Service Provider
Systems Administration

User Manual

Table of Contents

About This Document 4

Purpose 4
Intended Audience 4
Document Control 4

Emersion® Umbrella System 5

Introduction 6

Document Conventions 7

Assumptions Made 7

Emersion® Security System 8

SSL Encryption 8
User Login Features 8
Gatekeeper 8
Permission System 8

Permission System Basics 9

Organisational Units 10
Roles 10

Managing Users 13

View Staff / Login Users 13
Create New Staff / Login Users 16

Managing Permissions 18

Managing Roles 25

Further Information 30

Emersion 30
Emersion Web Site: 30

Notes 31

About This Document

Purpose

The purpose of this document is to describe the operation of the Emersion Systems Administration Module (SAM) and the Permission Management System (PMS). Other Emersion User manuals will describe the use and operation of other system modules, such as the Entity Management System and Billing Sub-System, which may be mentioned of referred to within this manual.

This manual outlines the processes and procedures that need to be followed by a Service Provider (SP) to setup, manage and maintain Cumulus Login Users and other Settings for their Service Provider.

Intended Audience

The audience for this User Manual are Service Provider Administrators who manage the Users and Service Providers Systems Settings within the Emersion System.

Document Control

Version	Date	Description	Author
0.1			
0.2			
0.3			
0.4	24/09/09		Jim Ritchie
0.5	25/09/09	Review	John Caval
1.0	27/09/09	Adding and Managing Staff Users and general introduction added.	Paul Dundas

Emersion® Umbrella System

The Emersion® Umbrella System was developed specifically to satisfy the needs of service providers selling complex products such as telephony, broadband and 3G mobile phone plans with bolt-ons to the wholesale and retail markets. The unique Emersion Umbrella Architecture allows products, services and packages to be created, provisioned, billed and managed as an end to end process using our Thunder™ Workflow Manager. This one Umbrella System will allow a service provider to be more efficient and reduce the human resource requirements to manage their operations, whilst providing complete control over customers and services from a single interface.

Emersion's end-to-end interfaces with Australia's leading national carriers and aggregators makes ordering, provisioning, and billing of data and telephony products and services effortless. The Umbrella System guides the user through the service qualification and ordering process, removing the confusion and complication and costly re-keying of information. Customer invoices are generated automatically for all charges associated with their services.

The Emersion Umbrella System comprises core systems developed on the robust Emersion Umbrella Architecture and a number of Emersion® Umbrella System modules managed and operated by Emersion, that interact to each other via the Umbrella Architecture and external systems via the Batch Mediation System (*BMS*) and Real-time Integration Management System (*RIMS*).

The B2B Application Programming Interface (API) interfaces with multiple carriers and service providers, internal and customer management systems using different communications protocols, such as web services (XML and SOAP) and FTP. CDRs and RADIUS data usage are retrieved from carriers or the service provider without user intervention.

Emersion's super-flexible Billing System allows plans for all types of products and services to be created. The Rating component allows rate cards to be created and managed to associate with plans, including shifting rates based on time, quantity or usage, call block partitions, and traffic zones. Plans can be linked making it easy to build packages and apply discounts or concessions without needing to create countless plans that are both confusing and difficult to manage.

As well as all the flexibility provided in the Plan and Rate components, Emersion also stores historical rate information allowing historical invoicing as well as re-rating to be performed. The Billing Engine integrates with the Invoice Generation system to automatically generate invoices for customers, whether they are service providers, agents or end users. A single, unified bill is presented, showing customers' packages, services and charges. Customers may view their bills on-line through the User Interface or receive them via email in Adobe® Acrobat® PDF format. Emersion also supports integration to external mail houses for paper invoice generation and posting.

Teamed with the other system modules for Customer Management, Support (Ticketing), Provisioning, Payment Services, Data Retrieval and verification the Emersion platform and Powerful Business to Business (B2B) API, developed on the Emersion Umbrella Architecture provide a degree of flexibility not often seen in services of this kind to date.

Emersion meets the requirements of even the most demanding client:

- Improved efficiency - provisioning, billing & support from one system (no re-keying) ✓
- Flexible pro-rata billing, rating and invoicing solutions, bundling, credit management and customer management solutions ✓
- Intuitive User Interface ✓
- Customisable Workflows ✓
- Documentation and training ✓
- Scalable, available and secure, ready to go equipment, software and solutions ✓
- Support backed by an industry leading Service Level Agreement ✓

Introduction

On behalf of the team at Emersion, we would like to take this opportunity to welcome you to Emersion. The Emersion Systems Administration interface is designed for effective management of your Staff and Service Settings.

Emersion may update the system to improve your experience, updates, additional features and changes may occur beyond the date of the creation of this document. Therefore, some information or screens in this version of the manual may become slightly out of date.

ⓘ Note that other Emersion modules referred to in this manual are not described in detail in this document. Please refer the specific Emersion system manual for further information about each module if required.

Your Wholesale Service Provider will provide you with a login to access to the Emersion Service Management System. The Emersion system components are seamlessly integrated and you will access the Emersion Customer Management System (CMS), and other modules from a single Web interface.

ⓘ Note the Service Provider Admin account provided is solely to be used to create and modify Staff Users and manage their permission. You should Create another Staff User for everyday use and set appropriate permission for this User Login per the instructions in this manual.

Document Conventions

The following conventions are used throughout this manual to describe information and procedures:

Italics	Indicates the name of a screen, field or setting. The capitalisation and punctuation are the same as displayed on the screen. For example: Complete the *Address* field.
Bold text	Bold text indicates either the name of a command, button or other interactive element. For example: Type the user's name in the *Customer Name* field, and then click **Search**.
BOLD CAPITALS	Text in bold capitals indicates the name of a key on a keyboard. For example: Enter your password, and then press **ENTER**.
Navigation >	Menu options or navigation paths are described in shorthand using the following convention: **Module > Functional Area > Option** For example, selecting the RBT area can be described as: Select **Services > STS > RBT** from the Menu**.**
`Monospace text`	Used to represent the text you must type in a field. For example Type `abc` in the *Search* field.
ⓘ	The ⓘ symbol indicates some useful information or a handy tip.

Assumptions Made

As this manual cannot hope to cover more than the operation of the Emersion system, the following assumptions have been made:

- You are familiar with the Emersion Customer Management System and you can competently use it.
- You have a computer less than 4 years old that you can competently operate.
- You have an Internet connection, and are capable of establishing a connection.
- A Web Browser capable of supporting Web 2.0 functionality is installed on your computer.

  Emersion recommends the use of Firefox 3.0 or greater.
- A PDF Reader installed on your computer.
- You have a basic understanding of computer and Internet terminology.
- You have an understanding of Windows Server Active Directory or equivalent.

Emersion® Security System

SSL Encryption

High Grade (AES-256 256 Bit) SSL Encryption by Entrust ensures that the pages you are viewing were encrypted before being transmitted over the internet. Encryption makes it difficult for unauthorised people to view information travelling between computers.

User Login Features

Each User Login is attached to a Contact in the Cumulus system, which in turn is linked to the Service Providers Account.

The Cumulus Framework integrates with the Umbrella Framework system wide to provide integrated and strong protection ensuring only authorised users have access to the system. Other features

Single Login - The Emersion Umbrella ™ system features a single login to all features the User has access to.

Cumulus user interface and user level security ensures that only system components that the user has permission to use will be rendered on the screen.

Usernames – Usernames are of the format *username@suffix.* The suffix is defined at the time of creation of the Service Provider and all Users created will have the same suffix. Usernames (username@suffix) must be unique

Password Security – The password rules that the Emersion System will follow are:

- The password is a minimum of 8 characters long and a maximum 40 characters long
- The password is case sensitive
- The password will contain a mix of upper and lower case alphabet characters and at least one numeric character and / or a special character e.g. !@#$.
- The password will not contain any three consecutive characters, such as Abc or aBc, nor will contain any more the four keyboard sequences such as Qwer or poiU
- The password cannot relate to the logon ID / username
- All passwords are encrypted

Single Session - When the user logs in, any other active session will be disconnected, which greatly enhances the security, and ensures that the user can still roam.

All Logins Logged - This provides an audit trail of all user logins and log in attempts.

- After 3 login attempts the Login will be locked out. Password must be reset by the SP Administrator.

IP Restrictions – Optional IP restrictions can be placed on user login's allowing then to only login from an authorised IP (or IP Range).

Gatekeeper

The gatekeeper function of the security system utilises the Permission System and User permission levels information to control access to functions and data for both User Interface and System Logins. This function is abstracted from the UI and controls all access. Users are assigned to one or more organisational groups, which in turn are assigned one or more roles with their inherent permissions. This hierarchical method of managing user permissions reduces the administration effort and overhead and is described further below.

Permission System

The functions each User or Supplier Specific Interface can access are configured in the Permission System. Roles and Permission Sets determine access levels in the Emersion Umbrella System. Each user is assigned to one or more Role and / or Permission Sets for each function in the applicable system. This determines whether the user can access the function, and to what level (Create, Read, Update or Delete).

