Technical White Paper

Designing User Roles

www.spitfiremanagement.com

Revision Number: 2018.02

Spitfire Management, LLC.

www.spitfiremanagement.com

Table of Contents

Introduction

Spitfire Contacts include all your Customers, Vendors, and Employees, plus any other person who may have some relationship to your projects. In the Spitfire Project Management System (sfPMS), a Contact can be assigned as a “responsible party” on an Item, a routee or meeting attendee on a Spitfire document, or a project team member on the Project Dashboard.

Access to sfPMS is granted by assigning a login ID and password to the Contact, thus making that Contact a Spitfire user. Making a Contact a member of a role allows that Contact specific access rights in Spitfire. In addition, assigning a role to Spitfire and non-Spitfire users allows you to identify those Contacts’ project responsibility.

The *Focus on System Administration* guide gives you detailed steps on how to use the Role tool. The *Focus on Contacts* guide describes how to assign those roles to Contacts.

This technical white paper explains concepts and describes how roles are built up.

After understanding concepts, see the Designing User Roles page on support.spitfirepm.com for links to all the capabilities available for your roles.

Note: modifying or creating roles requires the complete, customizable version of the Spitfire Project Management System.

Overview of Roles

Functions

A role has two functions:

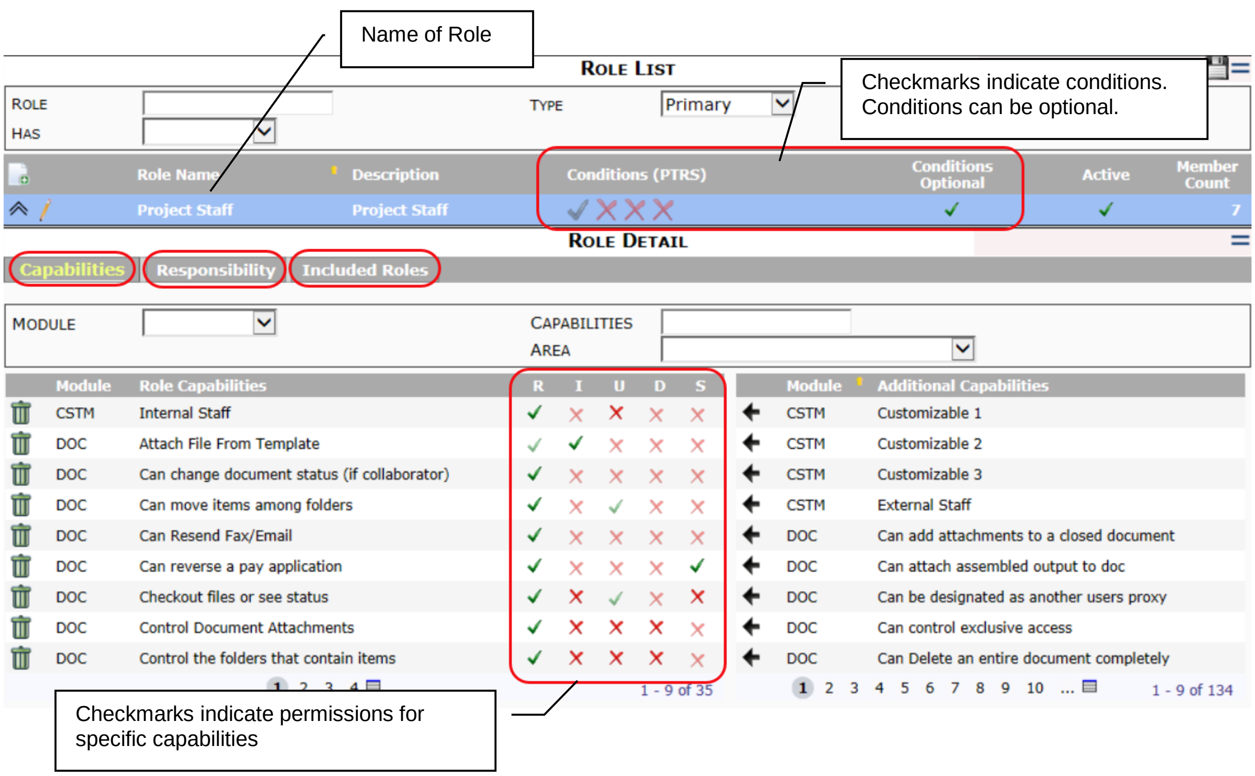
- First, it is a collection of capabilities that grants a Spitfire user specific access rights to Spitfire functions and data.
- Second, it identifies a responsibility within a project. By identifying a Contact's responsibility on a project, the routing system can successfully resolve role-based routes. In addition, various reports in sfPMS use this information.

