cBRAIN
The Process Company

F2

Administrator manual

Version 6.1

6.1.0.40069

Table of contents

Reading guide

This manual is intended for existing, new and potential users of F2 who have one or more administrator roles. All functions that are available for an F2 administrator will be described in regards to configuration and functionality.

Commands (i.e. the buttons on which to click) are displayed in **bold**. Any reference to a field or a list is in "quotation marks".

Any references to other documentation in which further information on a specific functionality may be found are written in *italics*.

The manual features a number of screenshots to help find the described functions.

Screenshots with lines and associated text show where to click in F2 whereas screenshots with blue squares point to areas with several functionalities.

We hope you enjoy using F2.

Installing cBrain F2

Immediately after installing F2, the administrators of F2 can begin their administrative tasks.

A number of administrative and technical decisions are made before the final installation. These include:

- Organisational structure
- User roles
- Email import
- Security groups
- Users and their roles
- Keywords
- Case help
- Management flags
- File types
- Request types
- Document templates
- File plans.

Please refer to the relevant technical installation guides and checklists.

The basic installation of F2

Based on the outcomes of the configuration workshops with cBrain, F2 is installed with:

- An organisation known as the top unit which is the uppermost unit in F2.
- One role of the "Administrator" type. For more information see the section *Roles in F2.*

A user with the "Administrator" role can now log into F2 for the first time.

Introduction to administrative tasks

F2 administrator

A user with F2 administrator privileges can set up and configure F2.

In F2 there are four predefined administrator roles:

- Administrator
- User administrator
- Business administrator
- Technical administrator.

The predefined administrator roles and their corresponding privileges are further described in the section *Administrator roles*. All of them include special privileges to set up and change the basic functionality of F2.

Administrator tasks in F2

Many of the administrative functions can be performed in F2 directly. These functions are typically managed by a user with an administrator role.

The typical administrative tasks can be split into these categories:

- User administration:
    - Users, units and role types.
    - Privileges.
    - Access security and security groups for confidential case areas, e.g. HR.
    - Delegating administrative tasks using system roles and privileges.
- Communication:
    - The external participant register.
    - Distribution lists.
- Setup of the user interface for F2's main window:
    - Fixed searches.
    - The column setup in the results list.
- Setup of the user interface for the record window:
    - Document templates.
    - Keywords.
    - Flags for personal and unit management.
- The administration of various value lists e.g. keywords, progress codes (add-on module), file plan and cPort (add-on module).

The administrators' management of these tasks is described in this manual.

The user interface for F2 administrators

Administrators and standard F2 users share the same user interface. However, administrators do have a number of extra functions at their disposal.

Many administrator's tasks are accessed using the "Administrator" tab in F2's main window. Administrator related functions for the setup and maintenance of F2 are found in the ribbon.

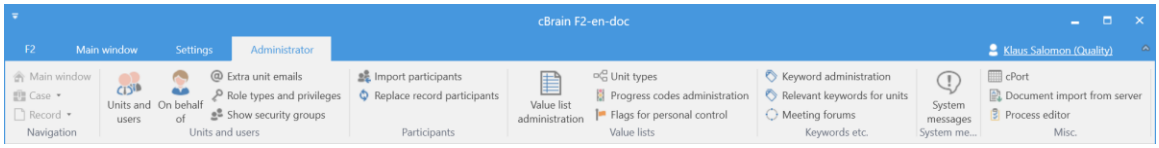


Figure 1: The ribbon on the "Administrator" tab in the main window

Note: The menu items available in the ribbon of the administrator tab will vary depending on the administrator's privileges and which add-on modules that are included in the F2 installation. Users may experience that some functions that are described and shown in this manual are not available in their F2 installation.

The unit structure in F2

It is important the user retains a general knowledge of F2 in order to understand the administrative tasks. For this, please refer to the F2 Desktop Functionality description.

Below follows a short explanation of how F2 organises authorities and units in a tree structure. In F2 all users are organised into units. A user is always attached to a unit.

To create a user, there must be at least one defined unit in an organisation. The reasoning behind this is that F2 in most cases relates read and write access to documents depending on the unit structure. F2's unit structure can, roughly, correspond to the structure of the organisation, although typically not in all facets.

The unit structure in F2:

- **Top unit/Organisation**: This unit is the parent unit in F2. It is established when installing F2. There can only be one top unit for each F2 installation. This can e.g. be a ministry or a company.
- **Authority**: This unit represents a legal unit in F2. Full separation exists between the different authorities in an F2 installation. There is no limit to the number of authorities that can be created in F2. An authority can e.g. consist of a department and a number of government agencies or a company with several subsidiaries.
- **Units**: An unlimited number of units and subunits can be created within an authority. These can mirror the overall organisation within the authority. Each record can be access restricted to a unit. This influences who can view and work on the records and documents.

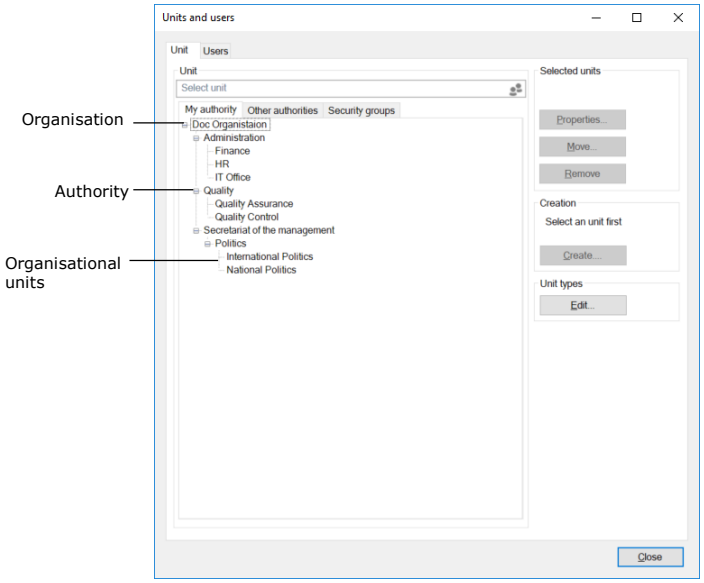


Figure 2: An example of F2's tree structure

Note: The top unit/organisation is only visible on the "Other Authorities" tab and not on the "My authority" tab".

Create an authority

An authority's internal structure is comprised by the units created in the "Units and users" dialogue.

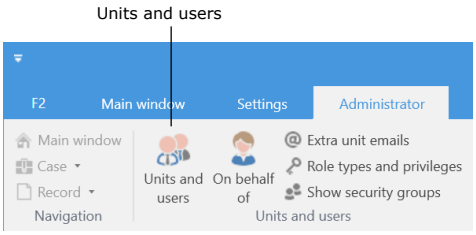


Figure 3: The "Unit and users" menu item

Click on **Units and users** in the "Administrator" ribbon of F2's main window to create a new unit. The dialogue below opens.

The dialogue shows an organisation called "Doc Organisation". This organisation has the authorities: "Administration", "Quality", and "Secretariat of management".

Another authority within "Doc Organisation" is to be created with the title "Digital Authority". Click on **Create** in the "Units and users" dialogue to open the "Create unit" dialogue.

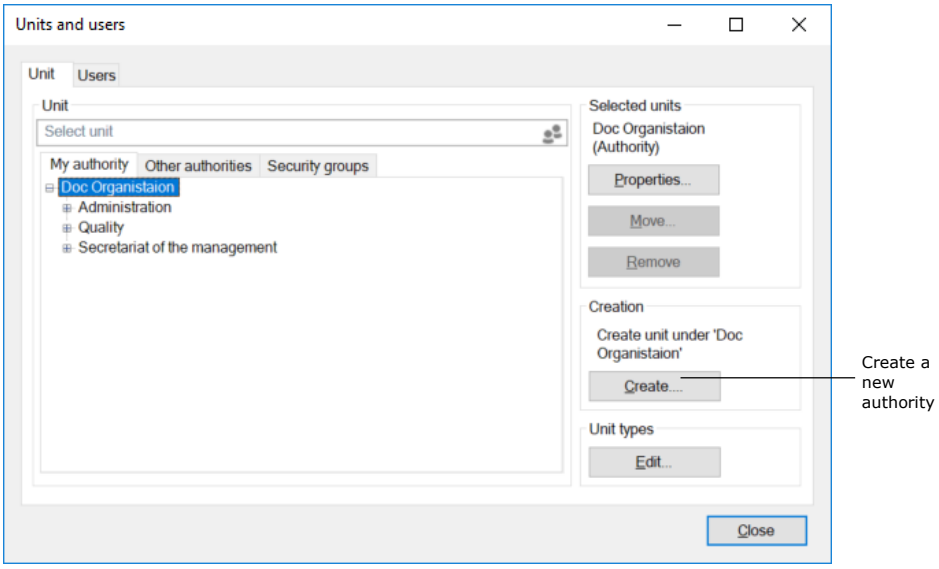


Figure 4: Create a new authority

Enter the relevant information about the Digital Authority in the dialogue.

Set the unit type to "Authority".

The system provides the location after the unit is created.

Additional fields can be filled out if needed.

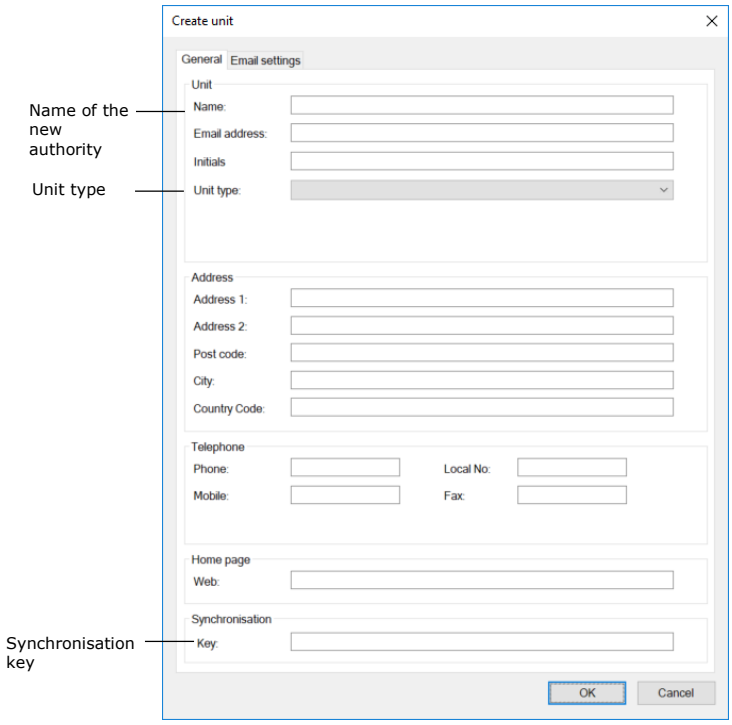


Figure 5: The "Create unit" dialogue

The authority's email settings can be modified on the "Email settings" tab.

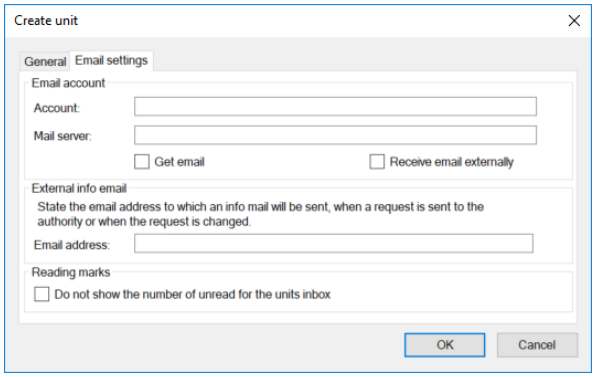


Figure 6: The "Email settings" tab in the "Properties for the unit Digital Authority" dialogue

Read more about email settings in the section *Managing emails.*

When the necessary fields have been filled out in the dialogue, click on **OK**. The warning dialogue below appears.

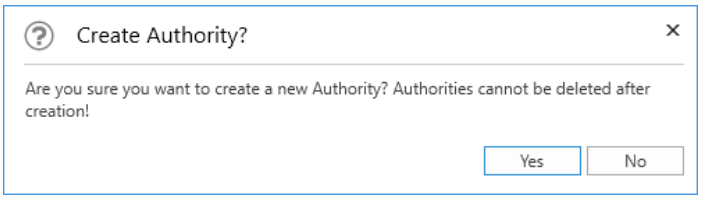


Figure 7: The "Create authority?" dialogue

The warning dialogue informs the administrator that once an authority is created it cannot be deleted.

Click on **No** to return to the "Create unit" dialogue.

Click on **Yes** to proceed. The authority "Digital Authority" is created, and units and users can now be created within this authority. View the newly created authority in the figure below.

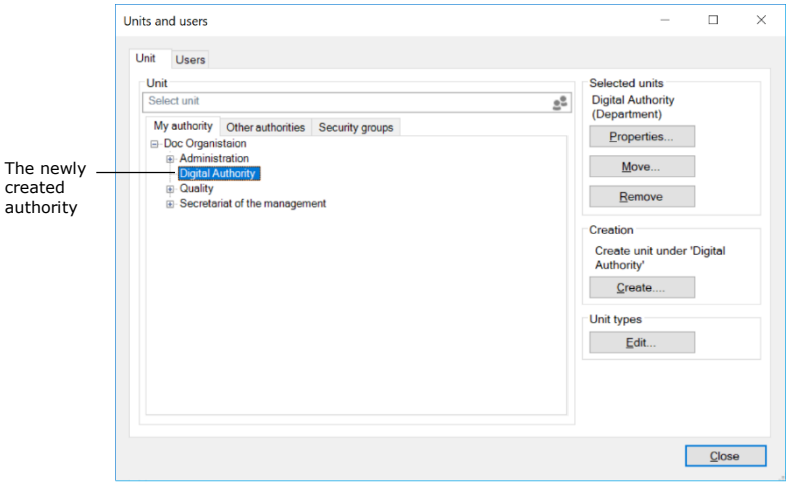


Figure 8: The newly created authority

Create units within an authority

In F2, the organisational structure is mirrored through a number of units. Units are created and maintained by administrators or user administrators.

One purpose of the units is, among other things, to tell F2 where to place the users when matching roles and units are synchronised using synchronisation keys during full AD integration. During standard AD integration the administrator creates the users in the units him/herself.

The user's affiliation with a unit is important as it influences their read and write access to records for which the access is set for the specific unit.

An administrator accesses units by clicking on the menu item **Units and users** in the ribbon of the "Administrator" tab.

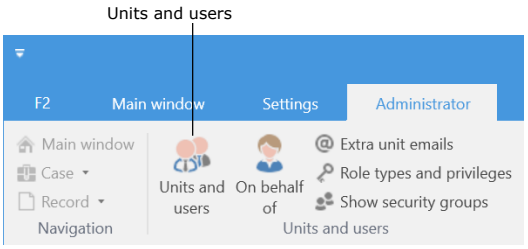


Figure 9: The "Units and users" menu item

The "Units and users" dialogue opens. Here a user with the "Unit administrator" privilege can create, edit, move and/or deactivate units.

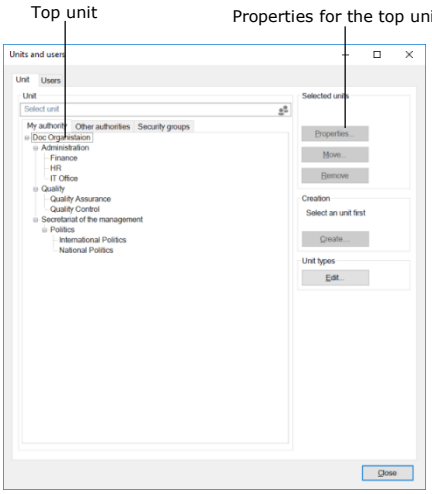


Figure 10: F2 is installed with only one top unit

As mentioned, F2 is installed with one top unit (organisation). The name of the top unit is adjusted to fit the organisation's name when F2 is installed. In the figure above "Doc Organisation" is the top unit. Edit the name by selecting the unit and then clicking on **Properties**.

Expand the top unit to view the "Authority" unit types that are created in the tree structure. These units can also be expanded to show the underlying units.

The "Unit" tab displays the units in F2. They are embedded in a tree structure. Create a new unit by selecting a "main unit" in the directory and click on **Create**.

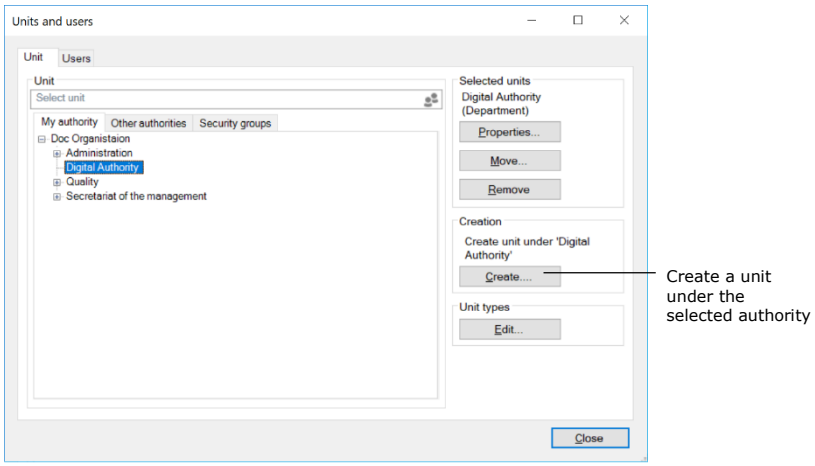


Figure 11: Create units within an authority

The "Create unit" dialogue opens as shown to the right.

Fill in the relevant information in the dialogue.

In the "Unit type" field, select which type this unit represents. See below for more information regarding the management of unit types.

Units are created in the same dialogue that is used for creating authorities.

An organisational structure within an authority can contain many units.

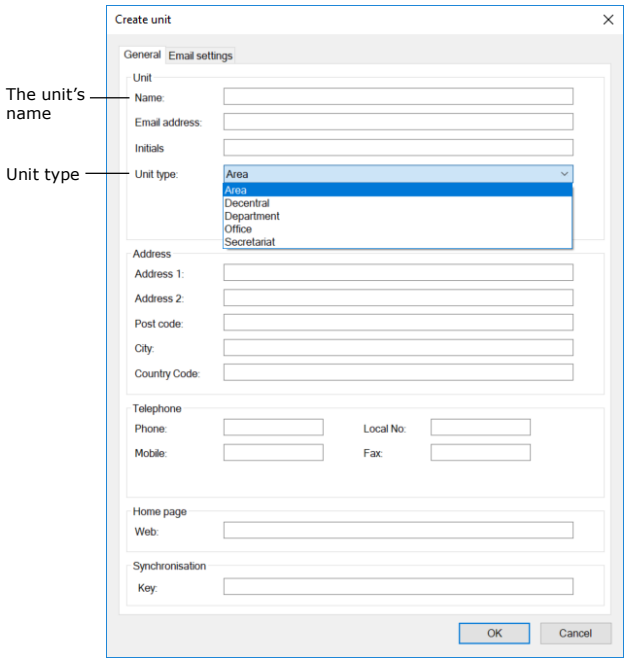


Figure 12: The "Create unit" dialogue

Read more about configuring email on the "Email settings" tab in the section *Managing emails.*

Create unit types for specific units

F2 categorises units into unit types. F2 contains definition of fixed unit types that are created during the installation of F2.

Some unit types cannot be deleted afterwards as they are used by F2. The names of these units may vary as they depend on the organisation. New unit types can be added later, and unit types that are not in use can be deleted again.

Click on "Unit types" in the ribbon on the administrator tab in F2's main window to manage the unit types.

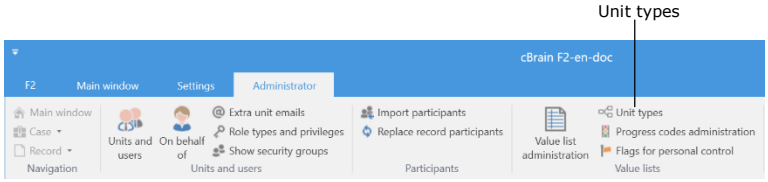


Figure 13: The "Unit types" menu item

Click on **Unit types** and the dialogue below appears. The unit types are managed here.

These are examples of the unit types available:

- Authority
- Organisation
- Department
- Office
- Area
- Secretariat.