Permission System Basics

The Emersion Permission System follows a similar pattern as used by Windows® AD (Active Directory) structure. You can use the Organisational units and Roles as you would security groups in a windows network.

In addition to the user defined permissions, there are global permissions that reflect business rules put in place to comply with privacy guidelines. These include the ability of suppliers being able to view services supplied by them to the service provider, but does not include the ability to view Customer Details or financial transactions associated with the service.

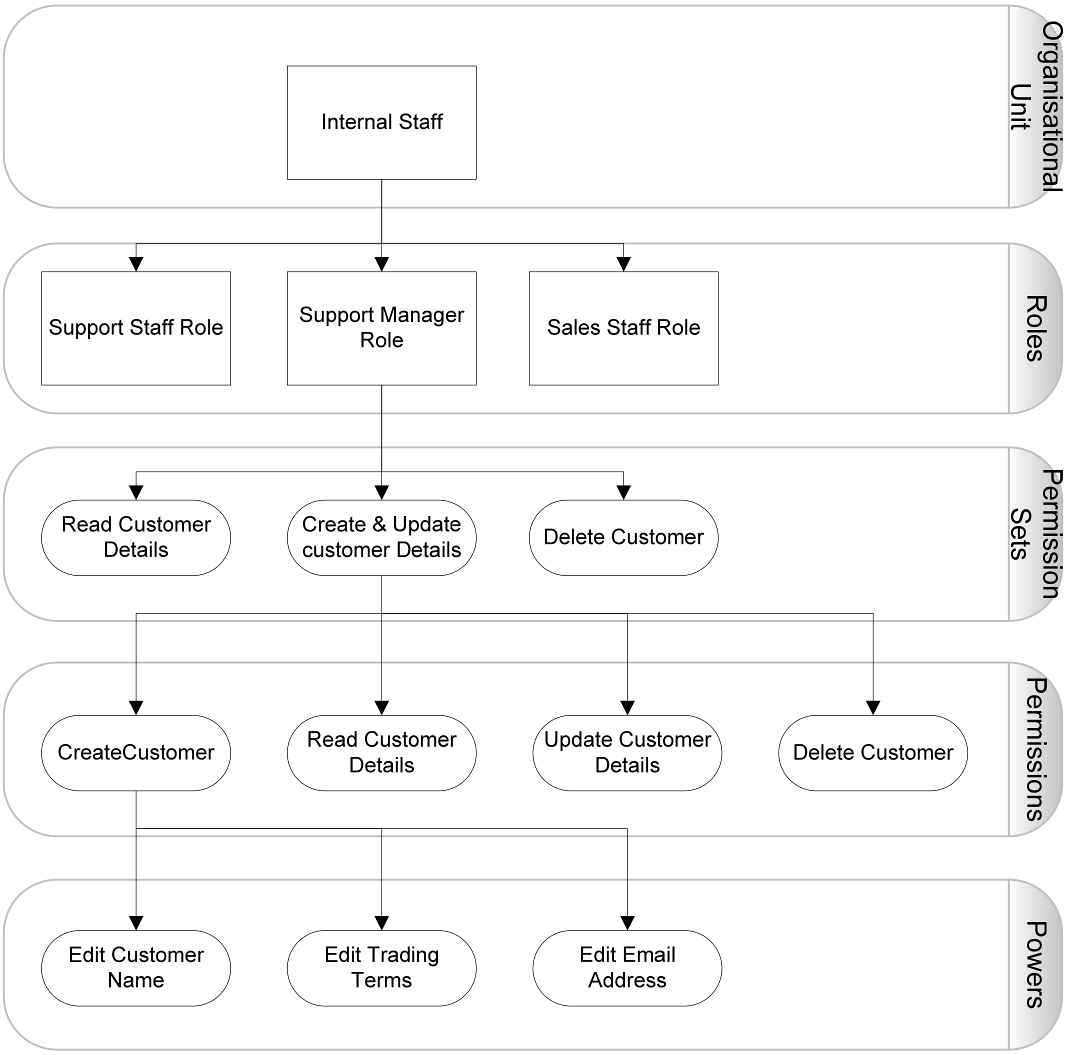
Emersion has a number of predefined roles which can be added to Organisational groups that you create. This gives you the ability to create a number of Organisational groups and assigned the correct roles to each of these groups. As user can only be a member of one OU at one time, it is important to ensure the OU has the correct roles needed for the staff member to perform in their position.

Once an account is set up there will be 11 default Organisational Units (*Org Unit*) and a similar number of *Role(s).* By combining the roles and grouping staff into organisational units, we can add permissions to the group as a whole.

Permission Groups may change in the future as services are implemented.

Users are often assigned to multiple Roles and / or Permission Sets to create the appropriate access level to perform their work. Roles may be assigned to Organisational Units to simplify the management of like permission levels.

The following diagram depicts the hierarchical relationships within the Permission System.



Organisational Units

The Emersion system comes with 4 default Organisational Units.

Organisational Unit	Summary of Roles
Administrator	Create Customer, Support
Management	enabling easy restriction for Reporting functions
Production Staff	Customer Service and Provisioning Staff
All Staff	the majority of users will be assigned to this organisational unit

Roles

Roles	Summary of the Roles Permission Sets
Support Staff	Create Customer, Support
Provisioning Staff	Create Order, Provisioning
Sales Staff	Create Customer, Create Order
Account Receivable	Account receive
Accounts Payable	Account Payable
Credit Management	Account receive, Credit management
Sales Management	Create Customer, Create Order, Credit management
Helpdesk Management	Create Customer, Create Order, Support
Provisioning Management	Create Customer, Create Order, Provisioning
Finance Management	Account receive, Account Payable, View Report
Platform Manager	Platform Administrator

The roles shown above contain the actions that are available to each role. By using Organisational unit to group together certain roles, you give the staff permission to access parts to the Emersion system.

All *Organisational Units* contain the role *User Detail.* This role allows the user to log into the Emersion system.

The default roles will have different abilities and actions within the Emersion system to enable them to create, view or edit customer details, create and modify customers.

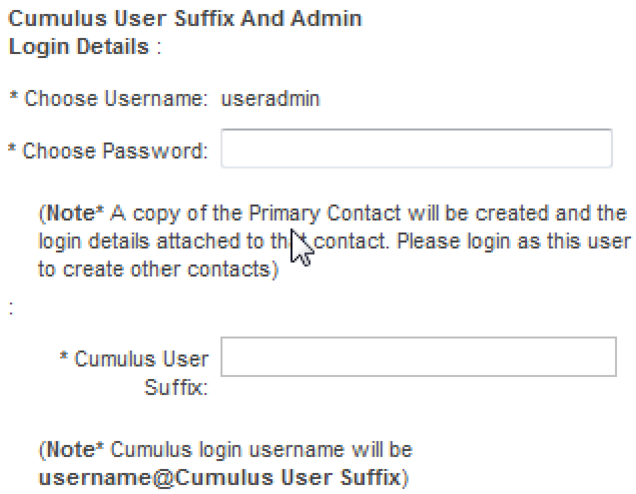
Permission group	Menu label	Module	Action
User Detail	My Details	home	My details
All staff are assigned this by default	Customer List	customer	list
	List All	service	list
	Management	plan	tabs
Create Customer	Create	customer	create
	List All	service	list
	Orders	service	list

Permission group	Menu label	Module	Action
Create Order	Orders	service	list
	New Order	service	new
	Provisioning	service	list
Account receivable	Invoice List	finance	list
	Receive Payment	finance	search
	Unallocated Payments	finance	search
	Debit	finance	search
	Disputed List	finance	list
	Transaction List	finance	list
Account Payable	Invoice List	finance	list
	Transaction List	finance	list
	Disputed List	finance	list
	Credit	finance	search
Credit management	Invoice List	finance	list
	Debit	finance	search
	Write Off	finance	search
	Refund	finance	search
	Security Payment	finance	search
	Security Refund	finance	search
	Pending Card lines	finance	list
	Pending Invoices	finance	list
Support staff	Quarantine	billing	summary
	Non Existent Service	billing	list
	Provisioning	service	list
	Migrations	service	list
Provisioning	Quarantine	billing	summary
	Non Existent Service	billing	list
	List All	service	list
	Orders	service	list
	Migrations	service	list
	New Order	service	new
	Provisioning	service	list
	Management	plan	tabs
View Report	Invoice List	finance	list
	Receive Payment	finance	search
	Unallocated Payments	finance	search
	Transaction List	finance	list
	Disputed List	finance	list
	Credit	finance	search

Permission group	Menu label	Module	Action
	Debit	finance	search
	Write Off	finance	search
	Refund	finance	search
	Security Payment	finance	search
	Security Refund	finance	search
	Pending Card lines	finance	list
	Pending Invoices	finance	list
	Finance Report	report	tabs
Platform Admin	Staff	admin	list
	Org Units & Roles	admin	tabs

Managing Users

When a Service Provider is created the first Login User will be known as the *useradmin@suffix*



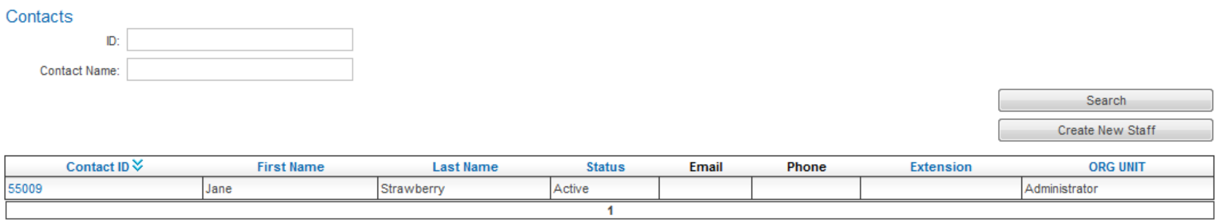
Screen shot of SP Account Create

All Service Provider Staff will be provided with a Cumulus User Login.
This is created when the user is created.

