Focus Guide

Alerts and Compliance

This Focus Guide is designed for Spitfire Project Management System users. In this guide you will learn about the use and setup of Document Alerts and Alert Subscriptions, the use of Compliance tracking, and the setup of Compliance types and everything else needed for Compliances to work.

Version 4.5

www.spitfiremanagement.com

Revision Number: 4.5.10.02.2014

Spitfire Management, LLC.
7 Skyline Drive, Suite 350
Hawthorne, NY 10532
ph. 914.273.0809
fax: 914.273.4208
www.spitfiremanagement.com

Table of Contents

About Our Documentation

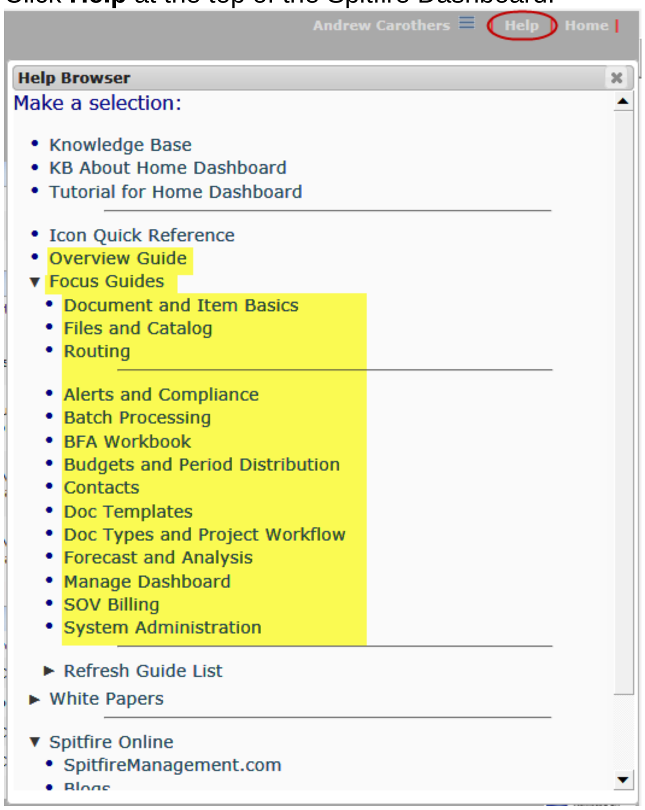
The Spitfire Project Management System (sfPMS) is extensive and powerful. Learning about all that you can do with it takes time. To help you learn, we provide various forms of documentation. Because one large all-inclusive manual would be too unwieldy and take too long to download, we provide smaller units of documentation—guides, knowledge base articles, and technical white papers.

Guides

Our guides, which include an *Overview Guide* and various other guides, focus on specific areas or tasks in sfPMS. Often, one Focus guide will refer you to a second Focus guide when an overlapping section is described in more detail in the second guide. By reading the guides, you will get a good understanding of the system in general and you will learn procedures for how to do many of the things that sfPMS allows you to do. We suggest you read the *Overview Guide* first, followed by other Focus guides as needed.

To access the guides:

1. Log in to sfPMS.
2. Click **Help** at the top of the Spitfire Dashboard:

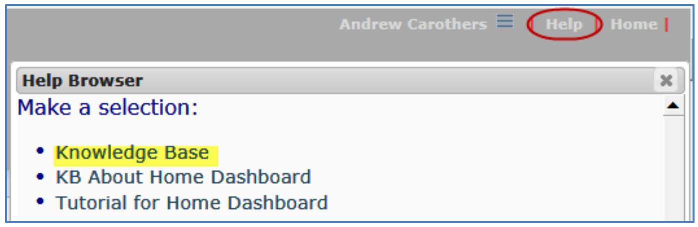


3. Select either **Overview Guide** or one of the choices under **Focus Guides**:

   The guide will appear as a PDF file.

The Knowledge Base

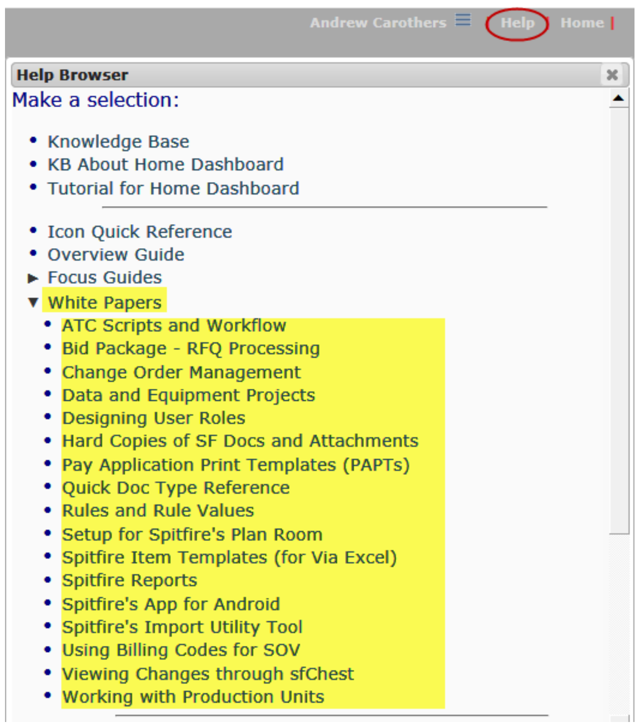
The Knowledgebase contains articles, in a question-and-answer format, that cover either more specific or more technical information about sfPMS. The Knowledgebase is accessed through the same Help menu as the guides:



Articles in the Knowledge Base are numbered, for example, KBA-01044.

White Papers

White papers (also known as Technical White Papers or TWP) are documents that delve into some of the more technical aspects of sfPMS. White Papers are accessed through the same Help menu:



Introduction to this Guide

Because the Spitfire Project Management System (sfPMS) tracks a vast amount of information, Alerts are used to keep you aware of important changes and information within your projects. Document Alerts let you know when documents, items, cost codes or routes are started, due or changed.

All Alerts appear right on your Home Dashboard. If you don't sign on to sfPMS very often, you can also receive emails (in your regular email application) notifying you that you have Alerts in sfPMS.

Compliance items are used to track various legal, documentation and business issues. When other parties fail to comply with their obligation, Compliance items can be configured to block approval of Pay Requests automatically. In addition, Compliance Notification documents are used to email or fax compliance notifications and requests to your subcontractors and vendors.

In order for Compliance to be incorporated into your site, some set up is required. This is generally done by the system administrator or others during implementation.

This guide focuses on Alerts and Compliances and is organized in three parts—Part I describes the use and setup of Document Alerts and Alert Subscriptions; Part II describes the use of Compliance tracking; and Part III describes the setup of Compliance types and everything else needed for Compliances to work.

This guide assumes some familiarity with sfPMS and its dashboards as described in the *Overview Guide*.

Note: Because sfPMS is configurable and because different users have different levels of access rights and permissions, the screens shown and the fields described in this guide may not be the same as those in your system.

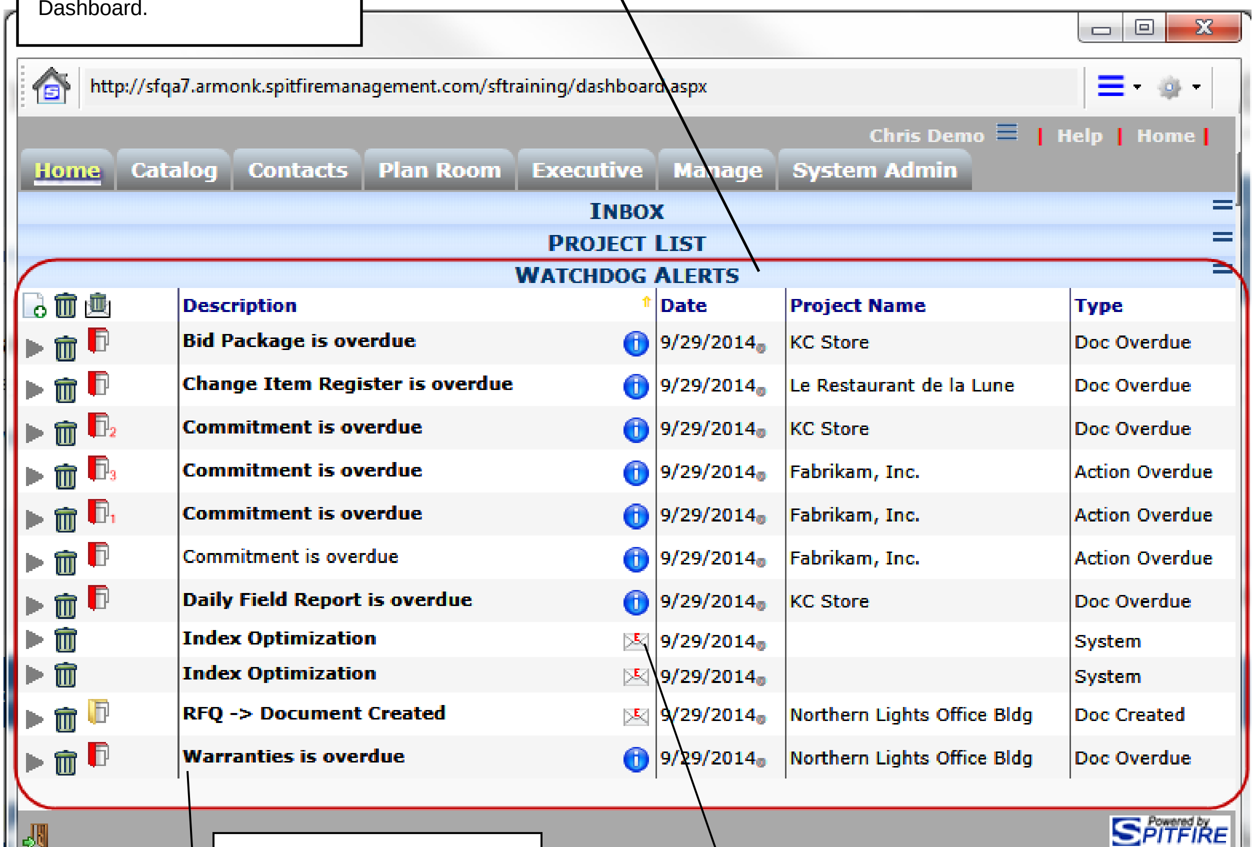
Note: section, chapters and text that are new or changed from the V4.4 documentation appear with **green text** and sometimes an *.

Part I: Alerts

The Watchdog Alerts Part

Once triggered, all Alerts arrive at your Watchdog Alerts part on your Home Dashboard. There you can open, forward, and delete your Alerts. You can also create stand-alone Alerts to send to others.

Your newest alerts (up to 200) are displayed on the Home Dashboard.



Alerts remain in your Watchdog Alerts part for 62 days or until you delete them.

When you mouse over or , information from the Alert appears.
indicates that the Alert was also sent to your email.

TIP

Email notification of Alerts is generally set up through the Alert Subscription tool. See the *Focus on the Manage Dashboard* for more information. See also page 19.

Columns

The Watchdog Alerts part displays the following information:

- **Description**: the header for the Alert.
- **Date**: when the Alert was generated.
- **Document**: the title of the document (if any) associated with the Alert.
  Note: this column might not be visible. It can be made visible through the Customization tool (Part = Alert List, Item = Document Col).
- **Project Name**: the name of the project associated with the Alert.
- **Type**: the type of Alert generated.

TIP
For more information about the Customization tool, see the *Focus on System Administration* guide.

Filters

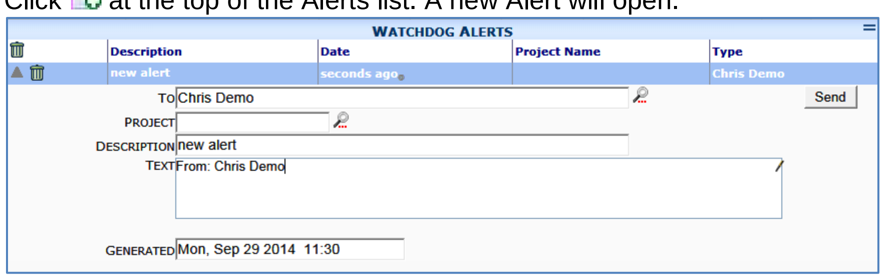
You can access filters for the Alert part either by clicking to open the options menu then selecting **Show Filter** or clicking the **Description** header to show the in-column drop-down menu.

- **Matching (Description)**: Enter one or more characters to filter by Alert Description.
- **Unviewed Only**: Check or select this filter to see only Alerts that have not been viewed yet. Those Alerts appear in boldface.
- **Web Only**: Check or select this filter to see only those Alerts that were not also sent via email. In other words, Alerts marked with the icon will not appear.

Alert Grid View

To send an Alert to another User:

1. Click at the top of the Alerts list. A new Alert will open.



2. Click at the **To** field to look up the person to receive the Alert.

3. (*optional*) Look up a **Project**.
4. Type a **Description**.
5. Use the **Text** field to type your Alert. Click to type in the Field Zoom window.
6. Click Send. The Alert will be sent to the other person.

To discard all Alerts at one time:

- Click at the top to clear the Alerts list.

To discard all Alerts that were also sent as email:

- Click at the top to clear out all Alerts that were also sent out as email by the system.

To open the document associated with the Alert:

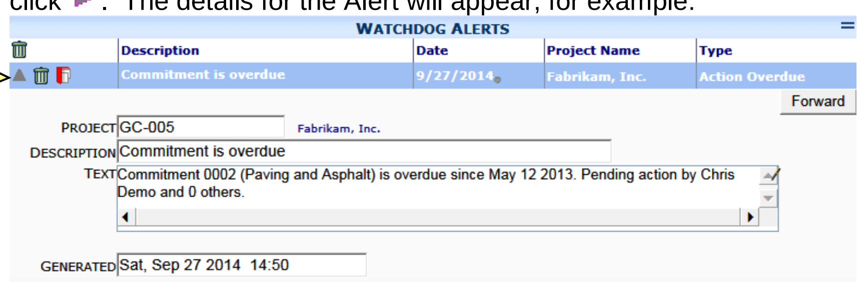
- Click on the row of the Alert to open the document.
  Note: email Alerts include a link to the document.

Alert Details

To open an Alert's details:

- At the Watchdog Alert list, either click on the Description of the Alert
  -or-
  click . The details for the Alert will appear, for example:

Click to return to the Alerts Grid view. Click to open the document associated with this Alert, if applicable.
Click to delete the Alert.



To forward an Alert:

1. In Detail view, click Forward. A **To** field will appear with your name, for example:

Notice that the Description now has an **Fw**: prefix.

Notice that the Text now indicates the **From** person.

2. Click at the **To** field to look up the person to receive the forwarded Alert.
3. (*optional*) Add text to the **Text** field.
4. Click Send. The Alert will be sent to the other person, but will still remain in your Watchdog Alerts part until you delete it (by clicking).

Document Alerts

Alerts can be set up in three different ways:

- Document-specific Alerts through the document's Options menu (see page 14).
- Alert Subscriptions from your Contact Detail window (see page 18).
- Alert Subscriptions for various users or roles through the Alert Subscriptions tool on the Manage Dashboard (see the *Focus on the Manage Dashboard* guide).

Alert Types

Spitfire ships with several default Alert types including an Other Alert that you can rename. Alert types can be modified only through the Alerts Type tool on the System Admin Dashboard (see the *Focus on System Administration* guide).

TIP
For more information about Code Maintenance, Routes or Items, see the *Focus on System Administration* guide, *the Focus on Routes* guide or the *Focus on Document and Item Basics* guide, respectively.

Document

- **Document Created**: triggered when a document is created and first saved. This Alert type is available for Alert Subscriptions only.
- **Document Due**: triggered when the document Due date (found on the Document Header part) comes due.
- **Document Due Change**: triggered if the due date has changed.
- **Document Status Change**: triggered if the status of the document (found on the Document Header) has changed. **Note**: this Alert type can be turned off for certain Doc types and statuses through the Code Maintenance tool.

Routee

- **Route Due**: triggered when the date by which a routee must take action on a routed document (found on the Route Detail tab) comes due.
- **Route Due Change**: triggered if the due date has changed.
- **Route Stage Change**: triggered if the route stage for the document has changed (found on the Route Detail tab).

Item

- **Item Created**: triggered when an Item is added to the document.
- **Item Due**: triggered when and Item due date (found on the Item's Detail view) comes due.

- **Item Due Change**: triggered if the due date has changed.
- **Item Status Change**: triggered if the status of the Item has changed.

Cost Code/Task

- **Cost Code Start**: triggered at the start date for the cost code in the work- breakdown-structure of the project.
- **Cost Code Start Change**: triggered if the start date of the cost code has changed.
- **Cost Code End**: triggered at the end date for the cost code.
- **Cost Code End Change**: triggered if the end date of the cost code has changed. **Note**: On systems that are integrated with Microsoft Dynamics SL, all these dates are based on the dates in Microsoft Dynamics SL's Project Maintenance Task tab.