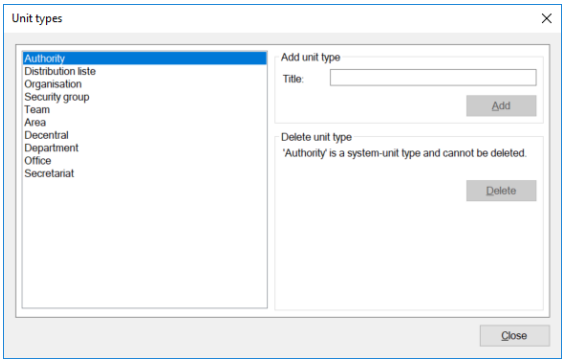


Figure 14: Management of unit types

Unit types such as teams and security groups are used to split users into teams and security groups across the authority.

When a unit type has been created, it can be used when creating units (the organisational division).

Decentral units

A unit of the "Decentral unit" type functions as any other F2 unit, but unlike normal units it is not synchronised with Active Directory (AD).

A decentral unit can be used for project cooperation across units, and extra email addresses can be attached.

Decentral units are created by a user with the "Decentral unit and user administrator" privilege.

In order to affiliate a user with a decentral unit, the user must have one of the three roles:

- **Decentral role:** This is a job role that lets the user login and work in a decentral unit.
- **Decentral read access:** This is a job role that lets the user search for records whose access is normally restricted to users in a decentral unit. The role is equivalent to the "Read access to another unit" role.
- **Decentral read/write access:** This is a job role that lets the user search for records whose responsibility lie with a decentral unit and whose access restriction is either "Unit" or "All". The role is equivalent to the "Write and read access to another unit" role.

Below is an example of when decentral units are useful:

An organisation has a number of units that work independently of the central administration. These units would like to maintain a unit structure across of standard F2 units. The F2 administrator gives one or more users in the organisation the "Decentral unit and user administrator" privilege, which lets them maintain the decentral units.

User administration

An administrator with the "User administrator" privilege can create users in F2. Users are created in an authority and can also be attached to a unit. A user needs to have a "job role" before he/she can log in to F2.

The creation of a new user is described below. Once the user is created, he/she needs to be assigned roles of which one must be a job role. The roles are affiliated with units and contain one or more privileges. Privileges let the user perform different actions in F2.

One or more role types must be defined before a user can be given a role. The role type "job role" must have been created. Read more about the creation of role types in the section *Create and administer role types.*

Create user

Access to different functions in F2 is controlled using roles. Every role is given one or more privileges. In order for a user to log in to F2, one of these roles must be a "job role". It is only possible for a user to access F2 through a job role.

Administrators/user administrators can create users in F2 by clicking on the **Units and users** menu item in the ribbon on the "Administrator" tab.

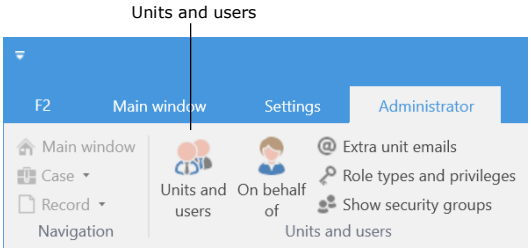


Figure 15: The "Units and users" menu item

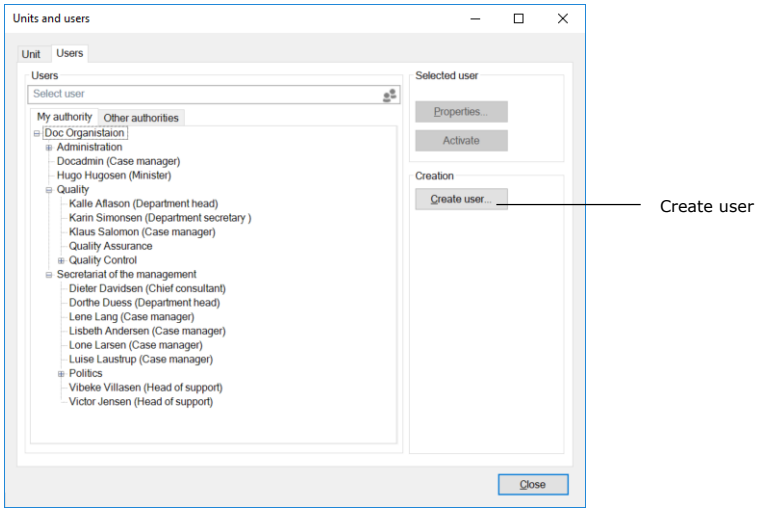


Figure 16: Create user

A dialogue opens in which the user's master data is entered.

Create user – information

For every user the master data, including name, initials, email address, user name, etc., must be added. This is done on the "Information" tab as displayed below.

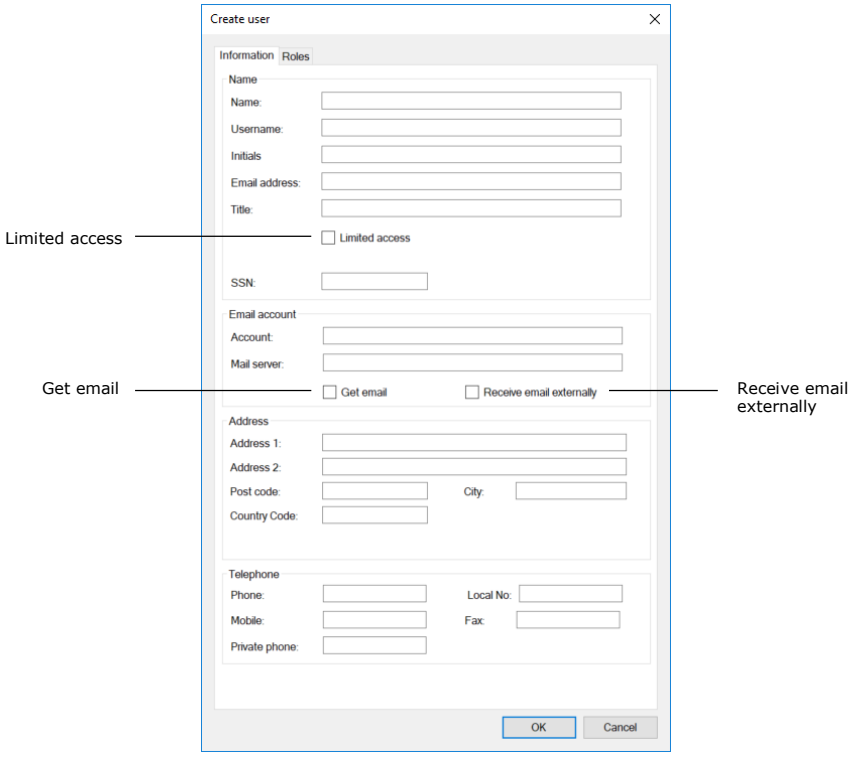


Figure 17: User information

The following table explains selected fields from the "Information" tab in the "Create user" dialogue.

Field	Function
"Limited access"	If the "Limited access" box is ticked, the user will only see the records to which he/she has been added in the "Access limited to" field on the record. The user must also have access to the record by e.g. being added as a supplementary case manager. The limited access function is used for F2 users that only need limited and controlled access to records.
"Get email"	The consequences of ticking this box depend on F2's configuration. For installations with full email import, F2 transfers all emails from Outlook's inbox to the user's F2 inbox. A record is created for every imported email. In this case, ticking the "Get email" box is not necessary. If email import is manual, the user must move relevant emails from Outlook using its "Move to F2" folder. The emails will then appear in both the "Moved to F2" folder in Outlook and "My inbox" in F2. The third option is to automatically transfer all emails from the inbox in Outlook that are replies to mails from F2. This is configured on the server by a technician.
"Receive email externally"	If this box is ticked, the user will only receive emails in Outlook. This also applies to emails sent internally in F2 to the user. Any other communication channels are not affected by a tick in the "Receive email externally" box. For example, chats and records that are either sent or for which the responsibility is allocated internally will still be found in F2 only.

Note: The "Get email" and "Receive email externally" boxes cannot both be ticked. Ticking "Receive email externally" lets the user work with a different email client alongside F2. In this case, emails must be manually transferred to F2 using the "Move to F2" folder.

Click on **OK** when the fields are filled in. The user then needs a job role. This is described in the next section.

Create user – roles

A new user must be assigned a job role. Fill out all the relevant fields on the "Information" tab and click on **OK**. The focus will then automatically shift to the "Roles" tab. Here, the user must be assigned a job role in either the top unit or in a unit.

Click on **Add role** on the "Roles" tab.

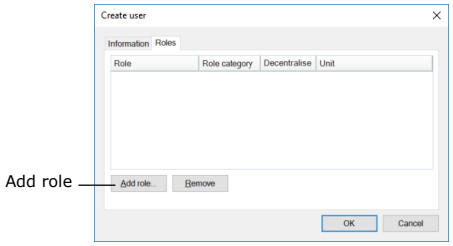


Figure 18: The "Roles" tab in the "Create user" dialogue

Note: An administrator can see which role types are categorised as "job" in the "Role types and privileges" dialogue that is accessible via the menu item on the "Administrator" tab. For more information about role types and privileges see the section *Create and administer role types*.

The "Add role to [user]" dialogue opens. Select the authority or unit with which the user must be affiliated. Then select a role type in the drop-down menu "Role type".

Click on **OK** and the "Add role to [user]" dialogue closes.

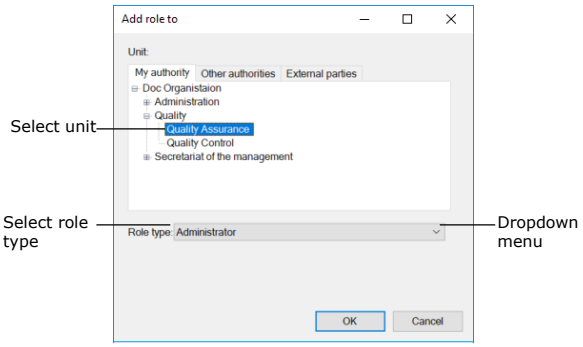


Figure 19: Add a role to a new user

Note: It is important to select the correct unit in which the user is given a role. The role and its location determines the user's authority a within the selected unit.

The "Roles" tab now shows that the new user has been assigned the role.

Click on **OK**. The user is created and can now log into F2.

When a user is created, he/she can be assigned several roles. Roles have associated privileges that lets the user perform different tasks in

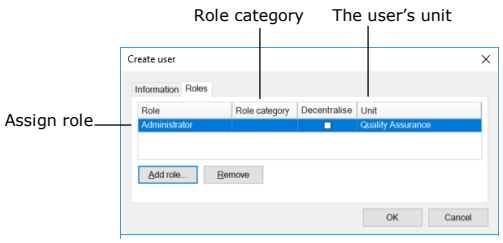


Figure 20: Assign a role to a new user

F2. Read more in the section *Roles in F2*.

> **Note**: New users are always created with the "Mailing list owner" role type. Read more about roles in the section *Roles in F2*.

Deactivate a user

It is not possible to delete a user in F2. A user can instead be deactivated. To deactivate a user, click on the menu item **Units and users** in the ribbon of the "Administrator" tab in the main window.

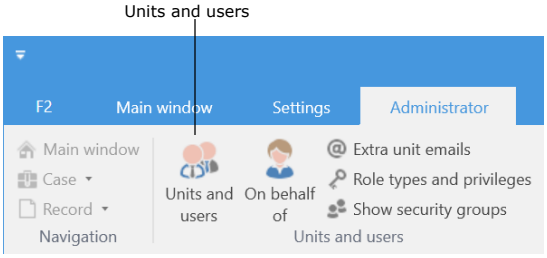


Figure 21: The "Units and users" menu item

The "Units and users" dialogue opens. In the dialogue, click on the "Users" tab. Select the user in the tree structure and click on **Deactivate**.

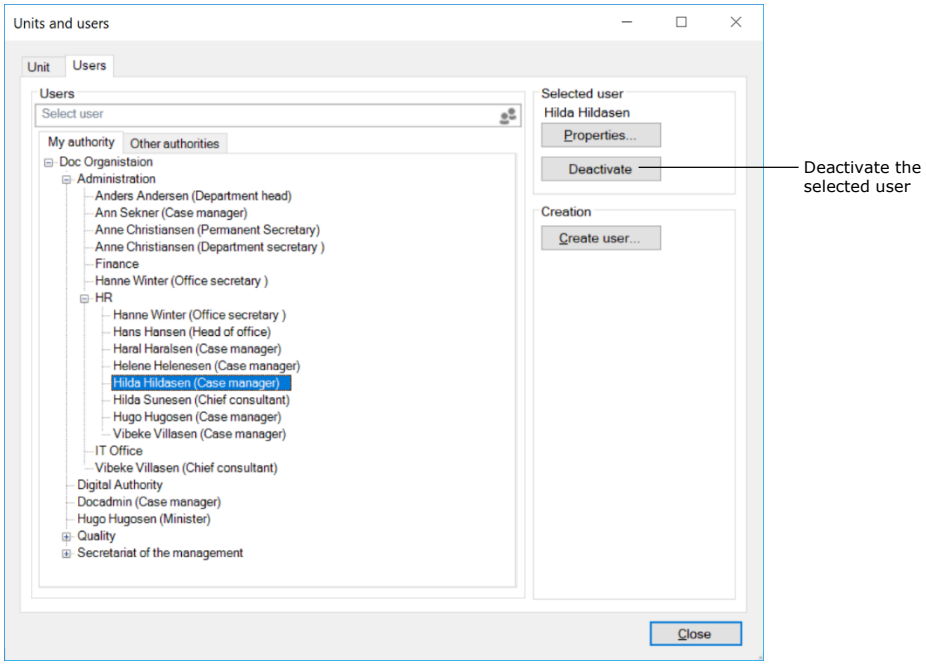


Figure 22: Deactivate a user

A warning dialogue opens. Click on **Yes** to continue deactivating the user.

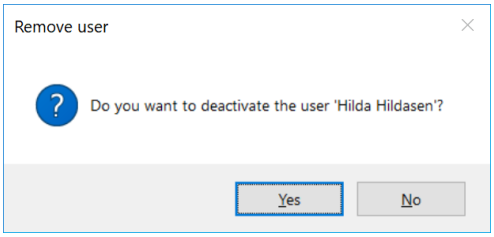


Figure 23: The warning dialogue when deactivating a user

A deactivated user is displayed in italics.

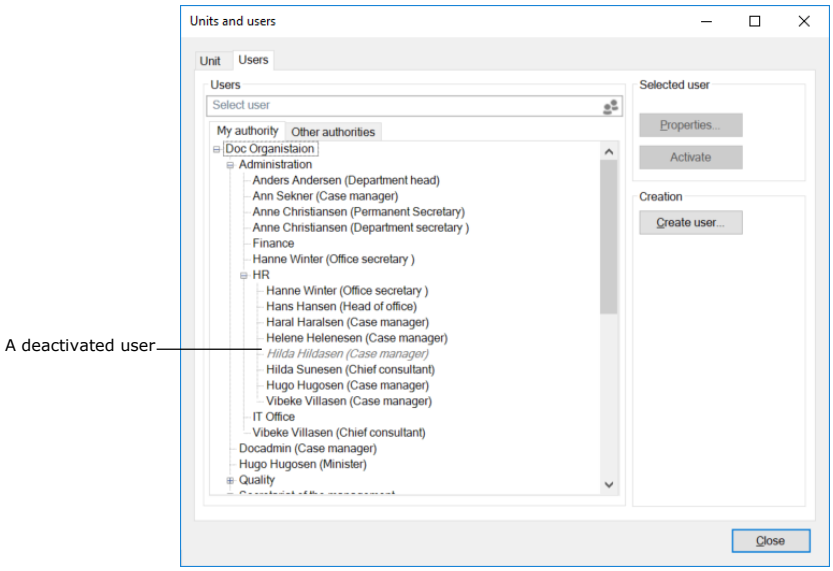


Figure 24: A deactivated user

Note: A user must be deactivated in both F2 and Active Directory. If the user is only deactivated in F2, the user will be reactivated via the AD import.

Activate a user

A deactivated user can be activated by clicking on the **Units and users** menu item in the ribbon of the "Administrator" tab in the main window.

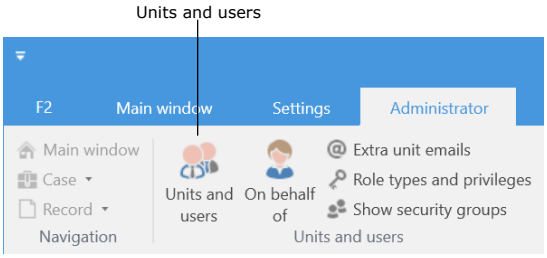


Figure 25: The "Units and users" menu item

The "Units and users" dialogue opens. In the dialogue, click on the **Users** tab. Select the user in the tree structure and click on **Activate**.

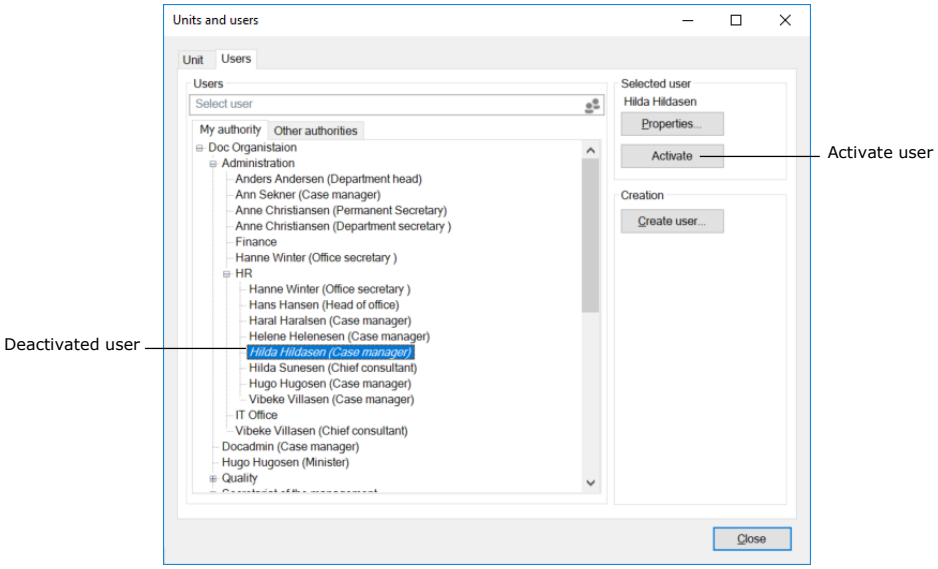


Figure 26: Reactivate a user

A warning dialogue opens. Click on **Yes** to reactivate the user. Select the user again and click on **Properties**. The "Properties for the user [user name]" dialogue opens.

When the user is deactivated, the user name field will state "Not employed". For the user to be reactivated completely, the "User name" field must contain the user's name, in this case Hilda Hildasen. Either the user's full name or an abbreviated version, e.g. the initials used for login and/or email, must be entered here.