View Staff / Login Users

Step 1. Login as *useradmin@suffix*.

Step 2. Navigate to the menu **Admin > Staff.**



Step 3. You may click on a user's *Contact ID to View / Edit* them.

Viewing Contact: Jane Strawberry

Personal Details:

Salutation:

* First Name: Jane

Middle Name:

* Last Name: Strawberry

Date of Birth:

Suffix:

Job Title:

* Job Code:

* Org Unit: Administrator

* Status: Active

Address:

Address Type: Residential

Unit Type:

Unit Number:

Level Type: Place

Level Number:

Street Number: 605

Street Number End:

Street Name: Funny

Street Suffix:

Suburb: FunnyVille

State: Victoria

Postcode: 8888

Country: Australia

Contact Details:

* Phone:

Mobile Number:

Fax:

* Email Address:

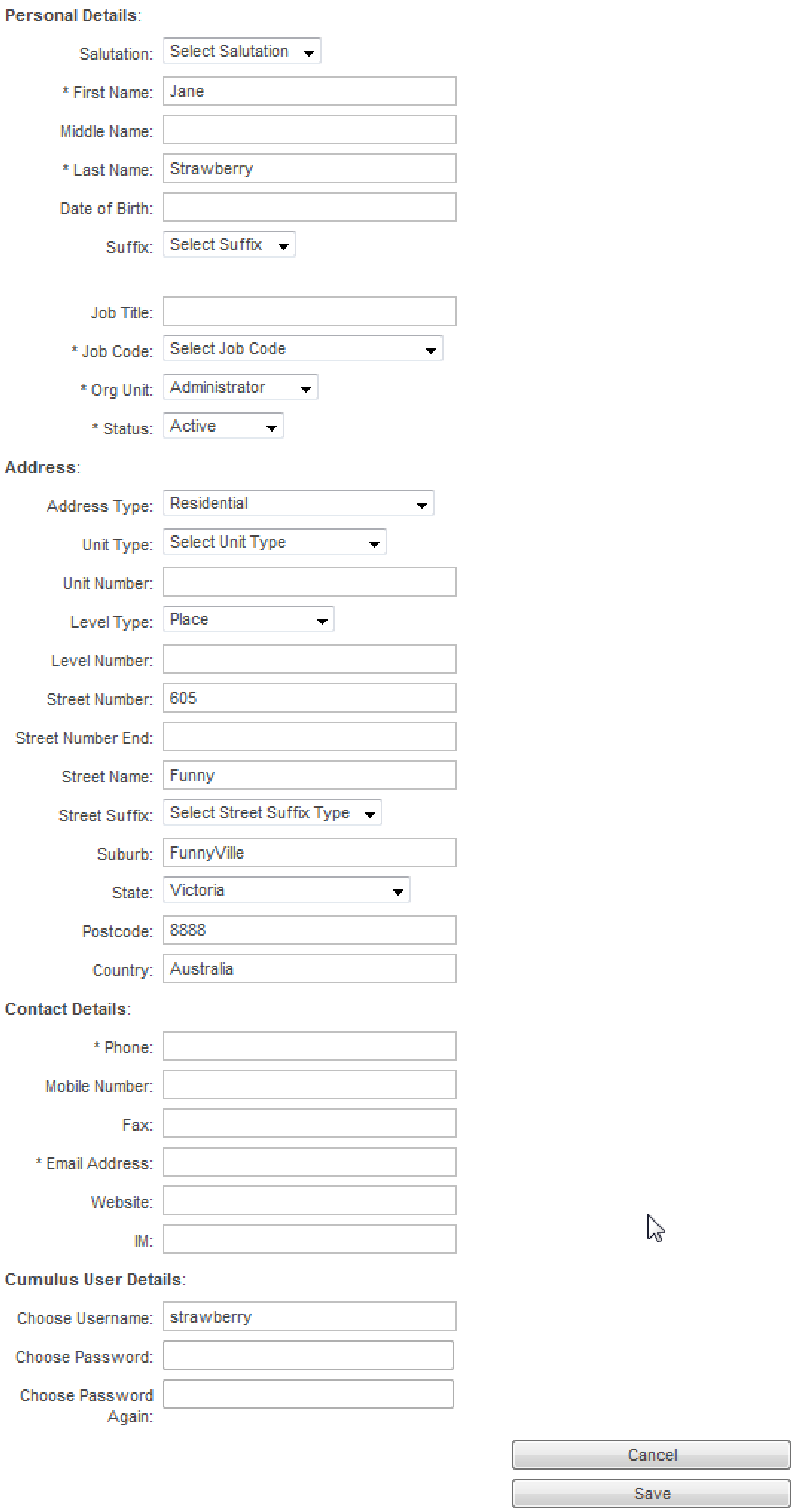
Website:

IM:

Cumulus User Details:

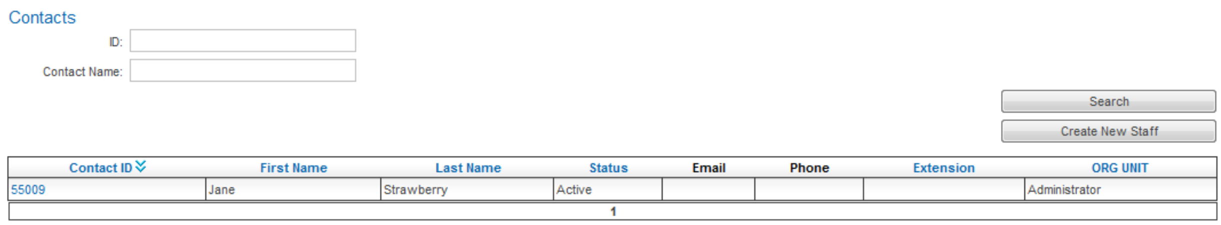
Choose Username: strawberry

Edit


Personal Details:
Salutation: Select Salutation
* First Name: Jane
Middle Name:
* Last Name: Strawberry
Date of Birth:
Suffix: Select Suffix
Job Title:
* Job Code: Select Job Code
* Org Unit: Administrator
* Status: Active
Address:
Address Type: Residential
Unit Type: Select Unit Type
Unit Number:
Level Type: Place
Level Number:
Street Number: 605
Street Number End:
Street Name: Funny
Street Suffix: Select Street Suffix Type
Suburb: FunnyVille
State: Victoria
Postcode: 8888
Country: Australia
Contact Details:
* Phone:
Mobile Number:
Fax:
* Email Address:
Website:
IM:
Cumulus User Details:
Choose Username: strawberry
Choose Password:
Choose Password Again:
Cancel
Save

Create New Staff / Login Users

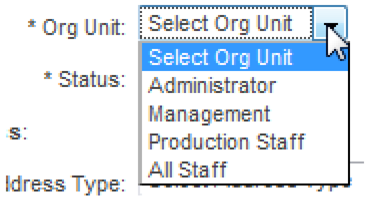
Step 1. Navigate to the menu **Admin > Staff.**



