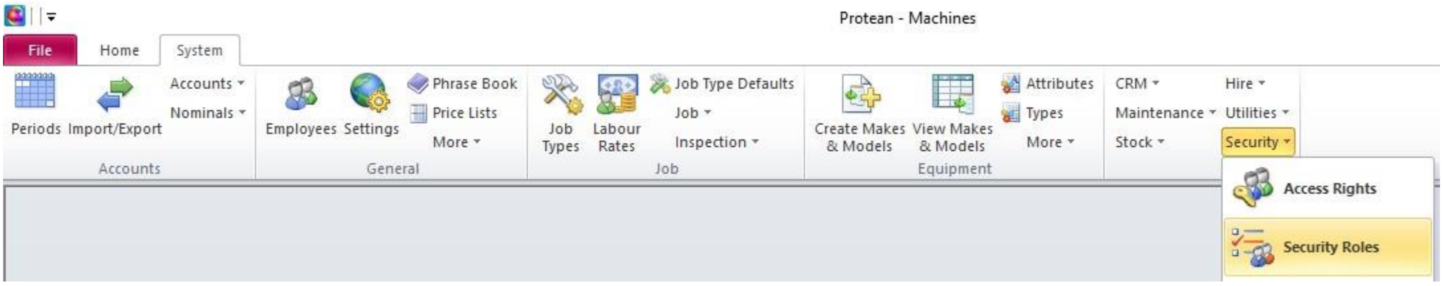
Access Rights & Security roles

How to restrict and grant access to different areas of your Protean.

Where are access rights and Security roles stored?

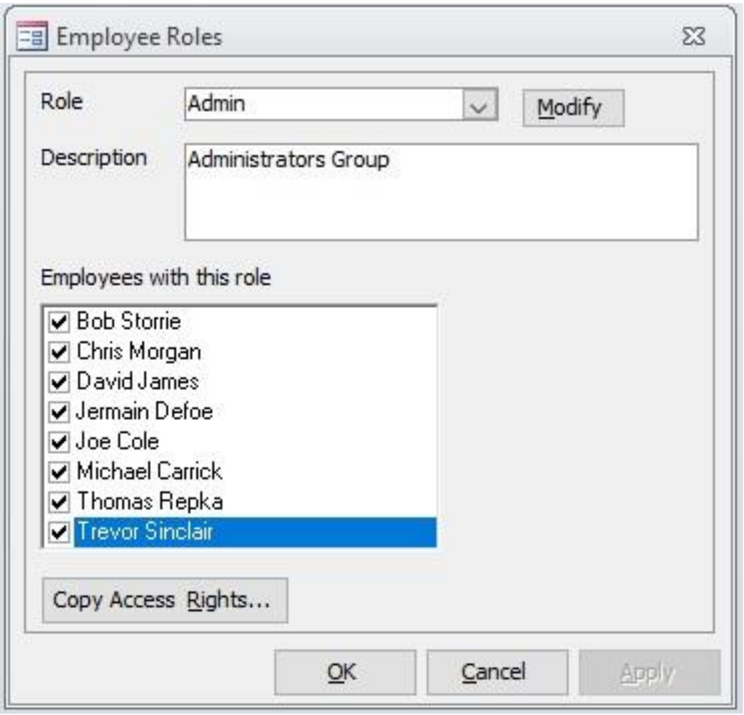
System > Security> Access rights / Security roles



All access rights and security roles are controlled within the System tab, Security drop down. If you cannot see the following options shown above speak with your system administrator.

How do I add new Security roles?

System > Security> Security roles



Role: Admin

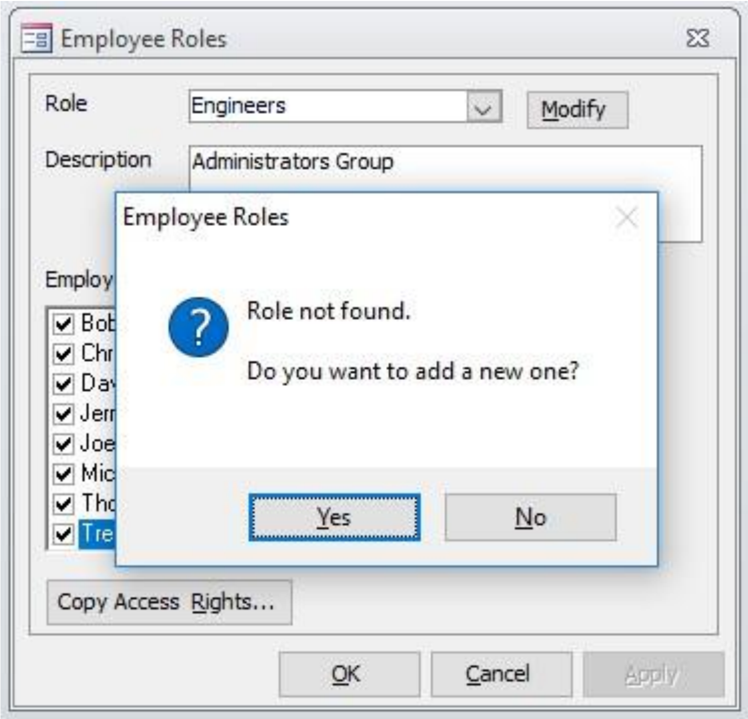
Description: Administrators Group

Employees with this role

- ☑ Bob Storrie
- ☑ Chris Morgan
- ☑ David James
- ☑ Jermain Defoe
- ☑ Joe Cole
- ☑ Michael Carrick
- ☑ Thomas Repka
- ☑ Trevor Sinclair

By over typing the *Role* field with the new role you want to add and hitting the enter key you'll be asked if you would like the add the new role. From this screen you can all select which employees you would like to link to that role.