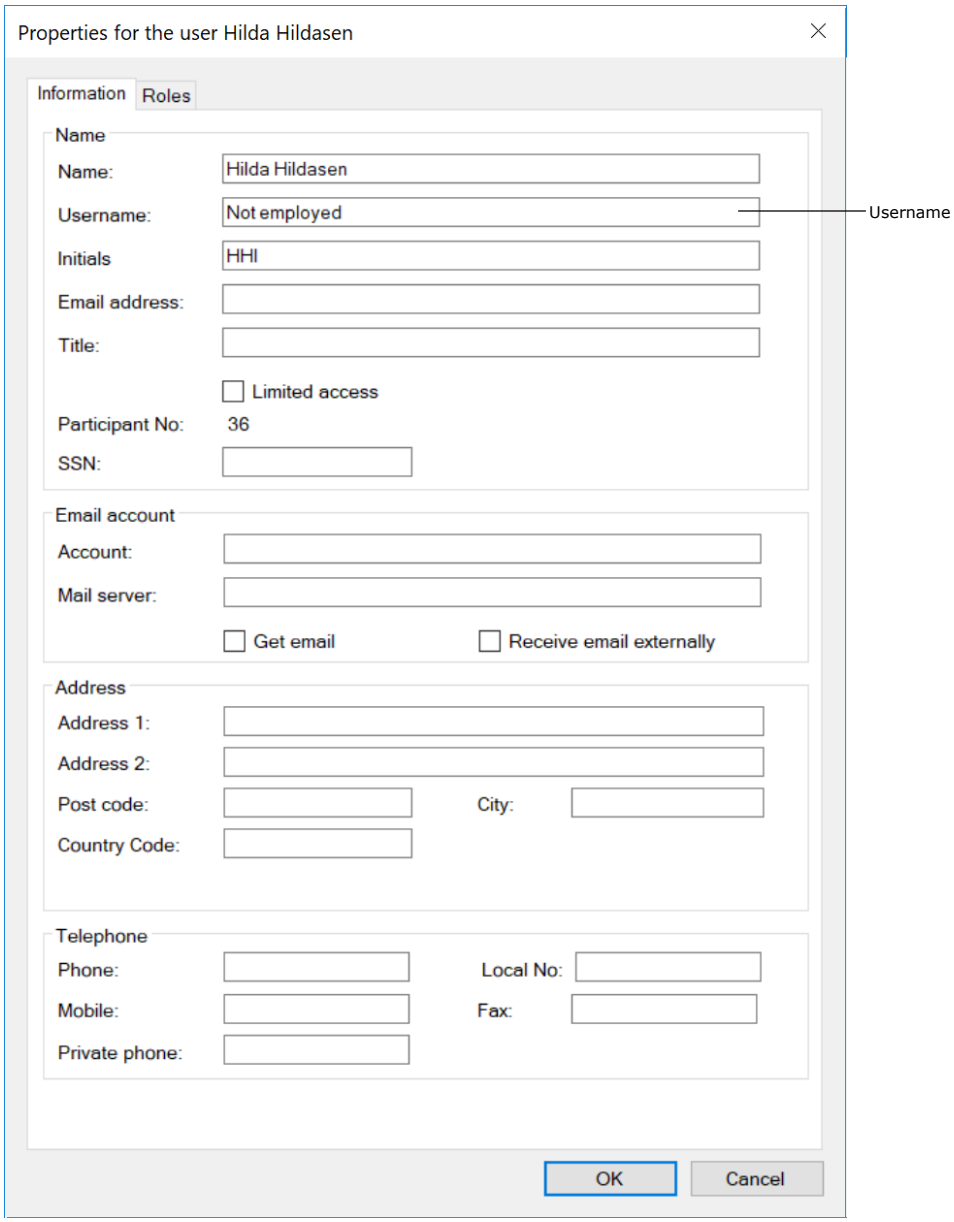


Figure 27: The "Properties" dialogue for the reactivated user

If F2 has not automatically executed this change during reactivation, it must be done manually.

Note: Only when the "Username" field contains the participant's username, does F2 consider the user completely activated.

Note: A user must be reactivated in both F2 and Active Directory. If the user is only reactivated in F2, the user will be deactivated via the AD import.

On behalf of

In a number of situations, a user may need access to another user's inbox for either a fixed time period or on a permanent basis. For example, a secretary may need access to his/her manager's inbox.

There are two ways of allocating "on behalf of" rights:

- A permanent allocation given by an administrator.
- An ad hoc allocation which can also be given by a user.

The permanent "on behalf of" allocation is managed by a user with the "On behalf of administrator" privilege.

A user who is allocated "on behalf of" rights has "on behalf of" access to another user's F2. This includes the records located in the user's "My private records" list. Two types of "on behalf of" rights exist:

- "Can perform all actions"
- "Can process approvals" (add-on module).

A user with the "On behalf of administrator" privilege can allocate "on behalf of" rights to other users. In the following section this is described in further detail.

Setup of "On behalf of"

Click on **On behalf of** in the "Administrator" tab to open the "On behalf of" dialogue.

The dialogue shows which users have "on behalf of" rights for other users. It is possible to assign or remove the "on behalf of" rights in this dialogue.

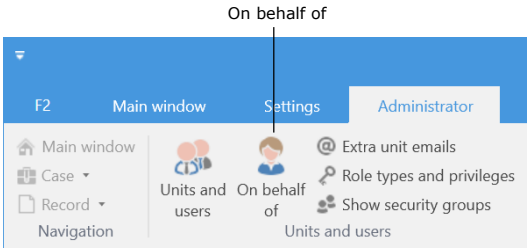


Figure 28: The "On behalf of" menu item

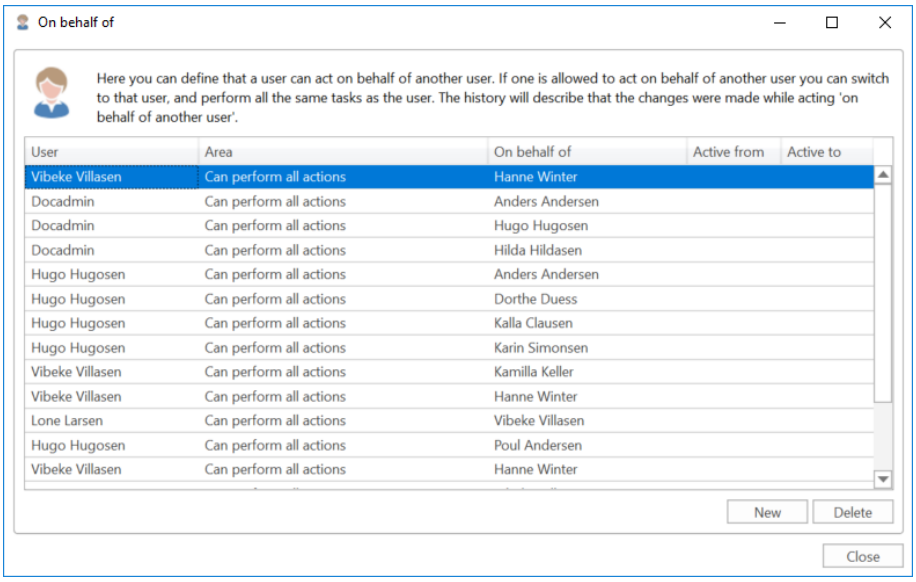


Figure 29: The "On behalf of" dialogue

Click on **New** to assign a new "on behalf of" relation. A dialogue opens in which the administrator can assign a user "on behalf of" rights to another user's F2.

The administrator also selects which type of "on behalf of" rights the user is assigned:

- "Can perform all actions". This is the full "on behalf of" rights.
- "Can process approvals" (add-on module). This a partial "on behalf of" right.

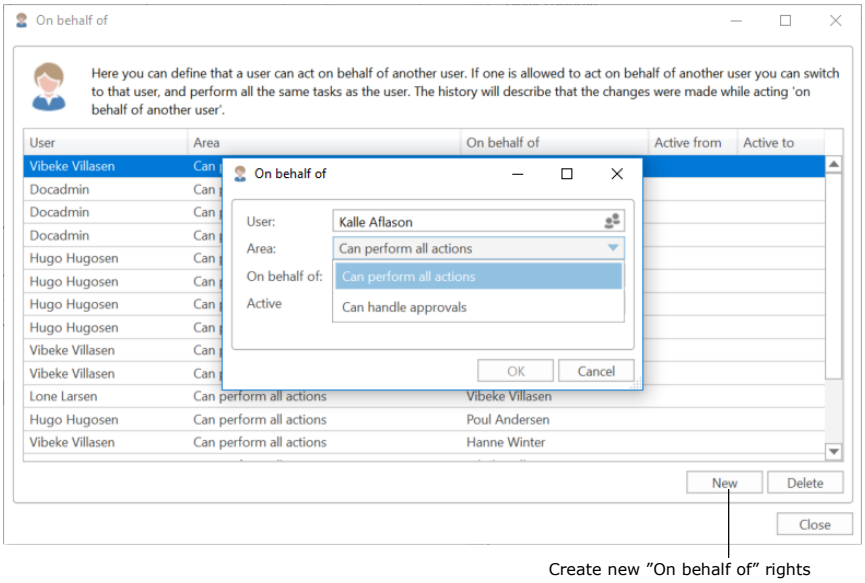


Figure 30: Assigning "on behalf of" rights for all areas

If a user is given rights to process approvals e.g. for his/her manager, it is possible to specify where approval notifications are received (add-on module).

The notification can be sent to either the user's personal inbox or in the unit's inbox.

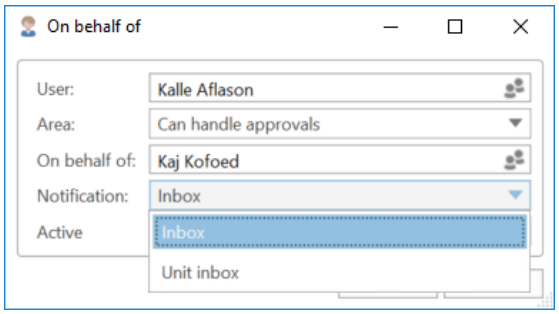


Figure 31: Select the location for approval notifications

The "on behalf of" access can be given a duration. If a duration is not set, the access is active from the time it is assigned until it is removed again.

Click on **OK** to complete.

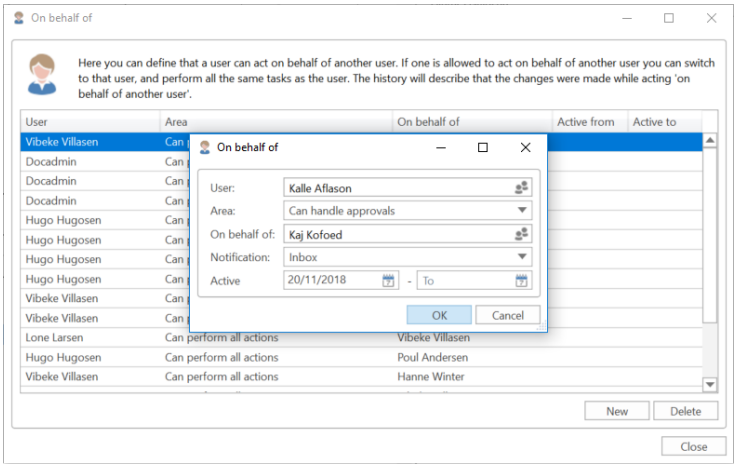


Figure 32: Assign "On behalf of" rights for processing approvals

Managing emails

F2 offers several variants of email integration with commonly used email systems.

Email settings can be configured in F2 on different levels: authority, unit and user. Using the add-on module F2 Shared mailboxes it is possible to create and set up shared mailboxes/email addresses for each unit.

This section describes the administrator's options for setting up emails during installation and during the ongoing work in F2.

Emails for users are set up during the installation of F2.

Set up mailboxes for authorities and units

This section describes how unit mailboxes are set up for an F2 authority and its units. A unit mailbox is a mailbox that belongs to a unit or authority in F2, for example an HR unit inbox for inquiries regarding HR cases.

Unit mailboxes may be automatically imported into F2 from a shared email address in e.g. Exchange. An administrator can facilitate this from the "Properties for the unit" dialogue as shown in the figure below.

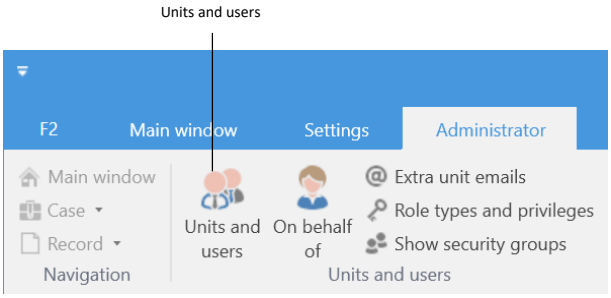


Figure 33: The "Units and users" menu item

Click on the **Units and users** menu item in the ribbon of the "Administrator" tab. Select the relevant unit from the tree structure in the dialogue and click on **Properties**.

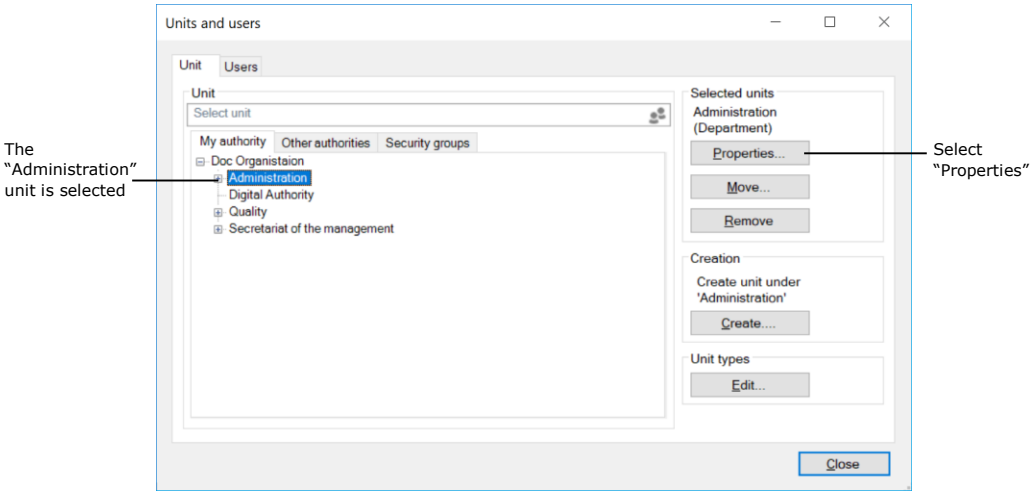


Figure 34: The "Units and users" dialogue

The "Properties for the unit [the name of the unit/authority]" dialogue opens as shown below.

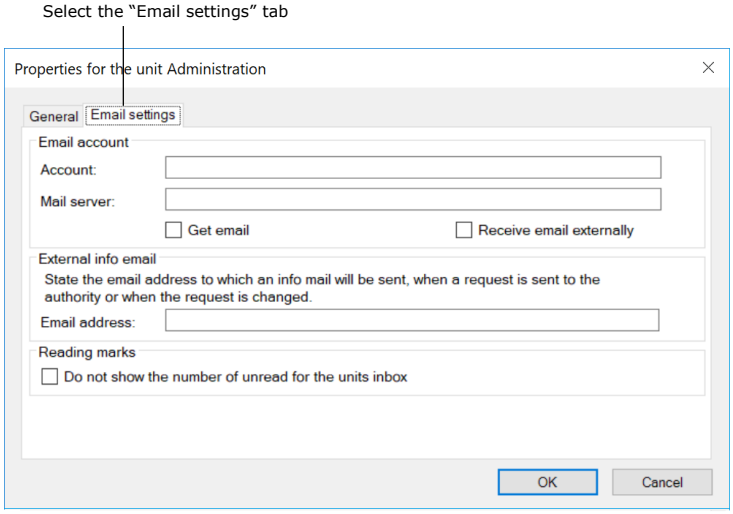


Figure 35: Setting up a unit inbox

Fill in the following fields on the "Email settings" tab to create a unit inbox for an authority or a unit:

Field	Description
"Account"	Enter the email address for the mailbox in the email system.
"Mail server"	Enter the name of the mail server. The organisation's IT department will know this.
"Get email"	Tick this box and all incoming emails will automatically be imported from the email server to the unit's inbox in F2.
"Receive email externally"	Tick this box and all incoming external emails for the unit will be received in an external email system.
"External info mail"	Insert a participant from the unit's external email here and he/she will receive a notification email when the unit receives an email or a request in F2. The participant also receives a notification email if a change is made to a request. External notification emails are mainly used in connection with group requests (add-on module).
"Read markings"	Tick this box to hide the number of unread emails in the unit's inbox next to its name in F2's main window.

Once the fields are filled in, F2 is able to import emails from the specified email address. Records are automatically created for the imported emails and the specified unit is set as the recipient.

Imported emails are automatically moved to the "Moved to F2" folder. Emails sent to the shared email address are placed in the "Unit inbox" om F2 so everyone in the unit can view them.

Create suffixes in the subject field of external emails

An administrator can configure the subject field of outgoing emails to contain either the record ID or the case number.

The purpose of attaching a record ID/case number as a suffix in the subject field is:

- To give the recipient a point of reference to the mail for later use.
- To automatically relate an email sent from F2 to an externally received reply.
- To automatically attach a reply email to the case of the original email.

The subject field for all of the authority's outgoing emails is configured on the "Email settings" tab in the "Properties for the unit" dialogue. Select the "Units and users" menu item on the "Administrator" tab to open the dialogue. Choose an authority from the list and click on **Properties**.

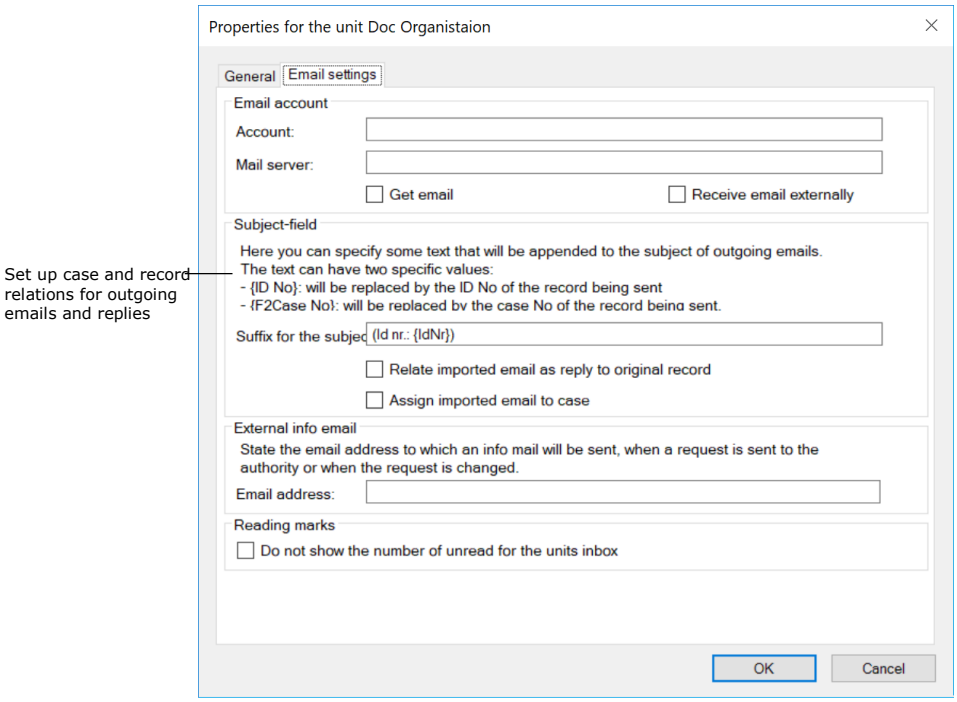


Figure 36: Configure the subject field for emails

The "Suffix for the subject" field found under the "Subject field" header is used to link outgoing emails' subject field to the record ID or to the sent email's case.

To add a suffix in an email's subject field for all outgoing emails in an authority, the fields below must be filled in. The suffix is critical for how the sent email is linked to the original record or case.

Field	Description
"Suffix for the subject"	This field makes it possible to link the subject field on outgoing emails to the record ID or to the sent email's case. The following can be inserted in the field: • Insert "`{IdNr}`" in the field to include the record ID in the subject field on outgoing emails. • Insert "`{F2CaseNumber}`" in the field to include the case number for the email's case in the subject field on outgoing emails. • Insert "`{IdNr}{F2CaseNumber}`" in the field to include both the record ID and the case number in the subject field on outgoing emails.
"Relate imported email as reply to original records"	Tick this box if F2 should relate an answer to the original email to its record ID. The field is only active when "`{IdNr}" is inserted in` the "Suffix for the subject" field.
"Assign imported email to case"	Tick this box if F2 should attach an answer to the original email to its the case. The field is only active when either "`{IdNr}`" or "`{F2CaseNumber}`" is inserted in the "Suffix for the subject" field.

Note: If only "`{F2CaseNumber}`" has been inserted in the "Suffix for the subject" field, a reply cannot be related to the original email record ID.

Static text can be inserted in the subject field. This text is added to all outgoing emails together with e.g. an ID or case number. The static text can e.g. be an abbreviation of an authority's name.

For example: "`FM – ID-no: {IdNr}, case no.: {F2CaseNumber}`"

The text outside the curly brackets will be inserted on all outgoing emails. The text inside the curly brackets will be replaced with the relevant record ID and case number.

Set up automatic transfer of replies to F2 emails

It may be desirable to receive replies to emails sent from F2 in F2, while other emails are managed in e.g. Outlook. In this case, Outlook can be configured to automatically place emails replying to emails sent from F2 in the "Move to F2" folder. The emails are then transferred to the F2 inbox. This configuration is done in the email system.

