Analysis sub-tree.
- iv. Landscape Masks were moved from the Incident sub-tree into the Analysis sub-tree.



- v. 'Extent' was changed to 'Landscape Extent' and moved from the top level of the tree into the Analysis sub-tree.
- vi. Planning Areas and Management Action Points are displayed in the Incident sub-tree. Perimeters and Points of Interest will be added to this sub-tree in a future release.

III. Miscellaneous Enhancements

a. Feature Information

- i. A Feature Information link was added to the Information sub-panel on the map pages. As with the other links within this sub-panel, the Feature Information link works in conjunction with the Identify map tool. That is, the link will display feature information for available map layers displayed at the specified latitude / longitude. The radius input field is not used in the context of Feature Information. The map layers currently enabled for Feature Information are the following:
 1. AK Fires 2000-2008
 2. CA Fires 1995-2008
 3. Class 1 Airshed
 4. Counties
 5. Critical Habitat
 6. Designated Areas
 7. Historical Fires 2001-2008
 8. NAA Ozone
 9. NAA Particulates
 10. NPS Structures
 11. Power Plants
 12. Surface Mgmt Agency
 13. Transmission Lines
 14. USFS Structures



- ii. Feature Information is displayed in a popup browser window. The popup browser window contains the latitude and longitude used for querying the data, a dropdown list for querying additional layers, the layers that have been queried, and the feature information available for the queried layers. (See the figure at the top of the next page for an example.) Note that if you are not displaying any layers for which feature information is available or if your latitude and longitude do not intersect and of these layers, then your feature information table will be empty (and consequently not displayed).

If a point or line layer is queried, a buffered point is used to intersect the point / line layer. The size of the buffered point is zoom-level dependent. That is, the buffer is larger when you zoom out.

You may query additional layers by selecting a layer from the layer dropdown list and clicking on the 'Query Layer' button. Once a layer has been queried, it is removed from the dropdown list and included in the list of 'Layers Queried'.

It is possible for more than one result to be displayed for a given layer. When this occurs, alternate results are shaded to allow users to distinguish between multiple results.

Selected Feature Information

Latitude Longitude
30.21695 82.60071

Query Additional Layer

Layers Queried: Historical Fires 2001-2008, USFS Structures, Surface Mgmt Agency

| Layer | Value |
|--|----------------------------------|
| <input type="checkbox"/> USFS Structures | |
| <input type="checkbox"/> Name | OSCEOLA WC SEEDLING COOLER/SHELT |
| <input type="checkbox"/> SubType | STORAGE |
| <input type="checkbox"/> Name | OSCEOLA WC OIL & PAINT HOUSE |
| <input type="checkbox"/> SubType | STORAGE |
| <input type="checkbox"/> Surface Mgmt Agency | |
| <input type="checkbox"/> Agency | USFS |
| <input type="checkbox"/> Unit Id | FLFNF |
| <input type="checkbox"/> Name | National Forests In Florida |

In the Feature Information example displayed above, three layers have been queried – the Historical Fire layer, the US Forest Service structures layer, and the Surface Management Agency layer. There were no results returned from the Historical Fire layer, two results from the US Forest Service layer (a seedling cooler / shelter as well as an oil & paint house), and one result from the Surface Management Agency layer.

b. Stratified Cost Index

- i. An informational message was added to the top of the SCI List page to inform users that the SCI model is not valid for fire sizes less than 300 acres.

Stratified Cost Index List

WFDSS only contains Stratified Cost Index models for US Forest Service incidents within the continental United States. The Stratified Cost Index model is NOT valid for estimated fire sizes less than 300 acres.

- ii. On the SCI parameters page, an informational message was added to the field set containing the alternative fire sizes. This message also informs users that the SCI model is not valid for fire sizes less than 300 acres.

Estimated Final Fire Size (acres)