Step 2. Click

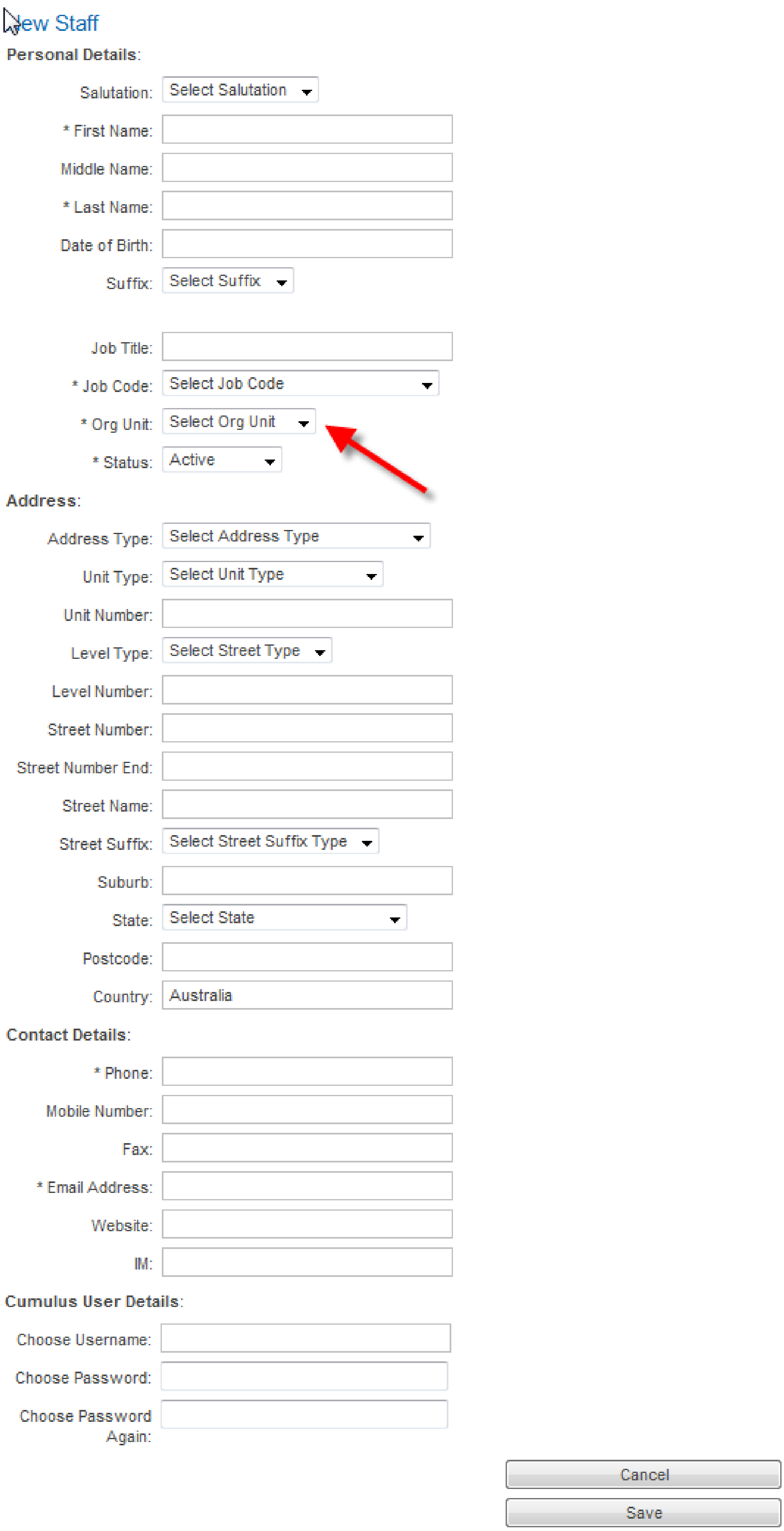
Step 3. Pay particular Attention to the Org Unit.

This defines the default permissions for the new Staff / User Login.



Step 4. Click Save.

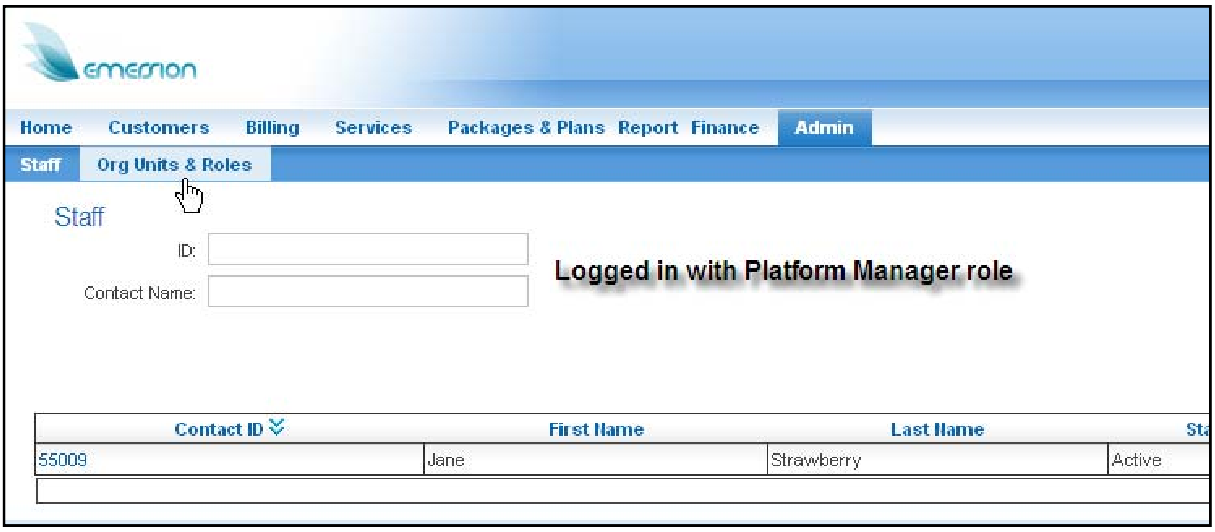
Full details of the Page are on the page following:


New Staff
Personal Details:
Salutation: Select Salutation
* First Name:
Middle Name:
* Last Name:
Date of Birth:
Suffix: Select Suffix
Job Title:
* Job Code: Select Job Code
* Org Unit: Select Org Unit
* Status: Active
Address:
Address Type: Select Address Type
Unit Type: Select Unit Type
Unit Number:
Level Type: Select Street Type
Level Number:
Street Number:
Street Number End:
Street Name:
Street Suffix: Select Street Suffix Type
Suburb:
State: Select State
Postcode:
Country: Australia
Contact Details:
* Phone:
Mobile Number:
Fax:
* Email Address:
Website:
IM:
Cumulus User Details:
Choose Username:
Choose Password:
Choose Password Again:
Cancel
Save

Managing Permissions

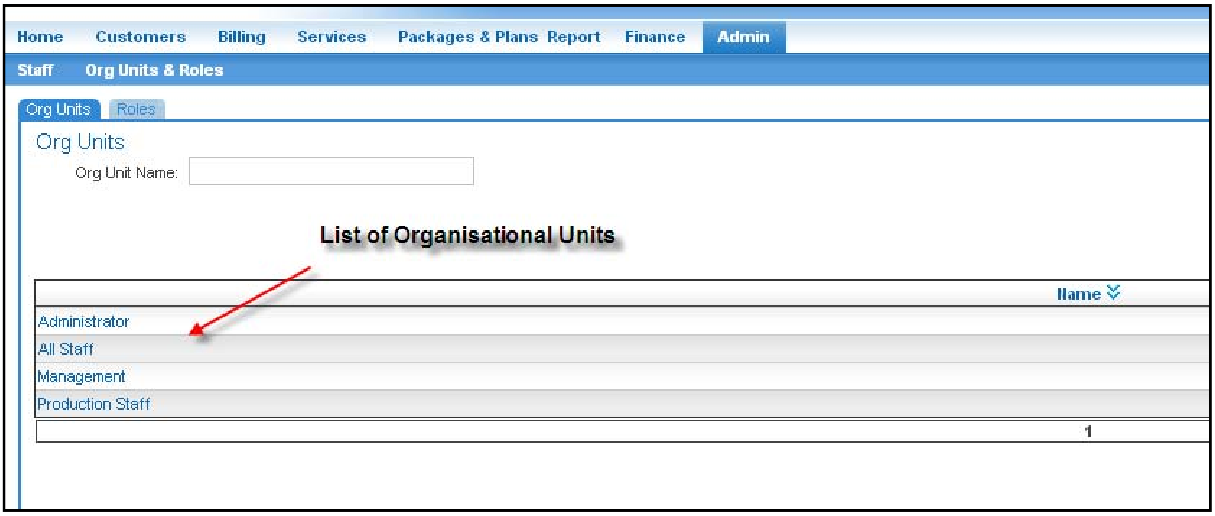
Permission in the Emersion system follows a similar pattern as used by Windows® AD (Active Directory).