Roles in F2

Privileges and the associated rights let an F2 user perform different tasks. Privileges are given to a user through the assignment of role types. For example, if a user must be able to delete notes, the user must be assigned a role type containing the "Can delete notes" privilege.

F2 comes with a number of role types including the four administrator roles. An administrator with the "User administrator" or "Administrator" role type can also create new role types.

The integrated role types in F2 are described below.

Administrator roles

The following section describes the available administrator roles and the associated privileges.

When F2 is installed a user with the "Administrator" role is created simultaneously. Additional users must be created afterwards. If an additional authority is created within an F2 installation, another user with the "Administrator" role must be created as with the first authority. The administrator user created for the second authority will then perform relevant tasks in this authority.

There are four integrated administrator roles:

- Administrator
- User administrator
- Business administrator
- Technical administrator.

An administrator's tasks can be changed by either assigning or removing privileges from each role type. Read more about assigning privileges to role types in the section *Assign a privilege to a role type*.

The assignment of the individual privileges is listed below.

The "Administrator" role type has the following rights:

- Access to cPort
- User administrator
- Distribution list editor
- Extra email administrator
- Keyword creator
- Unit administrator
- Unit type administrator

- Flag administrator
- Settings administrator
- Can import documents from the server (add-on module)
- Can import parties
- Meeting forum administrator (add-on module)
- Editor of participants
- Privilege administrator
- On behalf of administrator
- Result list administrator
- Security group administrator
- Template administrator
- Progress codes administrator (add-on module)
- System messages administrator
- Search administrator
- Team administrator
- Team creator
- Value list administrator.

The rights associated with the "Administrator" role type are not divided into privileges. This means that it is not possible to change the rights for the "Administrator" role type.

As a standard, the "User administrator" role type has the following privileges:

- User administrator
- Extra email administrator
- Keyword creator
- Unit administrator
- Unit type administrator
- Flag administrator
- Settings administrator
- Can import documents from the server (add-on module)
- Can import parties
- Meeting forum administrator (add-on module)
- Editor of participants
- Privilege administrator
- On behalf of administrator
- Security group administrator

- System message administrator
- Team administrator
- Team creator.

As a standard, the "Business administrator" role type has the following privileges:

- Access to cPort
- Distribution list editor
- Keyword creator
- Unit type administrator
- Flag administrator
- Can import documents from the server (add-on module)
- Meeting forum administrator (add-on module)
- Template administrator
- Progress codes administrator (add-on module)
- Value list administrator.

As a standard, a technical administrator does not have any privileges assigned. The organisation decides which privileges are relevant for this administrator role.

The different privileges are described in the section *Overview of privileges*.

Assigning roles

A user in F2 must have one or more roles. A role contains one or more privileges in a given authority, allowing the user perform different tasks within.

F2 is installed with an Active Directory (a central administration of users) integration. As a standard, F2 uses one of two possible AD integrations:

- "Full integration" in which roles and privileges in F2 are controlled using AD. As a standard it updates F2's users once a day.
- "Standard integration" in which an administrator must assign updated users to their respective units.

The following sections are based on an F2 installation with a standard AD integration, i.e. the users are set up manually.

Assign a role to a user

Roles are assigned to a user through the "Properties for the user [Name]" dialogue. Open the dialogue by clicking on the **Units and users** menu item. The user's master data can also be added here.

The step by step guide below describes how Klaus Salomon from Quality is assigned the business administrator role.

After clicking on the **Units and users** menu item in the "Administrator" tab, click on the **Users** tab in the dialogue.

Find and select the user who needs a new role, in this case Klaus Salomon.

Click on **Properties**.

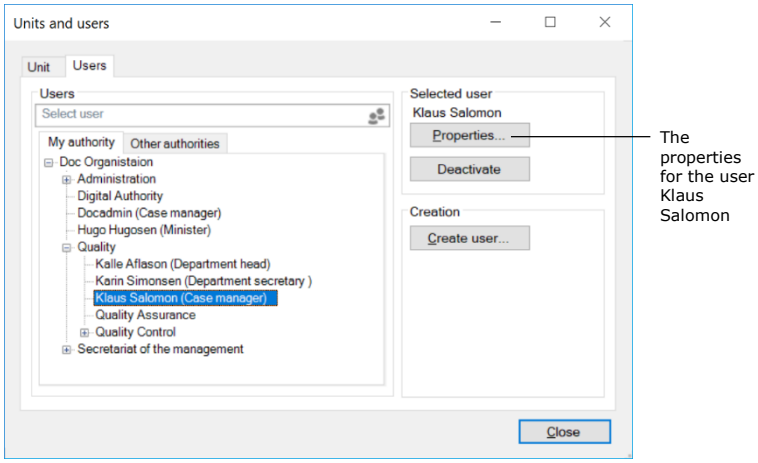


Figure 37: Select user

In the "Properties for the user Klaus Salomon" dialogue, click on the **Roles** tab and then on **Add role**.

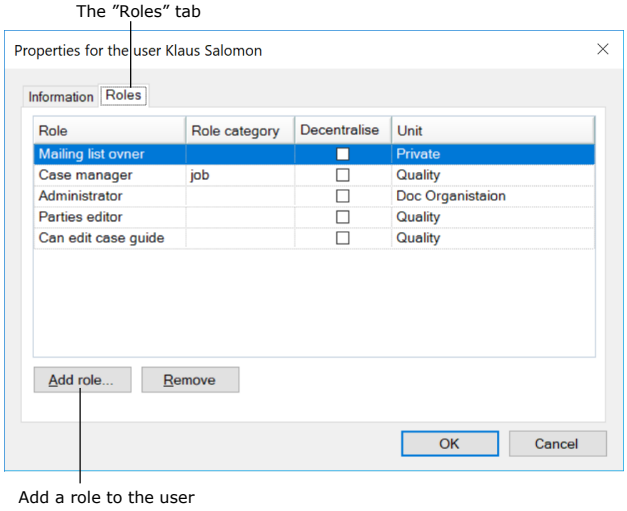


Figure 38: Assign a role to the user

To add a role first select a "Role type", in this example "**Business administrator**". Next select a unit to which the role must be applied. In this case it is the "**Quality**" unit.

Click on **OK** to assign the role to Klaus Salomon.

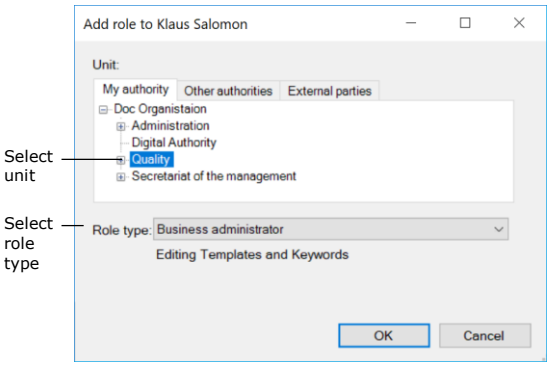


Figure 39: Assign a role type to a user

The role is now assigned and appears in the overview of the user Klaus Salomon's roles and job roles.

To remove a role from a user, select the role and click on **Remove**. The role is then removed from the user.

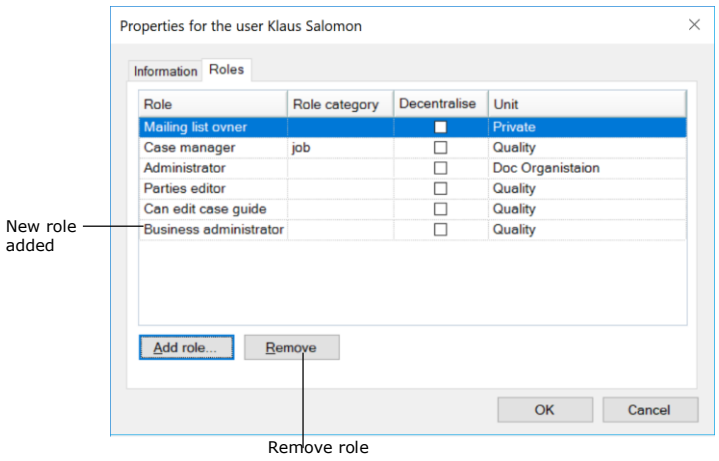


Figure 40: Add/remove a role from a user

Note: It is important to select the correct unit when assigning the user a role. Both the role and its location determine which privileges the user has in a given unit.

Create and administer role types

An administrator can create role types as needed. To create new role types, the administrator must have either the "User administrator" or "Administrator" role type.

To view available role types, click on the **Role types and privileges** menu item in the ribbon of the "Administrator" tab.

A dialogue opens and a list of the organisation's role types can be seen clicking the drop-down arrow in the "Role type" field.

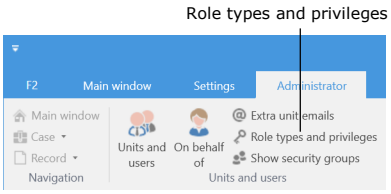


Figure 41: The "Role types and privileges" menu item

In this dialogue role types can also be created and edited. To create a new role type click on **New role type**, and to edit a role type click on **Edit role type**.

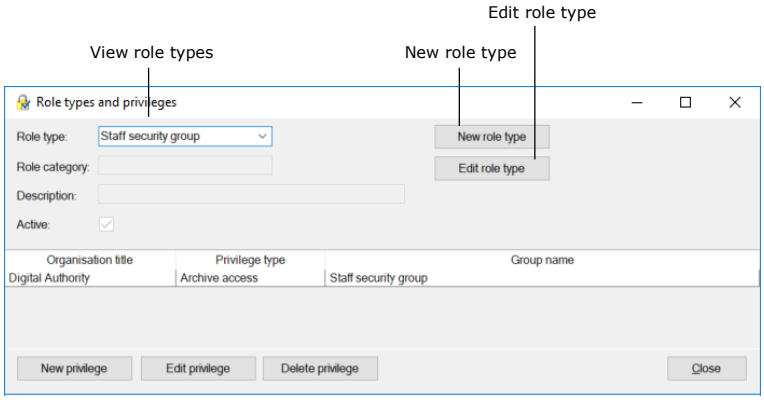


Figure 42: Role types and maintaining them

Click on **New role type** to open the "New role type" dialogue which is used to create new role types. Add the following in the dialogue:

- The name of the role type.
- A description of the role type's function e.g. "Access to edit templates and keywords".
- The synchronisation key if using full AD integration.
- Tick the "Active" box to activate the role type so it can be assigned to users.

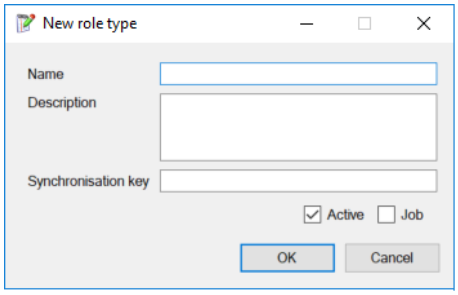


Figure 43: The "New role type" dialogue

If the "Active" box is unticked, the role type is deactivated. This means the role type can no longer be assigned.

If the "Job" box is ticked, this role type can be used to log into F2. A user must have at least one job role to log into F2.

In order for a user to perform extended actions in F2, one or more privileges must be assigned to one of his/her role types. This is described in the section *Privileges*.

Note: The "Job" box must be ticked during creation for the role to become a job role. It cannot be ticked after the role is created.

Note: A role type cannot be deleted, only deactivated.

Privileges

Privileges are assigned to role types so these can perform extended actions in F2. This lets all users with the same role type obtain a privilege assigned to it. A privilege cannot be directly assigned to a user, but must first be assigned to a role type. The role type can then be given to the user.

Assigning privileges to role types requires the "Privilege administrator" role type. Privileges and role types are managed in the "Role types and privileges" dialogue. Open the dialogue by clicking on the **Role types and privileges** menu item in the ribbon of the "Administrator" tab.

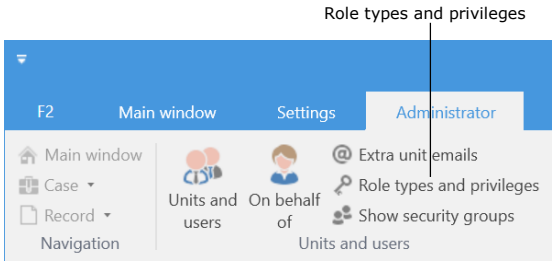


Figure 44: The "Role types and privileges" menu item

The organisation's appointed privilege administrator can distribute privileges to role types and assign authorities and security groups. It is not possible to create, delete or edit the names or rights of the privileges.

In the "Role types and privileges" dialogue new roles can be created and assigned privileges. Read more about managing role types in the section *Assigning roles.*

Assign a privilege to a role type

Here privileges are assigned to a role type. Select a role type that needs a privilege assigned in the "Role type" field, e.g. "Staff security group" as shown in the figure below.

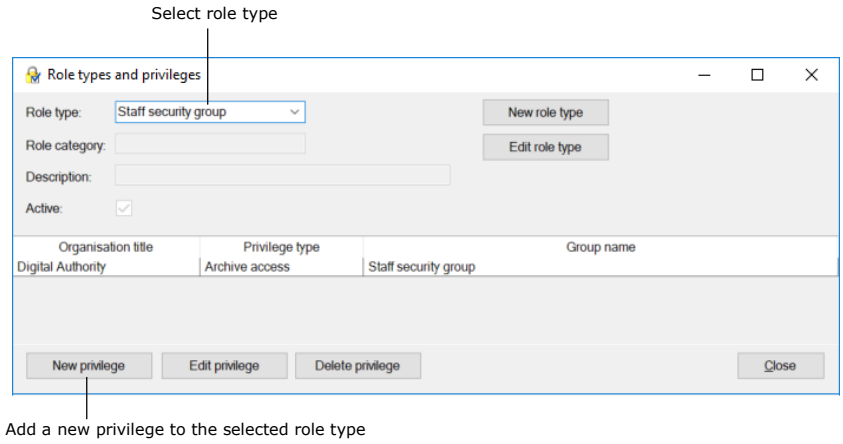


Figure 45: The "Role types and privileges" dialogue

Click on **New privilege** and the "New privilege" dialogue opens. See the figure below.

Select a new privilege to add to the role type in the dialogue. Also select which authority to which the privilege must be applied. A security group can also be attached to the privilege.

Click on **OK** to finish.

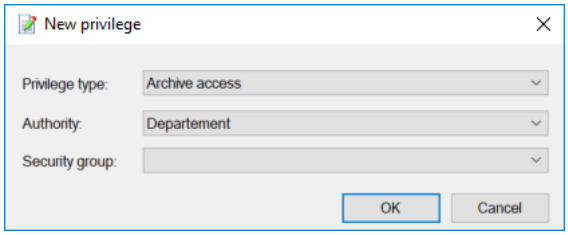


Figure 46: The "New privilege" dialogue

All users with the role type "Staff security group" now have archive access to the security group in the chosen authority.

Edit or remove privileges from a role type

Privileges can be edited or removed from a role type. To do this, select a privilege in the list of current role type's privileges, e.g. "Archive access" as shown in the figure below.

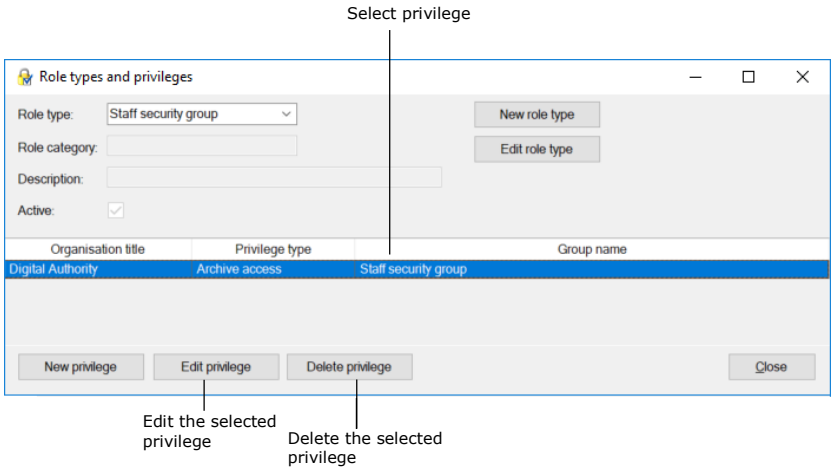


Figure 47: Edit or delete a privilege

Edit an existing privilege by clicking on **Edit privilege**. The "Edit privilege" dialogue opens. See the figure below.

Select another privilege, another authority or another security group.

Click on **OK** to finish.

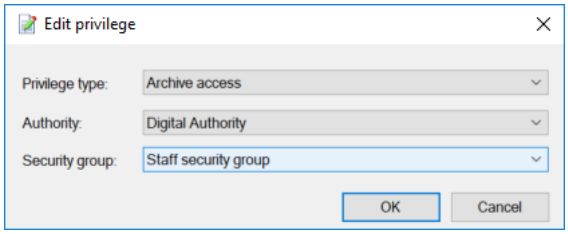


Figure 48: The "Edit privilege" dialogue

An existing privilege is removed from the current role type by clicking on **Delete privilege**. The action cannot be undone and no warning appears.

Overview of privileges

The privilege list is the same for all F2 installations (if using the same version of F2). Some privileges are only available if the relevant add-on module is active.

An administrator with the "Privilege administrator" privilege can assign privileges and their associated rights to users via role types. Privileges and associated rights are presented in the table below.

Privilege	Description of associated rights
Access to cPort	Provides access to use cPort. Exports are made across access levels and security groups. They do not show content, only titles and records.

Privilege	Description of associated rights
Administrator read access to all records	Can read all records in F2 despite the access levels. For further information, see the section *Administrator read access to all records*.
Archive access	Assigns a role to a security group. This lets an administrator add participants to security groups. Read more in the section *Archive access*.
User administrator	Can create, edit and delete users and edit user images.
CBrainInstaller	Can perform configuration changes in the F2 installation. cBrain recommends that all configurations are done in cooperation with cBrain.
CBrainSuperSetter	Can perform configuration changes in the F2 installation. cBrain recommends that all configurations are done in cooperation with cBrain.
CBrainSetter	Can perform configuration changes in the F2 installation. cBrain recommends that all configurations are done in cooperation with cBrain.
F2Setter	Can perform configuration changes in the F2 installation. cBrain recommends that all configurations are done in cooperation with cBrain.
cSearch access (add-on module)	Can perform searches using the add-on module cSearch.
Distribution list editor	Can create and edit the shared distribution lists in F2. For further information, see the section *Distribution list editor*.
Decentral unit and user administrator	Can create decentral units. Can assign decentral roles to existing users for selected levels in the organisation.

Privilege	Description of associated rights
Extra email administrator (add-on module)	Can create extra emails for units.
Keywords creator	Can create, edit and delete keywords as well as assign keywords to a unit. For further information, see the section *Keywords creator*. The user must have the "Keywords administrator" privilege in order to see the dialogue in which keywords are edited.
Keyword administrator	Can create, edit and delete keywords as well as assign keywords to a unit. Read more in the section *Administration of keywords*.
Unit administrator	Can create, edit, move and deactivate units.
Unit type administrator	Can create and delete unit types.
Flag administrator	Can create, edit and delete flags.
Phrase administrator (add-on module)	Can edit phrases for merging documents.
Reopener case	Can reopen cases.
Does not have bookmarks active in F2 Manager (add-on module)	Cannot see bookmarks in F2 Manager.
Does not have meeting planner active in F2 Manager (add-on module)	Cannot see the meeting planner in F2 Manager.
Does not have approvals active in F2 Manager (add-on module)	Cannot see approvals in F2 Manager.
Settings administrator	Can create, edit and delete user settings along as well as assign them to individual users, new users and from the users' roles.

Privilege	Description of associated rights
Can import documents from the server (add-on module)	Can import documents from the server, if this is configured. The configuration is done in cooperation with cBrain.
Can import participants	Can import external participants.
Can quality assure cases (add-on module)	Can quality assure cases on the case tab.
Can edit ext. participant no.	Can edit an external participant's synchronisation number.
Can see access information	Can see access information for records (right-click function), i.e. who can view the records, and how they received the access. Read more in *F2 Desktop – Records and communication*.
Can delete shared records for everyone	Can delete a record for everyone, even if the record is shared. For further information, see the manual *F2 Desktop – Management and organisation*.
Can delete notes	Can delete record notes.
Can add/change/remove case guides in existing cases (add-on module)	Can edit the case guides for existing cases.
Can change responsible on all records	Can change the responsible user/unit on a record. This privilege is meant for users who allocate many records and may need to reallocate responsibility, e.g. if responsibility on a record has been allocated to the wrong user/unit.
Can change responsible on all cases	Can change the responsible user/unit on a case.
Closer cases	Can complete cases.
Meeting forum administrator (add-on module)	Can create, edit, deactivate, activate and delete meeting forums.