As shown in the below screen shots below:



Role: Engineers

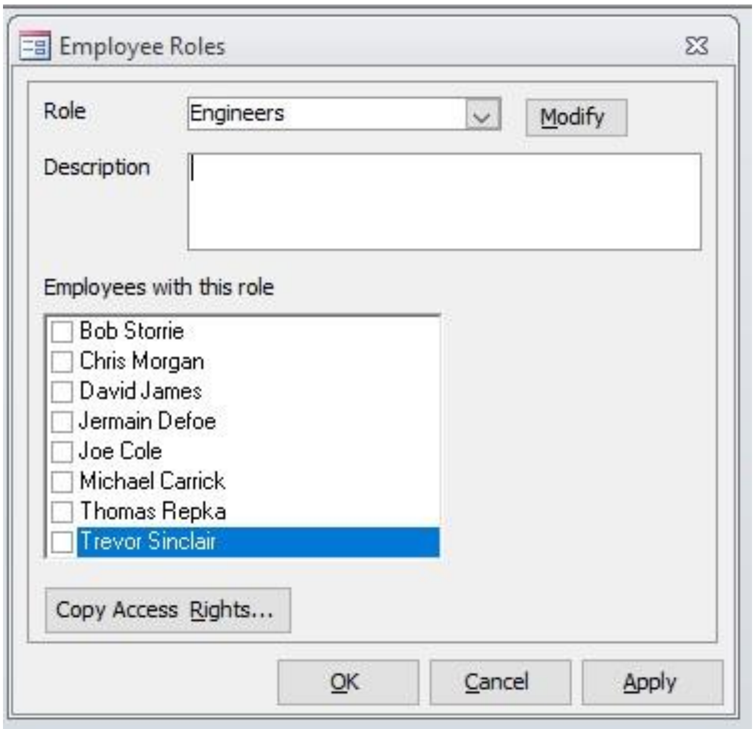
Description: Administrators Group

☑ Bob
☑ Chr
☑ Dav
☑ Jerr
☑ Joe
☑ Mic
☑ Tho
☑ Tre

Employee Roles

Role not found.

Do you want to add a new one?



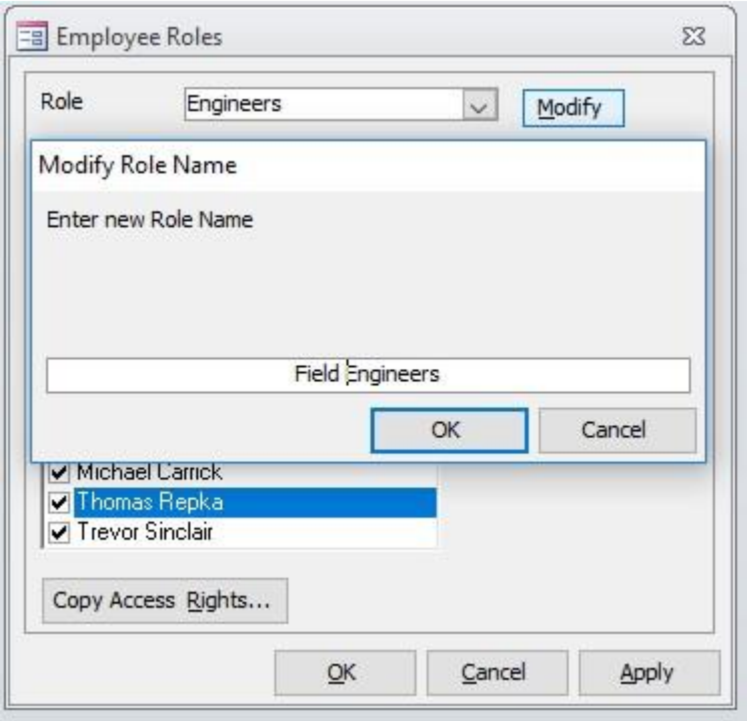
Role: Engineers

Description:

Employees with this role

□ Bob Storrie
□ Chris Morgan
□ David James
□ Jermain Defoe
□ Joe Cole
□ Michael Carrick
□ Thomas Repka
□ Trevor Sinclair

If at any point you would like to rename the new or existing role, simply click on the *Modify* button to the right of the drop down. This will allow you to over type without creating a new role.