TIP

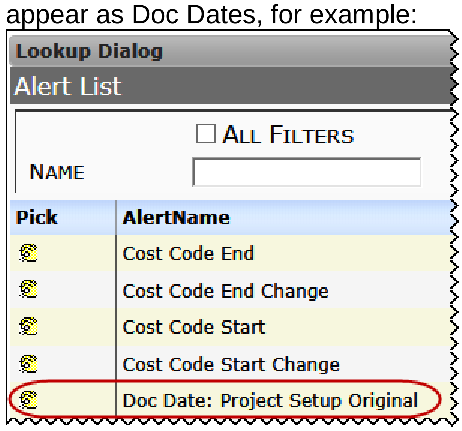
A special System Update Available alert will appear in the system administrator's Watchdog Alerts part when the system knows that an update is available.

Compliance

- **Out-of-Compliance:** triggered when a document is out of compliance.
- **Out-of-Compliance:** *compliance type:* triggered when the specific compliance type is out of compliance.

Doc Date

- **Doc Date**: *date type:* triggered if the specified date is within lead days. This Alert type is available for Alert Subscriptions only. **Note**: only date types that have been marked for Alerts will appear as Doc Dates, for example:



TIP

For information on how to set up dates for Alerts, see the "Date Types" chapter of the *Focus on System Administration* guide.

Outbound Routing

- **Send Failed**: triggered when outbound email or fax cannot be sent. The text of the alert contains details.
- **Unable to Send**: triggered when the routee has no email address (or fax number). The text of the alert indicates which.
- **Warning**: **Email Service Delayed**: triggered when ATC is not sending or receiving email. All users receive this alert in such cases.
- **Warning**: **Inbound Email Service Delayed**: triggered when ATC is sending but not receiving email.

System Alerts*

- **First Login**: triggered when a new user logs in for the first time.
- **Index Optimization**: triggered when the system tries to optimize an index automatically, but the index remains less-than-optimal. **Note**: only users with the **SYS | Site Configuration** capability receive this Alert.
- **System Update Available!**: triggered when an update is available (for example, from 4.4.5100 to 4.4.5155).
- **Version Upgrade Available:** triggered when a new version is available (for example, from 4.4 to 4.5).

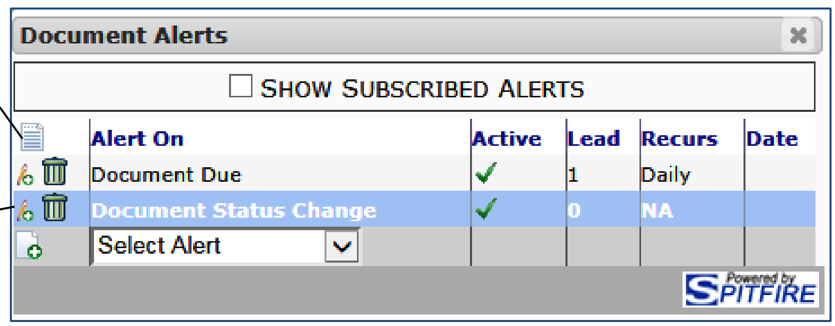
The Document Alert Option

Spitfire documents include a way to add Alerts through the Document Alerts Window.

Document Alerts Window

Click to open the Document Alert Summary report.

Click to edit and to delete an Alert.



The Document Alerts window lists the Alerts that were created from within the document. The columns on the Alerts tab tell you, for each Alert:

- **Alert On**: the type of Alert.
- **Active**: if the Alert is currently in use in sfPMS.
- **Lead**: used in two ways:
  - (*If the Alert is for a due date*) the number of days before or after the date, indicating when the Alert should be triggered. (Leads for *after the date* are expressed as negative numbers.)
  - (*If the Alert is for the change of a date*) the number of days that the date needs to change in order to generate an Alert.
- **Recurs**: how often the Alert will be sent.
- **Date**: if there is a specific date for this Alert.

Adding Document-Specific Alerts

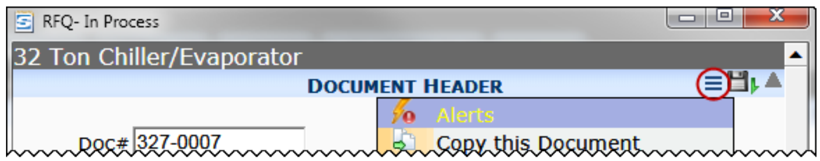
TIP
For more information on documents, see the *Focus on Document and Item Basics* guide.

TIP
For more information about role capabilities, see the technical white paper, *Designing User Roles*.

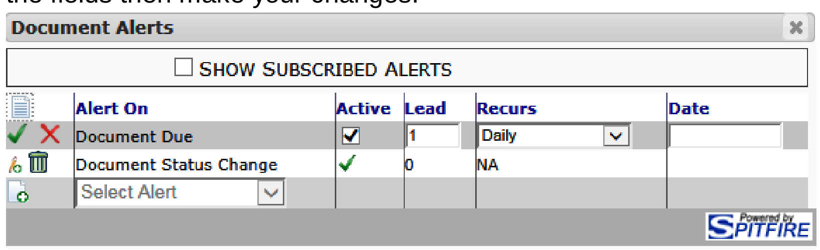
Alerts set up from within a document apply to that document only.

To add an Alert for a specific document:

1. Create or open the document.
2. At the document header, click ☰ to open the options menu then select **Alerts**. A Document Alerts window will appear. **Note**: you can add or edit Alerts specific to the document only if you have permission to do so through the **DOC | Document Alerts** role capability.



3. Use the **Alert On** drop-down to select the type of Alert you want for this document.
4. Click . The Alert will be listed with its defaults.
5. *(optional)* If you want to change the defaults, click to get to the fields then make your changes:



   - Click ✓ to accept your changes.

6. To save your Alert, click to close the Document Alerts window, then click to save the document with its new Alert.

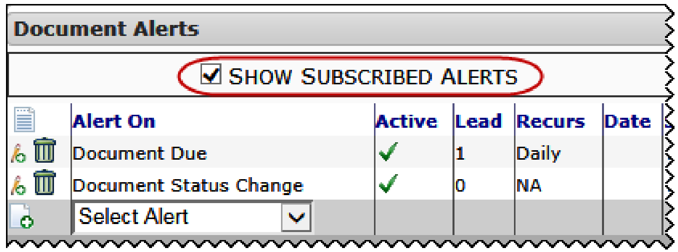
Show Subscriptions from Documents

You can see if Alert Subscriptions apply to a Spitfire document from within the document. (Alert Subscriptions are described in more detail, starting on page 18.)

To show the Alert Subscriptions that apply to a document:

1. At the document header, click ☰ to open the options menu then select **Alerts**. The Document Alerts window will appear, listing all Alerts that are local to the document (i.e., were set up through the document).

2. Click the **Show Subscribed Alerts** checkbox.



Now both Alerts that were set up through subscriptions and local Alerts will be listed in the grid.

Disabling and Removing Alert Subscriptions

Except for the Active status, Subscribed Alerts cannot be edited from within the document. They can, however, be removed from specific documents.

TIP

Disabling or removing an Alert on the document will prevent even those who have Alert Subscriptions from receiving the Alert on this document. Use with caution.

To disable an Alert Subscription for a document:

1. On the Document Alerts window, click the **Show Subscribed Alerts** checkbox.
2. On the row of the Subscribed Alert that you want to disable, click .
3. Click on the **Active** checkbox to uncheck it.
4. Click to accept your change.
5. Click to close the Document Alerts window.
6. Click to save the document and Alert changes.

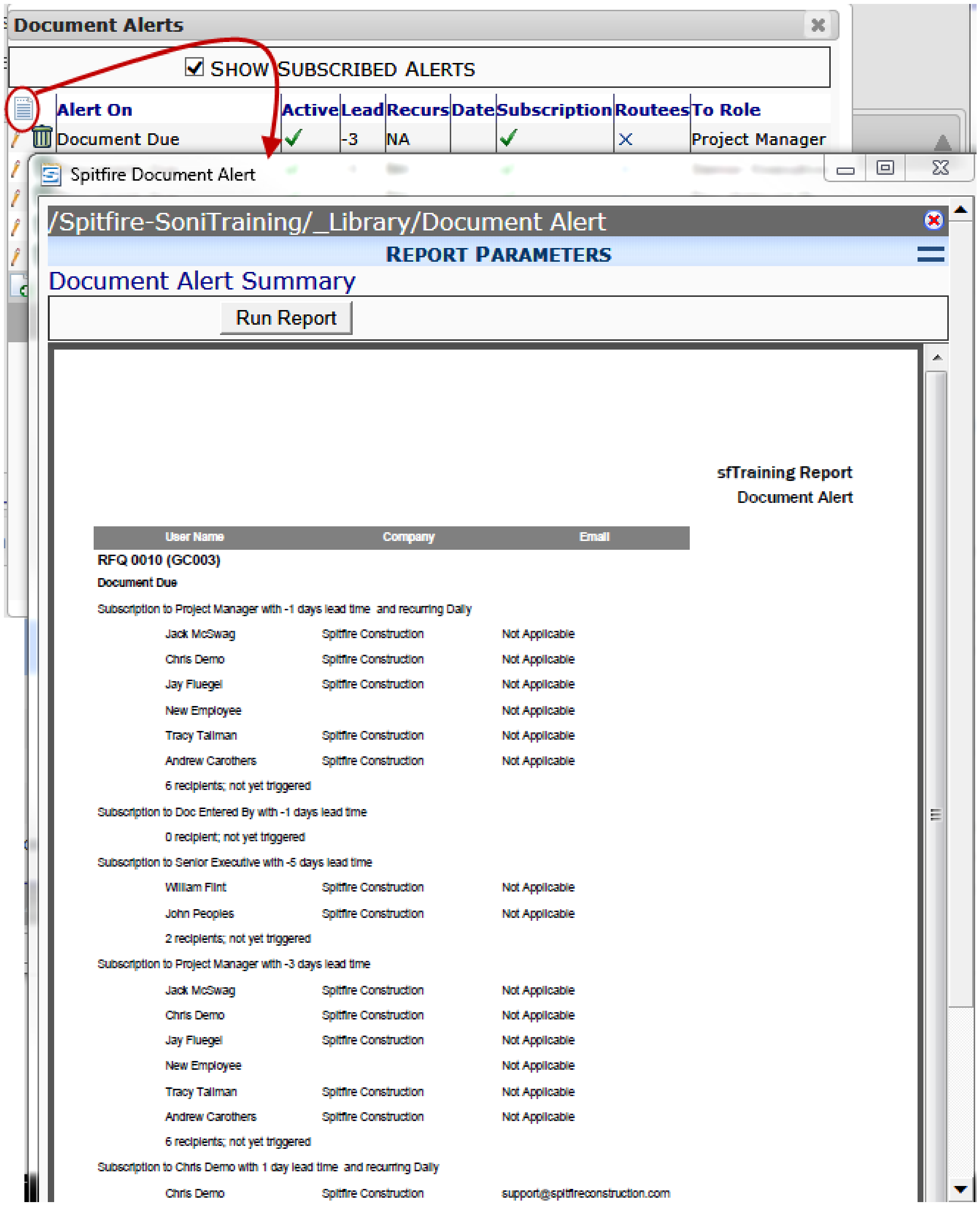
To remove an Alert Subscription for a document:

1. On the Document Alerts window, click on the **Show Subscribed Alerts** checkbox.
2. On the row of the Subscribed Alert that you want to remove, click . The Alert will be removed from the grid.
3. Click to close the Document Alerts window.
4. Click to save the document and Alert changes.

Alerts Report

To show who gets the Alerts for the document:

- On the Document Alerts window, click to open a report on all the users who get Alerts based on this document:



Alert Subscriptions for Documents

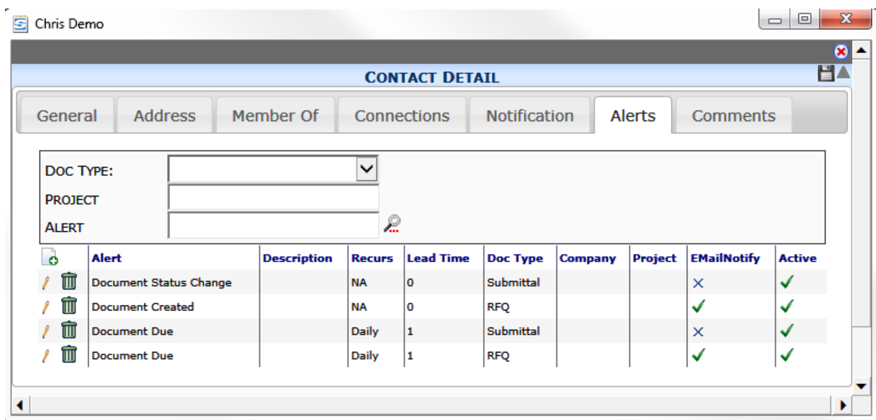
While the ability to set up an Alert for a particular document is useful, having to do so for every document of a certain type, or for every document routed to a certain person, would be tedious. sfPMS, therefore, allows Alert Subscriptions. Alert Subscriptions can be set up through Contact Detail windows and the Manage Dashboard.

Important: If you set up too many Alerts, the Watchdog Alert part will quickly fill up with those Alerts and the Alerts will lose their importance. Before setting up Alert Subscriptions, consider carefully what is really important enough to require your (or others') attention.

Subscriptions from the Detail Window

If you have permission to do so (i.e., if you have the **DOC | Document Alerts** role capability), you can set up Alert Subscriptions from the Alert tab in your own Contact Detail window. Otherwise, at this tab, you will only be able to view existing Alert Subscriptions (created by others) for example:

TIP
For more information about the Contact Detail window, see the *Focus on Contacts* guide.



The Alerts Tab

There are three filter fields and nine columns of information in the Alerts tab.

TIP
A wildcard is assumed after what you type in the Project field (so G means "all projects that begin with G"). The wildcard % can also be used before or around text (so %010% means all projects with 010 in the name).

Filters

You can filter Alert Subscriptions by

- **Doc Type:** Click the checkbox to be able to select a Doc type from the drop-down.
- **Project:** Type all or some of a Project ID.
- **Alert:** Select a type of Alert from the lookup.

Columns

Alert Subscriptions include the following information:

- **Alert**: the type of Document Alert. Alerts types are generally configured by the system administrator. They describe the conditions that, when met, send out an Alert. Default Alert types are described on page 12.
- **Description**: a description of the Alert Subscription.
- **Recurs**: how often the Alert should be sent (for example, daily, weekly, monthly, yearly, bi-monthly, etc.).
- **Lead Time**: can be used in two ways:
    - (*If the Alert is for a due date*) the number of days before or after the date, indicating when the Alert should be triggered. (Leads for *after the date* are expressed as negative numbers.)
    - (*If the Alert is for the change of a date*) the number of days that the date needs to change in order to generate an Alert. (For example, if you enter 3, then you'll receive an Alert if the date changes by three or more days, but you will not receive an Alert if the date changes by a day or two).
- **Doc Type:** the Doc type to which this Alert should apply. If blank, the Alert will apply to all Doc types.
- **Company:** the company to which this Alert should apply. If blank, the Alert will apply to all companies.
- **Project:** the project to which this Alert should apply. If blank, the Alert will apply to all projects.
- **EMailNotify:** if an email should be sent to the Contact whenever an Alert is sent to his or her Watchdog Alerts list. This duplication of notification is useful for people who do not log in to sfPMS very often.
- **Active:** whether this Alert Subscription is currently being used.

New Subscriptions

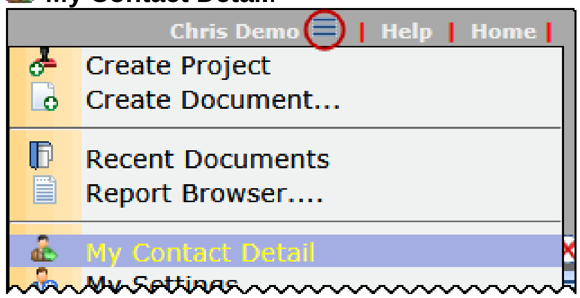
Once an Alert Subscription is created (and active), new documents, routes, items and cost codes in sfPMS are checked against these subscriptions. When the specified conditions are met, Alerts are sent to the user.

Important: Older documents, routes, items and cost codes will not be checked for newer subscriptions. However, you can set up individual Alerts for these conditions from a document, as described on page 14.

TIP
If you have the PAGE | User/Contact Display (U) capability, you can also create Alert Subscriptions for other users from their Contact Detail windows. See the *Focus on Contacts* guide and the technical white paper *Designing User Roles* for more information.