Privilege	Description of associated rights
Can send on behalf of everybody in the authority	Can send records both internally and externally on behalf of all users and units in the authority.
SSN Synchronizer (add-on module)	Can access the SSN register via the properties dialogue for participants and users and update participant information from there.
Creates cases	Can create new cases.
Editor of participants	Can create, edit and delete external participants as well as change the images for external participants. **Note**: The privilege MUST be attached to a node under external participants. Read more in the section *Editor of participants.*
Privilege administrator	Can create new roles and assign, remove and edit privileges for a role.
Process editor (add-on module)	Can start the Process editor tool. This tool is used for editing case guide templates.
On behalf of administrator	Can create and delete "on behalf of" privileges for all users.
Result list administrator	Can create standard column settings for all users.
Security group administrator	Can create, edit and delete security groups.
Template administrator	Can create, edit and delete document templates and global approval templates (add-on module).
Progress code administrator (add-on module)	Can create, edit and delete progress codes.
System message administrator	Can create, edit and delete system messages.
Search administrator	Can create saved searched for all users.
Team administrator	Can create, edit and delete teams.

Privilege	Description of associated rights
Team creator	Can create teams across the authority.
Value list administrator	Can create, edit and delete value lists.

To see a list of available privileges, click the drop-down arrow in the "Privilege type" field which appears in both the "New privilege" and the "Edit privilege" dialogues. See the figure below.

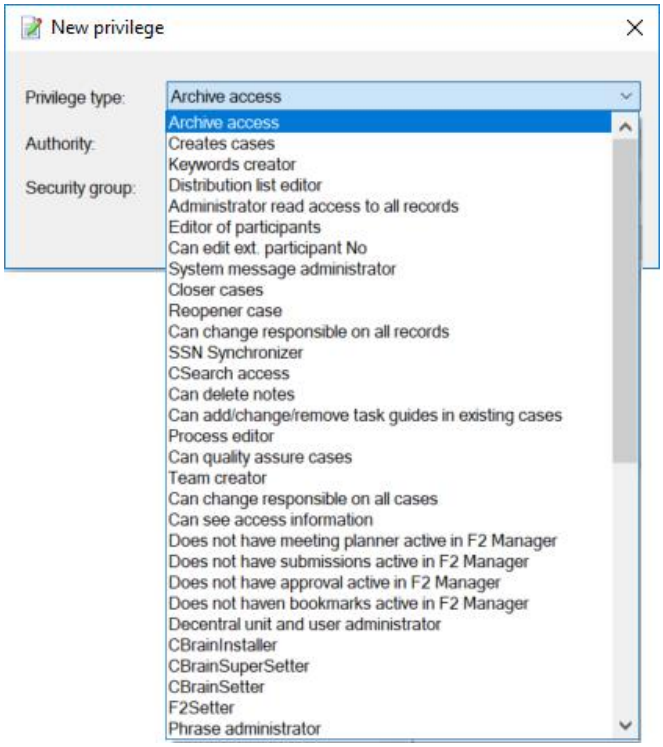


Figure 49: Assignable privileges

Further explanation of selected privileges

The following sections describe selected privileges in further detail.

Archive access

The purpose of this privilege is to attach a group of users to a security group within an authority. It must be decided which role type is to be connected to the security group.

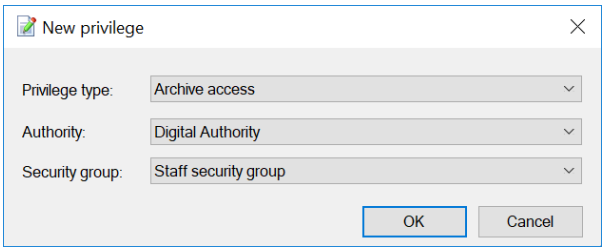


Figure 50: A new privilege type - "Archive access"

A user with a role containing the above privilege becomes a member of the security group. This privilege is attached to a role type and describes an interconnection between a security group and an authority.

Creates cases

Users can create new cases in F2 if they have a role to which the "Create cases" privilege is attached. The privilege depends on a connection between a role type and an authority. In other words, the access to create cases is subject to an authority.

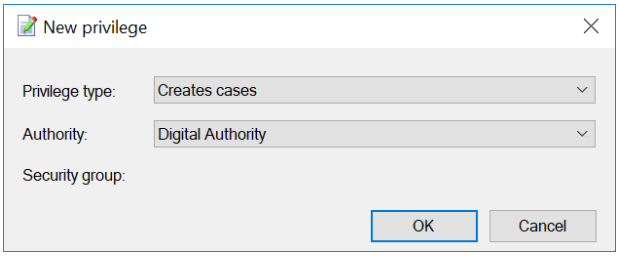


Figure 51: The "Creates cases" privilege

This means that users with this privilege can create new cases in the selected authority only.

Keywords creator

All users can add existing keywords to records and cases. However, only users with a role to which this privilege is attached can manage keywords in F2. This means that this privilege lets the user create new keywords, deactivate and change the name of existing keywords.

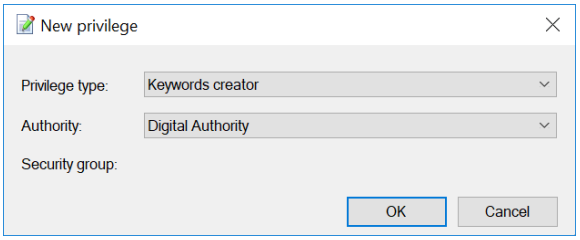


Figure 52: The "Keywords creator" privilege

For further information on keywords in relation to departments and authorities, see the section *Keywords.*

Note: Keywords work across all the authorities in a F2 installation.

Distribution list editor

All users can create personal distribution lists. However, only users with a role to which this privilege is attached can create and manage shared distribution lists in F2.

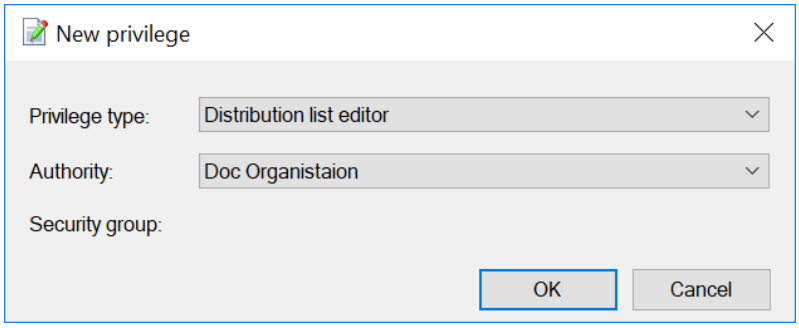


Figure 53: The "Distribution list editor" privilege

The editing distribution lists is described in the manual *F2 Desktop – Settings and setup*.

Administrator read access to all records

This privilege should be treated with caution. A user with this privilege can search and find all records within his/her authority except for the records in the users' "My private records" lists.

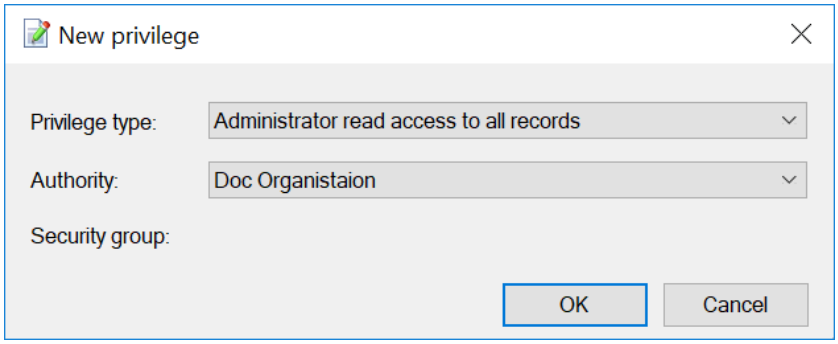


Figure 54: The "Administrator read access to all records" privilege

This privilege can be used e.g. when an employee leaves the organisation and the records for which he/she is responsible must be reallocated.

Editor of participants

Users who have a role with this privilege can view and edit all external participants. External participants are shared across authorities.

All users can create private participants, but only users with a role to which this privilege is attached can manage the shared external participants in F2.

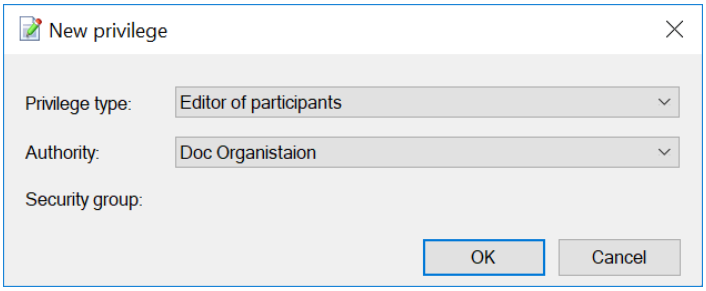


Figure 55: The "Editor of participants" privilege

Security groups

Security groups are used to limit the access to data in F2. An administrator with the "Security group administrator" privilege can manage the organisation's security groups. Users must have a role with a privilege pertaining to a specific security group to be included in that group. A number of roles can refer to the same security group.

Use the following approach to create a security group:

1. Create a security group in the menu of **Units and Users**. The "Security groups" tab is found in the "Units" dialogue.
2. When the security group is created, it must be assigned one or more privileges. Click on **New privilege** under **Role types and privileges** to assign a new privilege.
3. Users can then be attached to the security group by assigning them a role type with the relevant privilege using the menu item **Units and users**.

For a more detailed description, see the section *Create a security group*.

All security groups created by an administrator are subject to an authority as they are created as a special unit type in F2's organisational structure.

An overview of the creation of security groups is displayed below.

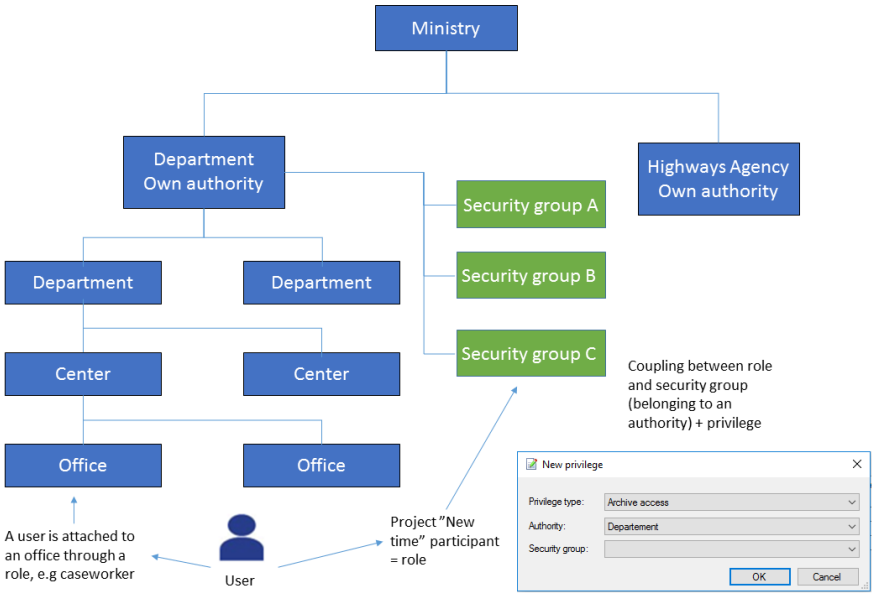


Figure 56: Security groups are created under an authority

A security group is placed one level under its authority. The figure below shows how the security group "Authority security group" is placed under the "Digital authority".

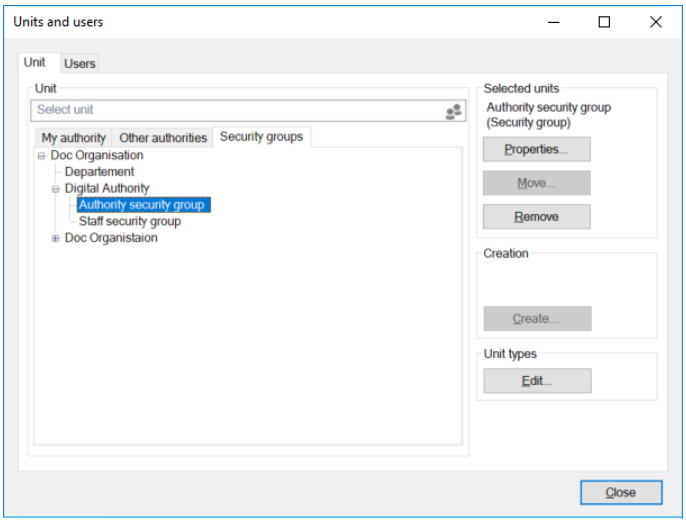


Figure 57: Authorities and security groups

Once a security group is established, users can be assigned to the group. This task is performed by a user who has the "Security group" privilege.

Only the users who are a member of a security group can add or remove the security group to/from the "Access restriction" field for cases or the "Access limited to" field on a record.

Create a security group

Security groups are created and edited in the "Units and users" dialogue. Click on **Units and users** in the ribbon of the "Administrator" tab in the main window to open the dialogue.

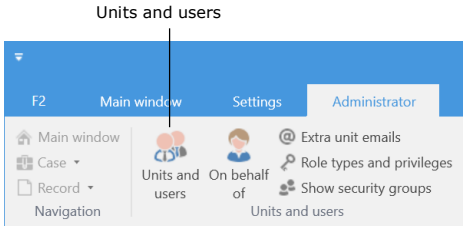


Figure 58: The "Units and users" menu item

In the "Units and user" dialogue click on the **Security groups** tab. Security groups are created under an authority. Select an authority in which to place the security group and click on **Create**.

Provide the security group with a name and click on **OK** to complete.

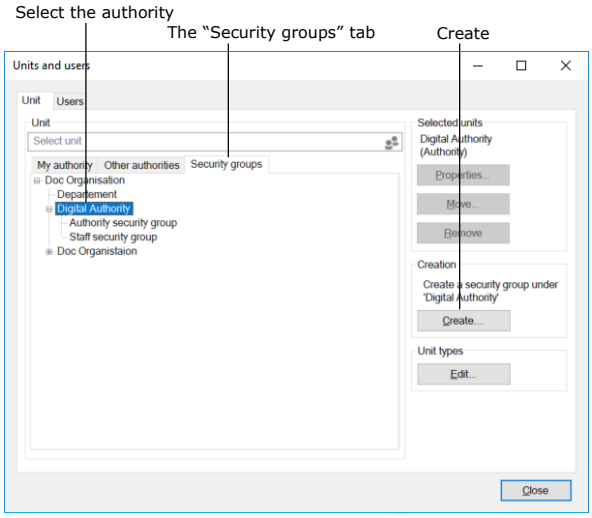


Figure 59: Create a security group

The newly created security group will then appear under the chosen authority in F2's tree structure. In this example the security group is placed under the "Digital authority".

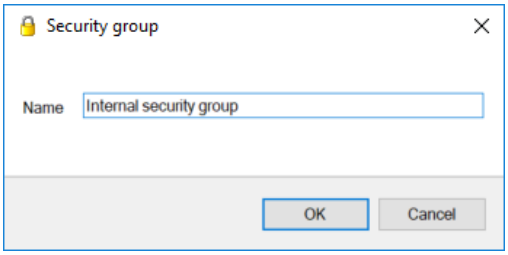


Figure 60: The "Security group" dialogue

Note: The **Create** function is only active if an authority has been selected.

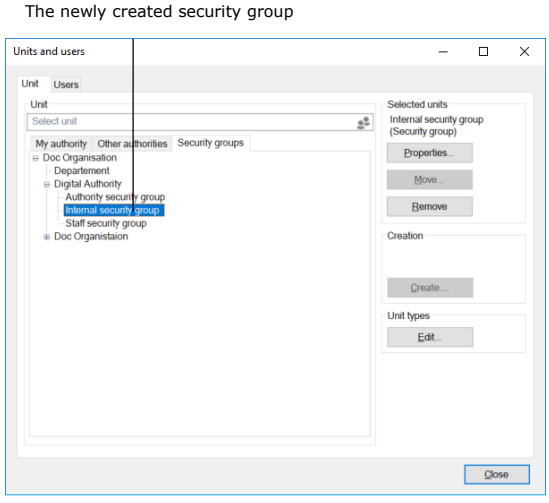


Figure 61: The newly created security group in F2's tree structure

As a user can have several roles, the administrator must create roles whose sole purpose is to define an association to a security group.

For example, the "Board member" role type can be attached to the "Employee security group" within the "Digital Authority".

This means that all users who are given the "Board member" role type will become a member of the "Employee security group". These users will have access to all cases and records which have their access limited to the security group.

Follow these steps to create a new security group and add a member:

- Create the security group in the "Units and users" dialogue.
- Create a new role type in the "Role types and privileges". For more information, see the section *Create and administer role types*.
- Attach a privilege to the role type that refers to the created security group and the relevant authority.
- Add the new role type to the user using the "Units and users" dialogue.

Note: If a user is not attached to a security group via a role, the user cannot see the security group and the user will not be able to assign the security group to a record.

Privileges for members of security groups are described in the section *Archive access*.

The following section describes how security groups and the assigned users are displayed in F2.

Show security groups

To view all security groups, click on **Show security groups** in the ribbon of the "Administrator" tab.

Records that have their access limited to a security group can only be accessed by users with a role that includes them in the security group. An administrator can add him/herself to security groups on a temporary basis if he/she needs to search for and access records with limited access.

An administrator can view security groups created in the authority by clicking on **Show security groups**.

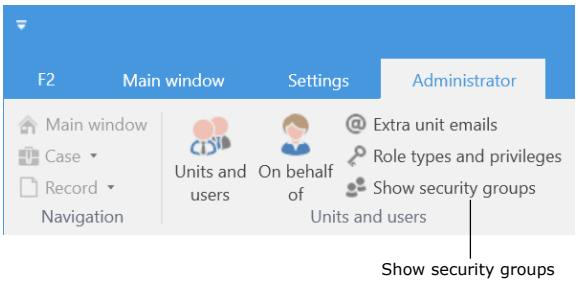


Figure 62: The "Show security groups" menu item

If an F2 organisation consists of several authorities, they are all displayed in the security group overview.

The security group overview can only be seen by a user with the "Security group administrator" privilege.

To see an overview of the members of a security group, right-click on the **security group** and then click on **Properties**.

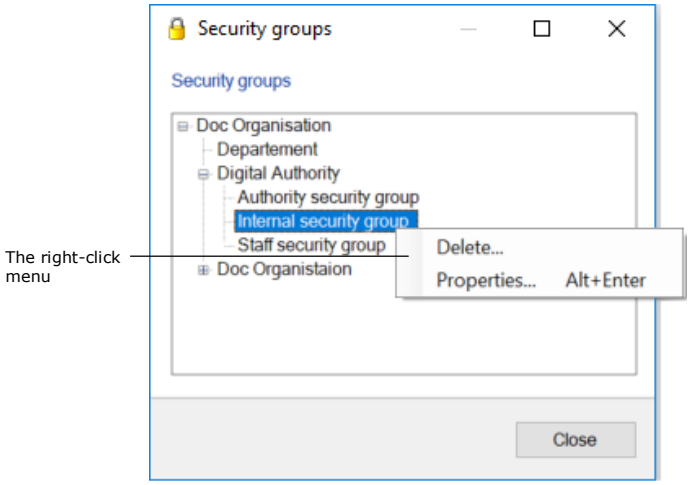


Figure 63: The "Security groups" dialogue

In the example to the right, Hugo Hugosen, Karin Simonsen and Lisbeth Andersen are members of the "Staff security group".