Components

Roles consist of five components:

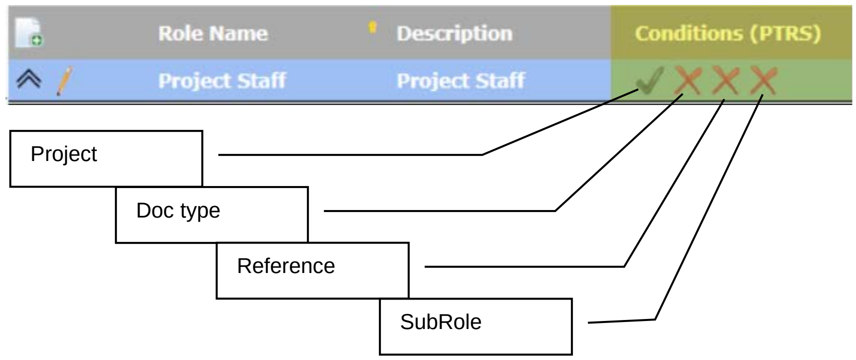
- **Conditions**, which can limit the role to a specific Project, Doc Type, Reference, Document or SubRole.
- **Capabilities**, which define access to a specific parts of the system.
- **Permissions**, which defines the level of access to a specific part.
- **Responsibilities**, which identify the role within a project.
- **Included Roles**, which indicate any SubRoles for the role.

For example, a role could include the Document Access capability and the permissions to read and insert (create new) documents with the condition to limit the capability to a specific project.



Conditions

Conditions allow you to limit your role to a specific component. When you create a role, you can select which condition should be used to limit that role. Later, when you assign the role to a Contact, you select the limiting factor. For example, if you limit your Project Manager role by the “project” condition, you can select which project a Contact will have access to when you assign the Project Manager role to that Contact.

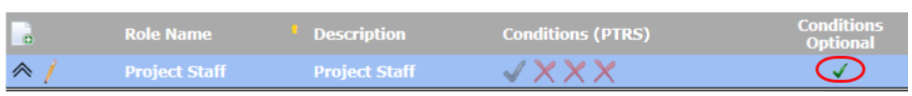


Conditions allow you to limit the role to a specific project, Doc type, or reference. It also allows you to designate the role as a SubRole (see page 9).

When you begin creating your system’s security, you’ll use the building block approach. A Contact can be assigned multiple roles. SubRoles can be included in primary roles.

Conditions Optional

When you limit a role by condition, you can also choose whether all Contacts who are assigned the role must be limited by the condition, or whether the condition can be optional for some Contacts.



For example, if you limit a role by project, but keep the condition optional, one Contact can be assigned the role with the project limitation removed (meaning “all projects”) and another Contact can be assigned the role for a specific project only. If the Conditions Optional flag is ✕, however, all Contacts must be limited by project.

Capabilities

Capabilities are grouped into modules; this grouping makes capabilities easier to review and select. Capabilities are divided into the following modules:

- **CSTM**: Configuration capabilities, meant to be used in the UI Configuration tool.
- **DOC**: elements on a Spitfire document (add Attachments, view Attachments, move Items among folders, etc.)
- **LIST**: all rather than assigned elements, such as all contacts, all projects, etc.
- **PAGE**: a Spitfire browser page (e.g., document page, Project Dashboard page, etc.)
- **PART**: parts of a Spitfire dashboard (e.g., Project List, Photo, Key Performance Indicators, etc.)
- **SYS**: access to Spitfire from Web services; usually used by the system's various programs like sfATC (OCR graphic files, etc.) Also tasks reserved for the System Administrator.