View Permissions

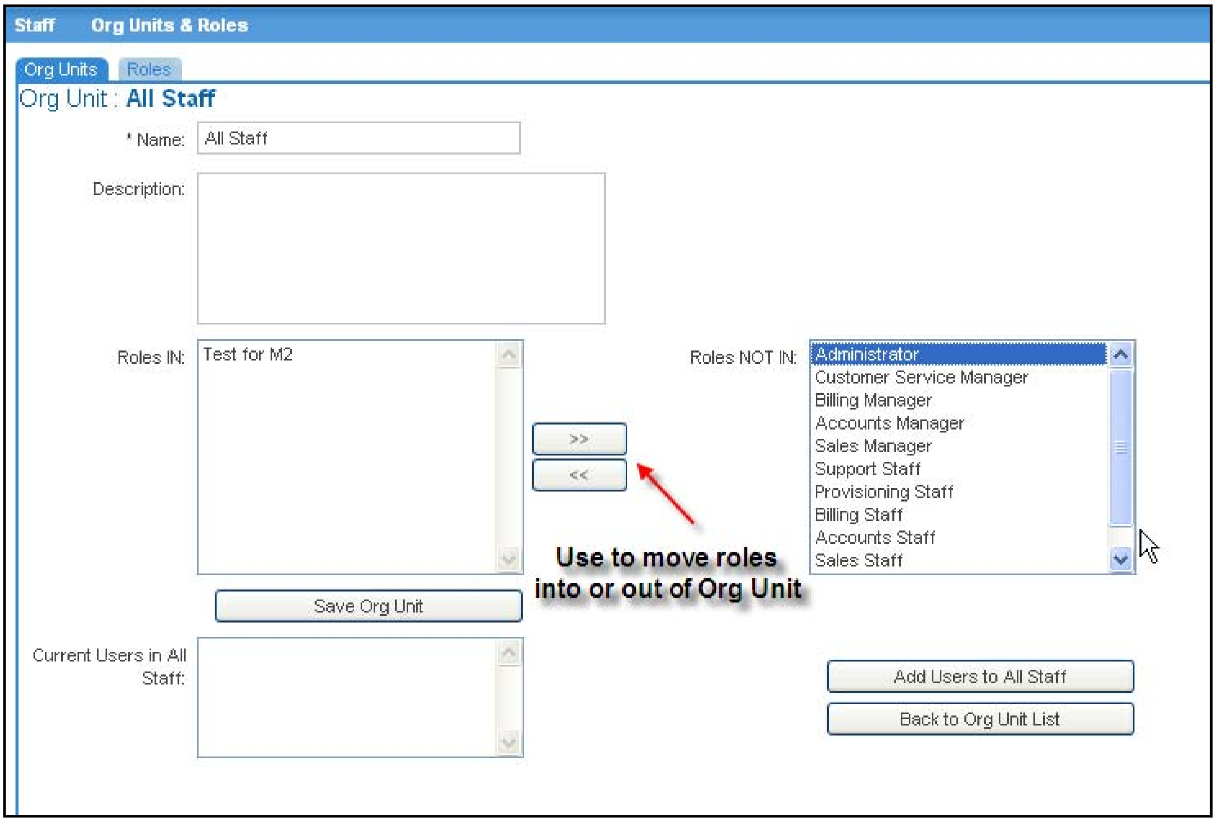


To view permissions the logged in account must have permission to view the *Admin* menu item.

From here the user will need to select *Org Units & Roles*.



Org Unit page



Roles contained in Org Unit view page

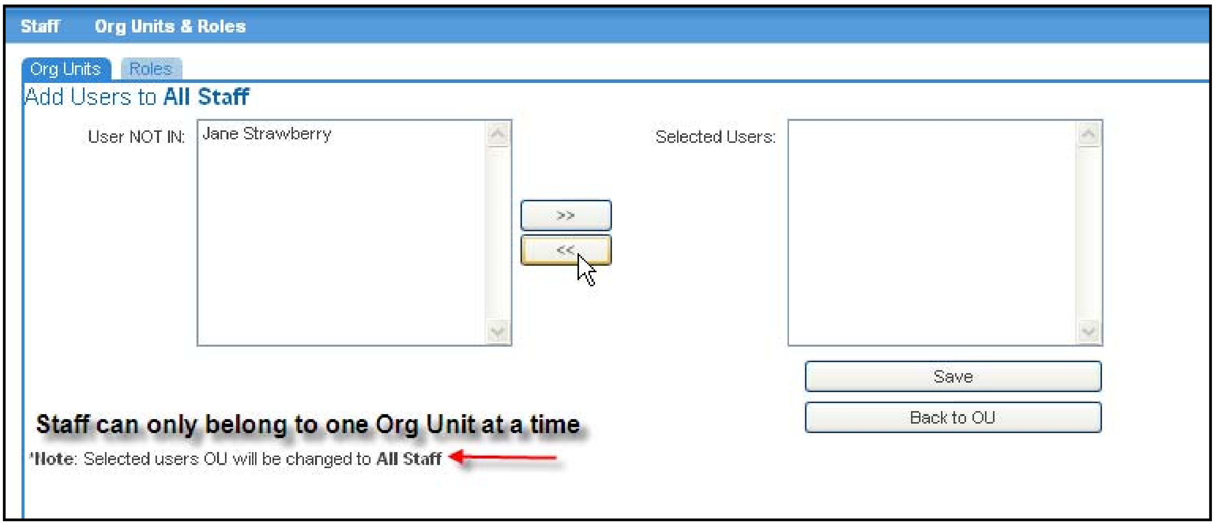
To Update Org Unit with Roles

Step 1. Select the *Admin* menu item

Step 2. Select Org Unit & Roles, from the 2nd level menu bar

Step 3. Use the hyperlink on the group you wish to update

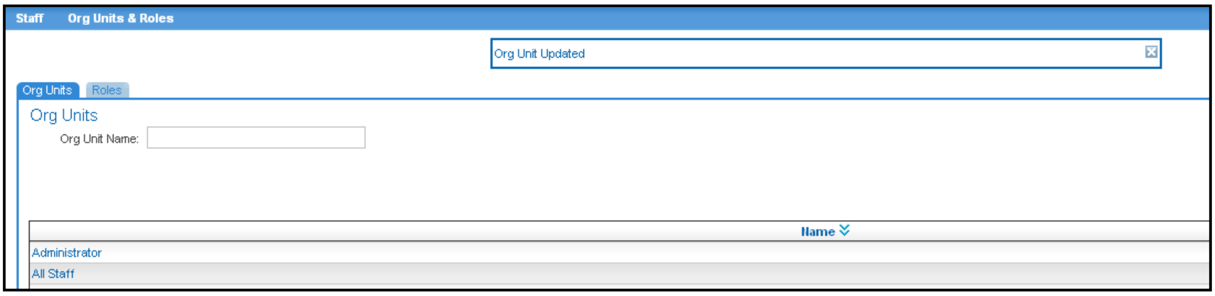
Step 4. You will then be shown a screen similar to the one above. It will show the *Org Unit* name, the roles that the unit has and staff that are in that unit. You will have options to add more users to the *Org Unit*. If you choose this option you must **SAVE ORG UNIT** before moving on.



After saving you will taken back to the previous page

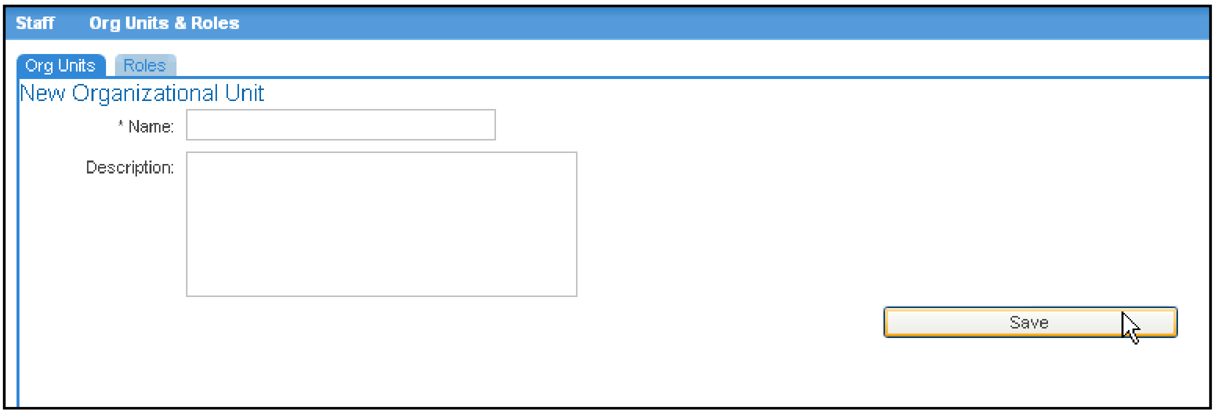
Step 5. Once you get back to the *Roles* page Use the **>>** or **<<** to add or remove roles to the Org Unit. Again using the **SAVE ORG UNIT** button to preserve the changes.

Step 6. You will then be taken back to list of Organisational Units.



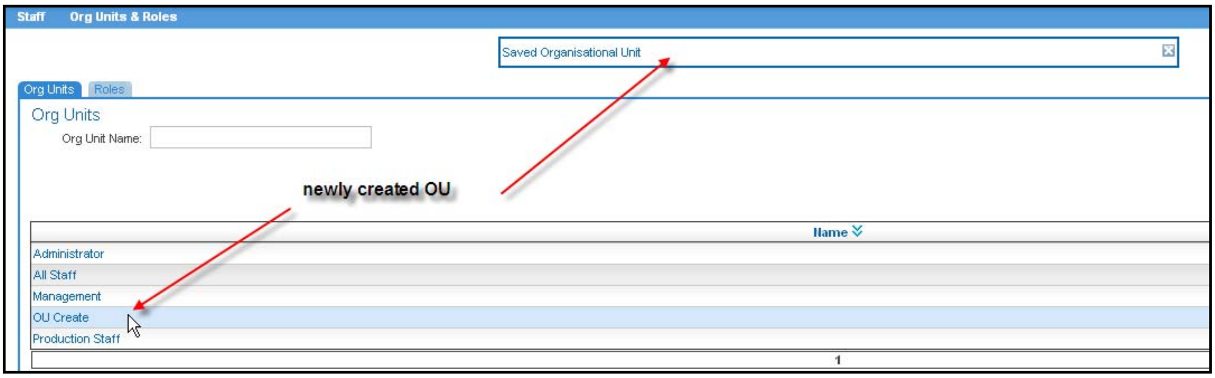
Creating a new Organisational Unit

Step 1. If there is not a current Organisational Unit (OU) that fulfils your requirement you can create a new OU. Simply **CLICK** on the *Create New* button