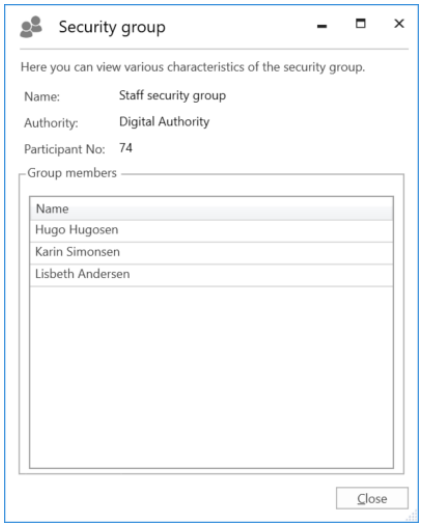


Figure 64: Properties for a security group

Import participants and replace record participants

Import participants

Users with the "Editor of participants" privilege can use the "Import participants" menu item located in the ribbon of the "Administrator" tab in the main window.

Click on **Import participants** to open the "Import participants" dialogue. Here, external participants can be imported or updated via a CSV file – a format that is used to transfer large amounts of data between different programmes and databases.

Every line in a CSV file correlates to an external participant. If the participant already exists in F2's participant register, the participant's data will be updated with data from the imported file. If the participant does not exist, it is created in the participant register.

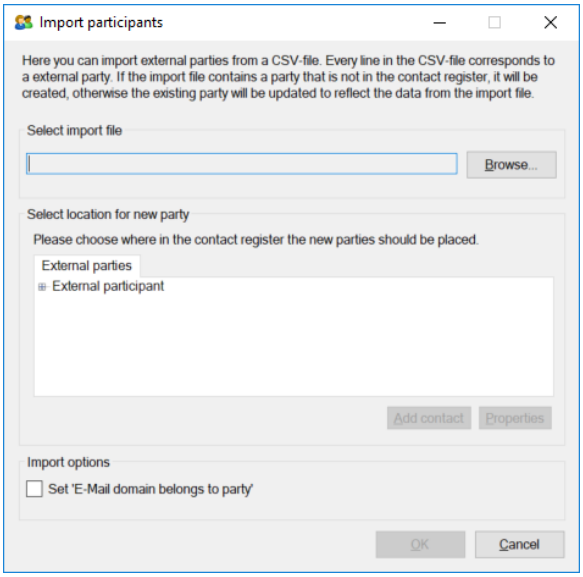


Figure 65: Import participants

The following fields in the "Import participants" dialogue must be considered:

Field	Description
"Select import file"	Click on **Browse** to select the file.
"Select location for new participant"	Select a location for newly created participants in the participant register. Scroll through the tree structure starting with "External participant" in the top. For example, if the import file contains a list of municipalities, an external party can be created with the name "Municipalities" under "External participants". This party can then be selected as the location for the new participants from the import file. To import/update the external participants click on **Add contact**. For more information about F2's participant register and the creation of external participants please see the section *The participant register*.
"Set 'Email domain belongs to participant'"	Decide if the "Email domain belongs to participant" field should be ticked in the creation dialogue for the participants listed in the import file.

Click on **OK** to complete the import.

If the import file contains data for existing F2 participants, the data in F2 will be updated so it corresponds to the data of the import file.

If one or more participants cannot be imported, it is possible to save a new CSV file. The new file will contain the participants that were not imported, along with an extra column containing error messages.

CSV file for importing participants

A CSV file used to import participants must contain the 31 columns from the table below. External ID and name must be filled in. The remaining columns may be empty.

#	Column heading	Description
1	External ID	The ID that is saved with the participant. If the participant is reimported, the participant with this ID will be updated with the new data from the CSV file.
2	(Not in use)	
3	Name	Name
4	Name, continued	

#	Column heading	Description
5	(Not in use)	
6	Contact person	
7	Address	Address
8	Address, continued	
9	Zip code	
10	City	
11	Country code	
12	Country name	
13	Telephone	
14	Fax/cell phone	The value in this field is saved as both a fax and a cell phone number.
15	Postage group	The postage group. Displayed on the participant along with the address.
16	Email	
17	Website	
18	CBR number	
19	CBR P number	
20	Created date	If this field is empty, today's date is used for new participants.
21	Edited date	If this field is empty, today's date is used.
22	Groupcode01	DB07 codes. The codes are saved to the participant and can be viewed using the participant properties dialogue.
23	Groupcode02	
24	Groupcode03	
25	Groupcode04	
26	Groupcode05	

#	Column heading	Description
27	Groupcode06	
28	Groupcode07	
29	Groupcode08	
30	Groupcode09	
31	Groupcode10	

Part of an import file is displayed in the example below.

Note: In the import file, semicolons are used as separators. There are **NO** column headings in the file.

Replace record participants

When importing external participants, situations can arise in which a deactivated external participant has the same email address as an active one.

It is possible to automatically replace such record participants and so avoid replacing all deactivated participants with the newly imported participants manually.

Click on **Replace record participants** in the ribbon of the "Administrator" tab to perform this task.

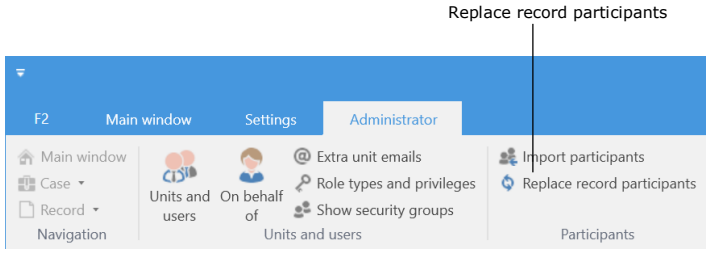


Figure 66: The "Replace record participants" menu item

This will replace the record participant reference (docID) to each deactivated participant on records with the newly imported active participant.

Only external participants can be replaced using this method. Internal F2 users cannot be replaced this way.

The add-on module F2 Access restriction for participants makes it possible to set an access restriction for external participants in F2's participant register. An external participant with access restriction can only be searched for and found by the unit who has set the access restriction.

If a participant with access restriction is replaced by a participant without access restriction, the record participant will refer to the latter. The access restriction is not changed for the participant that is replaced. Replacing record participants can only be done using email addresses.

Value lists

Value lists contain a number of lists that apply to the entire organisation. The individual value lists represent individual groups of standardised texts used in connection with different tasks.

> **Note**: Value lists apply to all authorities within an organisation. For further information on authorities and organisations, see the section *The unit structure in F2*.

For example, request types can contain texts like:

- Office reply
- Report
- Alert
- For information.

An organisation's participant types are also managed using value lists.

Value list administration

As a standard, value lists are created in connection with the F2 installation and maintained in the "Value list administration" dialogue.

To open the dialogue, click on **Value list administration** in the ribbon of the "Administrator" tab.

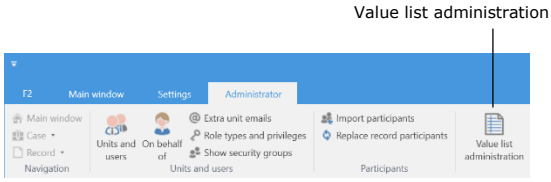


Figure 67: The "Value list administration" menu item

Click on the **drop-down arrow** in the "Value list administration" dialogue to select one of F2's value lists.

The figure to the right shows examples of value lists that are available in an F2 installation.

The list varies depending on the available add-on modules.

Once a list is chosen, its items are displayed in the window. Items are created as sub points for different types of value lists.

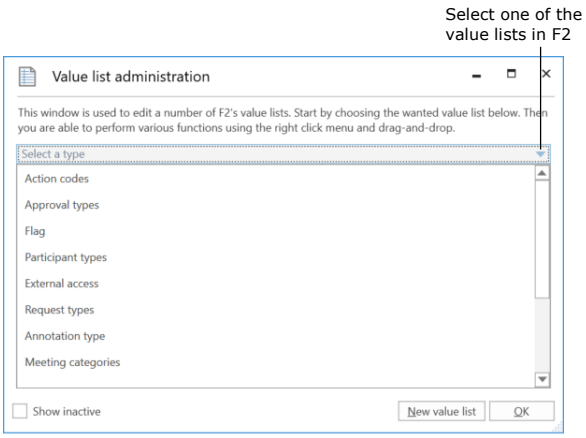


Figure 68: The "Value list administration" dialogue

Right-click on a value list and the following options become available:

- Create element
- Rename value list
- Import value list
- Export value list

Right-click on an item below a value list and the following options become available:

- Create item
- Rename item
- Deactivate item
- Selectable item
- Import/Export item
- Properties for the value.

If "Selectable" is ticked, the text (type) can be chosen. If "Selectable" is unticked, the text (type) can still be seen, but not be chosen.

Non-selectable texts are used as titles for value list nodes with sub-classifications such as file plans.

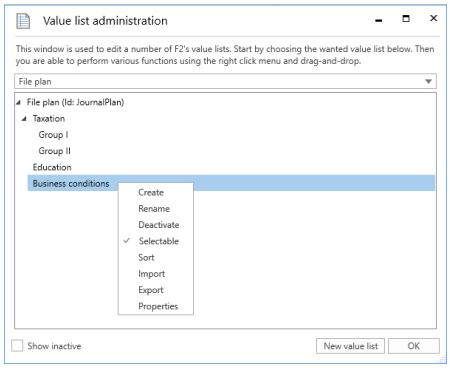


Figure 69: The right-click menu of a value list

Note: An value list item cannot be deleted, only deactivated. This is important for the administrator to consider when he/she is working in the dialogue.

Create a new value list

Business administrators can create new value lists in the "Value list administration" dialogue. Open the dialogue and click on **New value list**.

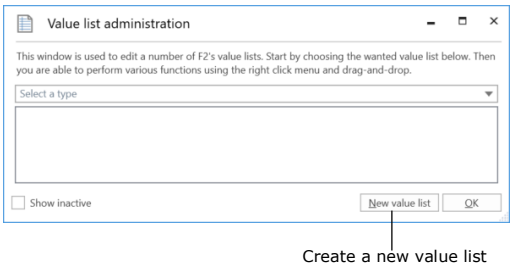


Figure 70: Value list administration

In the "Create new value list" dialogue enter the value list's name and ID.

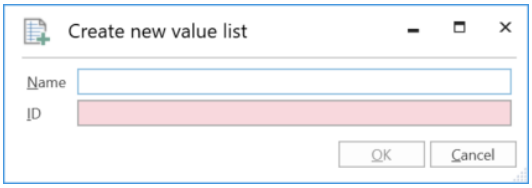


Figure 71: Create a new value list

Note: Usually, new value lists will only be created in connection with the add-on modules F2 Management Cabinet, F2 Search templates and F2 Case guides. The value list ID is used in these modules when customising F2.

Setting up flags

Users can organise their work with records by using flags for either personal or unit management in both the record and main windows. To assign a control flag to a record, see below.

A user with the "Flag administrator" privilege can define which flags are available to in an F2 authority.

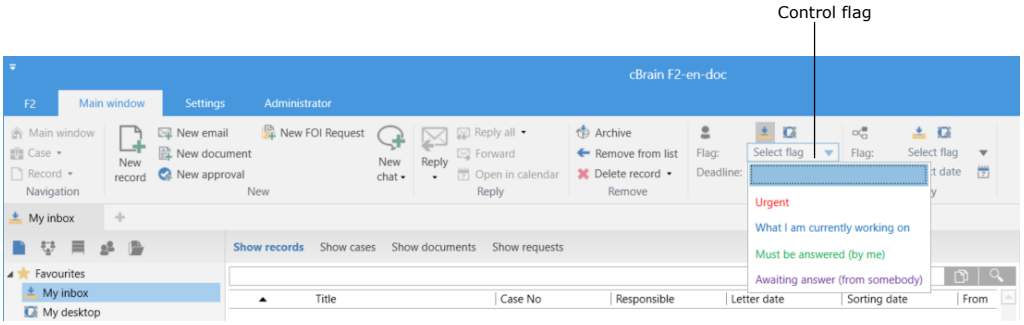


Figure 72: Example of the personal control menu on a record

Control flags are created, edited and/or deleted in the "Flags for personal control" dialogue. Click the **Flags for personal control** menu item in the ribbon of the "Administrator" tab to open it.

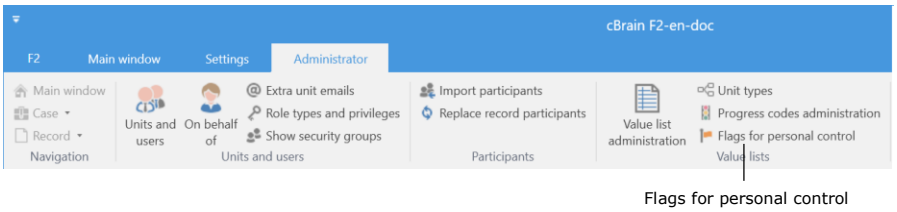


Figure 73: The "Flags for personal control" menu item

In the "Flags for personal control" dialogue an administrator can:

- Create new flags
- Edit flag types
- Edit flag colours
- Change flag number sequence
- Delete flags.

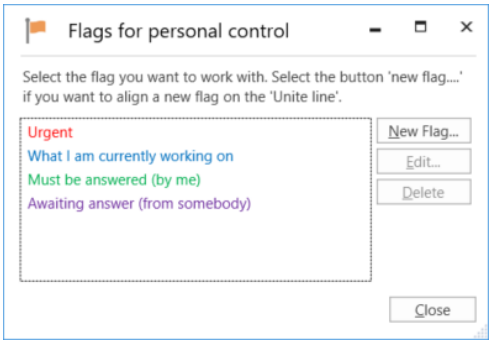


Figure 74: The "Flags for personal control" dialogue

When a new control flag is created it must be given a title, colour and priority. The priority determines the flag sequence. It is possible to search for flags e.g. in order to group them.

Click on **OK** to save the control flag.

Control flags can be used by all users in the organisation.

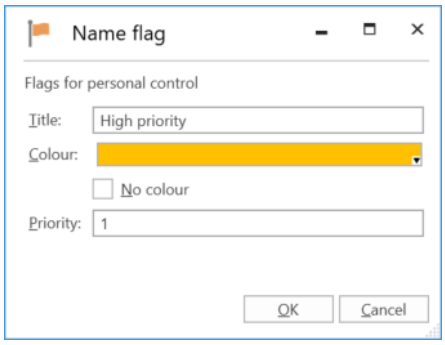


Figure 75: Name the personal control flag

If a control flag's title is changed, the change will apply to all records on which the flag is in use.

If a flag is deleted, it is removed from all records on which it is in use.

Note: If an administrator changes a flag's colour, the change can be seen in the results list immediately by pressing **Ctrl+F5**. The flag's colour in the management menu in the main window ribbon and in the right-click menu is not updated until F2 is restarted. This also applies to other changes to flags.

Keywords

Keywords help facilitate knowledge sharing within the organisation. Keywords can be assigned to records and cases, providing the organisation with a flexible method for searching for and organising information in F2.

Users with the "Keyword creator" privilege can create, manage and remove keywords in F2.

Administration of keywords

Keywords are managed using the "Keyword administration" menu item, located on the ribbon of the "Administrator" tab.

> **Note**: Keywords are shared by all users in all authorities in an F2 installation.

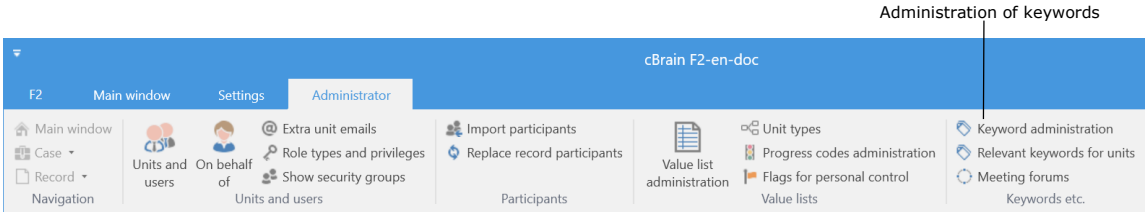


Figure 76: The "Keyword administration" menu item

Click on the **Keyword administration** menu item to open the dialogue in which keywords can be created, deleted and/or edited. See the figure below.

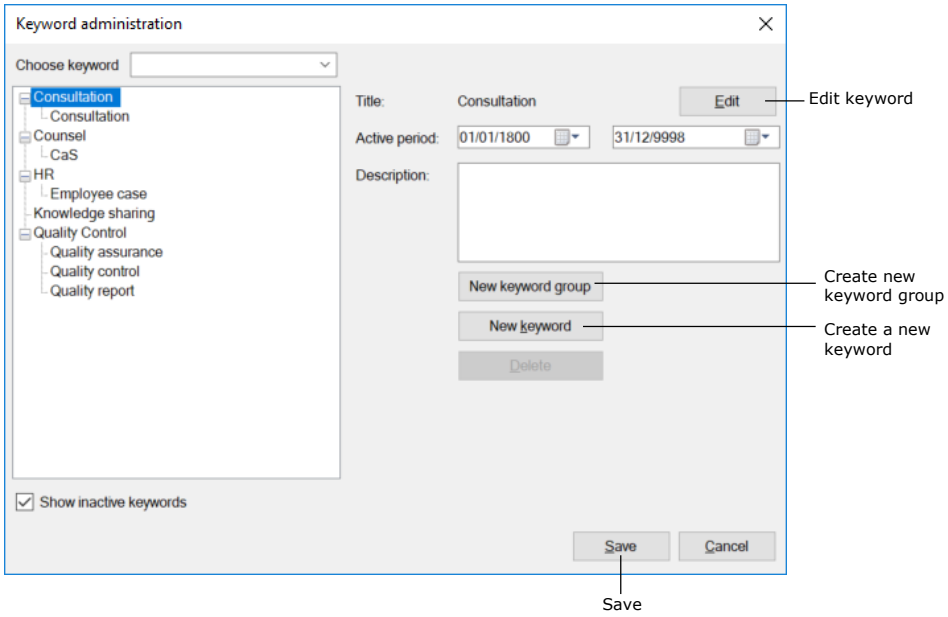


Figure 77: Administration of keywords

Keywords are divided into keyword groups. Click on **New keyword group** to create a one.

To create a new keyword, first select a keyword group and then click on **New keyword**. The new keyword will then be placed in the chosen keyword group.

A keyword can be given a description and a duration, i.e. the keyword can be set as active for a limited period of time. Entering an end date is not required.

Only active keywords can be added on records and cases. Deactivated keywords will remain on records and cases and can still be used in searches.

Click on **Save** to create the keyword.

Note: If a keyword is used on a record or a case, it cannot be deleted in the keyword overview. However, it can be deactivated by entering an end date in the "Active period" field. In other words, a keyword cannot be used after the end date, but it can still be used in searches.

Note: If a keyword is edited, records and cases on which it is used will be updated with the edited keyword.

Relevant keywords for units

The "Relevant keywords for units" menu item on the "Administrator" tab is used to allocate specific keywords to a unit. This helps the unit's users select relevant keywords.

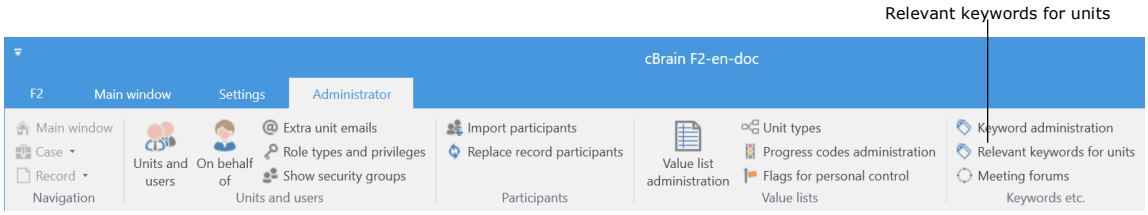


Figure 78: The "Relevant keywords for units" menu item

The organisation may assign relevant keywords to the individual units via the "Relevant keywords for units" window, as shown below. This makes it easier for the user to select the keywords for his/her records and cases.

The unit keyword allocation also means that when a user starts typing a keyword, F2 automatically displays relevant keywords.