To create a new Alert Subscription from your Contact Details:

1. At any dashboard, click ☰ to open the options menu then select **My Contact Detail**.



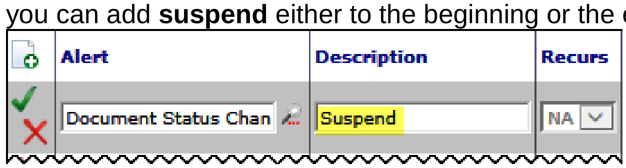
   Your Contact Detail window will open.
2. Click on the **Alerts** tab.
3. Click to add a new row.
4. Look up an **Alert** type.
5. Use the other fields, depending on how you want to set up the Alert Subscription.
6. Click ✓ to accept your changes and to save them.
7. All of your Alert Subscriptions will appear in the grid, for example:

	Alert	Description	Recurs	Lead Time	Doc Type	Company	Project	EMailNotify	Active
	Document Status Change		NA	0	Submittal			×	✓
	Document Created		NA	0	RFQ			✓	✓
	Document Due		Daily	1	Submittal			×	✓
	Document Due		Daily	1	RFQ			✓	✓

Existing Alert Subscriptions

To modify (edit, suspend, delete) an Alert Subscription:

1. Open your Contact Detail window (as described on the previous page) and click on the Alerts tab.
2. (*optional*) Use the filters to find the subscriptions that you want to modify.
3. To delete a subscription, click on the Alert row.
4. To edit a subscription, click on the Alert row and make your changes in the fields.
   - To suspend a subscription, type the word **suspend** in the Description field. If text already exists in this field, you can add **suspend** either to the beginning or the end.



TIP
Making an Alert Subscription inactive may prevent new documents from monitoring for the Alert. However, a suspended Alert Subscription will still generate Alerts, but not deliver them.

- To re-activate a suspended subscription, remove the word **suspend** from the Description field.

5. Click ✓ to accept your changes and 💾 to save them.

Subscriptions from the Manage Dashboard

While many users can set up Alert Subscriptions for themselves, those with the **PART | Alert Subscription Maintenance** role capability can set up Alert Subscriptions for other users or for specific roles through the Alert Subscription tool.

The Alert Subscription tool is found on the Manage Dashboard. For more information, see the *Focus on the Manage Dashboard* guide.

Setting Up Document Alerts

The only setup required for Document Alerts is the configuration of Alert types through the Alert Types tool. You can edit default Alert types, create additional Alert types to be used in sfPMS and, more commonly, make some of the default Alert types inactive. A description of default Alert types can be found on page 12. Alert types appear on drop-downs on a document's Alert window or in the Alert Subscription tool on the System Admin Dashboard. Using the Alert Types tool, you can control which Alert types are active or inactive. You can also create a version of the "Other" Alert. The Alert Types tool is found on the System Admin Dashboard. For more information, see the *Focus on System Administration* guide.

Part II: Compliance Tracking

During implementation, some Compliance requirement types may be set up as requirements for certain Doc types, such as Commitments, Pay Requests and Vendors. Other Compliance types may be set up as optional for certain Doc types. Compliance types are managed through the Compliance tab. A message on your document (Commitment, Pay Request, etc.) will indicate if a requirement is out of compliance.

Compliance Types

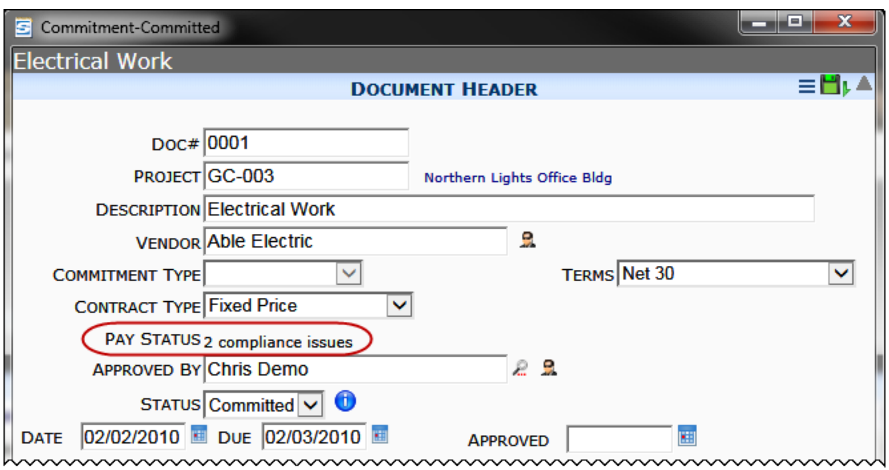
Spitfire ships with a few default Compliance types. Sites often add their own Compliance types during implementation through the Compliance Types tool (see page 46).

Examples of Compliance Types

- Automobile Insurance
- Executed Contract Returned
- General Liability Insurance
- Lien Waiver
- Performance Bond
- Project Manager Hold
- Workman Comps Insurance

Messages on the Document Header

A message on a document's Document Header indicates if everything is in compliance or if there are document compliance and vendor compliance issues.

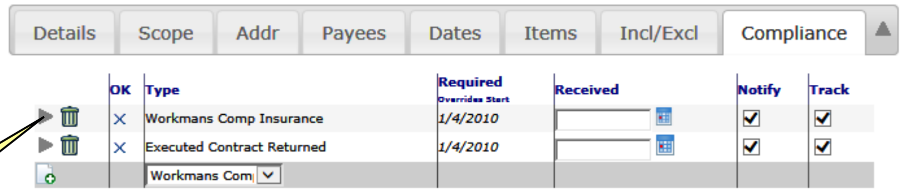


To investigate those issues, look at the document or Vendor document's Compliance tab.

The Compliance Tab

A Spitfire document can include a Compliance tab as one of its mid-section tabs. Through this tab you can add or edit compliance items specific to the Doc type.

Compliance Grid View



Click to get to Detail view for the Compliance.

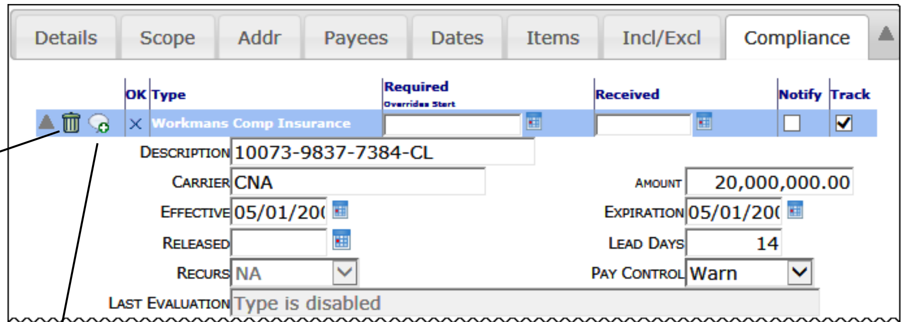
The Compliance tab lists the compliance items that are required for the document and, depending on configuration, allows you to add other types of compliances items for the document. The columns on the Compliance tab tell you the following information for each compliance item:

- **OK**: means that the Compliance item is in compliance; means that it is out of compliance; and means that the compliance status is unknown (as is the case when information for a required Compliance item has not yet been entered or a new document has not yet been saved.)
- **Type**: the type of Compliance. Required Compliance types are listed when a new document is created; optional Compliance types are selected from a drop-down.
- **Required**: the date that proof of compliance is required. The Commitment Start date is used by default until another date is entered. (If there is no Commitment Start date, the document's Due date is used.) If the Required date has passed and there is no Received date, the item will be out of compliance.
- **Received**: the date that proof of Compliance was received. Once a Received date is entered, the item will be in compliance if all other conditions are also met (see page 27).
- **Notify:** means that a Compliance Notification document will be automatically created, based on an automatic workflow script (see page 48), when this item is out of compliance; means that no Compliance Notification document will be created.
- **Track**: means that the compliance item is currently being tracked; means that the compliance item is being ignored.

Compliance Item Detail View

Grid view of a compliance item allows you to directly edit the **Received** date field as well as the **Notify** and **Track** checkboxes. Detail view allows you to also edit the **Required** field and displays several new fields:

Only optional Compliances (that you add) can be deleted.



Use the icon to add remarks.

- **Description**: a longer description of the compliance item, if any.
- **Carrier**: the name of the carrier for this compliance item.
- **Amount**: the amount of coverage.
- **Effective**: the date the compliance item goes into effect. If the Effective field is active (i.e., you can select a date from the calendar icon) and you leave the field blank, the item will be out of compliance. If you enter an Effective date, it will be checked against the Current Start and Finish dates on the Dates tab.
- **Expiration**: the date the compliance item expires.
- **Released**: the date the compliance item is released. Releasing the compliance item overrides the Effective/Expiration dates and the Required/Received dates.
- **Lead Days**: the number of days before the Expiration Date that a Compliance Alert should be sent.
- **Recurs**: how often the Compliance Alert should be sent.
- **Pay Control**: the Pay Control option for this compliance item. Pay Control options are
    - **Auto**: The compliance item is evaluated based on the Commitment's Current Date and the Compliance requirements. If anything is out of compliance, the Pay Request associated with the Commitment or Vendor will not allow approval.
    - **Block**: The compliance item is manually set to out of compliance and therefore, the Pay Request associated with the Commitment or Vendor will not allow approval.
    - **Warn**: The compliance item is evaluated based on the Commitment's Current Date and the compliance item's requirements. If anything is out of compliance, warning messages appear on Commitment and Pay Request documents. However, the Pay Request can be approved.

TIP

Some of Spitfire Compliance features are designed to work with your integrated Accounting system's Accounts Payable modules. Normally, Compliance Notifications and Warnings block payments lacking compliance from reaching Accounts Payable.

- **Last Evaluation**: a message indicating why the item is in or out of compliance.

Last Evaluation Messages

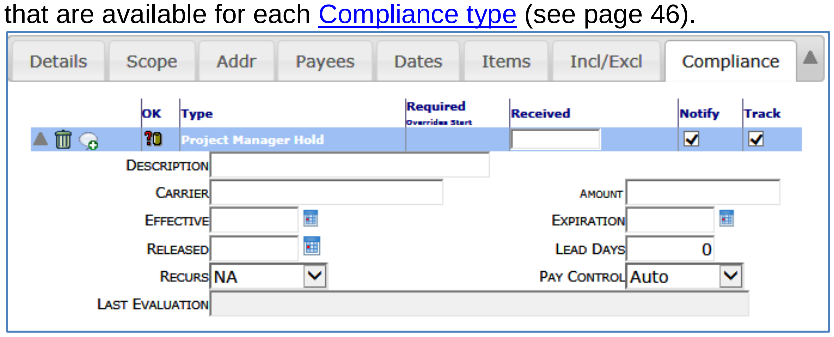
Required, not met	Out of compliance because of a Required date but no Received date.
Expired	Out of compliance because of an Expired date that is within the Start and Finish dates of the Commitment.
Required, but not Effective	Out of compliance because of a Required date, but no in-range Effective date.
Amount insufficient	Out of compliance because of a required Amount, but the amount is less than the total current amount of the Commitment.
TIN missing	Out of compliance because of a missing Vendor Taxpayer Identification Number.
Manually blocked	Out of compliance because the Pay Control for this requirement is set to Block.
Released	In compliance because of a Released date for or prior to today.
Conditions met	In compliance because it has met all conditions.
Vendor covers requirement	In compliance because the associated Vendor has already complied with the requirement of the same type (see page 32).
Expires soon	In compliance but the Expired date is approaching and within the lead days interval.
Required soon	In compliance because of a Required date in the future, but that date is approaching and is within the lead days interval.
Required soon (Effective late)	In compliance because the Required date is in the future, but the Effective date will not cover the Required date when it arrives.
Not required yet	In compliance because the Required date is far in the future (outside the lead days interval).

Note: messages shown in brown above will generate a Compliance Alert even though the compliance items are still in compliance.

Adding and Editing Compliance Items

To add a Compliance item:

1. Open your document and click the Compliance tab. Any required Compliance items will already be listed in Grid view.
2. Use the **Type** drop-down to select a new Compliance type for your document.
3. Click  to get to Detail view for your new Compliance item.
4. Fill out the desired fields and checkboxes, using lookups and calendars as appropriate. **Note**: Not all fields apply to every Compliance type. The system administrator configures the fields that are available for each Compliance type (see page 46).



TIP

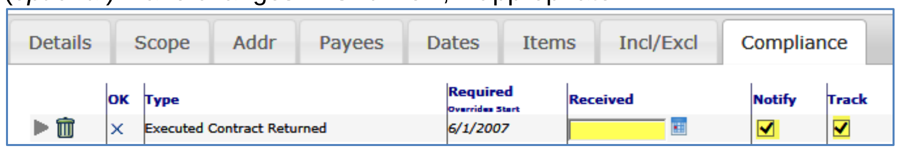
You can edit compliance on closed or approved documents if you have the DOC | Maintain Compliance Items role capability.

For more information, see the *Designing User Roles* technical white paper.

5. Click to return to Grid view.
6. Click to save your changes.

To edit a Compliance item:

1. Open your document and click the Compliance tab. Any required Compliance items will already be listed in Grid view.
2. (*optional*) Make changes in Grid view, if appropriate.

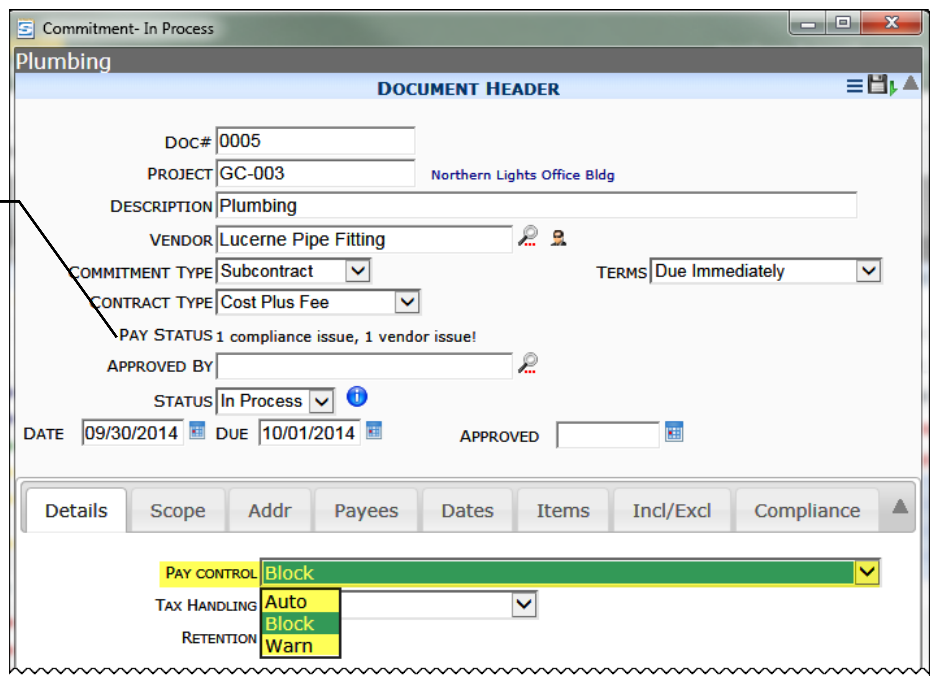


3. Click at the Compliance item if you need to edit other fields. The details for that Compliance item will appear.
4. Make changes to the appropriate fields.
5. Click to return to Grid view.
6. Click to save your changes.

Pay Control on the Details Tab

Through customization (Part = **Doc Detail-Standard**, Item = **PayControl**), the System Administrator can include a Pay Control field on a document's Details tab.

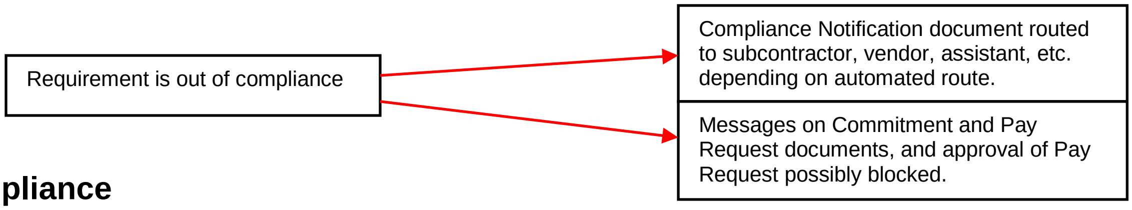
An **!** at the end of the message indicates that Pay Request Approval is blocked.



This Pay Control option on the Details tab overrides any Pay Control options selected on the Compliance tab (described on page 24).

How Compliance Works

When Compliance has been properly set up at your site (see Part III of this guide), you can expect the following actions.