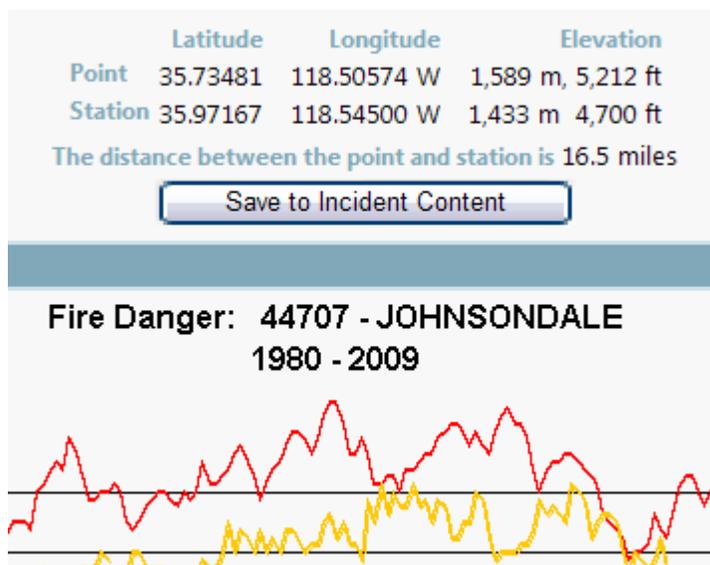
| | | | |
|----------------------------------|----------------------|----------------------|----------------------|
| *Alternative 1 | Alternative 2 | Alternative 3 | Alternative 4 |
| <input type="text" value="350"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

SCI is NOT valid for fire sizes less than 300 acres.

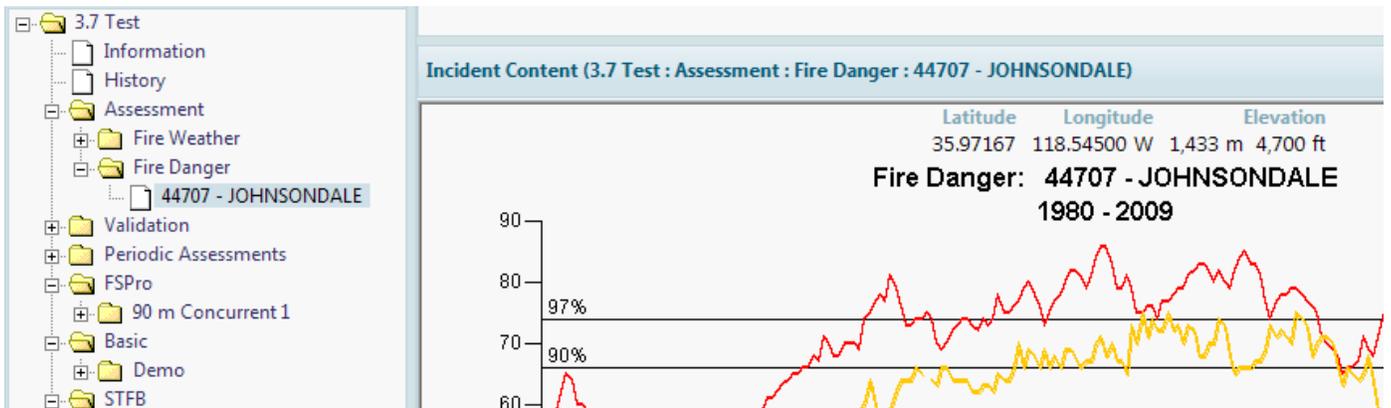
- iii. The first alternative is auto-populated. If the current incident size (as entered on the Incident Information page) is greater than or equal to 300 acres, the current incident

size is used for the first SCI fire size. Otherwise, the first SCI fire size is set to 300 acres.

- c. When an analysis is copied, the informational page for the copy of the analysis is displayed. This is the case for all analysis types.
- d. Incident Approvers automatically receive editing privileges when an incident owner grants the approver their approval privileges. The incident owner can choose to remove the incident editing privileges for the approver.
- e. Fire Danger Rating Graphs
 - i. Links to the Fire Danger Rating Graph were added to the following pages:
 - 1. New Basic Fire Behavior
 - 2. View Basic Fire Behavior Information
 - 3. New Short Term Fire Behavior
 - 4. View Short Term Fire Behavior Information
 - 5. FSPRO ERC Classes
 - ii. Adding Fire Danger Rating Graphs to the Incident Content Tree
 - 1. Fire Danger Rating Graphs can be added to the incident content tree provided that the user has incident editing privileges for the associated incident (note that an associated incident does not exist if the Fire Danger Rating Graph was accessed from the Intelligence Map).



2. Once a Fire Danger Rating Graph is added to the incident content tree, it can be selected for inclusion in an incident decision or a custom report. The RAWS station will appear in a Fire Danger sub-folder of the Assessment folder in the content tree.



If a graph is included in a Decision, the content of the graph will update (on a daily basis) until the Decision is Reviewable, at which time the content becomes static. If a graph is included in a Custom Report, the content of the graph will update (on a daily basis) until the report is published.