Permissions

Permissions allow you to define the level of access for a capability. Permissions for each capability are indicated through **RIUDS** checkboxes. Some capabilities require only an **R** permission, some capabilities require an **R** permission and another permission (**IUD** or **S**) and other capabilities offer flexibility so that more or less permissions can be given. Often (but not always), RIUDS means

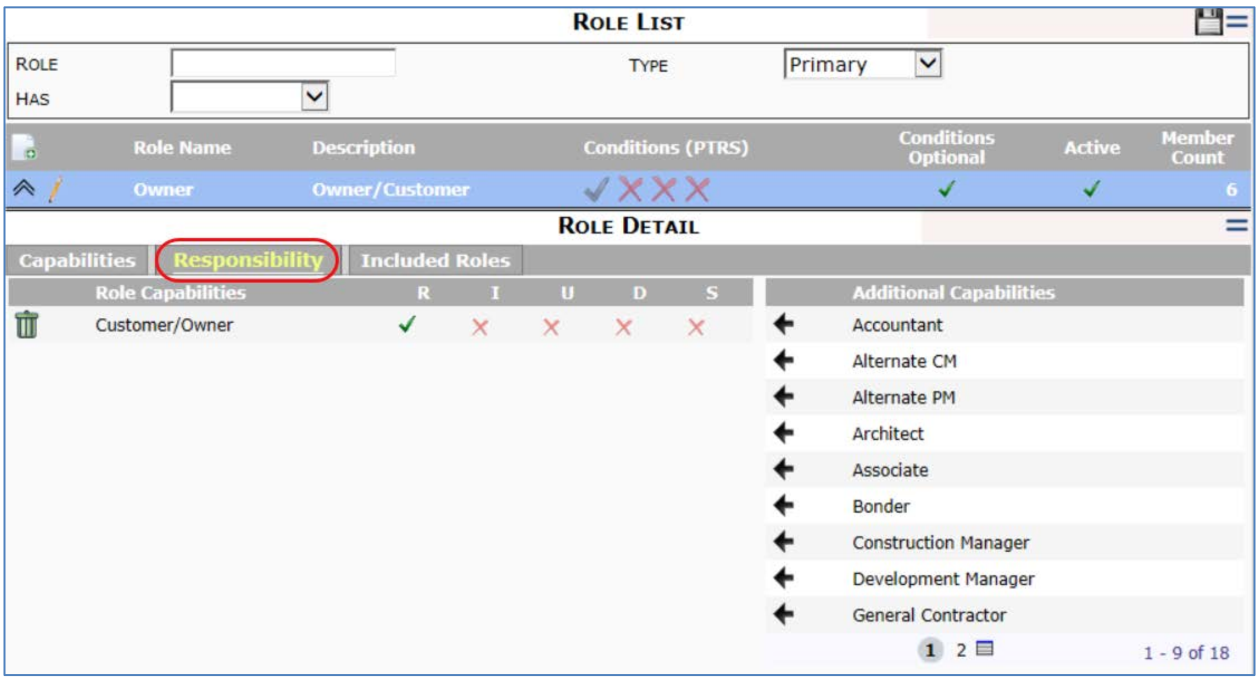
- **R**ead—allows a user to view the specific element covered by the capability.
- **I**nsert—allows a user to create a new element covered by the capability.
- **U**pdate—allows a user to change or edit the specific element covered by the capability.
- **D**elete—allows a user to delete the specific element covered by the capability.
- **S**pecial—allows the user something specific to the capability; only a few capabilities have the Special permission.