Role: Engineers

Modify Role Name

Enter new Role Name

Field Engineers

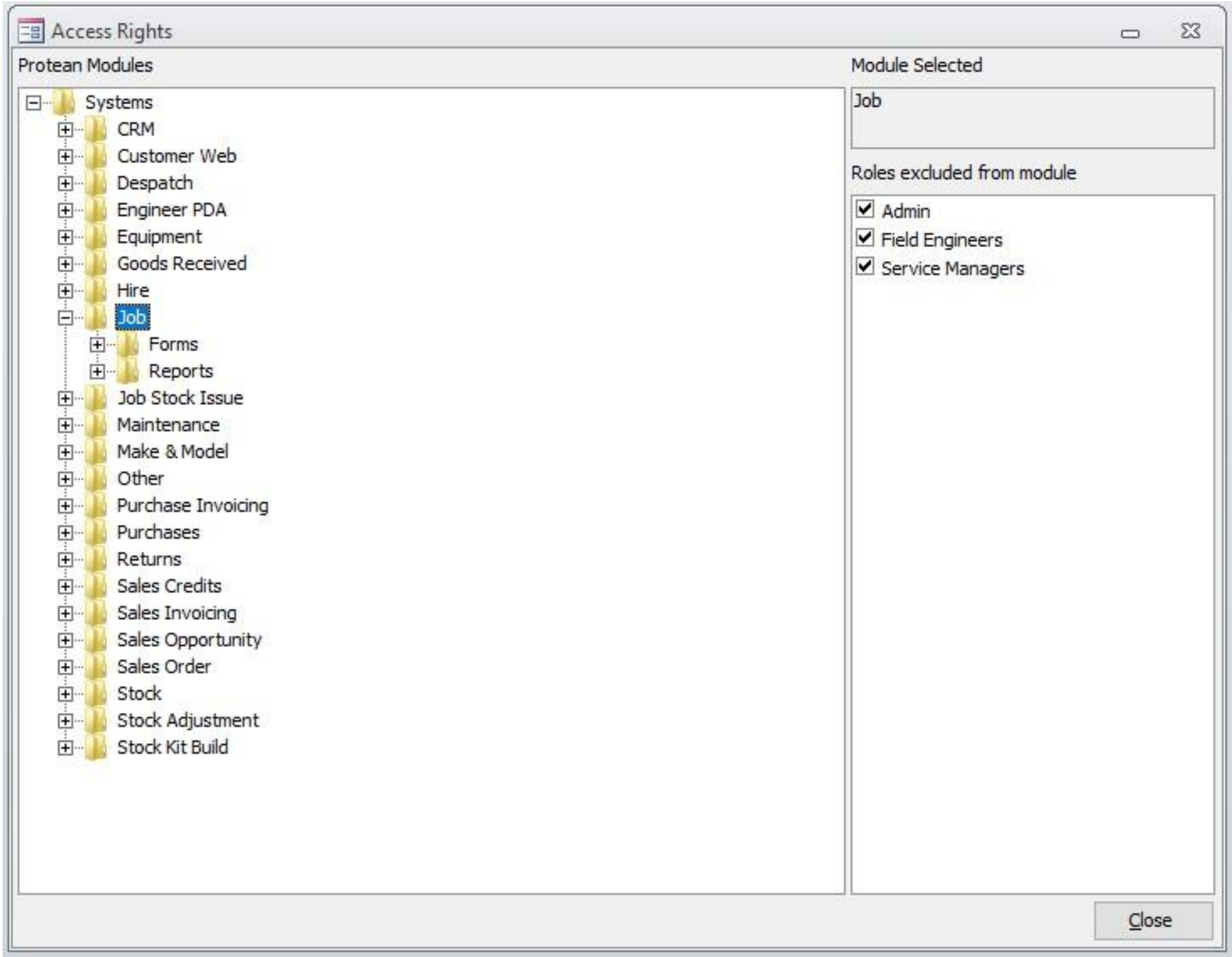
☑ Michael Carrick
☑ Thomas Repka
☑ Trevor Sinclair

Access rights, how to restrict and grant access to different areas of Protean

System > Security> Access Rights

Within the screen below is where the roles we have created come into play. With each role we can specify exactly what whole modules, reports or specific buttons we would like them to have access to.

Each module is broken down into individual lists, expanding each module then gives you the options *Forms* & *Reports*.