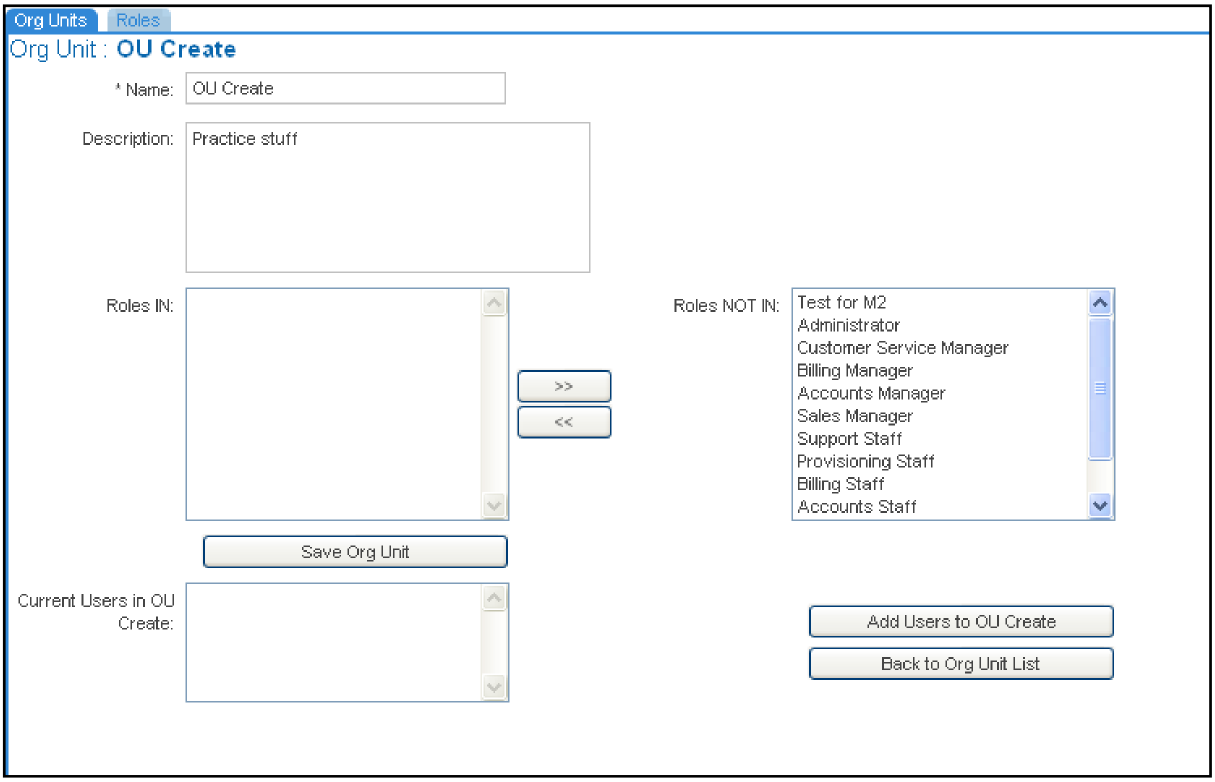


Step 2. Simply **enter** a name for the OU, we suggest that you make it something that shows its function, which will enable people to find it easily in the future. Enter a description to make it very clear what this OU does. **CLICK** *Save.*

Step 3. The new OU should now appear in the OU list. You now need to add permissions to the OU. To this by selecting the new OU.

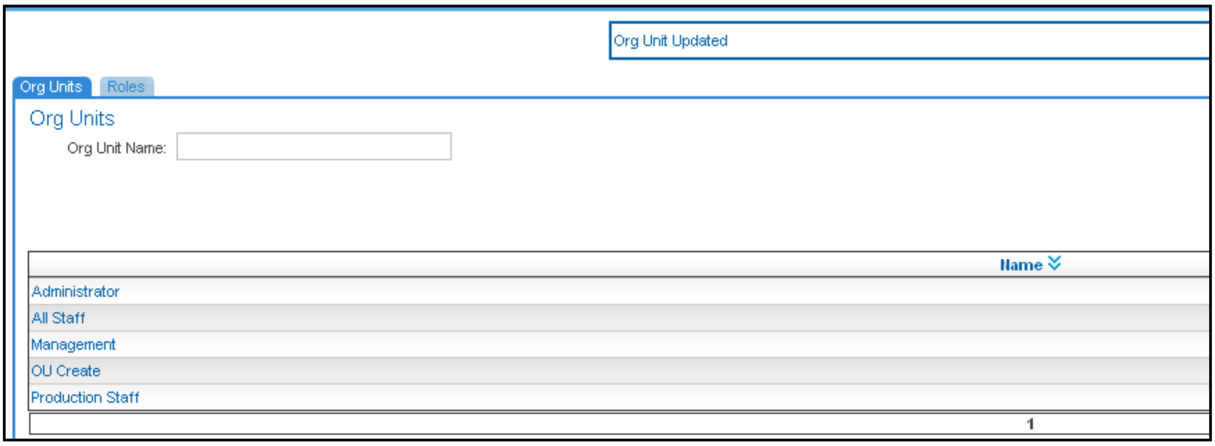


Updated OU list



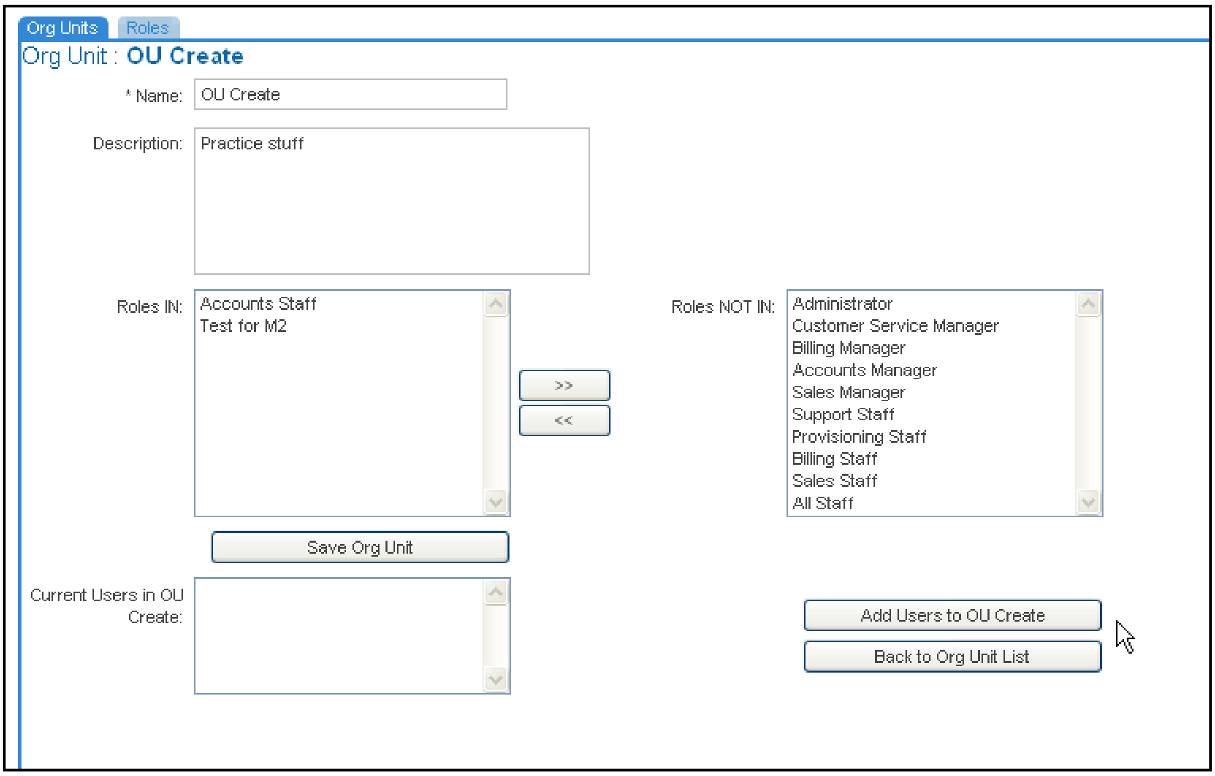
Step 4. You now need to add *Roles* to the OU. Do this by selecting which roles you need and using the **<<** button add them to the OU. Then **CLICK** the *Save Org Unit* button. Here we will select *Test for M2* and *Accounts Staff.* You can use the Control Key to highlight multiple selections

Step 5. The page will return to the OU list page. To add staff to the OU you will need to select the OU form the list.