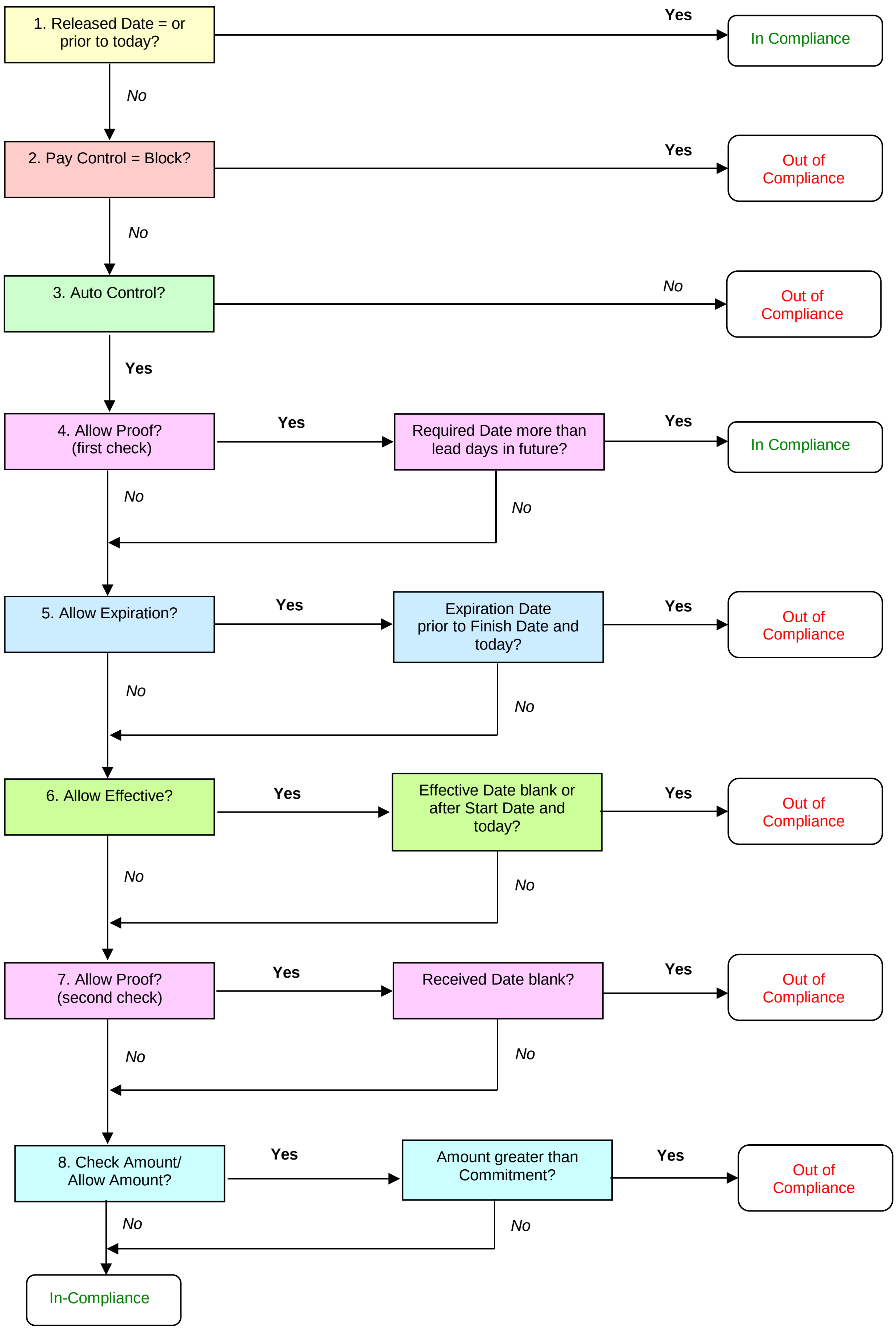
Compliance valuation

Compliance items are evaluated and determined to be either in compliance or out of compliance. Commitment, Pay Requests and Vendor documents are evaluated every time you open or save the document. Other documents are evaluated for compliance issues once a day at whatever time was set up during implementation.

sfPMS uses a series of questions when evaluating Compliances. Depending on the answer to the questions (as shown on the next page), a requirement is deemed in compliance or out of compliance.

> **TIP**
> Options for Compliance types are described on page 46. Most users will not need to concern themselves with these behind-the-scenes options, which are set during implementation.

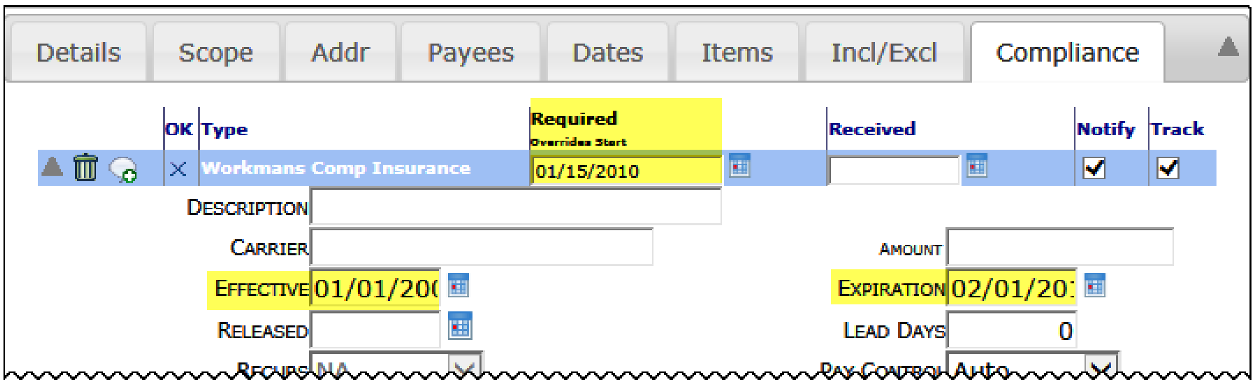
1. Is there a Released date that is equal to or prior to the current day?
2. Is Pay Control equal to Block?
3. Does the Compliance type have the Auto Control option checked (turned on)?
4. Does the Compliance type have the Allow Proof option checked (turned on)? **Note**: When Allow Proof is on, the Required and Received dates allow your input.
    - o Is the Required date set to a date more than the lead days in the future?
5. Does the Compliance type have the Allow Expiration option checked (turned on)?
    - o Is the Expiration date prior to today and prior to the Commitment Finish date (found on the Date tab)?
6. Does the Compliance type have the Allow Effective option checked (turned on)?
    - o Is today greater than the Commitment Start date minus lead days and is the Effective date blank or greater than both today and the Commitment Start date?
7. Once more, does the Compliance type have the Allow Proof option checked (turned on)?
    - o Is the Received date empty and has the Required Date passed?
8. Does the Compliance type have the Check Amount and Allow Amount options checked (turned on)?
    - i. Is the Amount greater than the Commitment?

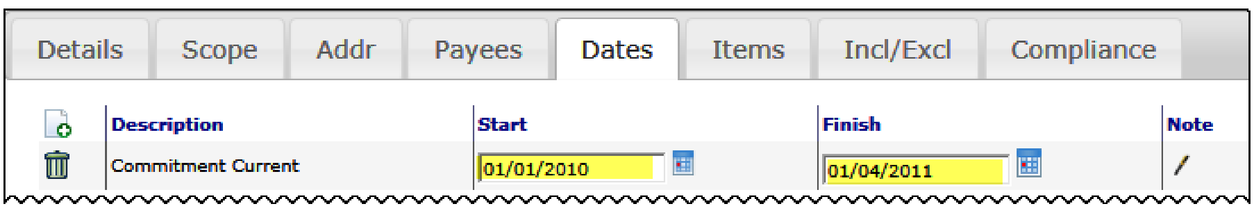

1. Released Date = or prior to today?
Yes
In Compliance
No
2. Pay Control = Block?
Yes
Out of Compliance
No
3. Auto Control?
No
Out of Compliance
Yes
4. Allow Proof? (first check)
Yes
Required Date more than lead days in future?
Yes
In Compliance
No
No
5. Allow Expiration?
Yes
Expiration Date prior to Finish Date and today?
Yes
Out of Compliance
No
No
6. Allow Effective?
Yes
Effective Date blank or after Start Date and today?
Yes
Out of Compliance
No
No
7. Allow Proof? (second check)
Yes
Received Date blank?
Yes
Out of Compliance
No
No
8. Check Amount/ Allow Amount?
Yes
Amount greater than Commitment?
Yes
Out of Compliance
No
No
In-Compliance

Example

Out of Compliance

In the document shown below, the Effective/Expiration date range (**1/1/2009** to **2/1/2010**) for the Workmans Comp Insurance does not cover the Start/Finish date range (**1/1/2010** to **1/4/2011**) on the Commitment. In addition, while the Workmans Comp Insurance is required, it has not yet been received. For both of these reasons, the Workmans Comp Insurance is out of compliance. (When it is received, it will still be out of compliance because of the expiration date.)





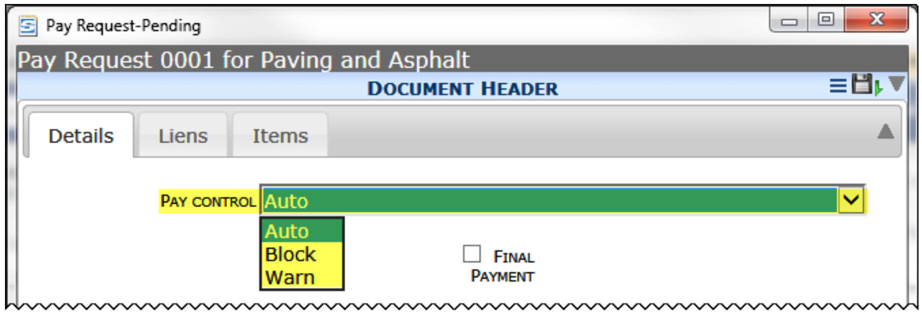
Blocked or Not Blocked

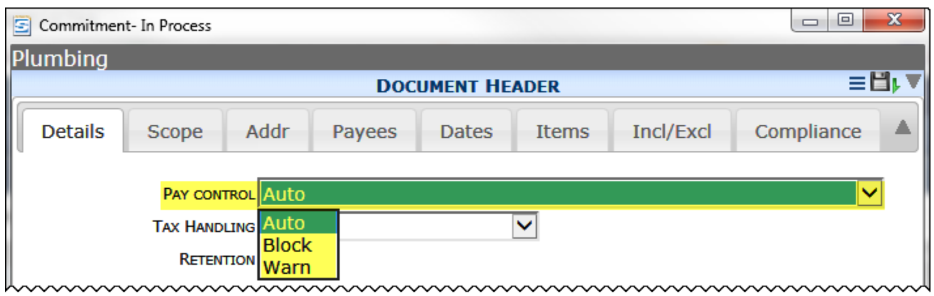
TIP

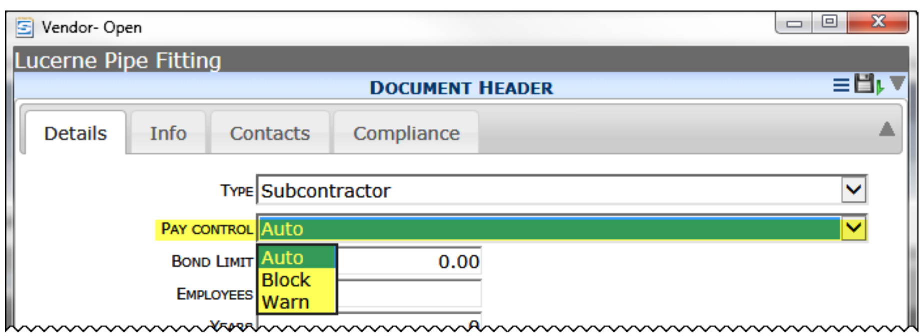
The Pay Control option is hierarchical: Vendor -> Commitment -> Pay Request. Setting a Vendor to Block affects all Commitments on all projects. Using Pay Control on the Pay Request affects that one payment only.

Whether a compliance item will block approval of Pay Requests is determined by several factors.

One factor is the PayControl option on the Details tab of the Pay Request, its Commitment, and the corresponding Vendor document.







Approval of a Pay Request will be blocked if

- Pay Control for the Pay Request, Commitment or Vendor is set to **Block,** (and therefore the Compliance item is always out of compliance).
  -or-
- Pay Control for the Pay Request, Commitment and Vendor are all set to **Auto** and the Compliance item is out of compliance.

A warning message will appear (but approval will be allowed) if

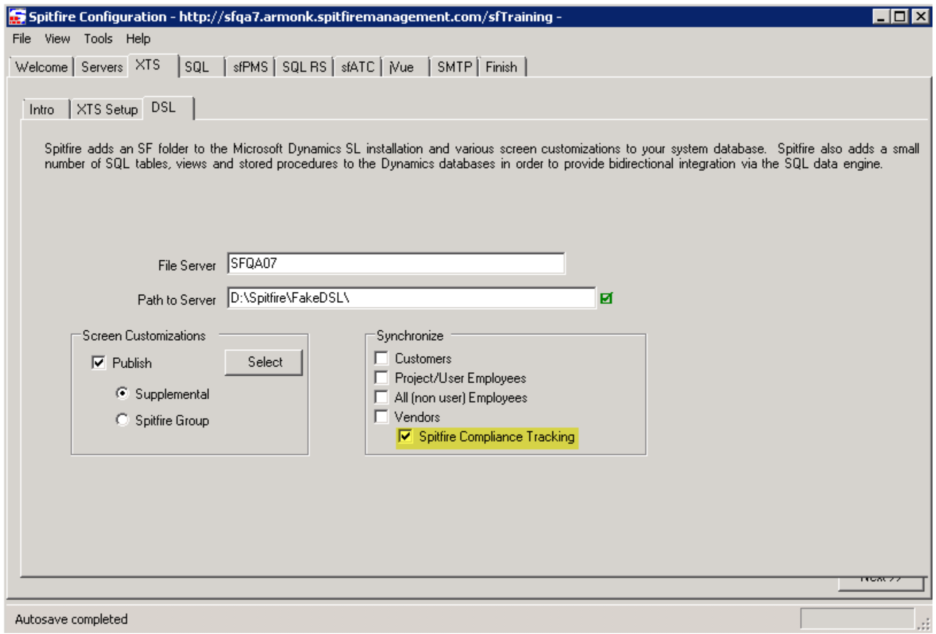
- Pay Control for the Pay Request, Commitment or Vendor is set to **Warn**.

What Gets Blocked

If the out-of-compliance item is	*Then*
on a Vendor document	approval of all Pay Requests for the Vendor will be blocked
on a Commitment or CCO	approval of all Pay Requests for the Commitment will be blocked
on a Pay Request	approval of that Pay Request will be blocked
on a Change Order	nothing will be blocked
on an Employee document	nothing will be blocked

AP Vouchers

If your site is integrated with Microsoft Dynamics SL and Spitfire Compliance Tracking has been checked in ICTool (as shown below) then out of compliance items will also affect AP Vouchers.



If the out of compliance item is	*Then*
on a Vendor document	all AP Vouchers for the Vendor will be placed on Hold
on a Commitment or CCO	all AP Vouchers for the Vendor's invoices linked to the referenced Commitment will be placed on Hold
on a Pay Request	all AP Vouchers for the Vendor's invoices linked to the referenced Commitment will be placed on Hold
on a Change Order	nothing will be placed on Hold
on an Employee document	nothing will be placed on Hold

Other Considerations

Compliance from Vendor

If both a Vendor document and related Commitment (or CCO) document include a Compliance item of the same type, the Vendor can provide compliance to the Commitment.

- While the Vendor requirement is in compliance, the same requirement on the Commitment will also be in compliance, even if, on its own, the Commitment's requirement would be out of compliance.
- If the Commitment's requirement is out of compliance and the Vendor requirement goes out of compliance, the Commitment will indicate that it is now out of compliance.
- If the Commitment's requirement is in compliance on its own, it will be in compliance even if the Vendor's requirement is or goes out of compliance.

% Paid

TIP

For more information about **%Paid**, see the chapter on Compliance Types in the *Focus on System Administration* guide.

If **% Paid** is entered for a Compliance type then that compliance requirement, when out of compliance, will be treated as follows (if Pay Control on the document is **Auto**):

- If the sum of all approved Pay Requests is a percentage of the current Commitment amount that is below the percentage indicated for that Compliance type, a warning message will appear on the Pay Request.
- If the sum of all approved Pay Requests is a percentage of the current Commitment amount that equals or passes the percentage indicated for that Compliance type, approval of that Pay Request (and future Pay Requests) will be blocked.