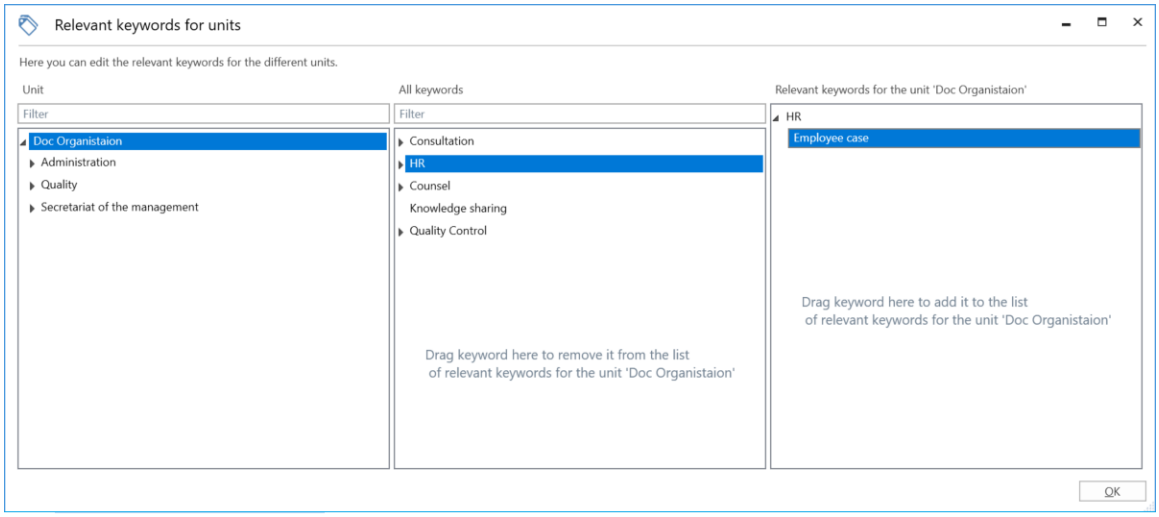


Figure 79: Select keywords

The three columns in the "Relevant keywords for units" window are described below.

Column	Content
"Unit"	Shows the organisational units created in F2.
"All keywords"	Shows an overview of available keywords that can be selected/deselected for the unit chosen in the "Unit" column.
"Relevant keywords for the unit [unit name]"	Displays the keywords that are relevant for the unit chosen in the "Unit" column.

Assign keywords to a unit

To assign one or more relevant keywords to a unit, select it in the "Unit" column. Drag the keywords from the "All keywords" column to the "Relevant keywords for the unit [unit name]" column. It is also possible to add a keyword by right-clicking on it and selecting "Add keyword".

Click on **OK** to mark the keyword as relevant for the selected unit.

Remove keywords from a unit

To remove a keyword, simply drag them from the "Relevant keywords for the unit [unit name]" column to the "All keywords" column. It is also possible to remove a keyword by right-clicking on it and selecting "Remove keyword".

Click on **OK** and the keyword is no longer marked as relevant for the selected unit.

System messages

Users with the "System message administrator" privilege can create system messages that are sent to the users of F2. This can be important messages about unscheduled downtime or other information pertaining to the performance of F2 and which affects all users.

A system message is displayed on the screen in front of all other windows if the user's F2 is active. Click on **System messages** to open system messages.

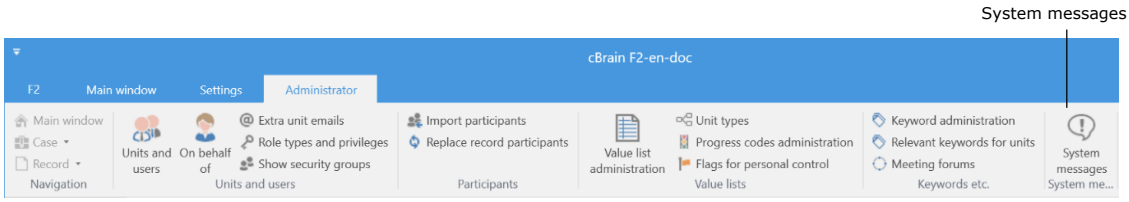


Figure 80: The "System messages" menu item

System messages can be created, edited and/or deleted in the dialogue that opens. There are two types of system messages:

- Start-up: The system message is only displayed when F2 is started.
- Push: The system message is pushed out to all users at a specific time. The message is displayed on the user's screen immediately.

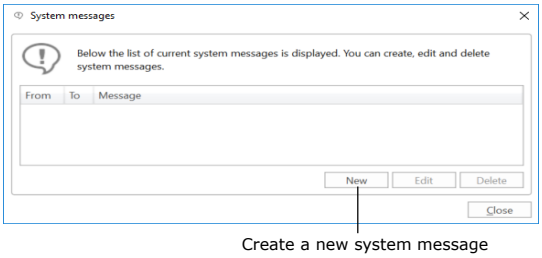


Figure 81: The "System messages" dialogue

The administrator can specify the system message type by clicking on **New** in the "System messages" dialogue. Select a type from the drop-down arrow in the "Type" field. Then enter a title for the system message, select when to display it and enter its content.

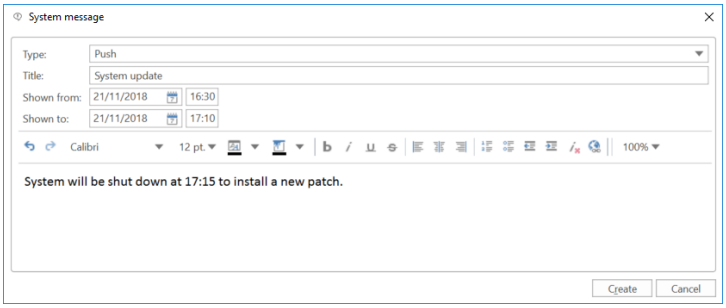


Figure 82: Create a new system message

The participant register

F2 contains a participant register that is shared by the entire organisation. It consists of participants that can be used by all F2 users regardless of unit.

To open the participant register, click on **Contacts** above the list view in the left side of the main window.

The participant register is then displayed as a tree structure in the list view, while the content of a selected list is displayed in the result list.

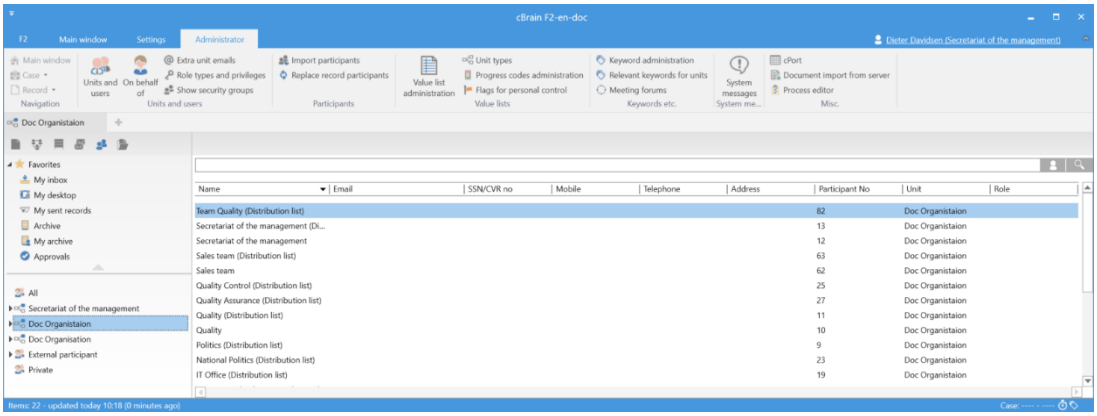


Figure 83: F2's participant register in the main window

The participant register consists of three types of participants:

- **Internal participants**: Users who are created and maintained in F2 via "Units and users". If a user is moved from one F2 unit to another, this change is applied to the participant register as well. The "Units and users" dialogue is used for managing internal participants. For more information, see the section *User administration*.
- **External participants**: Participants who are either created manually by a participant editor or automatically. F2 automatically creates an external participant when an email is sent from or received in F2 and the recipient or sender is unknown to the participant register.
- **Private participants**: Participants that are created manually by a user without the participant editor privilege are private participants. If an F2 user receives an email from a sender that is unknown to the participant register, the user can choose to place that participant in the "Private" node.

  Participants created as "Private" can only be seen and maintained by the user who created them.

When an external participant is assigned to a record or a case, his/her information is copied over from the participant register. However, if the register is updated with new information on the participant, e.g. an address change, the records and cases on which the participant is already added are not automatically updated with the new address.

Participants are created in a tree structure with the organisation's name at the top, then the unit and lastly contacts.

External participants

External participants are used as senders, recipients and case participants on a record or case.

Users with either the "Editor of participants" or "Administrator" privilege can create and edit the shared external participants in F2, i.e. information on contacts and their organisation.

Using a configuration setting it is possible to allow all users to create and edit external participants. As a standard this configuration setting is disabled. Configuration is done in cooperation with cBrain.

Create external participants manually

External participants can be created manually by users with the "Editor of participants" privilege. The participants are organised in a hierarchy and can be moved around. This means that both organisations and individual contacts can be managed in the participant register.

To create a new external participant, right-click a unit in the "External participant" node. Then click **Create new participant** to create an external participant in that unit.

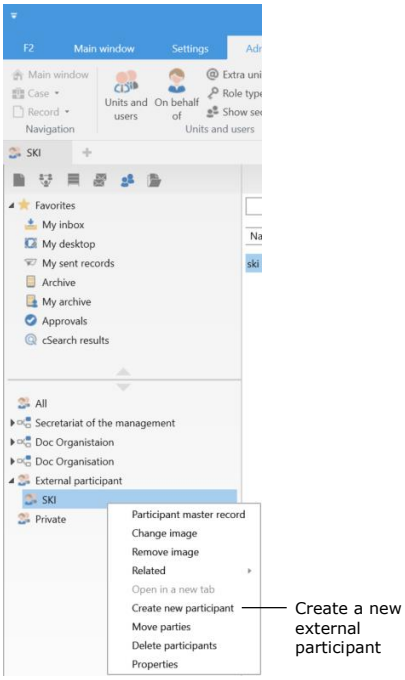


Figure 84: Create external participant

The "Create new participant" dialogue opens, and the relevant fields must be filled in. See the figure below.

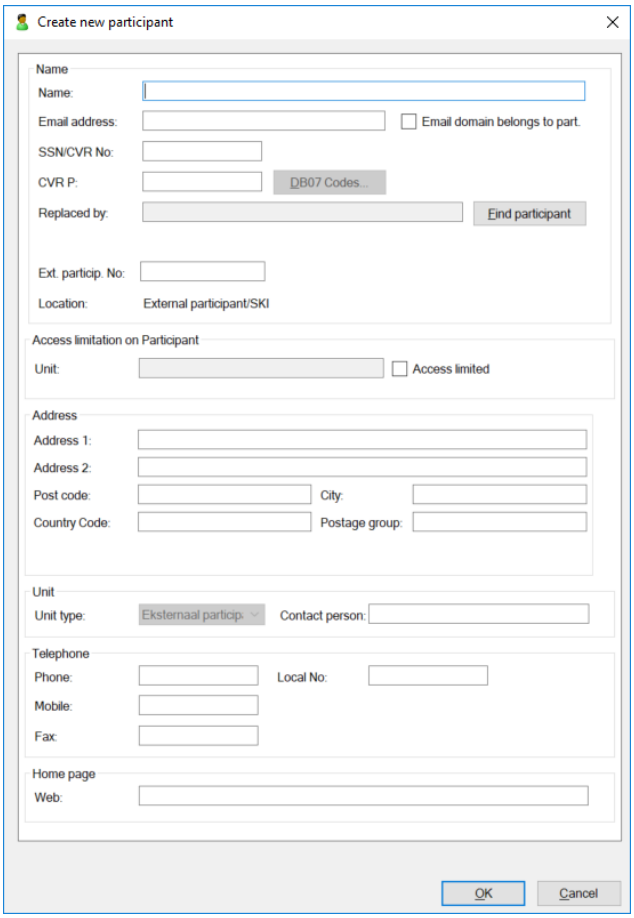


Figure 85: The "Create new participant" dialogue

Click on **OK** and the participant is registered as an external participant in the selected organisation.

Create external participant automatically

If an email is sent from or received in F2, and if the external sender or recipient is unknown to the participant register, F2 can be configured to automatically suggest creating the unknown participant in the shared participant register. To do this, click on **Setup** in the "Settings" tab in the main window. In the dialogue, tick the "Show match dialogue for unknown participants" box found under "Create participant" on the "Record" tab.

The example below shows an email sent from F2 to "Administrator". The dialogue informs the user that this participant cannot be found in the database/participant register and may either be created as a new participant or replace an existing participant.

F2 has also registered that that unknown receiver is using the domain @admin.dk, and that other participants in the participant register have the same domain. Therefore, F2 suggests placing the unknown participant in the same domain group.

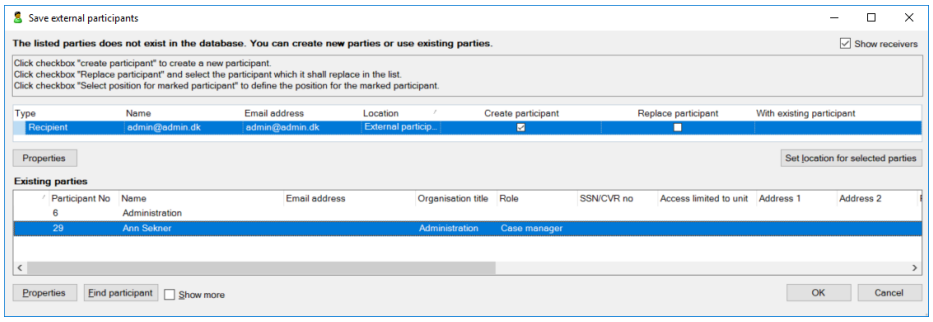


Figure 86: F2 suggests placing a new participant under an existing one

When the email domain is found on an existing participant and the box "Email domain belongs to part." is ticked, F2 suggests placing the new participant with this domain under the existing one in the tree structure. For example, the participant Ann Sekner owns the domain @admin.dk as shown to the right. Click on **OK** in the dialogue above to save "Administrator" under the same participant as Ann Sekner.

An administrator should regularly check that newly created participants are placed correctly in the external participant hierarchy.

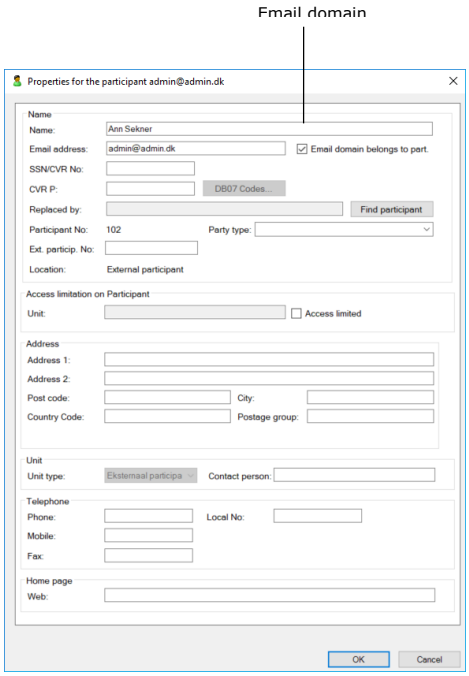


Figure 87: Participant who owns an email domain

User and participant images

In the participant register images can be added, changed or removed for users, units and external participants. A user with the "Editor of participants" privilege can add, change or remove images for external participants. A user with the "User administrator" privilege can add, change or remove images for other users in the authority. A user with the "Unit administrator" privilege can add, change or remove images for units within the authority.

To add or change an image, select "Change image" in the right-click menu of the participant in the participant register. Click on **Contacts** in the navigation bar in the main window to open the participant register. Right-click on the participant and select **Change image**. To remove an image, select "Remove image" in the right-click menu.

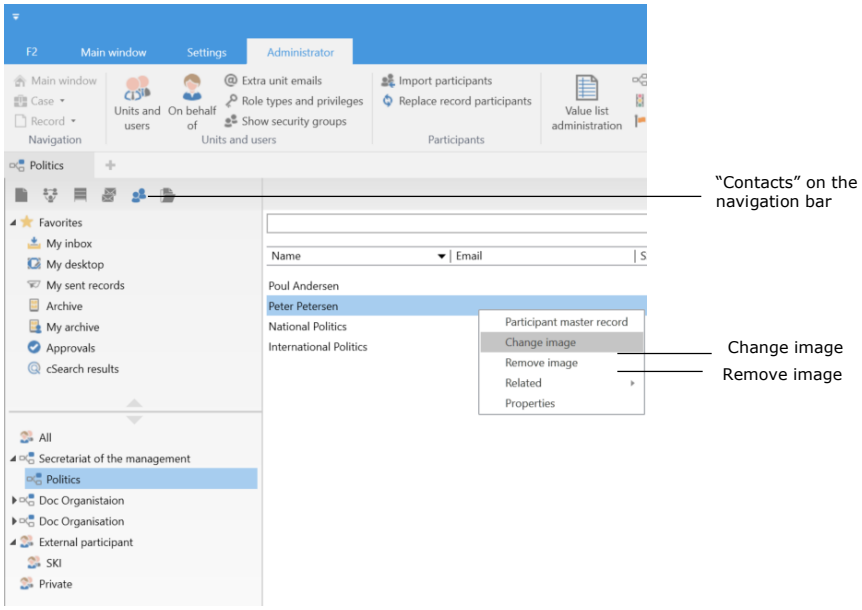


Figure 88: Right-click on a participant

In the "Change image" dialogue, click **Browse** to select an image from either a local or external drive on the computer. Use the zoom buttons **-** and **+** to select the size of the chosen image. Then click on **OK** and the image is either added or changed.

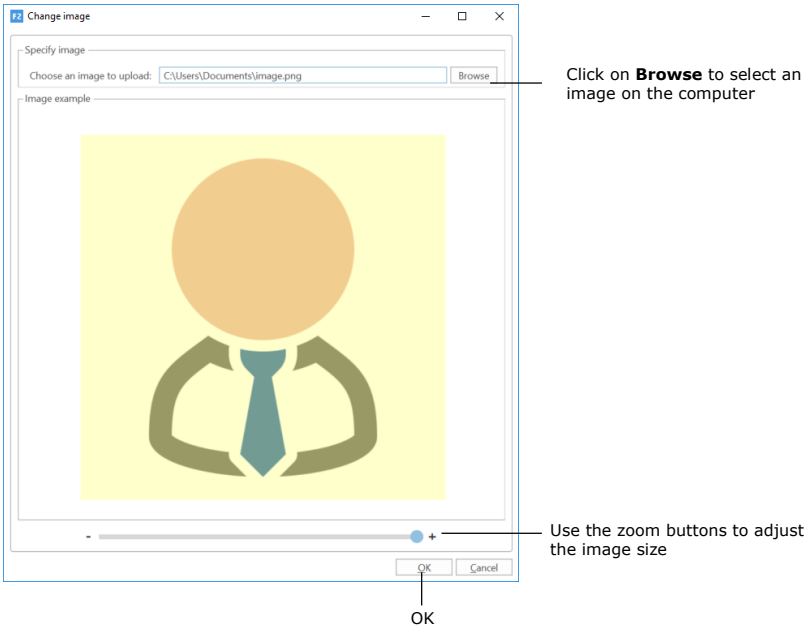


Figure 89: The "Change image" dialogue

F2 users can change their own image through the user identification in the upper right corner of the main, record and case windows.

Teams

A team is a group of F2 users from different units within the same authority.

Teams in F2 are used for different purposes:

- As access groups in the "Limited access" field on records and cases.
- As supplementary units on a record.
- As an email, chats and notes recipients.
- As participants or stakeholders on meetings that are managed via the add-on modules F2 Manager (ad hoc meetings) and F2 Meetings.

Teams can be created by users with roles that have been assigned the "Team creator" privilege.

Teams are managed in the "Teams" dialogue. Click on **Teams** on the "Settings" tab in the main window to open the dialogue.

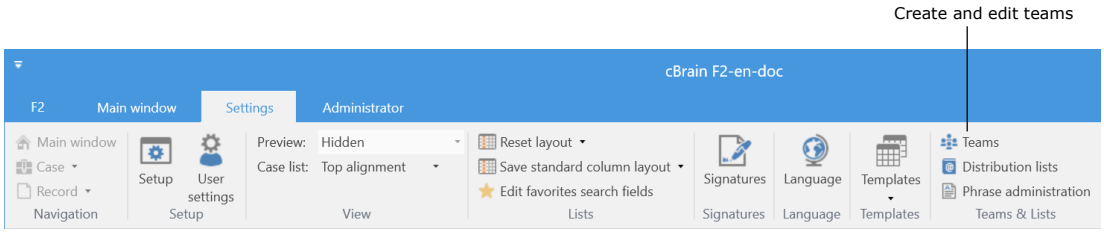


Figure 90: The "Teams" menu item

The "Teams" dialogue opens. Here teams can be added, edited, displayed and/or deleted.