Module Selected

Job

Roles excluded from module

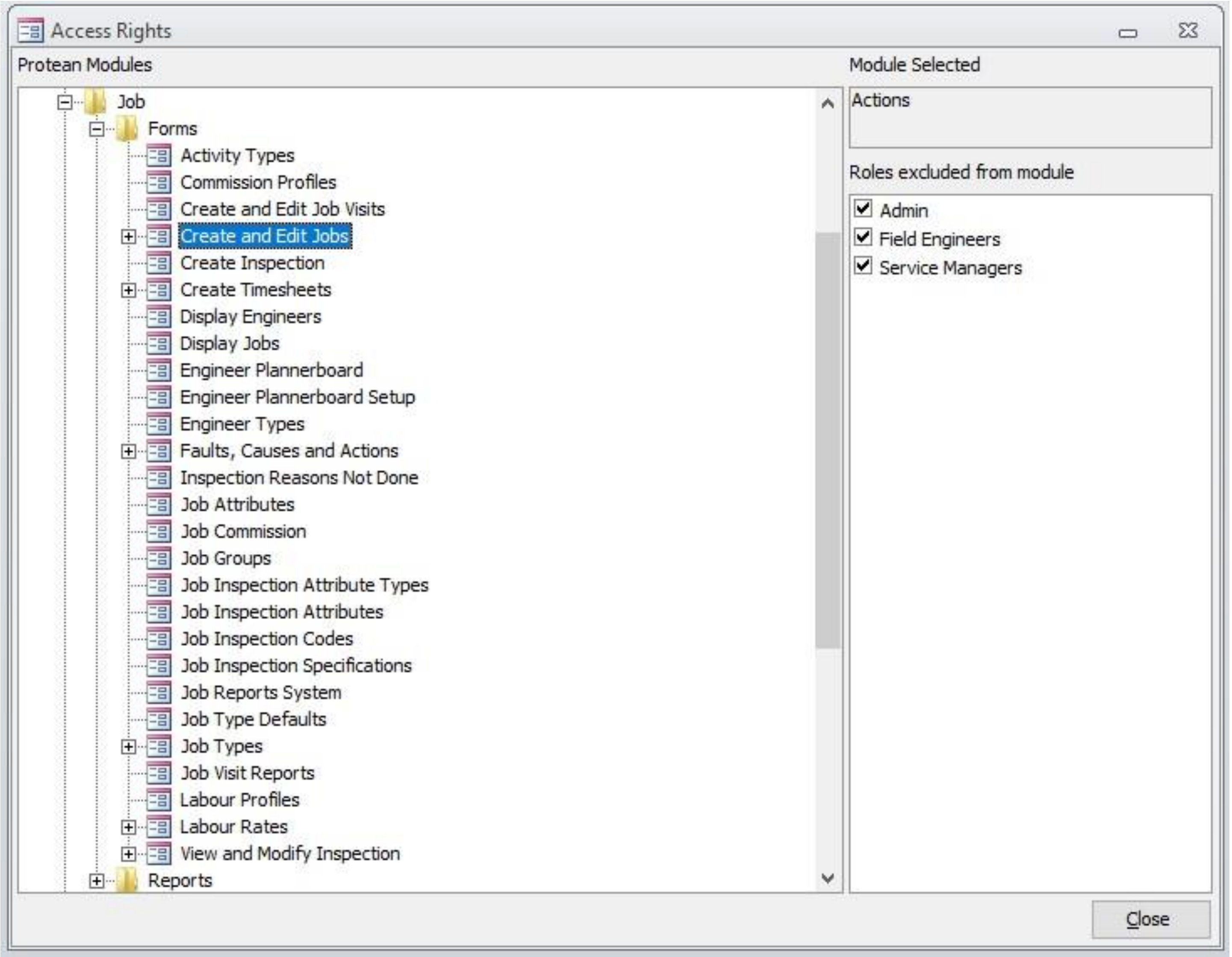
☑ Admin

☑ Field Engineers

☑ Service Managers

Taking *Jobs* as an example, we can see that expanding *Forms* gives us a list of both actions and configuration settings.

Ticking the box next to the *Role* allows us to exclude that role from being able to perform that action, same goes for any reports.



Access Rights

Protean Modules

- Job
  - Forms
    - Activity Types
    - Commission Profiles
    - Create and Edit Job Visits
    - Create and Edit Jobs
    - Create Inspection
    - Create Timesheets
    - Display Engineers
    - Display Jobs
    - Engineer Plannerboard
    - Engineer Plannerboard Setup
    - Engineer Types
    - Faults, Causes and Actions
    - Inspection Reasons Not Done
    - Job Attributes
    - Job Commission
    - Job Groups
    - Job Inspection Attribute Types
    - Job Inspection Attributes
    - Job Inspection Codes
    - Job Inspection Specifications
    - Job Reports System
    - Job Type Defaults
    - Job Types
    - Job Visit Reports
    - Labour Profiles
    - Labour Rates
    - View and Modify Inspection
  - Reports