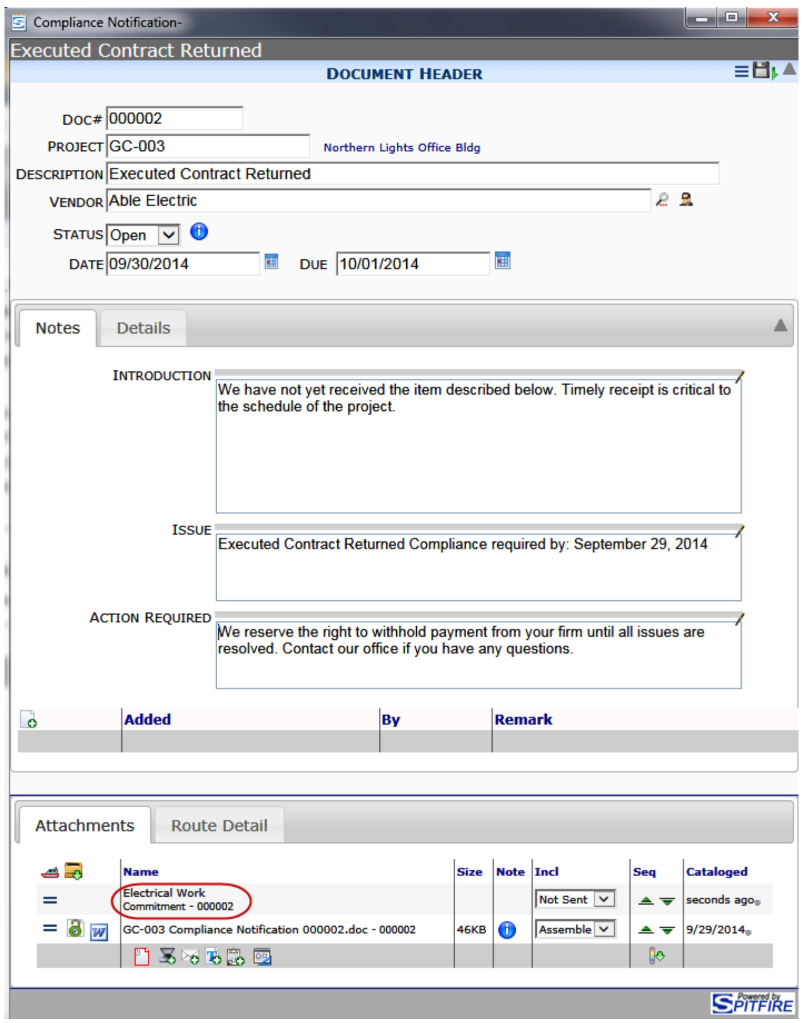
Compliance Notification Document

When a Compliance item with the Notify option triggers an out-of-compliance signal, a Compliance Notification document is created through an automatic workflow script. Based on routing rules and Contact setup (described in Part III of this guide) the Compliance Notification is routed to the appropriate people, for example, a Spitfire user (employee at your company) and the subcontractor or vendor who is out of compliance.

When a compliance requirement that has routed a Compliance Notification document…

- goes in compliance, the Compliance Notification document is automatically closed.
- remains out of compliance after the allotted recurrence interval, the existing Compliance Notification document is automatically closed and a new Compliance Notification document is routed.

Note: any closed Compliance Notification documents that are in a user's Inbox are removed from the Inbox automatically.



Note: the document that triggered the Compliance Notification document is attached to the Compliance Notification document.

If additional Compliance Notification documents are created for the same issue, previous Compliance Notification documents are closed and attached to the current Compliance Notification document.

If the Compliance Notification document is routed via email or fax, or if a hard copy is printed, the routee will receive a printout created through a template (seen as an attachment in the previous picture), for example:

Vendor Compliance Notification

September 30, 2014

Able Electric
111 Meandering Lane
Lakeridge, OR 99999

GC003 Northern Lights Office Bldg

We have not yet received the item described below. Timely receipt is critical to the schedule of the project.

Issue
Executed Contract Returned

Compliance required by: September 29, 2014

Action Required
We reserve the right to withhold payment from your firm until all issues are resolved. Contact our office if you have any questions.

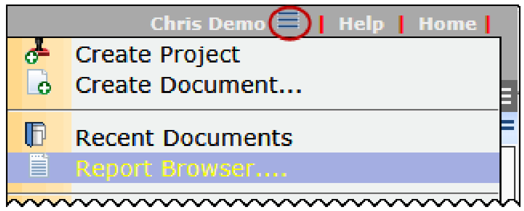
Elizabeth Keyser-Rubble
Clerk
Armonk, NY 10504
(914) 273-0808
bettyr@spitfireconstruction.com

Compliance Log

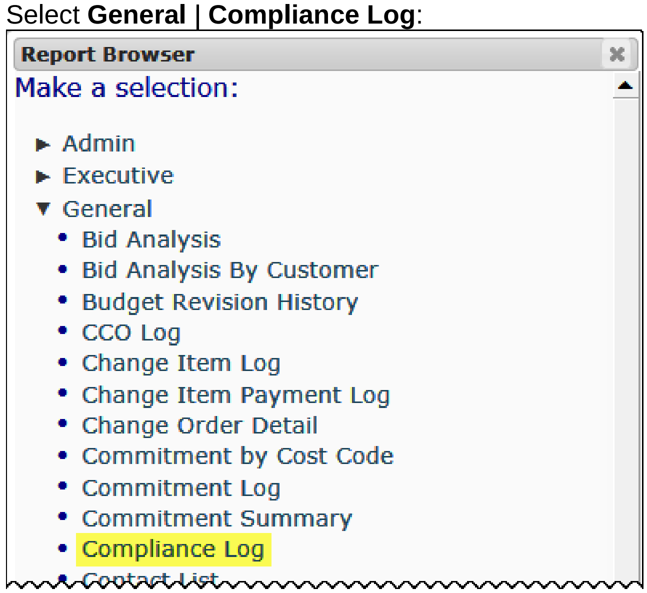
The Compliance Log lists all compliances being tracked in your projects. You can filter the report.

To open the Compliance Log:

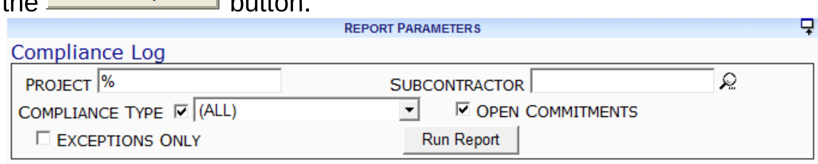
1. Click to open the options menu then select **Report Browser.**



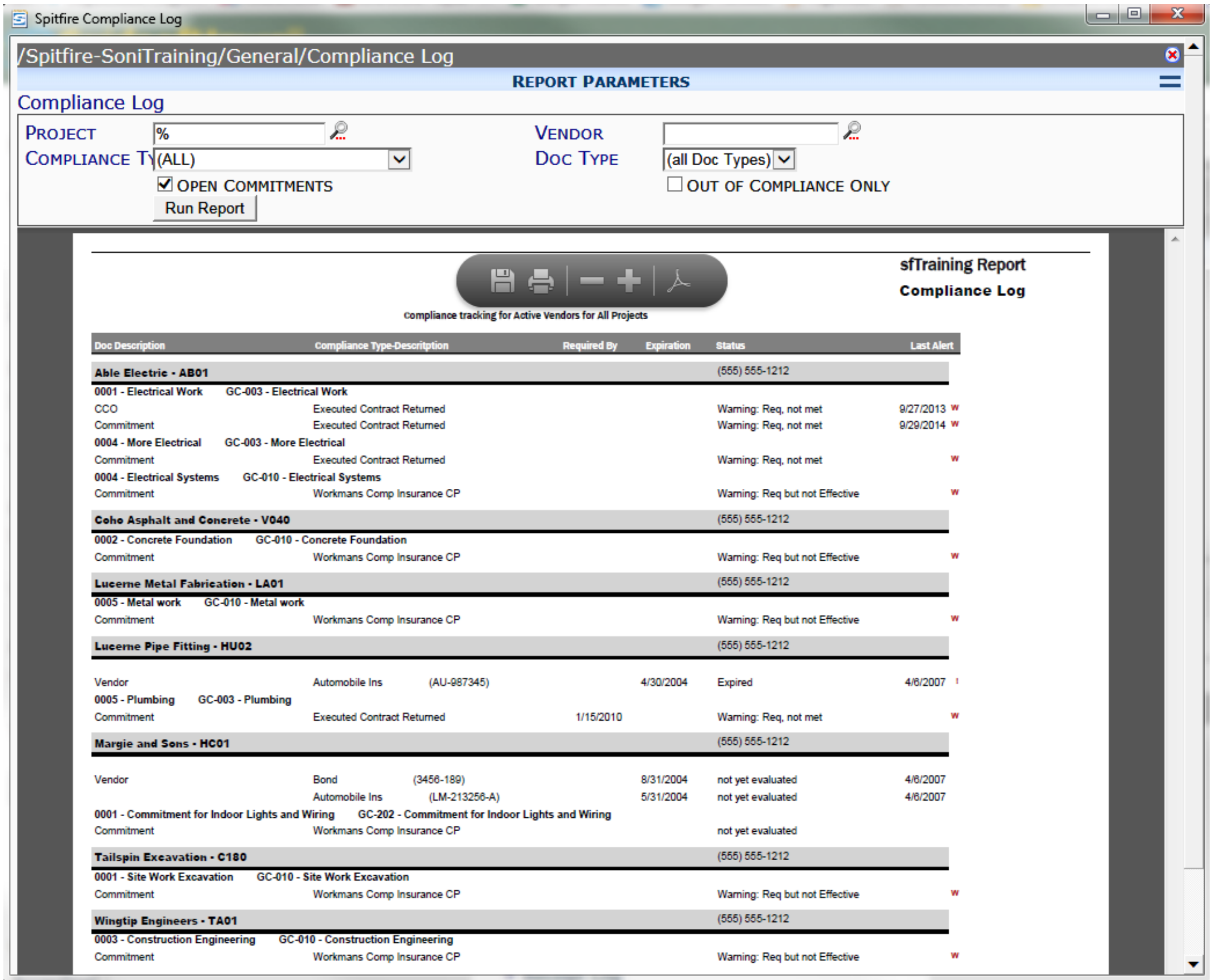
2. Select **General | Compliance Log**:



3. (*optional*) In the window that appears, filter the report by Project ID, Vendor, Compliance Type, Doc Type, Open Commitments and/or exceptions (out-of-compliance requirements) and clicking the Run Report button.



4. Click ✕ to close the report.



Doc Description	Compliance Type-Description		Required By	Expiration	Status	Last Alert
Able Electric - AB01					(555) 555-1212	
0001 - Electrical Work	**GC-003 - Electrical Work**					
CCO	Executed Contract Returned				Warning: Req, not met	9/27/2013 W
Commitment	Executed Contract Returned				Warning: Req, not met	9/29/2014 W
0004 - More Electrical	**GC-003 - More Electrical**					
Commitment	Executed Contract Returned				Warning: Req, not met	W
0004 - Electrical Systems	**GC-010 - Electrical Systems**					
Commitment	Workmans Comp Insurance CP				Warning: Req but not Effective	W
Coho Asphalt and Concrete - V040					(555) 555-1212	
0002 - Concrete Foundation	**GC-010 - Concrete Foundation**					
Commitment	Workmans Comp Insurance CP				Warning: Req but not Effective	W
Lucerne Metal Fabrication - LA01					(555) 555-1212	
0005 - Metal work	**GC-010 - Metal work**					
Commitment	Workmans Comp Insurance CP				Warning: Req but not Effective	W
Lucerne Pipe Fitting - HU02					(555) 555-1212	
Vendor	Automobile Ins	(AU-987345)		4/30/2004	Expired	4/6/2007 !
0005 - Plumbing	**GC-003 - Plumbing**					
Commitment	Executed Contract Returned		1/15/2010		Warning: Req, not met	W
Margie and Sons - HC01					(555) 555-1212	
Vendor	Bond	(3456-189)		8/31/2004	not yet evaluated	4/6/2007
	Automobile Ins	(LM-213256-A)		5/31/2004	not yet evaluated	4/6/2007
0001 - Commitment for Indoor Lights and Wiring	**GC-202 - Commitment for Indoor Lights and Wiring**					
Commitment	Workmans Comp Insurance CP				not yet evaluated	
Tailspin Excavation - C180					(555) 555-1212	
0001 - Site Work Excavation	**GC-010 - Site Work Excavation**					
Commitment	Workmans Comp Insurance CP				Warning: Req but not Effective	W
Wingtip Engineers - TA01					(555) 555-1212	
0003 - Construction Engineering	**GC-010 - Construction Engineering**					
Commitment	Workmans Comp Insurance CP				Warning: Req but not Effective	W

Part III: Setup of Compliance Tracking and Notification

Setup of Compliance tracking and notification requires the use of various Manage and System Admin tools and features of sfPMS.

Steps Involved

Step 1: Prepare (see page 38)

- Gather information.

Step 2: Use the Code Maintenance tool (see page 40)

- Create subtypes for your vendors and subcontractors.

Step 3: Use the Customization tool (see page 42)

- Customize Vendor, Commitment and/or Pay Request Doc types.

Step 4: Use the Compliance Types tool (see page 46)

- Edit existing Compliance types.
- Create new Compliance types.
- Review the automatic workflow for your Compliances.

Step 5: Use the Doc Type tool (see page 49)

- Activate the Compliance Notification Doc type.

Step 6: Use the Rules Maintenance tool (see page 51)

- Set up the text for Compliance Notification documents .

Step 7: Get the Template (see page 55)

- If necessary, upload the distributed Attachment (auto) template for Compliance Notification documents.

Step 8: Use ICTool (see page 58)

- Turn on Automatic Workflow on the sfATC tab of the Spitfire Installation and Configuration tool.

Step 9: Use the Roles tool (see page 59)

- Create a role to receive the Compliance Notification document.

Step 10: Use the Routes tool (see page 60)

- Create a predefined route for the Compliance Notification document.

Step 11: Use the Contacts tool (see page 62)

- Give one or more users the “Compliance Staff” role.

Step 12: Test Compliance Tracking and Notification (see page 63)

- Make sure you have set things up correctly.

Step 1: Prepare

Information Gathering

Before setting up compliance tracking in sfPMS, you'll need to gather the following information:

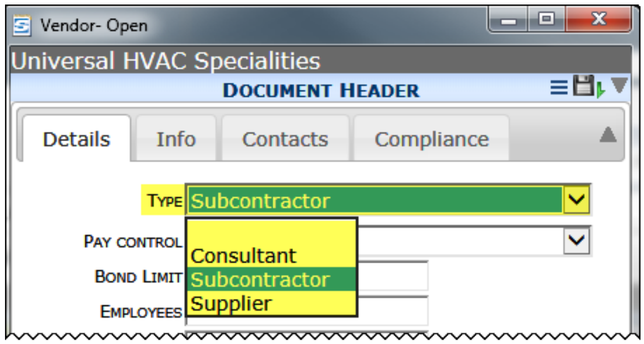
- What Compliance types does your company track?
- Which of these Compliance types are required and which are optional?
- Which of these Compliance types are tracked at the vendor level and which are tracked at the commitment level? Do you want to track lien waivers on Pay Request documents?
- Will all vendors require the same Compliance types? sfPMS allows you to assign Compliance types by Vendor subtype, so before assigning Compliance types to Vendors, you'll need to determine if you will create two or more Vendor subtypes and then build Compliance types for each Vendor subtype.
- Will all commitments require the same Compliance types? sfPMS also allows you to assign Compliance types by Commitment subtype, so before assigning Compliance types to Commitments, you'll need to determine if you will create two or more Commitment subtypes and then build Compliance types for each Commitment subtype.
  Note: Pay Requests inherit subtypes from their corresponding Commitments.
- Will you want to track certain requirements on Pay Requests (e.g., Lien Waivers) or Change Orders (e.g., Executed Contract Returned)?
- What text do you want in your Compliance Notification document?
- What persons or roles will receive the Compliance Notification document?
- Will you be routing the Compliance Notification via email, fax or hard copy and therefore need an Attachment template for Compliance Notification?
- What persons will be given the newly created "Compliance Staff" role?

Step 2: Code Maintenance

Assuming you use different types of commitments (subcontracts) and vendors, you may need to set up these subtypes in sfPMS, if subtypes were not already configured during implementation.