Role Capabilities	R	I	U	D	S
Internal Staff	✓	✗	✗	✗	✗
Attach File From Template	✓	✓	✗	✗	✗
Can change document status (if collaborator)	✓	✗	✗	✗	✗
Can move items among folders	✓	✗	✓	✗	✗
Can Resend Fax/Email	✓	✗	✗	✗	✗
Can reverse a pay application	✓	✗	✗	✗	✓
Checkout files or see status	✓	✗	✓	✗	✗
Control Document Attachments	✓	✗	✗	✗	✗
Control the folders that contain items	✓	✗	✗	✗	✗

Responsibilities

The Responsibility tab is used to identify a Contact's project responsibility. Since roles can be created by users, sfPMS uses responsibilities for the software's business logic.

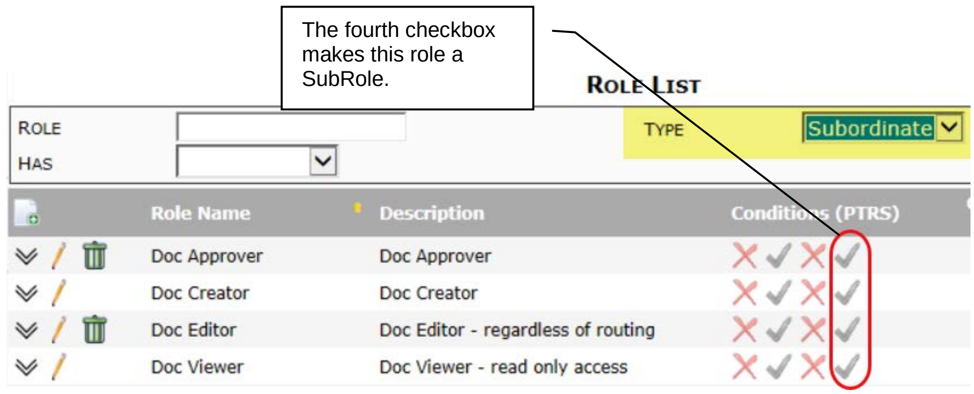
For example, you could create a role named Client, or Customer, or Owner. You and your users would understand that a Contact with this role is the person paying the bill on this project. Unfortunately, sfPMS cannot recognize your custom role name as easily as your users can, but when you add the responsibility of "Customer/Owner" to your role, the software can immediately recognize that this Contact on the Project's Contact list is the person paying the bills.



- A role can have only one responsibility.
- All possible responsibilities are provided by sfPMS.

Included Roles (Subordinate Roles)

Using the building block approach allows you to define a role as a subordinate role and then use within a primary role. Later, if the subordinate role is modified, your change will affect all the primary roles in which it is a part. You designate a role as a subordinate role through the fourth Condition checkbox:



For example, the role called Doc Creator (above) is limited by DocType and is to be used as a subordinate role. This Doc Creator role includes all the capabilities and permissions required to create a Spitfire document. Later, Doc Creator can be included in primary roles, such as Project Manager and Project Staff.

To continue with the example, Doc Creator can be included in the Project Manager role without a Doc type limitation (because Conditions Optional = ✓).

In the Project Staff role, Doc Creator can be included and limited to the Team and RFI Doc types.

Note: **Doc Approver**, **Doc Creator**, **Doc Editor, Doc Viewer** and **Subcontractor Base** are distributed subordinate roles.

Concepts

Access to a Routed Document

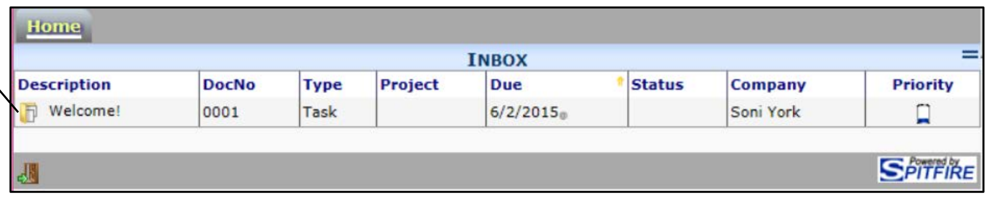
If a user is given minimum access to Spitfire, that user will have some automatic rights if a Spitfire document is routed to him or her.