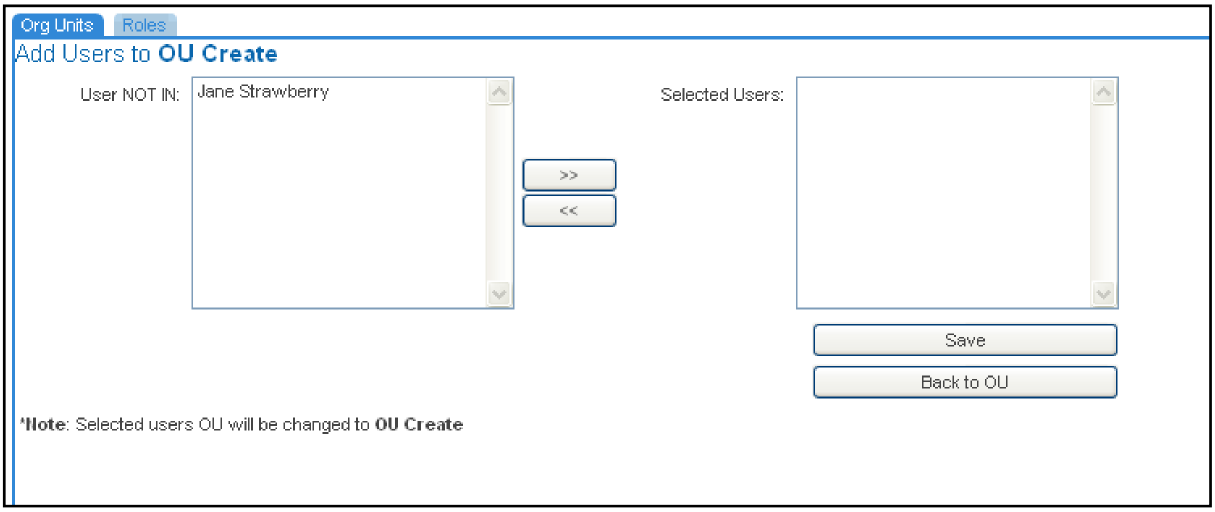
Once you have done that you will be returned to the details page of the OU

Step 6.



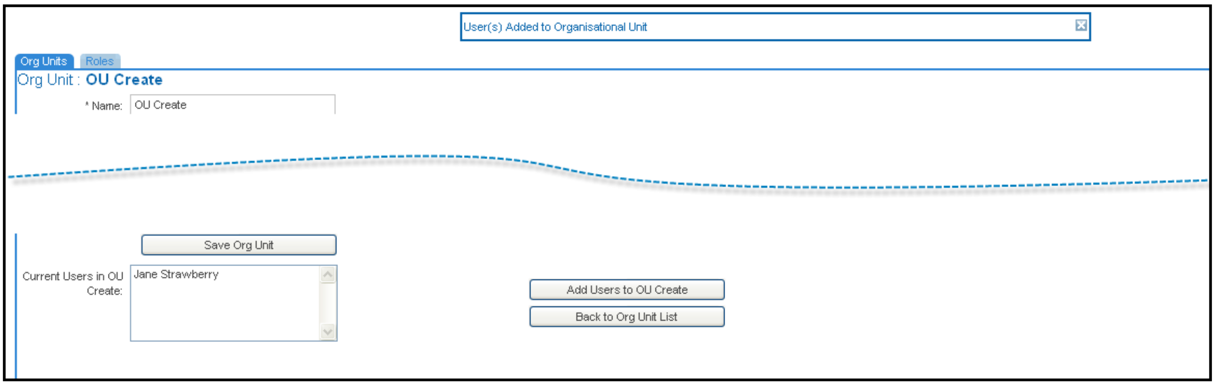
CLICK *Add Users to 'OU Create'.*

Step 7.



In this case we can only choose one staff member. Select the names you want to add to the OU and use the **>>** to move the staff members into this OU.

Remember this will remove those staff me members chosen from their original OU's

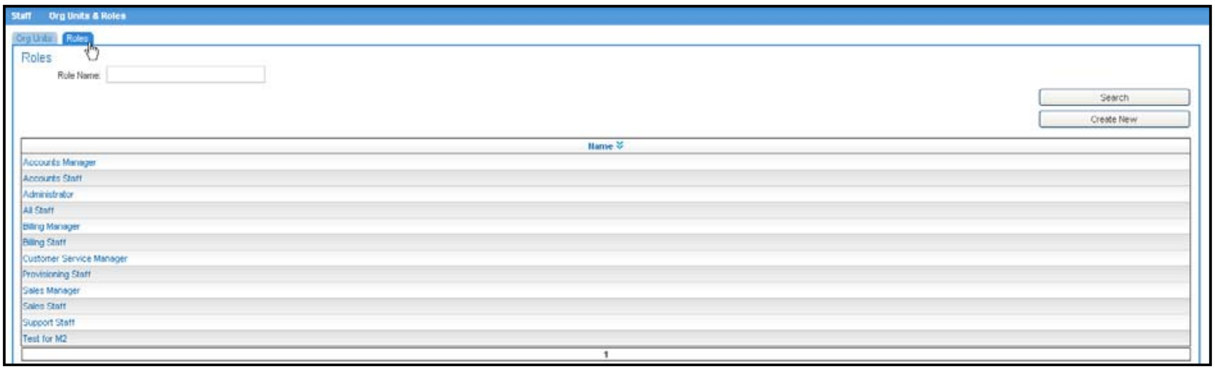


You can now see the use is part of this OU. The update to the user's permissions will take effect next time they login in.

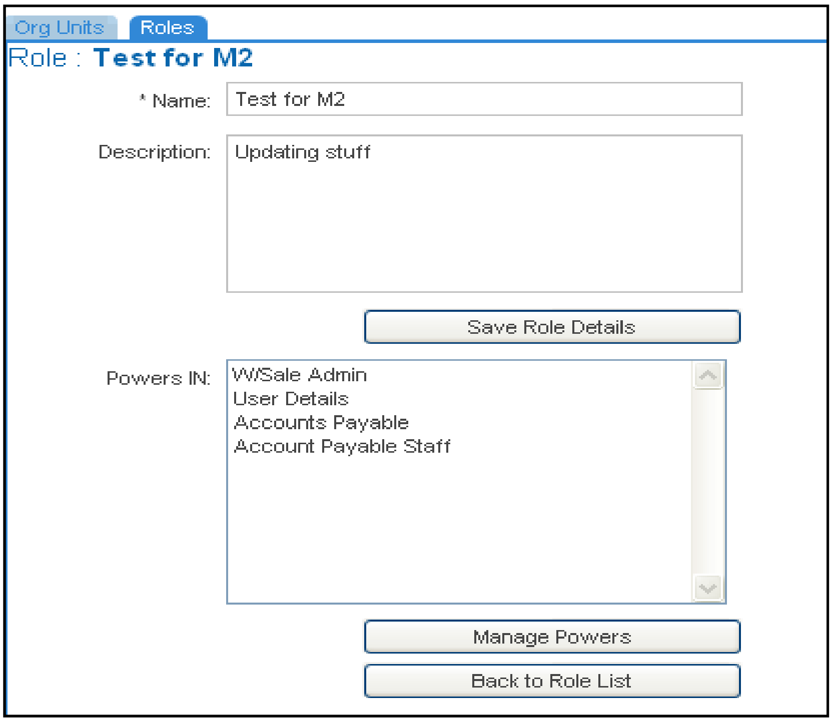
Managing Roles

Permission in the Emersion system follows a similar pattern as used by Windows® AD (Active

Roles contain the permissions needed to use the Emersion Cumulus CMS. As roles are basically containers you can add a number of permissions to each *Role.* When you select the roles tab you will be presented with a list of roles already in use.



To view a specific Role, you need to CLICK on the link and this will bring up the details of that role.



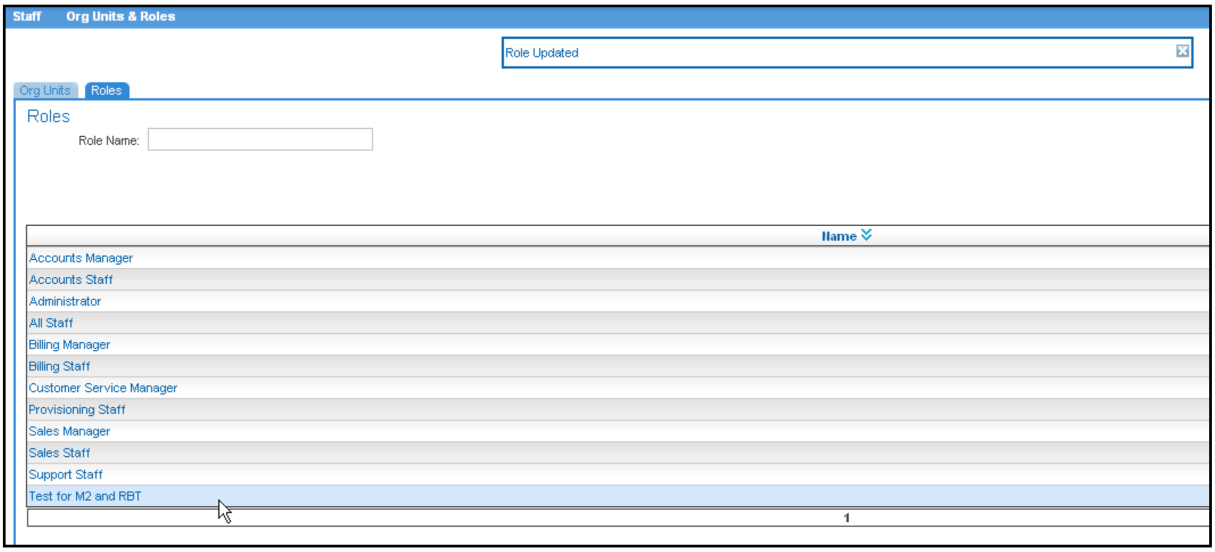
Role detail view

To Update a role

To update the name and description

Step 1. From the details page simply type in a new or description or both and **CLICK** the *Save Role Details*