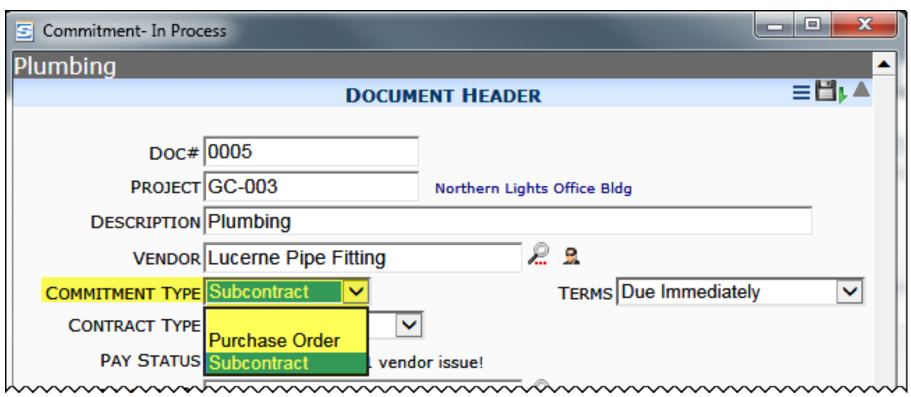
Vendor Subtypes

You will then be able to select a vendor subtype from a Vendor document's **Type** drop-down on the Details tab, as shown in below:



Commitment Subtypes

You will then be able to select a commitment subtype from a Commitment document's **Commitment Type** drop-down on the Document Header, as shown below:



Note: When a Pay Request document is created and linked to a Commitment, it will inherit its subtype from the Commitment.

Subtypes are created and defined through the Code Maintenance Tool.

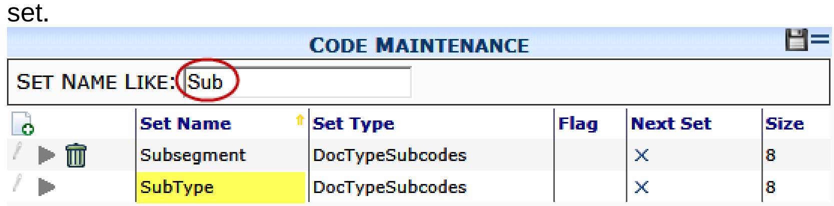
Code Maintenance Tool

The Code Maintenance tool is found on the System Admin Dashboard. For complete information about the Code Maintenance tool, see the *Focus on System Administration* guide.

Adding Vendor and Commitment Subtypes

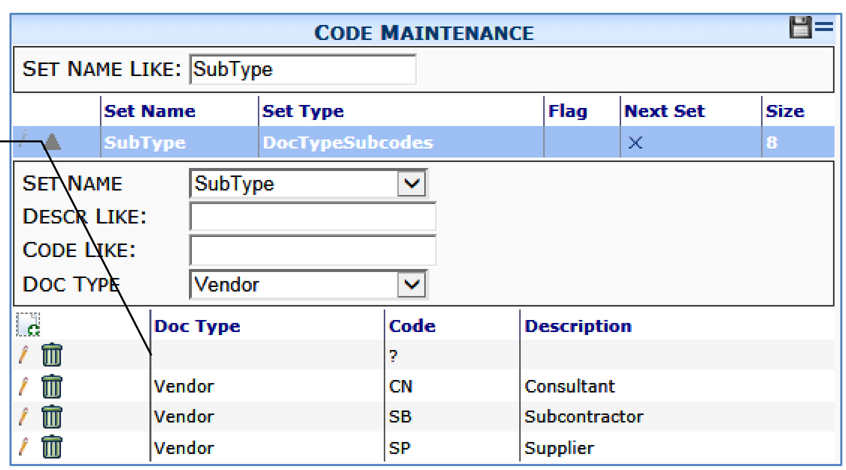
To add your Vendor subtypes:

1. Open the Code Maintenance tool on the System Admin Dashboard.
2. Enter **Sub** at the Set Name Like filter to get to the SubType code set.



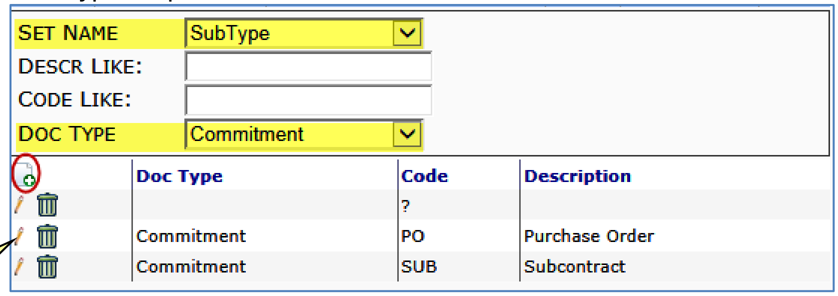
3. Click to get to Detail view for **SubType**.
4. Select **Vendor** from the Doc Type drop-down filter.
5. Click to add a vendor subtype.
6. Enter a one- to eight-character code in the **Code** field.
7. Enter a description for this code in the **Description** field.
8. Click to accept your new subtype.
9. Repeat steps 2 through 5 for each subtype.
10. Click to save your changes, for example:

Types and subtypes can include an empty choice, which appears first by default in the drop-down.



To add your Commitment subtypes:

1. Still in Detail view for SubType, select **Commitment** from the Doc Type drop-down filter:



If you want to edit any of the existing subtypes (to change the descriptions, for example), click , make your changes then click to accept the changes.

Notice that sfPMS ships with a few commitment subtypes. If you still want to add more, continue with the next steps.

2. Click to add a Commitment SubType.
3. Enter a one to eight character code in the **Code** field.
4. Enter a description for this code in the **Description** field.
5. Click to accept your new subtype.
6. Repeat steps 2 through 5 for each new subtype.
7. Click to save your changes.

Step 3: Customization

Adding Drop-down Fields and Tabs to Doc Types

Once you have set up your subtypes to be used on Commitment and Vendor documents, you need to make sure that these subtypes appear on the appropriate drop-downs on your documents (e.g., the Type or Commitment Type drop-downs as shown in the examples on page 39). In addition, if want to set Pay Control on the Commitment level, you need to add the Pay Control drop-down to the Commitment's Detail tab and, if you want to track lien waivers on your Pay Requests, you need to add the Compliance tab to your Pay Request Doc type.   Drop-down fields and Compliance tabs are controlled through the Customization tool.

Customization Tool

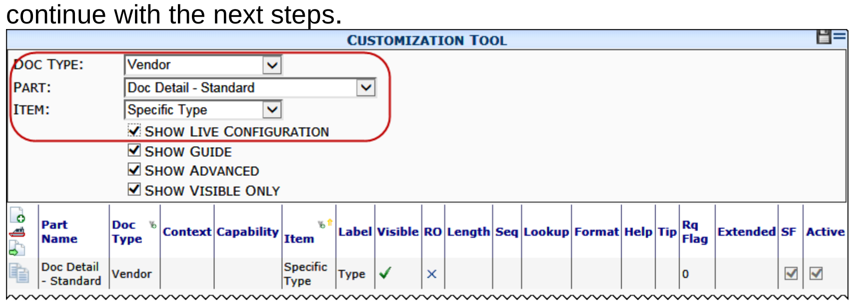
The Customization tool is found on the System Admin Dashboard. For complete information about the Customization tool, see the *Focus on System Administration* guide.

Customizing Doc Types

Vendor Documents

To edit the subtype drop-down on your Vendor Doc type:

1. In the Customization tool, select **Vendor** from the Doc Type drop-down.
2. Select **Doc Detail - Standard** from the Part drop-down.
3. Select **Specific Type** from the Item drop-down.
4. Click the **Show Live Configuration** checkbox. By default, the Vendor Doc type shows the Specific Type item. This is the drop-down that offers your commitment subtype options. If you like the label "Type," you need not change anything. Otherwise, continue with the next steps.



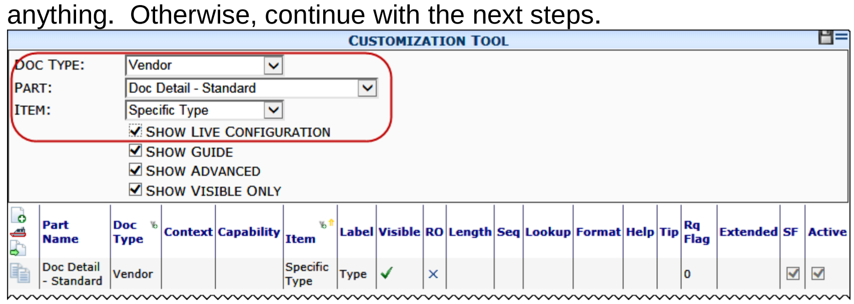
5. Click to copy the **Doc Detail Standard | Specific Item** row.

6. In the **Label** field, enter new text for the subtype field's label, for example, **Vendor Type.**
7. In the Visible and Active column, make sure that each is selected (☑).
8. Click ✔ to accept your entry.
9. Click to save your changes.

Commitment Documents

To edit the subtype drop-down on your Commitment Doc type:

1. In the Customization tool, select **Commitment** from the Doc Type drop-down.
2. Select **Doc Header - Commitment** from the Part drop-down.
3. Select **Commitment Type** from the Item drop-down.
4. Click the **Show Live Configuration** checkbox. By default, the Commitment Doc type shows the Commitment Type item. This is the drop-down that offers your commitment subtype options. If you like the label "Commitment Type," you need not change anything. Otherwise, continue with the next steps.

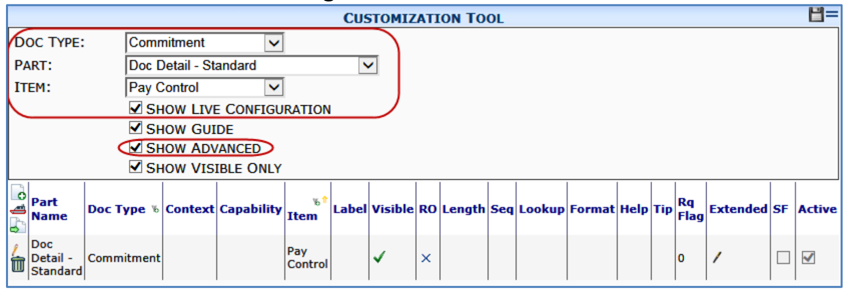


5. Click to add your own label for the commitment drop-down.
6. In the **Label** field, enter new text for the subtype field's label.
7. In the Visible and Active column, make sure that each is selected (☑).
8. Click ✔ to accept your entry.
9. Click to save your changes.

To make the Pay Control drop-down visible on the Commitment Doc type:

1. In the Customization tool, select **Commitment** from the Doc Type drop-down.
2. Select **Doc Detail – Standard** from the Part drop-down.
3. Select **Pay Control** from the Item drop-down.

4. Click the **Show Live Configuration** checkbox.



5. Click to copy the **Doc Detail – Standard | Pay Control** row.
6. In the Visible and Active column, make sure that each is selected (☑).
7. Click to accept your entry and to save your changes.

Pay Request Documents

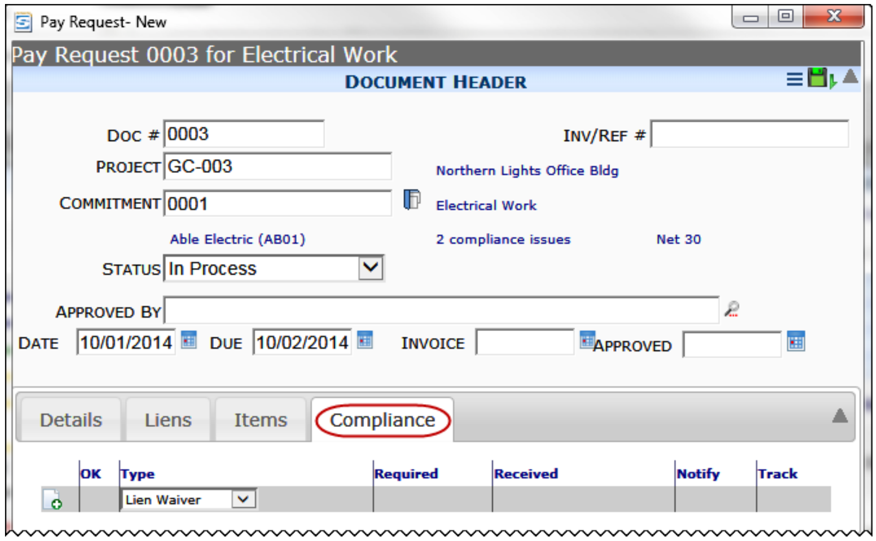
To add a Compliance tab to your Pay Requests:

1. In the Customization tool, select **Pay Request** from the Doc Type drop-down.
2. Select **Doc Tabs** from the **Part** drop-down.
3. Select **Compliance Tab** from the Item drop-down.
4. Click the **Show Live Configuration** checkbox.
5. (*If necessary*) Click the **Show Visible Only** checkbox to uncheck it. By default, the Pay Request Doc type does not have the Compliance Tab visible.

6. Click to copy the **Doc Tabs | Compliance Tab** row.
7. In the Visible and Active column, make sure that each is selected (☑).
8. Click to accept your entry and to save your changes.

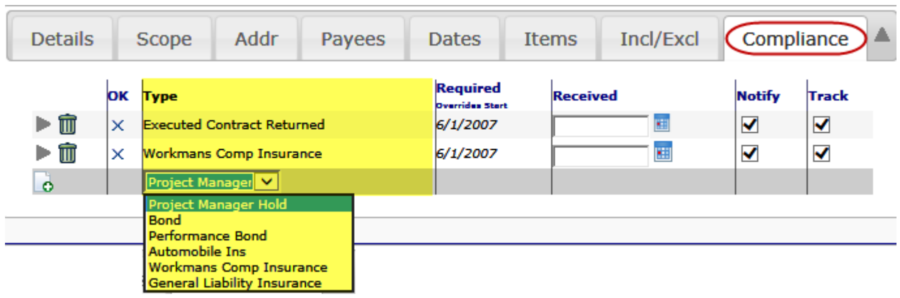
Your Pay Request documents will now show the Compliance tab, for example:

TIP
You can add Compliance tabs to other Doc types in the same way.


Pay Request- New
Pay Request 0003 for Electrical Work
DOCUMENT HEADER
DOC # 0003
INV/REF #
PROJECT GC-003
Northern Lights Office Bldg
COMMITMENT 0001
Electrical Work
Able Electric (AB01)
2 compliance issues
Net 30
STATUS In Process
APPROVED BY
DATE 10/01/2014
DUE 10/02/2014
INVOICE
APPROVED
Details
Liens
Items
Compliance
OK
Type
Required
Received
Notify
Track
Lien Waiver

Step 4: Compliance Types

A Compliance type defines the type of compliance requirement needed in your project, for example General Liability Insurance, Workman's Comp Insurance, etc. Common Compliance types are listed on page 22. Compliance types can be set up as required or optional for specific Doc types. You can edit default Compliance types and create new ones. These Compliance types show up on the Compliance tab of your document, for example:



Compliance types are created and edited through the Compliance Types tool.

Compliance Types Tool

The Compliance Types tool is found on the System Admin Dashboard (and the Manage Dashboard). For complete information about the Compliance Types tool, see the *Focus on System Administration* guide.

Editing Compliance Types

To edit an existing Compliance type:

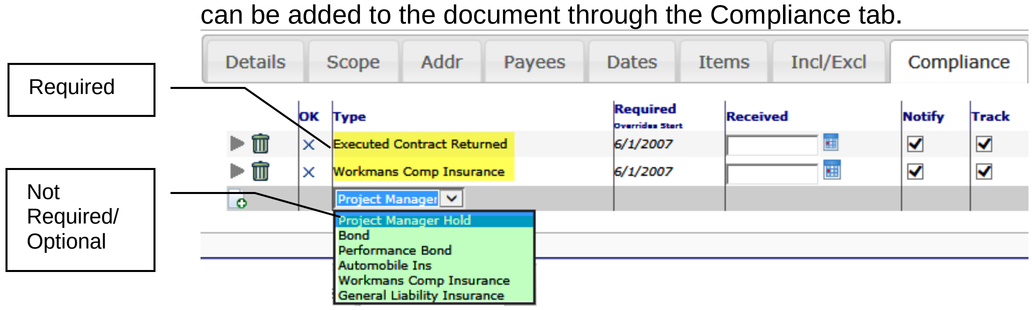
1. In the Compliance Types tool, use a filter to find the Compliance type that you want to modify.
2. Click ▶ at the Compliance type row.
3. Click ✏ to edit any of the fields for the Compliance type, including the Active checkbox.
4. Click ✔ to accept your changes or ✘ to ignore your changes.
5. Click 💾 to save your changes.

Mapping Compliance Types to Doc Types

You need to tell sfPMS which Compliance types are required and available for which Doc types. You do this by mapping each desired Compliance type to one or more Doc types.