In order for a user to be able to see the Home Dashboard after logging into sfPMS, that user must have the **PAGE | Home Dashboard** capability with the **R** permission. This one capability allows users to view Spitfire documents that have been routed to them and any Watchdog Alerts sent to them.

Below are screen shots of what users see if they have only the **PAGE | Home Dashboard** capability in an assigned role:

A document has been routed to the user.

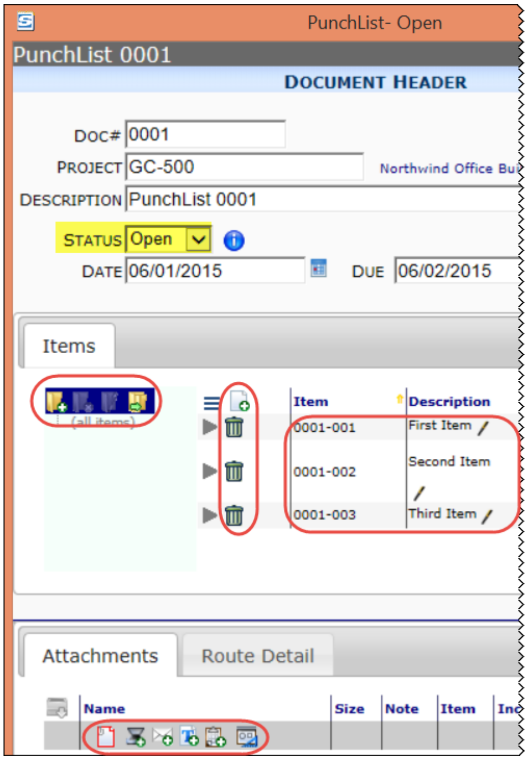
The Home tab is the only tab unless other capabilities are given.



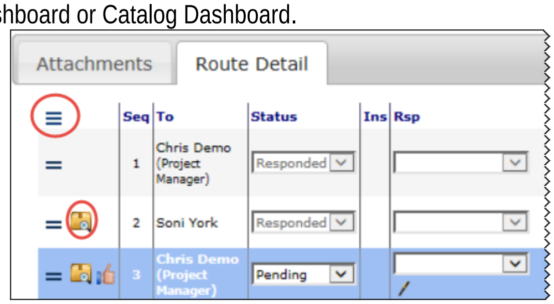
If a Spitfire document is routed to the user's Inbox, he or she automatically has the access rights to view that document. In addition, the user has access to any files attached to the routed document. Following are screen shots comparing what the document's creator (who has been given full access rights to the document) and what the recipient (who has minimum access rights) sees when each opens the document.

Full Access Rights

Notice that the user has the ability to edit the document and can add new Attachments. In addition, on the Items tab, all Items are visible and can even be deleted. And the user can create folders.

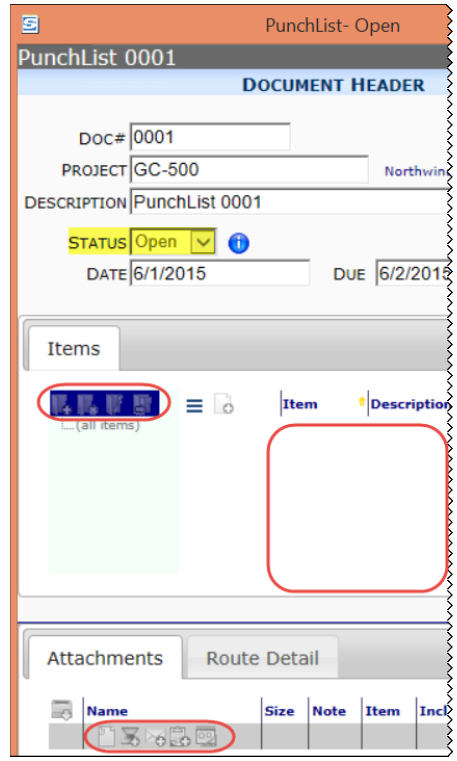


On the Route Detail tab, the user can view all routees, add new ones, delete upcoming ones and review the content sent to a previous routee. Once the user sends the document on its route, he or she can access the document later from either the Project Dashboard or Catalog Dashboard.