Module Selected: Actions

Roles excluded from module

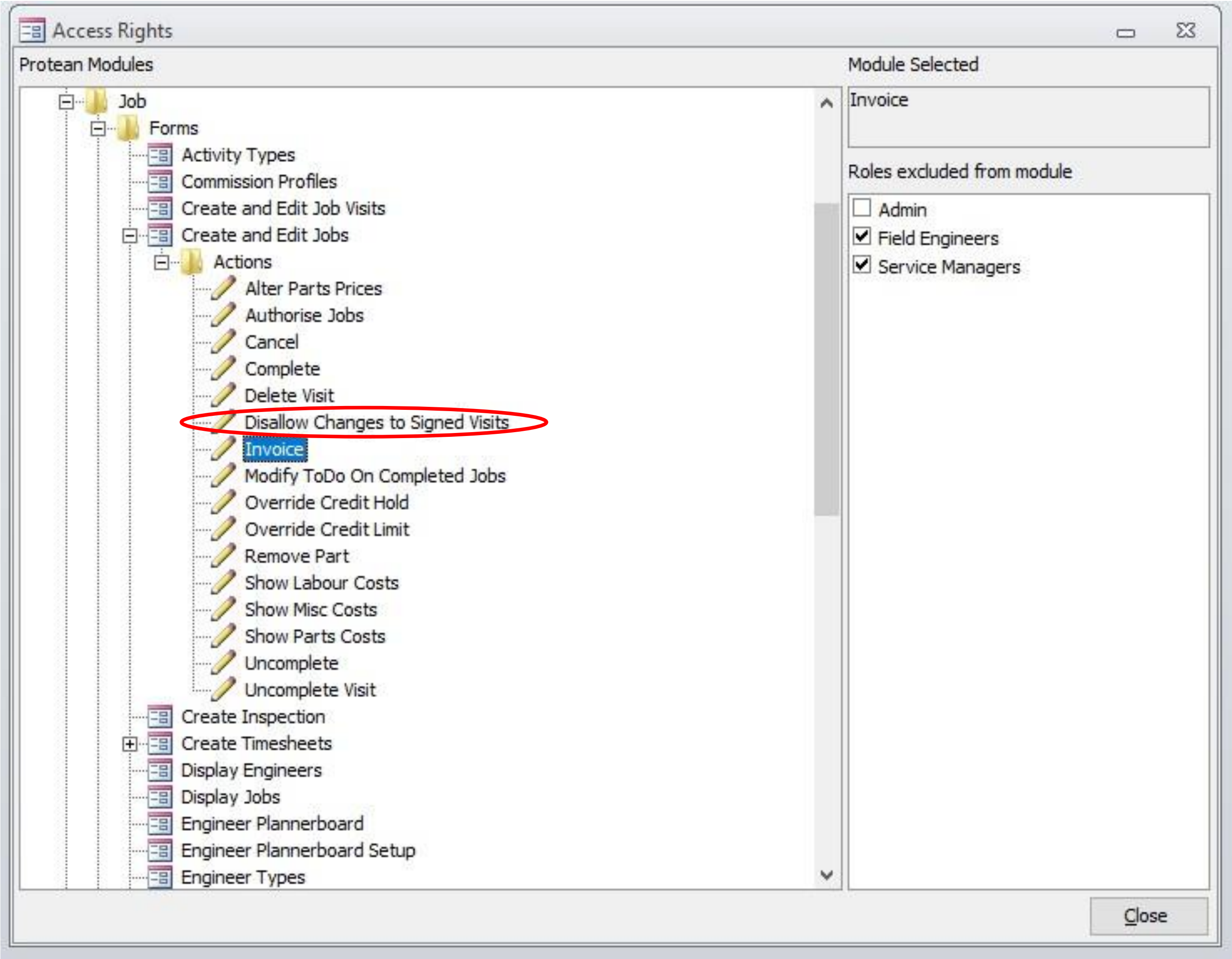
☑ Admin

☑ Field Engineers

☑ Service Managers

Going into more detail, expanding *Create and Edit jobs* now gives a list of job specific actions which we can now restrict.

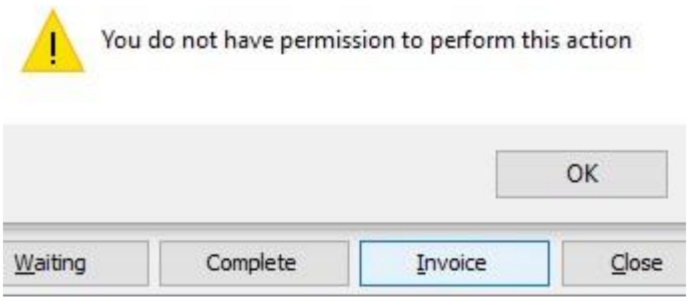
As shown below *Field engineers* & *Service managers* now do not have access to *Invoice* jobs. Result, when the user clicks on the invoice button within a job they will get a message to say *You do not have permission to perform this action.*



Module Selected: Invoice

Roles excluded from module

☐ Admin
☑ Field Engineers
☑ Service Managers


You do not have permission to perform this action

NOTE:

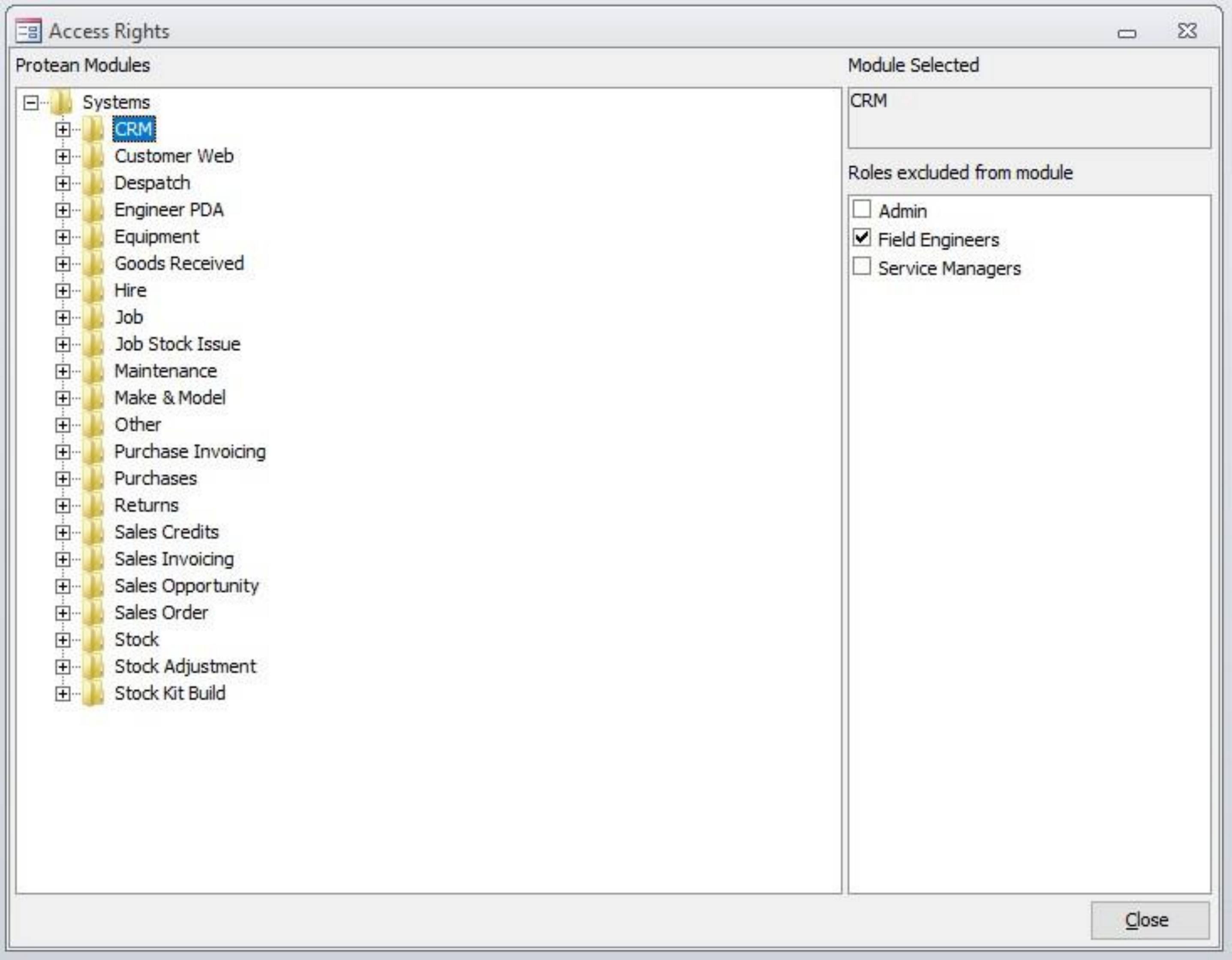
Exclusions to this rule are the named *Disallow* options (highlighted above). Whereas the others are ticked to *Exclude* the user from being able to perform that action, the *Disallow* options work in the opposite way.