To map a Compliance type to a Doc type:

1. In the Compliance Types tool, use a filter to find the Compliance type that you want to modify.
2. Click at the Compliance type row.
3. In the Mappings section, select a **Doc Type** from the drop-down or leave blank to indicate that the Compliance type should apply to all Doc types.
4. Click to edit the new row.
5. (*optional*) If the Doc type you selected has subtypes, select a Sub Type from the drop-down or leave blank to indicate that the Compliance type should apply to all subtypes.
6. (*optional*) If the Compliance type is to be optional on the Doc type + subtype, click the **Reqd** checkbox to uncheck it. Required Compliance types appear on the document's Compliance tab when the document is first created; optional Compliance types can be added to the document through the Compliance tab.



7. Leave the **Active** checkbox checked unless you want the Compliance type to be inactive for the designated Doc type + subtype.
8. Click to accept your row and to save your mapping.

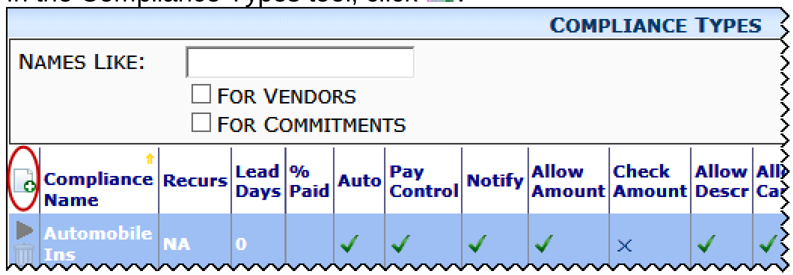
To edit your mapping:

- To edit an existing mapping, click .
- To delete an existing mapping, click .

Creating New Compliance Types

To add a Compliance type:

1. In the Compliance Types tool, click .



2. Give a descriptive name for your Compliance type at the **Compliance Name** field.
3. Fill in the remaining fields and checkboxes as desired.
4. Click to accept your row and to save.

Automatic Workflow

There is automatic workflow for the Compliance type. The commands in the automatic workflow tell sfPMS what to do whenever a Compliance requirement is out of compliance.

It is possible to replace the Spitfire-generated workflow script with one of your own, if you deem it necessary. For more information, see the "Compliance Type" chapter in the *Focus on System Administration* guide.

Step 5: Doc Type

Compliance Notification Doc Type

If you want a Compliance Notification document to be routed to an appropriate person whenever some requirement goes out of compliance, you'll need to activate the Compliance Notification Doc type. An example of a Compliance Notification document is found on page 33.

Doc types are activated (and disabled) through the Doc Types tool.

Doc Types Tool

The Doc Types tool is found on the System Admin Dashboard. Complete information about the Doc Types tool can be found in the *Focus on System Administration* guide.

Activating the Compliance Notification Doc Type

To activate the Compliance Notification Doc type:

1. In the Doc Types tool, click the **Show Inactive Doc Types** checkbox. The Compliance Notification Doc type will appear in the list:

DOC TYPES

DOC TYPE LIKE:

☑ SHOW INACTIVE DOC TYPES

Doc Type	Site Name	Project Dashboard	Create From Dashboard	Plan Room	Site Active	Custom
File Batch	AP Scans	×	×	×	×	×
AR Invoice	AR Invoice	✓	×	×	×	×
Bid	Bid	✓	✓	×	✓	×
Bid Package	Bid Package	✓	✓	✓	✓	×
Bid Package Addendum	Bid Package Addendum	✓	✓	✓	✓	×
Budget	Budget	✓	✓	×	✓	×
Cash Trans	Cash Trans	✓	×	×	×	×
Catalog File Router	Catalog File Route	×	×	×	✓	×
CCO	CCO	✓	✓	×	✓	×
Certificates and Approval	Cert & Appr	✓	✓	×	×	×
Change Item Register	Change Item Register	×	×	×	✓	×
Change Order	Change Order	✓	✓	×	✓	×
DSL Charge Entry	Charge Entry	✓	✓	×	×	×
Commitment	Commitment	✓	✓	×	✓	×
Compliance Notification	Compliance Notification	✓	×	×	×	×

2. Click to get to edit mode.
3. (*optional*) If you would like this Doc type to have a different name at your site, enter a new **Site Name**.
4. Leave the **Create From Project Dashboard** unchecked. Compliance Notification documents are created through automatic workflow (see page 48) so will not need to be created from the Project Dashboard.
5. Click the **Site Active** checkbox to make the Compliance Notification document type available at your site.
6. Click to accept your changes and to save.

Step 6: Rules

Compliance-NotificationText Rule

The **ComplianceNotificationText** rules are used to establish the text that will be used in the Introduction, Notification and Action parts of the Compliance Notification document. This text will also be included in any template-generated printout created for the document.

The ComplianceNotificationText rule is defined in the Rules Maintenance tool.

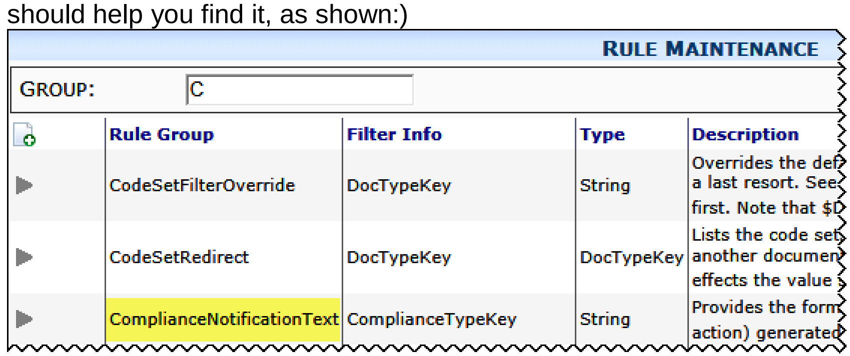
The Rules Maintenance Tool

The Rules Maintenance tool is found on the System Admin Dashboard. Complete information about rules can be found in the *Focus on System Administration* guide and the *Rules and Rule Values* technical white paper.

Establishing Text for Compliance Notifications

To use the ComplianceNotificationText rule:

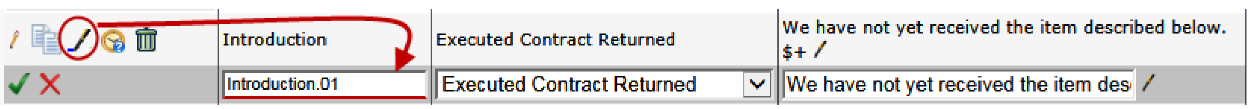
1. In the Rules Maintenance tool, enter a "**C**" in the **Group** filter and press the Enter key. (You could also type more of ComplianceNotificationText rule group in the filter, but "C" alone should help you find it, as shown:)



2. Click at ComplianceNotificationText rule group to open the Rule Entries for this rule.
3. From the drop-down, select **Introduction.**
4. Click .
5. Select a Compliance type from the **Filter Value** drop-down.

6. Enter the text of your introduction in the **Result Value** field. Your text can include placeholders (see page 54). This text will appear in the first Note of your Compliance Notification document for the specified Compliance type. **Note**: there is a 196 character limit in the Result Value field. If your text is longer than 196 characters, you'll need to:

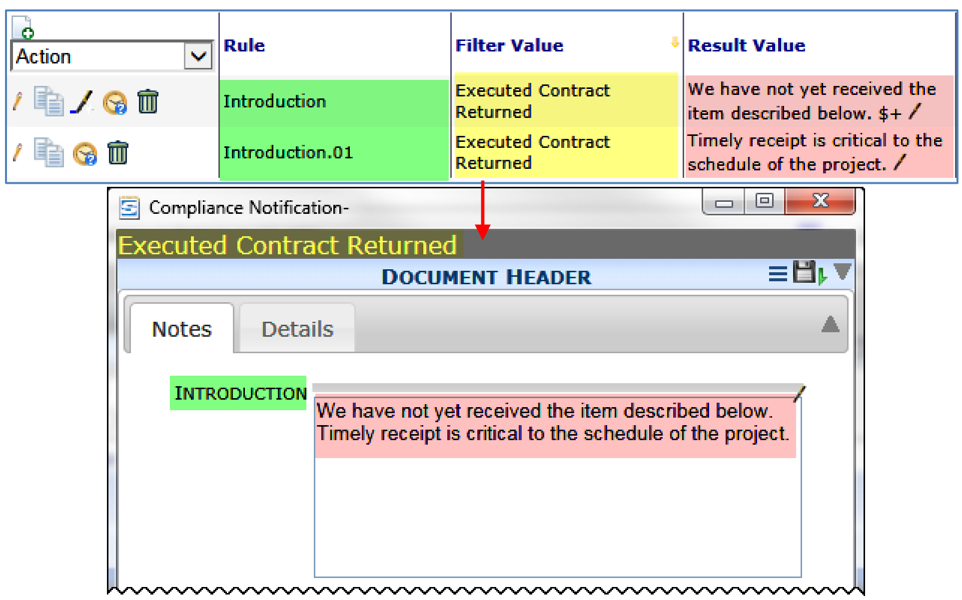
    - o Split your Result Value into smaller segments, each of any length up to 196 characters
    - o Append **$+** to the end of each segment, except for the last one.
    - o Click to accept the segment.
    - o For each segment, click on the row to extend the rule. The new rule that appears will have a name that indicates it is a continuation of the first rule, for example, Introduction.01.



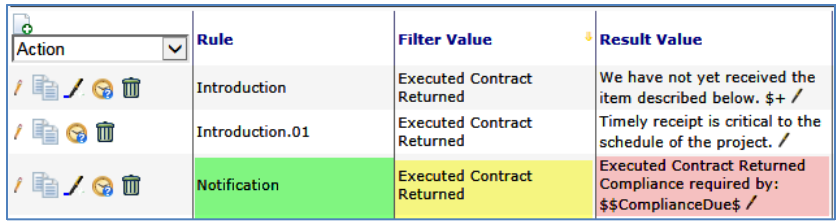
    - o Click at the Result Value to edit the text.
    - o Click to accept the segment.

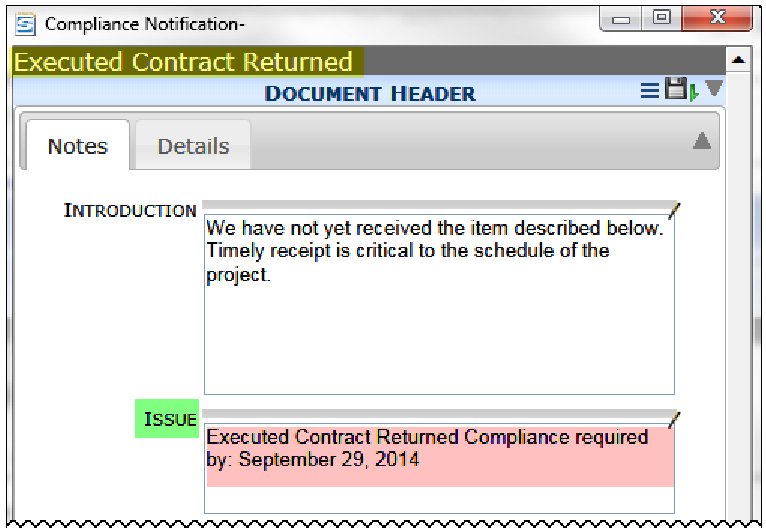
    When sfPMS sees the **$+ ,** it will merge the Result Values text, for example:

TIP
It is usually convenient to use $+ to break at a word or sentence boundary.

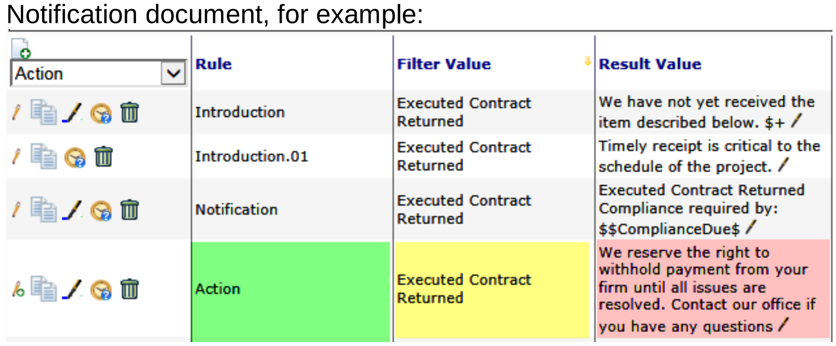


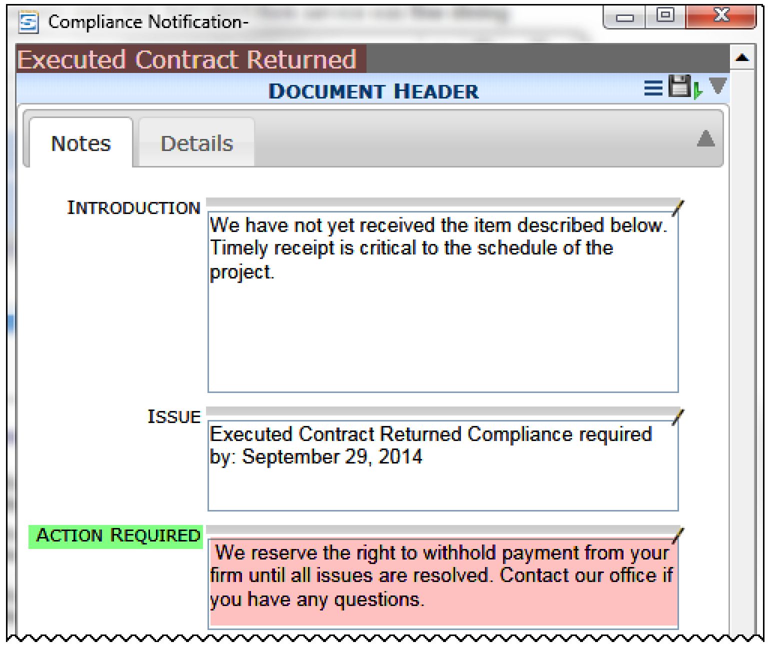
7. From the drop-down, select **Notification**.
8. Click again.
9. Select the same Compliance type in the **Filter Value** drop-down.
10. Enter the text for your notification in the **Result Value** field. This text will appear in the second Note of your Compliance Notification document, for example:





11. Click to accept your Notification.
12. From the drop-down, select **Action**.
13. Click again.
14. Select the same Compliance type from the **Filter Value** drop-down.
15. Enter the text explaining required action in the **Result Value** field. This text will appear in the third Note of your Compliance Notification document, for example:





16. Click to accept your Action.
17. Click to save all your text for this Compliance Type.
18. Repeat steps 3-18 until you have set up text for all your desired Compliance types.

Placeholders in the Text

Your Compliance Notification text can include the following placeholders:

Placeholder in text	***Is replaced by***
\n	A new line
$$ComplianceAmount$	The Compliance item amount, if any
$$ComplianceCarrier$	The Compliance item carrier, if any
$$ComplianceDescription$	The Compliance item description
$$ComplianceDue$	The Compliance item Required Date and time
$$ComplianceExpiration$	The Compliance item Expiration Date, if any
$$ComplianceName$	The Compliance Type name

In addition, you can use **\?** … **\?**. The section enclosed by \? is removed if the section includes empty replacements. For example: **\?Please provide a bond of $$ComplianceAmount$ as soon as possible\?**

will appear with an amount (e.g. **Please provide a bond of $1000 as soon as possible**) or not at all.

Step 7: Attachment (Auto) Template

Compliance Notification Printout

If the Compliance Notification document will be routed to someone via email or fax (or printed out in hard copy), you will need a template for the Compliance Notification Doc type. Most likely, this template will be of the type **Attachment (auto)** so that a printout will be generated automatically. Spitfire provides a distributed template that you can upload through ICTool.

Note: whether the Compliance Notification document is routed within Spitfire or is sent in PDF form through an email, fax, or hard copy depends on how you have set up routing for your subcontractors and vendors. For more information on routing, see the *Focus on Routes* guide.

The Templates Tool

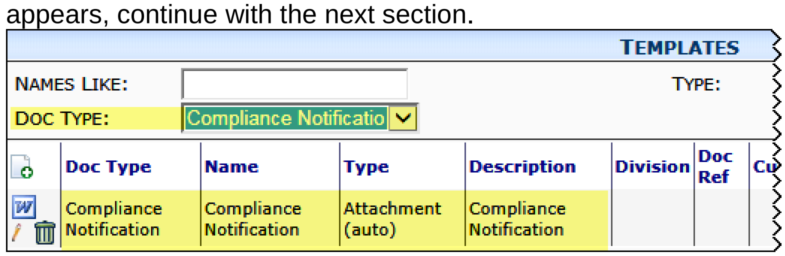
The Templates tool is found on both the Manage and System Admin Dashboards. More information about the Templates tool can be found in the *Focus on the Manage Dashboard* guide.

Look for a Template

It is possible that an Attachment (auto) template for Compliance Notification documents was uploaded into your system during implementation. You should look to see if you already have the template file.