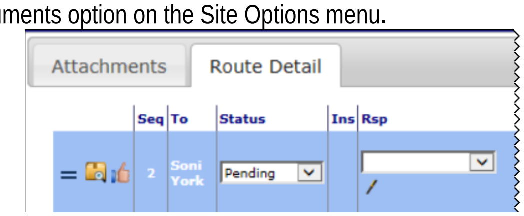


Minimum Access Rights

Notice that the fields are read-only (see Status) and that the user cannot add new Attachments. In addition, Items are not visible, and the Item Folder's toolbar is inactive.



On the Route Detail tab, the user sees only his/her route line and cannot add to or edit the routing list. Once the user sends the document on its route, the document will no longer be in the user's Inbox on the Home Dashboard. Therefore, the user will no longer have access to the document, except through the Recent Documents option on the Site Options menu.



Updating a Document

A user with minimum access will not generally be able to update documents routed to him or her. However, other factors come into play with regard to updating a document.

- A user who has been given permission to create documents of a particular Doc type can also be given the capability to “own” all such documents through the **DOC | Owns documents created, routed, global** capability. As the owner of a document, the user would then be able to update the document and in particular do the following:
  - Change the document title at any time,
  - Change a confidential document to no longer be confidential,
  - Add attachments to the document at any time, even after the document has been closed,
  - View all Items at any time.
  - View all routes at any time.
- A user who is given Collaborator status on a particular document can update that document while it is in his/her Inbox. (See the *Focus on Routes* guide for more information.)
- A user with a role that has been designated as a proxy for another user, who has update permission for certain or all documents, will also be able to update those documents.
- A user given the U permission on the **PAGE | Document Access** capability can update documents. [**Important**: This is **not** recommended because the permission overrides many of the other permissions on other capabilities.]
- A user given the U permission on the **DOC | Permissions for any item on the document** capability can update the Items on documents.

Using Roles for Routing

This second function, identifying a Contact’s responsibility within a project through the role, is the more elusive function, yet it is a very powerful function that will be key in your decision on which roles to create and assign to Contacts.

Each Project Dashboard includes a Team Contacts part. This Team Contacts part lists the Contacts that are assigned or associated with the project. Some of the Contacts will be Spitfire users; others will not be.

TEAM CONTACTS				
	Name	Company	Phone	Role
	Jack McSwag	Spitfire Construction	(914) 273-0809	Project Manager
	Jason Sunderson	Able Electric Corp	(555) 555-1212	Subcontractor
	Chris Demo	Spitfire Management	(203) 952-6552	Superintendent
	Ken Lathe	Universal HVAC Specialities	(914) 273-7263	Subcontractor
	Northern Lights	Northern Lights	(555) 555-1212	Owner

Throughout your project's life cycle, Spitfire documents will be created and routed to these Contacts. To accomplish this routing workflow, you have two choices:

1. Require the document's creator to manually add named individuals to each document.
2. Create predefined routes for documents that the document's creator can edit as needed. (For information on creating predefined routes, see the *Focus on the Manage Dashboard* guide.)

For example, if the following route

Seq. No.	User/Role
2	Project Manager
3	Subcontractor
4	Owner
5	Doc Entered By

were applied to the Contact list shown above, the result would be the following routees:

Seq 1 *Doc Entered By* = whoever created the document (Seq 1 is always automatic)

Seq 2 Project Manager = **Jack McSwag**

Seq 3 Subcontractor =**Jason Sunderson** and **Ken Lathe** (the document would be routed to both at the same time).

Seq 4 Owner = **Northern Lights**

Seq 5 *Doc Entered By* = whoever entered the document.