Ticking the box for that *Role* enables the action for that user, example above is the *Disallow Changes to Signed Visits* if ticked any user associated with that *Role* will be able to make changes to job visits regardless if the visit has a signature from the customer or engineer.

Access Rights & Security roles

How to restrict and grant access to different areas of your Protean.

To restrict access to a whole module you do not need to tick each box when expanded. Simply highlight the module folder (CRM, Customer Web etc.) and tick the box next to the *Role*. This will restrict access to every item within that module.



Module Selected: CRM

Roles excluded from module

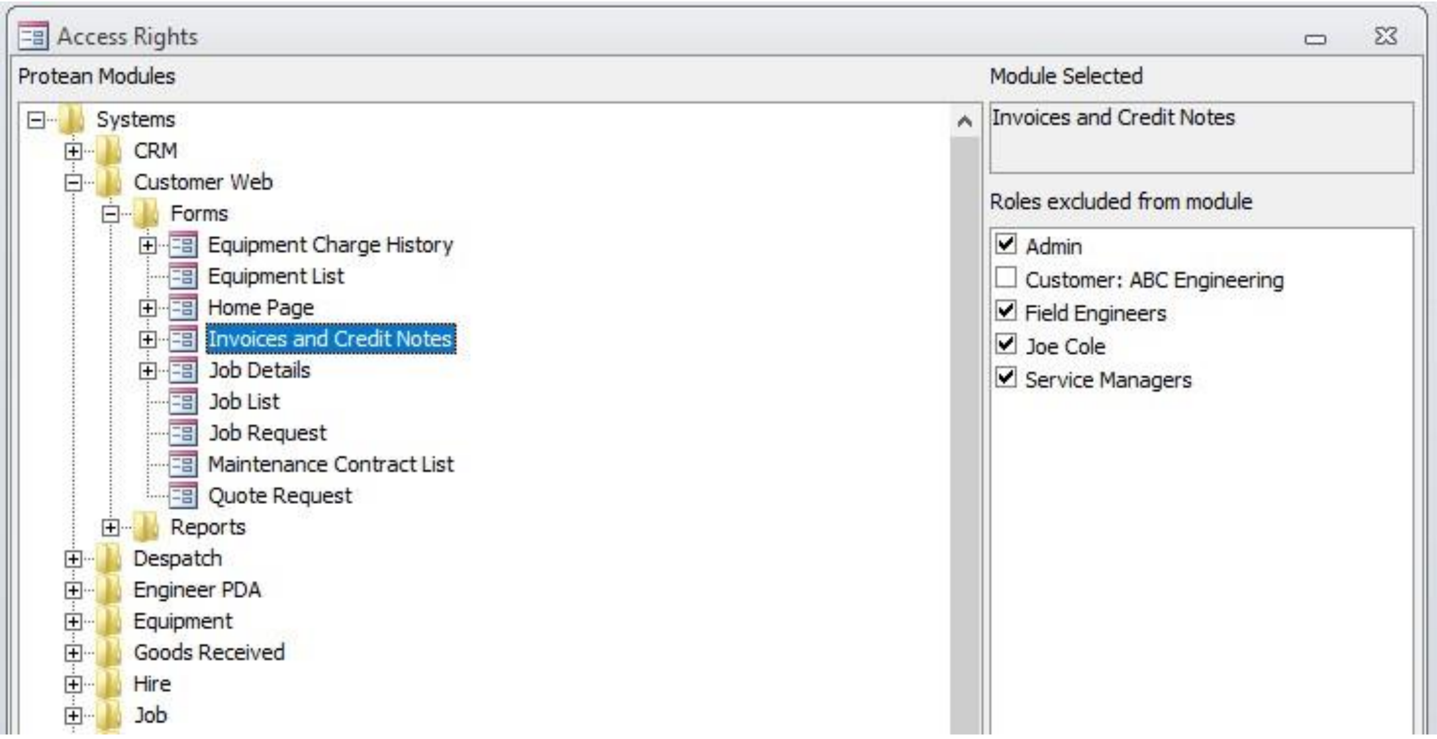
- □ Admin
- ☑ Field Engineers
- □ Service Managers

How are access rights determined for Mobile engineers and Customer Web logins?