To find a template for Compliance Notifications:

1. In the Templates tool, select **Compliance Notification** from the **Doc Type** drop-down.
2. If a template is listed for the Compliance Notification Doc type (as shown below), you need not do anything else. If no template appears, continue with the next section.



Upload from ICTool

If no template was uploaded into your system during implementation, you can upload the distributed Compliance Notification template from the Spitfire Installation and Configuration tool (ICTool.exe).

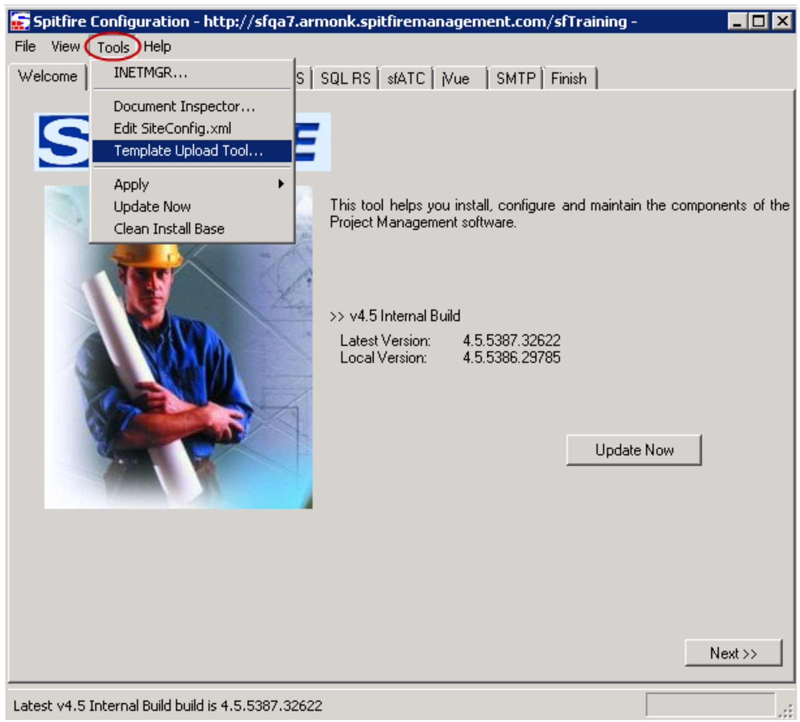
Note: ICTool is a stand-alone tool outside of the Spitfire Dashboard. If you do not have access to ICTool, contact Spitfire Support, who can upload the template for you.

TIP

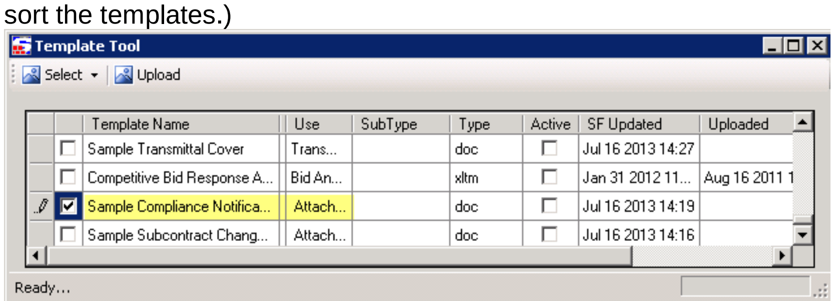
If you choose to create and upload your own template instead of the distributed template, keep in mind that the automatic workflow will make the last person on your route the first ("from") person and therefore, you can use the FromAddr_ bookmarks in your template.

To upload the distributed Template:

1. Open ICTool and select **Template Upload Tool** from the Tools menu:



2. Look for and check the **Compliance Notification** Attachment (auto) template. (You can click on the Template Name header to sort the templates.)



3. Click the 

button.
4. Close ICTool.

5. Go to sfPMS and open the Templates tool on either the Manage or System Admin Dashboard.
6. In the Templates tool, click the **Doc Type** checkbox and select **Compliance Notification**. The newly uploaded Doc Template will be listed.

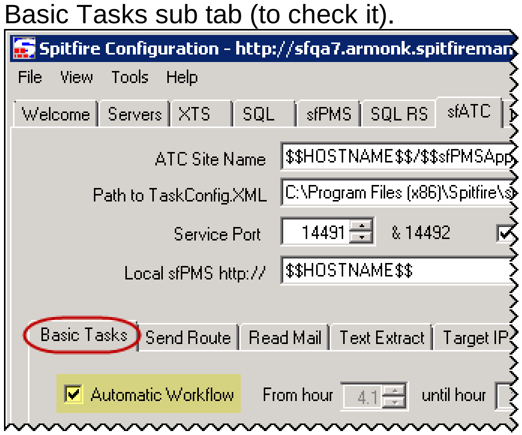
Step 8: Spitfire Configuration

If you will use an automatic workflow for a Compliance type, you need to ensure that Automatic Workflow is turned on in the Spitfire Installation and Configuration tool (ICTool.exe).

ICTool

To turn Automatic Workflow on in ICTool:

1. Open ICTool and select the sfATC tab.
2. If necessary, click the **Automatic Workflow** checkbox on the Basic Tasks sub tab (to check it).



3. Click ☒ to close ICTool.

Step 9: Roles

Because compliance tracking is not limited to specific projects, it is wise to create a Spitfire role to give to the person(s) who will receive Compliance Notification documents—for example, the office assistant in charge of compliance management.

Roles are created in the Roles tool.

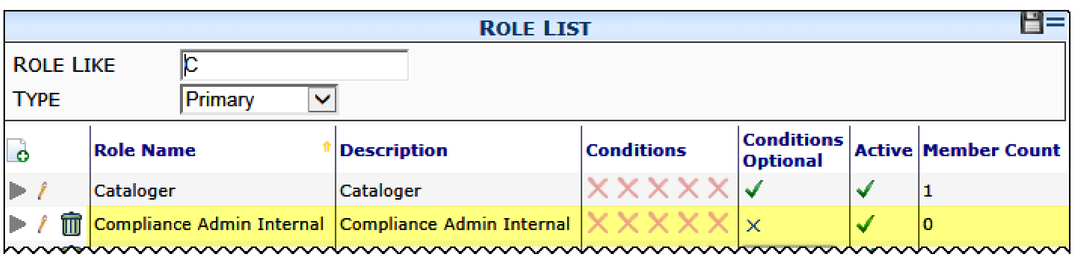
Role Tool

The Roles tool is found on the System Admin Dashboard. More information about roles can be found in the *Focus on System Administration* guide, the *Focus on Contacts* guide and the technical white paper *Designing User Roles*.

Creating a Role

To create a “Compliance Staff” role for Compliance management:

1. At the Roles tool, click to add a new row.
2. In the Role Name field, type a name for the role, for example, **Compliance Staff**.
3. Click to accept your entry and to save your changes.



Note: you can add capabilities to this role; however, you do not need to. This role is primarily for identification purposes. It is assumed that the person who receives this new role will also be given a capability-based role that will govern his or her access level in sfPMS.

Step 10: Routes

Predefined Routes

When some requirement in your project is out of compliance, you will want the right people to receive the Compliance Notification document. You can create a predefined route that will be added to the Compliance Notification document automatically whenever it is created. The Compliance Notification document will then be routed to your specified list of people. If the document is routed to someone via fax or email, the printout generated by the **Attachment (auto)** template will be sent.

Predefined routes are created through the Routes tool.

The Routes Tool

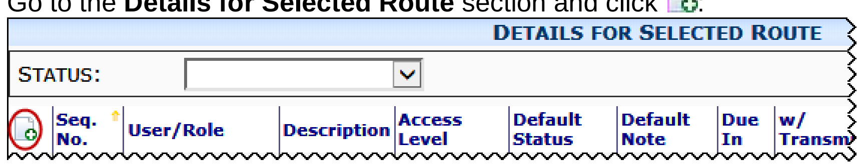
The Routes tool is found on the Manage Dashboard. Routes and routing rules can be involved. Complete information about predefined routes can be found in the *Focus on the Manage Dashboard* guide.

Creating a Predefined Route for Compliance Notification

TIP
The last person on your predefined route will be considered the first, and therefore, "From" person for the Compliance Notification document. Keep this in mind when setting up your routees (and when designing your template).

To create a predefined route for Compliance Notification:

1. On the Route List, click .
2. In the Route Name field, enter a name for your new route, for example, **Compliance Notification.**
3. Click to accept your Route name then click at the top of the Route List to save your Route name.
4. Click to open the details for your new route. (You may have to look for it.)
5. Go to the **Details for Selected Route** section and click :

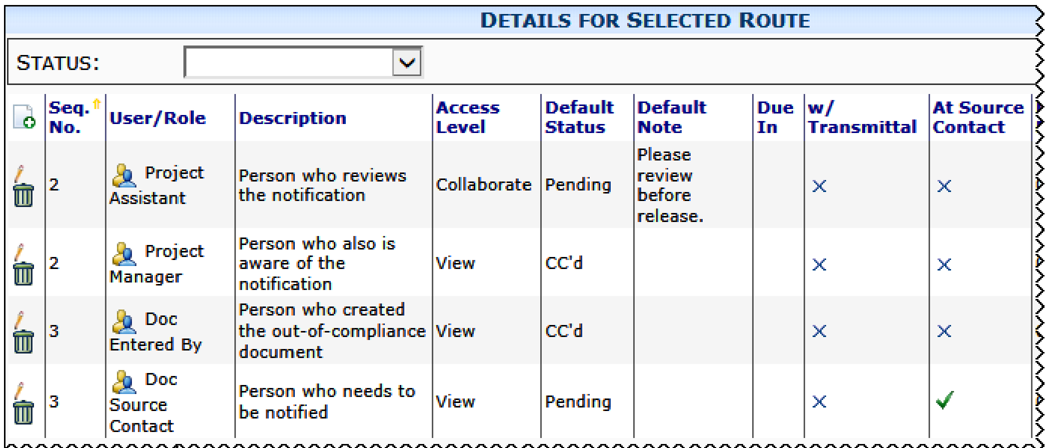


6. (*optional*) Click to switch the User/Role lookup to Roles. Roles are preferred over individual names in predefined routes.
7. Click to look up the first role on your route. This could be the role of the person who reviews the Compliance Notification document and perhaps adds to it before it goes to the person who needs to be notified of the out-of-compliance requirement (for example, the Compliance Staff–or equivalent--role that you created on page 59).

8. (*optional*) If you want to ensure that the routee will be able to edit the document, change the Access Level to **Collaborate**.

9. Enter other information for your first routee then click to accept your information.

10. Click to enter each routee you want to add, depending on how Compliance Notifications are to be handled in your organization. Remember to click to accept each routee. You are building the route for the Compliance Notification document, for example:



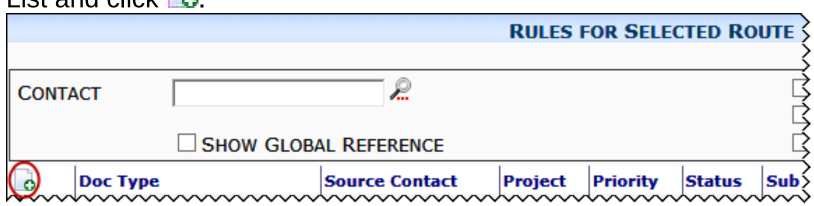
DETAILS FOR SELECTED ROUTE

STATUS:

	Seq. No.	User/Role	Description	Access Level	Default Status	Default Note	Due In	w/ Transmittal	At Source Contact
	2	Project Assistant	Person who reviews the notification	Collaborate	Pending	Please review before release.		×	×
	2	Project Manager	Person who also is aware of the notification	View	CC'd			×	×
	3	Doc Entered By	Person who created the out-of-compliance document	View	CC'd			×	×
	3	Doc Source Contact	Person who needs to be notified	View	Pending			×	✓

In this example, the Compliance Notification document will be routed to a Project Assistant with a Courtesy Copy to the Project Manager. When the Project Assistant sends the document on, the Compliance Notification document will be routed to the Source Contact (Vendor) with a Courtesy Copy to the person who entered the document that has the out-of-compliance item.

11. Go to the **Rules for Selected Routes** section below the Route List and click .



12. Select **Compliance Notification** from the Doc Type drop-down list.

13. (*optional*) Add other conditions for your route, if desired.

14. Click to accept your rule.

15. Click to save your predefined route.

Step 11: Contacts

If you have created a new role (such as Compliance Staff) and used it in a predefined route (as described in the previous chapter), you need to give that role to one or more Spitfire users. You do this through the Contacts Dashboard.

The Contacts Dashboard

The Contacts Dashboard and corresponding Contact list is described in detail in the *Focus on Contacts* guide.

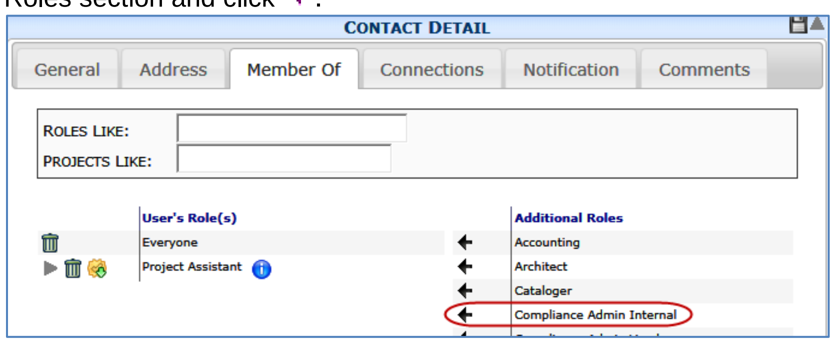
Note: these instructions assume that your subcontractors and vendors were added to sfPMS during implementation.

Giving a Contact a Role

You can give the Compliance Staff (or your equivalent) role to any Contact; however, since this person will be getting Compliance Notification documents in the Inbox, the person should be a Spitfire User.

To give a Contact the "Compliance Staff" role:

1. Go to the Contact view on the Contacts Dashboard.
2. Using the filters if helpful, find the Spitfire user whose Details you want to edit and click .
3. Click the **Member Of** tab.
4. Find the role you want (e.g., Compliance Staff) in the Additional Roles section and click .

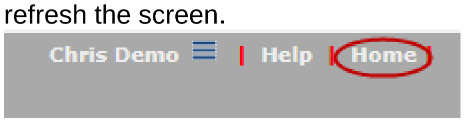


5. Click to save your changes and to return to the Contact list.

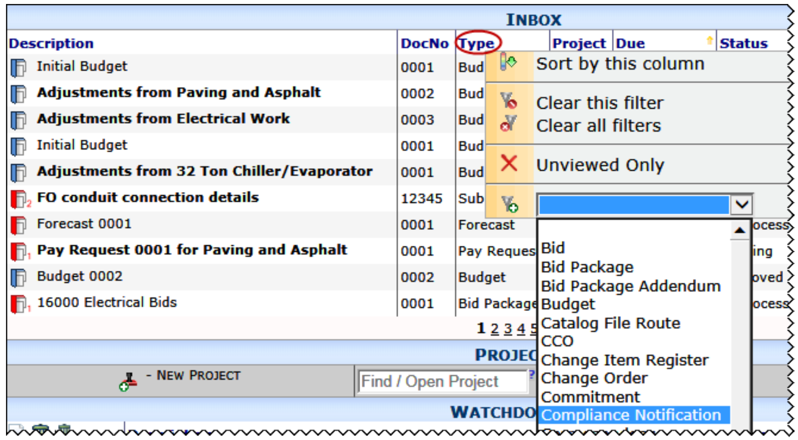
Step 12: Test

You can run through this test to see if all is working as you expect. If there are problems, go back over all the steps to see if you missed anything.

To test Compliance tracking and notification:

1. Create a test Commitment document. If you have set up Compliance requirements for a Commitment subtype, be sure to select that subtype at the **Commitment Type** field.
2. Look up a **Vendor**.
3. Click to save the document.
4. Click on the Compliance tab and either click to edit a required Compliance item or select a Compliance Type then click to add an optional Compliance item.
5. Enter a **Required** date that is past (for example, yesterday).
6. Click to return to grid view. There should be an **X** in the OK column of the Compliance item.
7. Change the status to **Committed**.
   Note: A Commitment must have a status of Committed for Compliance tracking to check it.
8. Click to save the document. The Pay Status field on the Document Header should mention at least one compliance issue.
9. You can close the Commitment document window.
10. Have the person who is to review the Compliance Notification document check his or her Inbox. If the document does not appear right away, click **Home** in the upper-right corner to refresh the screen.
    

    If the document still does not appear, wait 45 minutes then check again.
    Note: if there are many documents in the Inbox, filter on Doc type to find the Compliance Notification document.



11. Open the Compliance Notification document and go to the Attachments tab.
12. Find the template printout and view it. Verify that the correction information is on the printout.