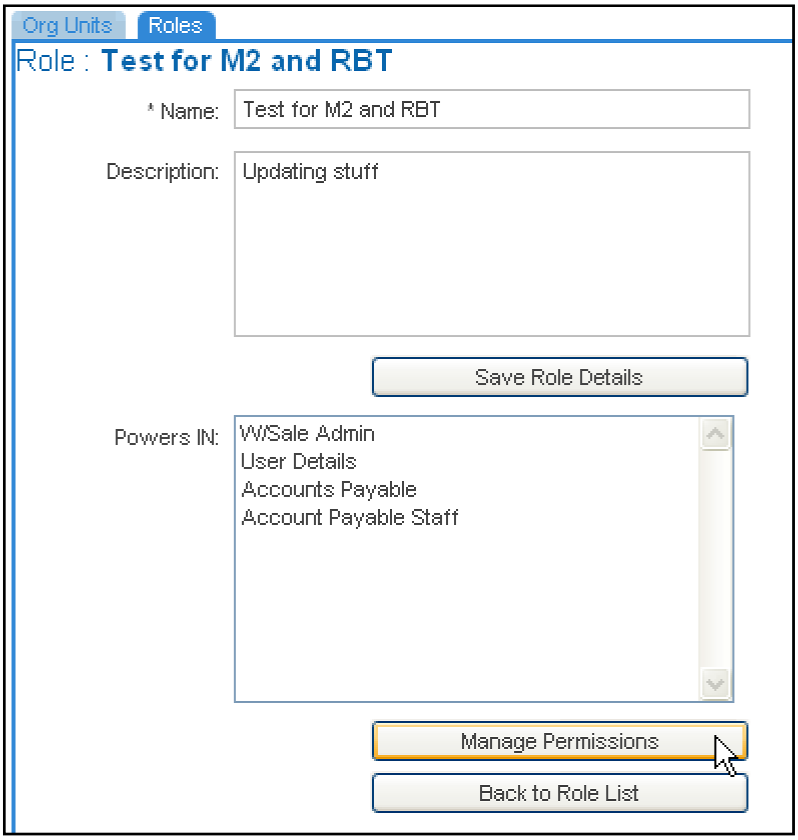
Step 2. You will be taken back to the list page for roles where you will see the updated role and an advisory box saying the role has been updated.



To add permissions to a role

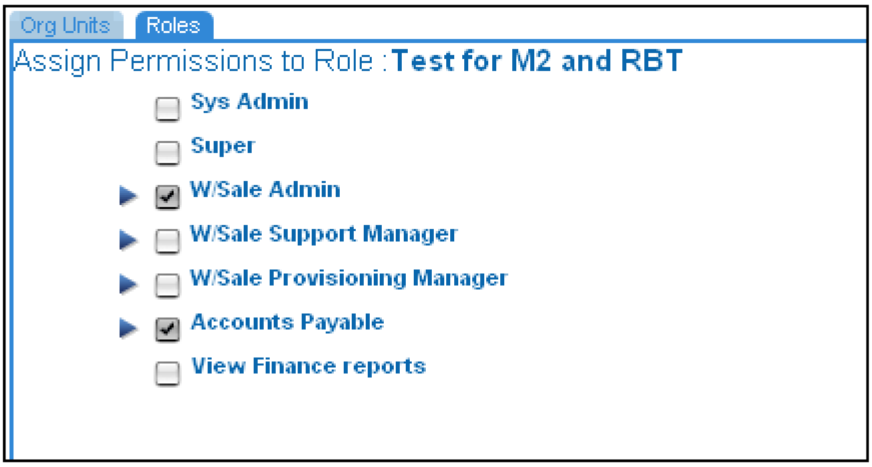
Step 1. Select the role you want to add permissions to and **CLICK** the link

Step 2. You will be taken back to the role details page



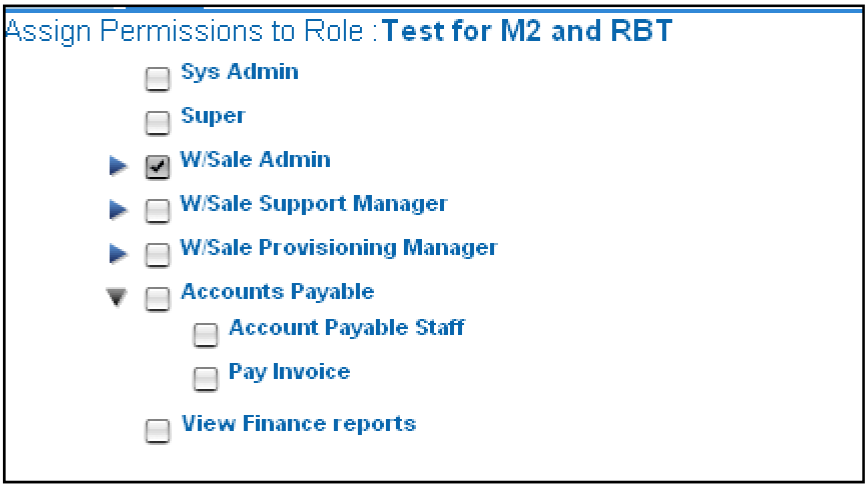
Step 3. **CLICK** on the *Manage Permissions* button

Step 4. You will see the following list



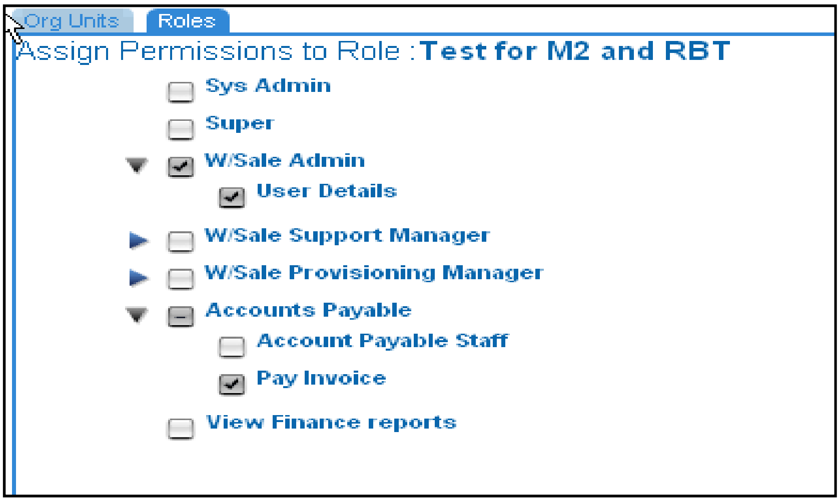
To add permissions to the role simply check one of the permissions displayed.

As you can see some of the permissions have a ▶ next to them. This means there are some additional options available within the permission. **CLICK** on the ▶ to see the additional options



Step 5. Select the permission you want to add to the role. If the permission is part of a group you can select that single permission only by expanding the list and checking the grey box beside the permission, or if you prefer check the grey box next to the parent and all will be selected.

As you can see form above the group W/Sale Admin has been chosen as a group. In the next figure we will show the content of the group and the result of choosing only a child of the group.



As you can see from above, if the whole group is chosen there is a tick in the grey box beside the permission, and if only some of the child permissions have been chosen the a dash will appear in the box. If nothing is chosen the box will show in the lighter grey colour.

Step 6. Chose the permission or group of permissions you wish to add the *Role,* and then **CLICK** the *Save Role Permission Groups* button located on the right hand side of the page.

To remove permission from a role

Step 1. Select the Role you want to remove the permissions from

Step 2. **CLICK** on the *Manage Permissions* button

Step 3. Uncheck the grey box for the permission you which to remove the role and **CLICK** the *Save Role Permission Group* button.

To create a new Role

Step 1. From the Role list page, chose the *Create New* button

Step 2. Choose a name for the new role, and enter a description

Step 3. **CLICK** the *Save* button

Step 4. You will be taken back to the list page, look for your new *Role* and **CLICK** the link

Step 5. You now need to add permissions to the Role using the same procedure as outlined above.

Further Information

For further information about Emersion's Service Management System (SMS), or other Emersion system modules, please contact Emersion.

If you are using Emersion on agreement from a supplier (i.e. in connection with the supply of a particular service or product), and have been provided a login for Emersion by your supplier, please contact your supplier directly for assistance.

Emersion

Phone: 1300 793 310

Fax: 1300 793 320

Emersion Web Site:

www.emersion.com.au

Notes