System > Security> Access Rights

Protean Mobile app and Customer Web login have their own access rights module folders.

Often we may find ourselves in a situation where we do not allow an apprentice engineer to create/allocate a job to themselves or a customer who requests access to be able to see all previous invoices. To do this we first need to create a new *Security role* for that engineer/Customer. Once that's done we can then drive into that folder and find the action we want to restrict or grant.

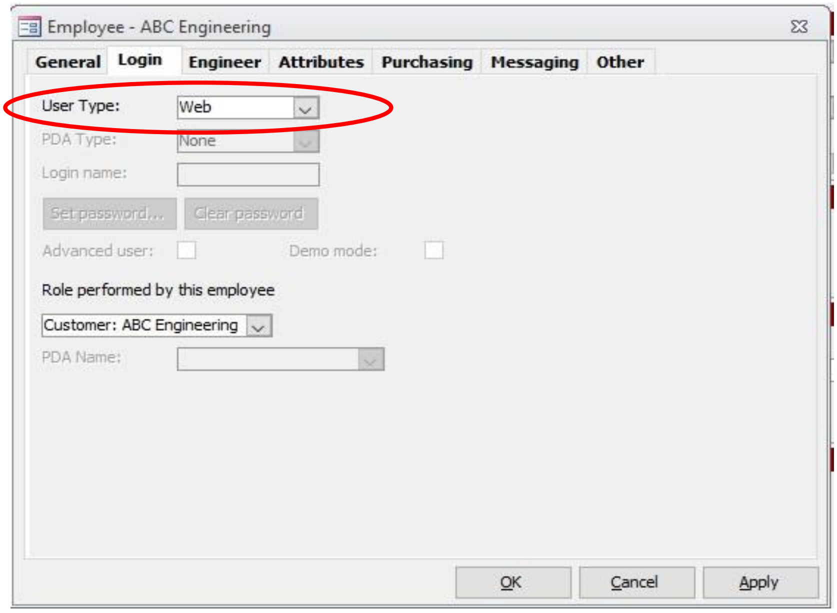


Module Selected: Invoices and Credit Notes

Roles excluded from module

☑ Admin
□ Customer: ABC Engineering
☑ Field Engineers
☑ Joe Cole
☑ Service Managers

Once you are happy with the access the customer will now have when logged in, you will need to create an *Employee* record within Protean for that customer and link the new *Role* to that *Employee*, mirror the configuration as shown below selecting *User type* as *Web*.



User Type: Web

PDA Type: None

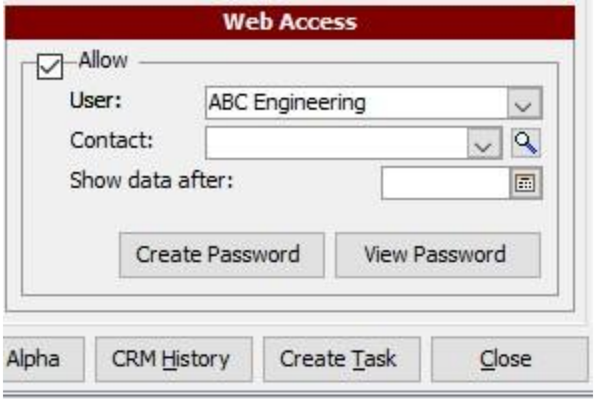
Login name:

Advanced user: □ Demo mode: □

Role performed by this employee: Customer: ABC Engineering

PDA Name:

Lastly, open the customer record and enable *Web Access* and in the *User* field select the new *Employee* we created:



Web Access

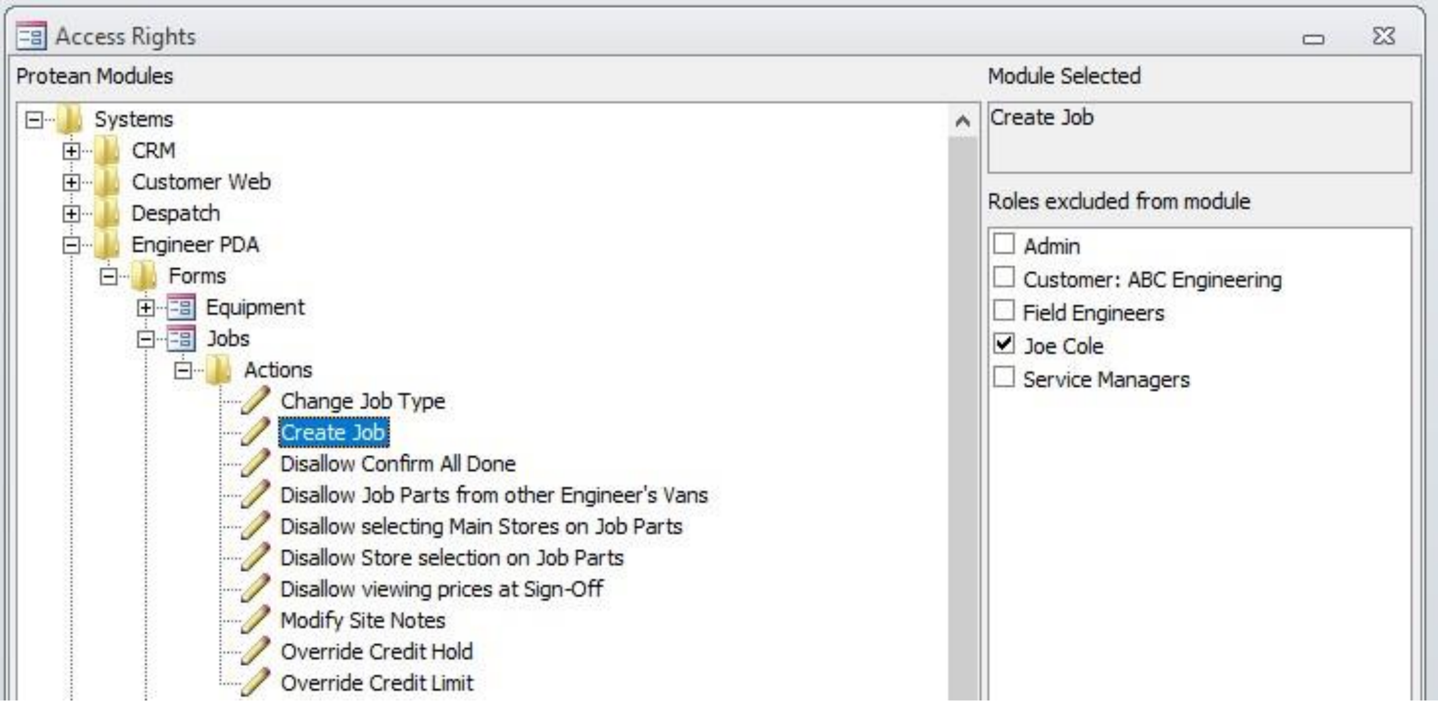
☑ Allow

User: ABC Engineering

Contact:

Show data after:

As for engineers, you'll first need to make the amendment in the *Access Rights* screen. And then simply link the *Role* to the *employee* record:



Access Rights

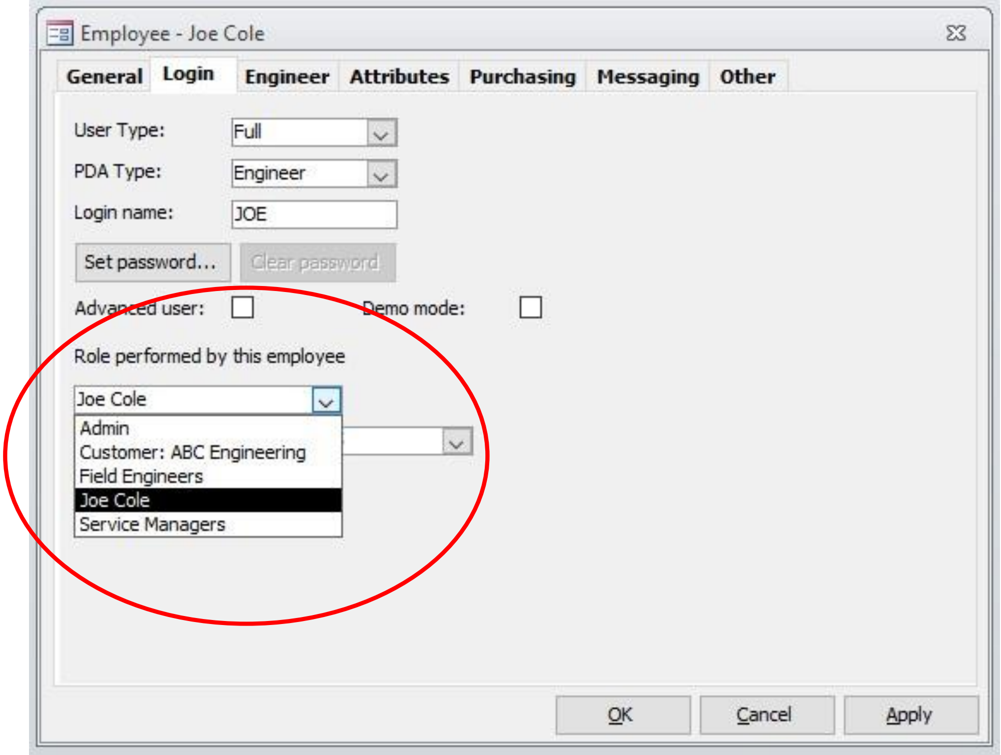
Protean Modules

- Systems
  - CRM
  - Customer Web
  - Despatch
  - Engineer PDA
    - Forms
      - Equipment
      - Jobs
        - Actions
          - Change Job Type
          - Create Job
          - Disallow Confirm All Done
          - Disallow Job Parts from other Engineer's Vans
          - Disallow selecting Main Stores on Job Parts
          - Disallow Store selection on Job Parts
          - Disallow viewing prices at Sign-Off
          - Modify Site Notes
          - Override Credit Hold
          - Override Credit Limit

Module Selected: Create Job

Roles excluded from module

- ☐ Admin
- ☐ Customer: ABC Engineering
- ☐ Field Engineers
- ☑ Joe Cole
- ☐ Service Managers



Employee - Joe Cole

User Type: Full

PDA Type: Engineer

Login name: JOE

Advanced user: □

Demo mode: □

Role performed by this employee

Joe Cole