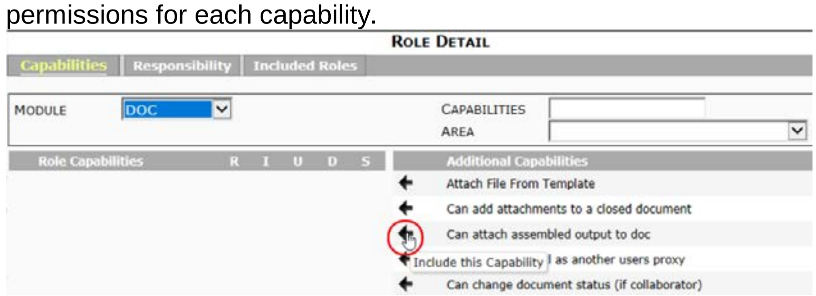
Bottom Line: When you plan your roles, you'll need to consider your company's workflow and how your documents will be routed. Building predefined routes based on roles is the most efficient way to set up a workflow policy and to route your documents accordingly.

Combining Concepts

Step One: Identify your company's needs. You will need to create and use enough roles to facilitate your company's workflow and routing.

Step Two: Through the Roles tool on the System Admin Dashboard do the following:

- Create new roles as needed. Spitfire ships with a few default roles.
- Add conditions to your roles that can be applied when the role is assigned to a Contact. Consider the focus of the role. For example, is it a project-focused or document-focused role?
- Create subordinate roles for specific functions (e.g., document authoring) or specific groups (e.g., your office employees, your field employees).
- Decide whether conditions (if any) will be mandatory or optional.
- Add or edit role capabilities and assign the appropriate permissions for each capability.

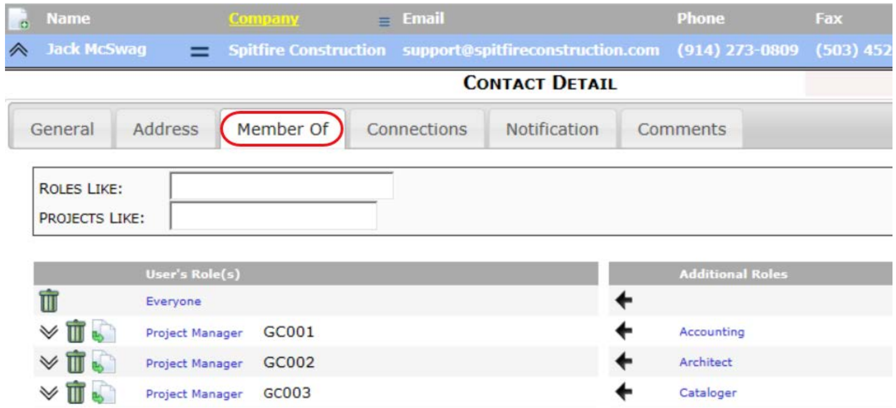


TIP
For a complete list of available capabilities and which permissions they accept, and what those permissions mean, see Designing User Roles on support.spitfirepm.com.

Note: In most capabilities, permissions work independently of each other so, for example, you can give a user **I**nsert and **D**elete but not **U**pdate permission for some capability, or only **U**pdate without **I**nsert permission for another capability. Some thought should be given when assigning capabilities so that correct permissions are granted. In all cases, the **R** permission should be given.

- Assign responsibilities to your Roles depending on the purpose of each role within a project.

Step Three: Through the Contacts tool, assign roles to your Contacts. Remember to limit roles to a specific project or Doc type when assigning roles, if appropriate. A Contact can have several roles. (See the *Focus on Contacts* guide for more information.)



TIP

If you want to limit access to projects on the Executive Dashboard based on a Project Manager's assigned projects, give the Project Manager role the Responsibility of Project Manager and the PAGE | Executive Dashboard capability but not the PART | Executive Project Summary .

Warning! Some capabilities cannot be limited and therefore should not be included in a role that is limited to a project or Doc type.

For example, the **PAGE | Executive Dashboard** and the **PART | Executive Project Summary** capabilities include all projects. If you include these capabilities in a role that is then limited by a Project, you will nullify access to the Executive Dashboard and the Executive Project Summary.