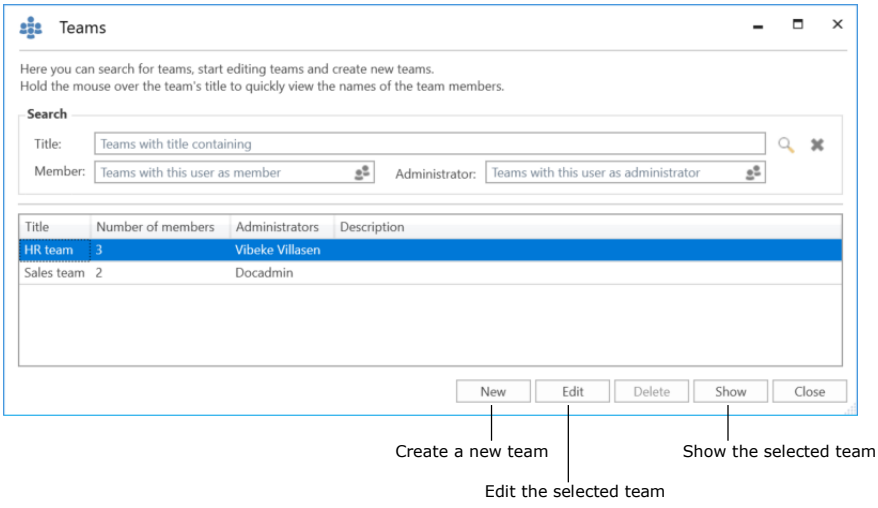


Figure 91: The "Teams" dialogue

Click on **New** to create a team. In the dialogue add:

- Title.
- Description.
- One or more team administrators to maintain the team.
- A synchronisation key if the team is to be automatically updated through synchronisation. The synchronisation will often be through AD, but can also be used or other systems (e.g. cBrain's M4 system) in which the team can also be managed.
- Tick the "Active" box to activate the team so it can be used on records and cases.

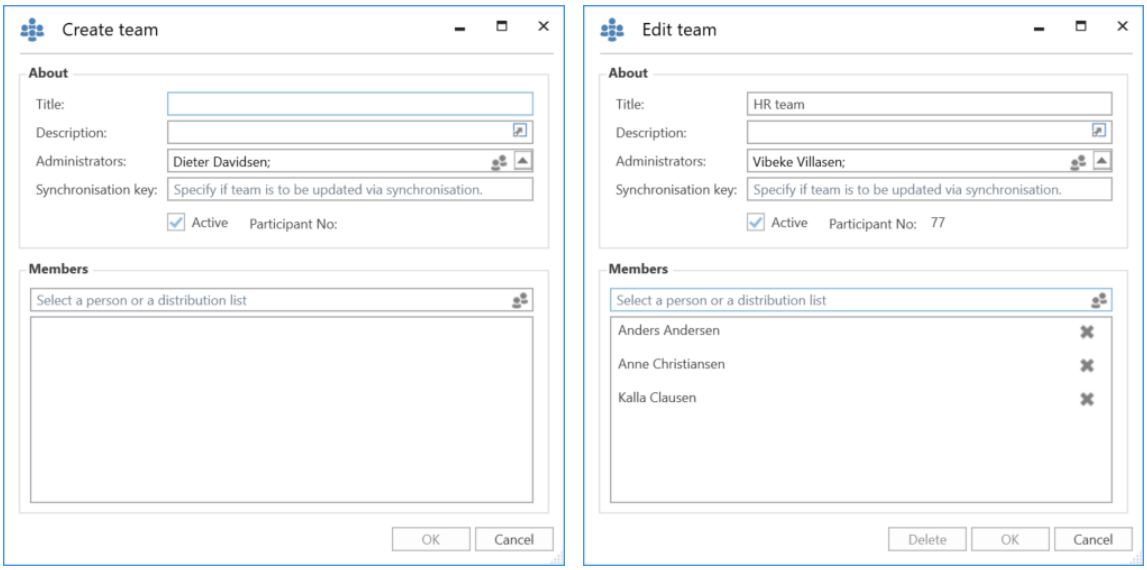


Figure 92: The dialogue in which teams are created and edited

Distribution lists

Users who have a role that is assigned the "Distribution list editor" privilege can create and manage the shared distribution lists in F2.

It is possible to add units and users (also from other F2 authorities) as well as external participants to a distribution list. A distribution list can contain a mix of participants from the user's own authority as well participants from other authorities, units and external participants.

It is also possible to add a distribution list to another distribution list, along with units, external participants and individual users. This makes it easier to maintain the distribution lists. If changes are made to the organisation it is only necessary to update the original distribution list. All distribution lists that contain the original list are then automatically updated.

Some distribution lists cannot be edited in F2. For example:

- Distribution lists that are synchronised with Exchange
- Distribution lists for units and teams.

For more information on creating and editing distribution lists, see the manual *F2 Desktop – Settings and setup.*

Note: Changes to a team or unit name will not be displayed on the team's or unit's distribution list. However, it is possible to edit the name of a unit's distribution list. To change the name of a team's distribution list, the team must be deleted and recreated with a new name.

Setting up the main window and the results list

The main window

This section describes how a user with the "Search administrator" privilege defines, creates and manages fixed or unit-specific searches that are displayed in the main window of the users within the authority.

Setting up fixed searches

F2 has a number of predefined standard lists (fixes searches). These are accessed on the left side of the main window. For more information about searches and the use of standard lists, see the manual *F2 Desktop – Search functions*.

Fixed searches apply to one of the following:

- The individual user (location: "Personal")
- An organisational unit (location: "Unit")
- All (location: "Standard").

The last two types of fixed searches can only be created by a user who has the "Search administrator" privilege, but be used by the users within the F2 authority. The following sections explain how fixed searches are created.

Create fixed searches

An administrator can create a fixed search by clicking on **Archive** from where the search is performed. A search is then performed either as a simple search or as an advanced search.

Display the advanced search fields by clicking on the **Advanced search** menu item in the ribbon of the main window. A list of search groups appears. To see the search fields of a group, hover the mouse over its name or click it.

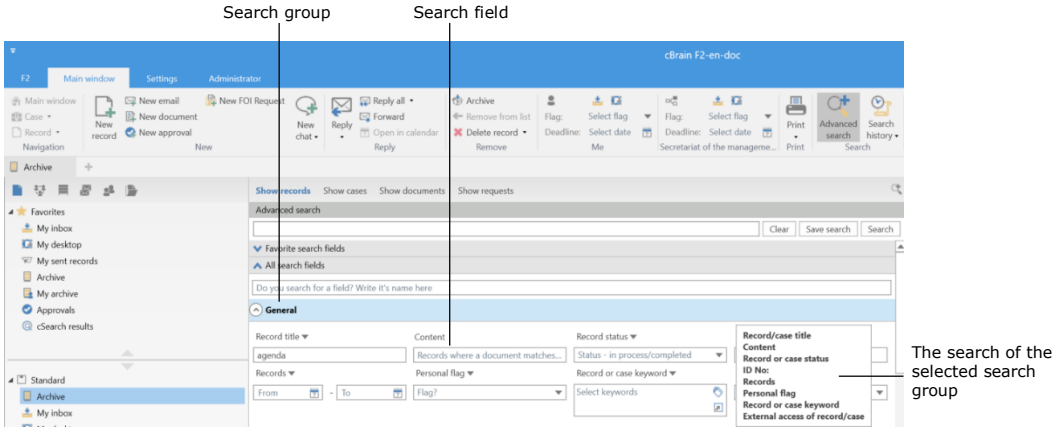


Figure 93: Advanced search

Fill in the relevant fields, and click on **Search** to perform the search. Click on **Save search** to save it.

The administrator chooses if the search will be available only to him/herself (Personal search), to all (Standard) or to selected units (Unit search). In case of a unit search, the unit must be specified. Give the search a title that correlates with the content of the search.

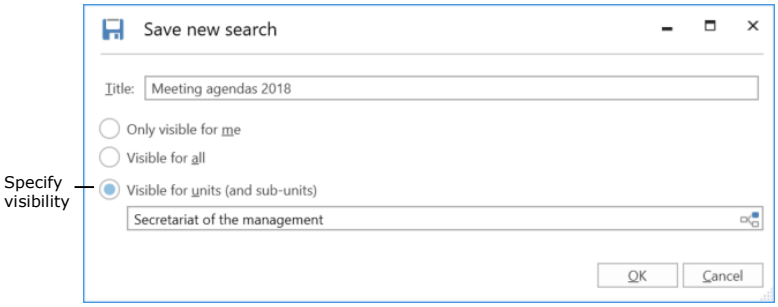


Figure 94: Save a search as a unit search

Click on **OK** to save the search in the main window under the "Standard", "Personal searches" or "Unit searches" list node.

Searches can be further qualified by entering more search criteria. For example, the table below shows the interrelated values of title, location and standard searches.

Standard searches

F2 comes with a number of standard searches that the administrator can either remove or edit. If a fixed search is created for a unit, it is available for all users in the unit and any sub-units.

A search can also be made available for all users in the authority or the entire organisation (several authorities).

All users can view the standard searches on the left side of the main window.

The standard searches shown below are located the "Standard" node.

Title	Description
My inbox	My personal inbox
My desktop	Desktop: Mine
My archive	Archive: Mine
My sent records	Sent records

The standard searches below are located in the organisation's top node in which all authorities in an installation are placed. The top node can be e.g. a ministry in which a department and government agencies are placed.

Title	Description
Inbox ([unit name])	My unit's inbox
Desktop ([unit name])	My unit's desktop
Archive ([unit name])	My unit's archive
In process: Me	Being processed by me
In process: Unit	Being processed by my unit
Deadlines tomorrow: Me	The deadline for me is tomorrow
Deadlines tomorrow: Unit	The deadline for my unit is tomorrow
F2 Requests to unit	F2 Requests to my unit
F2 Requests from unit	F2 Requests from my unit
Post list: Mine – The past 2 days	My post list
Post list: Mine – The past week	My post list, weekly
Post list: The unit's – The past two days	The unit's post list the past two days
Post list: The unit's – The past week	The unit's post list, the past week

Delete fixed searches

A user who creates and saves a personal search can also delete it.

If a technical administrator or an administrator creates a fixed search in either "Standard" or "Unit", it can only be deleted by an administrator.

This type of search can be deleted as shown below.

The administrator must choose to show all unit searches in the main window in order to access them. To do this, right-click on the record icon above the lists in the upper left corner of the main window. Then click on **Show all**.

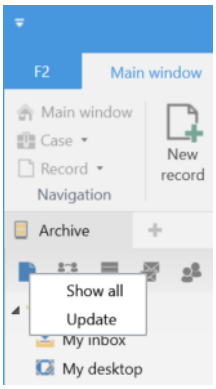


Figure 95: Show all units

The main window expands to display all of F2's units. A search within a unit can then be deleted using the right-click menu.

Return to the standard view of the main window by right-clicking on **Records** and then on **Show as user**.

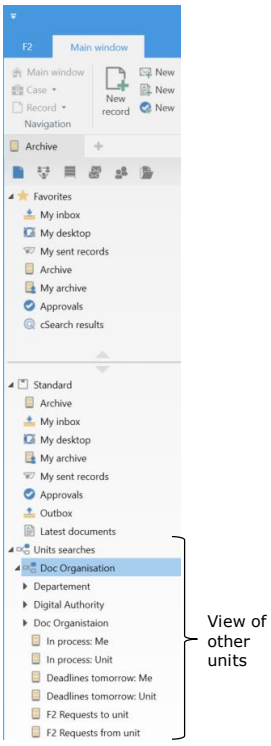


Figure 96: Unit overview

Shared folders in the main window

Shared folders can be created, edited and deleted by all users. However, it is recommended that the administrator takes on the responsibility of maintaining the overall structure of and/or guidelines for folder composition.

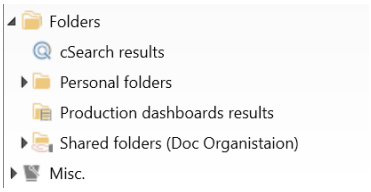


Figure 97: Shared folders in the main window

Shared folders can be accessed by everyone within an authority. It is advisable to create two general folders:

- An area of responsibility or organisational folder.
- A folder for cross-organisational areas such as projects, etc.

Setting up standard column layouts for search results and folders

In F2, the results list display settings are referred to as the column layout. The column layout is used in the main, record and case windows and contains information on:

- Which columns the table contains
- Column sequence
- Column width
- Sorting sequence
- Grouping, if applicable.

F2 defines the following levels of column layout:

- **Basic column layout**: Predefined column settings that are present in F2 upon installation.
- **Global standard column layout**: Administrator-created column settings. In F2 these are called "Global standard column settings".
- **Personal standard column layout**: The users' own column settings. In F2 these are called "Standard column settings".

The following applies to all the three levels of column layout:

- The basis column layout is delivered with F2 and cannot be edited.
- If an administrator creates a new unit search, the current column layout is saved as the standard column layout for the new search.

- If an administrator creates a new standard column layout, this is applied to all the users within the organisation.
- If a standard user makes changes to a column layout, this can be saved as a personal column layout (standard column settings).

Read more about personal column layouts (standard column settings) in *F2 Desktop – Settings and setup.*

Create a standard column layout (global standard column settings)

A user with the "Result list administrator" privilege can define, create and maintain the standard column layouts in F2. This layout applies to all users within the organisation who have not created a personal column layout.

It is the administrator's setup of the standard column layout that determines how the results list is presented to the users. This means that an administrator can help improve the results list for F2 users.

Four different types of standard column layouts can be created based on the following views:

- Records
- Cases
- Documents
- Requests (add-on module).

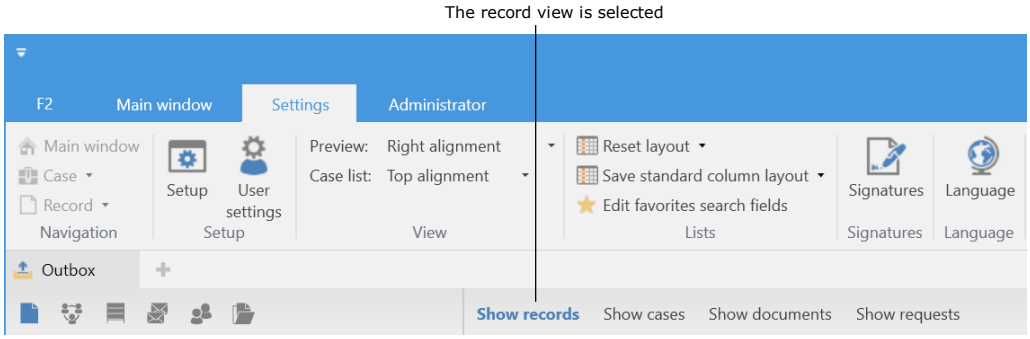


Figure 98: The view in the main window

A standard column layout is created for each view. The following elements can be adjusted:

- Which columns to display
- Column sequence
- Column width
- Sorting sequence, so that results are sorted by a column, e.g. the "Responsible" field on records.

- Grouping, if applicable. The administrator decides whether auto grouping is toggled.

The following example goes through the steps of creating a standard column layout for the record view:

1) Click on **Records** above the results list.
2) Right-click on a random column and then select **Columns** from the right-click menu.
3) The "Select columns" dialogue opens. Select the wanted columns and then close the dialogue.
4) Rearrange the columns in the results list by dragging one column at a time. Adjust the column width by pulling on the sides of the column titles.
5) Select a column by which to sort the results list. In this example, the "From" column is selected.
6) Toggle auto grouping by clicking on **Auto grouping** in the ribbon of the "Settings" tab.

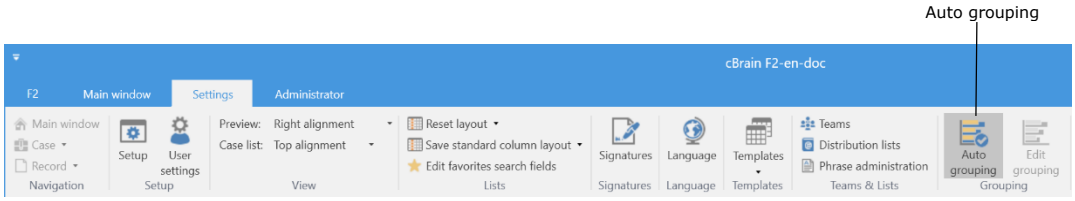


Figure 99: Activate auto grouping

The created standard column layout for the record view is shown below.

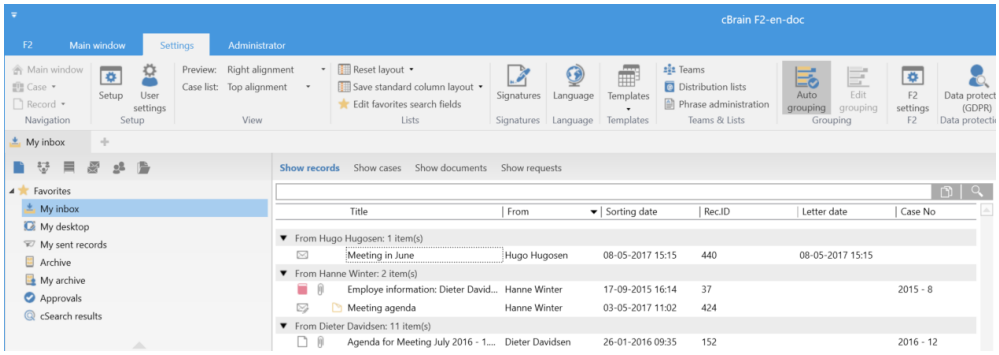


Figure 100: Created standard column layout for the record view

A standard column layout is saved by clicking on the **drop-down arrow** in the "Save standard column layout" field located in the ribbon on the "Settings" tab. Then click on **Save global standard column settings**.

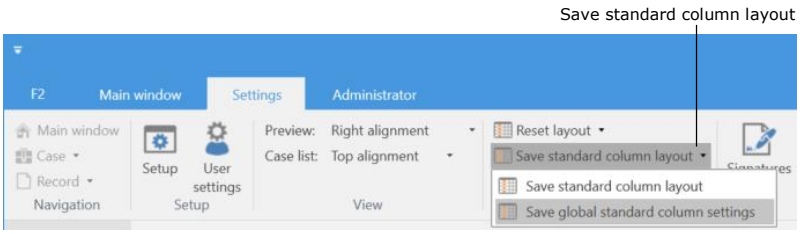


Figure 101: Save the global column settings

The standard column layout will then be applied to all users who have not made a personal column layout (standard column settings).

> **Note**: If a set of global standard column settings already exists, this will be overwritten when a new standard column layout is saved. It is always the most recently saved standard column layout that is applied.

The same procedure is used for creating standard column layout for case, document and request views.

The column layout

Administrators should be aware that defined standard searches need to be updated if changes (additions/deletions) are made to metadata fields in connection with an F2 update.

User settings

The "User settings" menu item provides access to defining and creating a number of user settings. User settings include user configurations and column settings.

As a standard, user settings are defined using a user's existing setup and column settings. It is possible to select all or parts of a user's setup and column settings as content for new user settings. The created user settings can be obtained by the user him/herself. An administrator can also assign certain settings to selected units and role types.

A user with the "Settings administrator" privilege can create, manage and assign user settings to other users. These administrators can also assign specific role types to user settings. This means that while new users are automatically given a setup that corresponds to their role, existing users will keep their own setup. This makes it possible to create user settings that differ from role to role.

If a user has multiple roles, the role priority decides which user settings is applied. Via "User settings", different user settings can be reused across the organisation.

The "User settings" menu item, located on the "Settings" tab in F2's main window, opens the "User settings" dialogue.

The "User settings" dialogue is used to manage and assign configurations and column settings to users or role types.

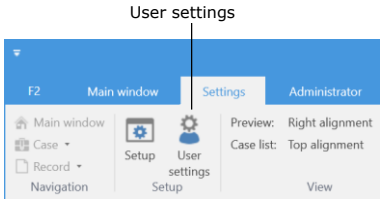


Figure 102: The "User settings" menu item

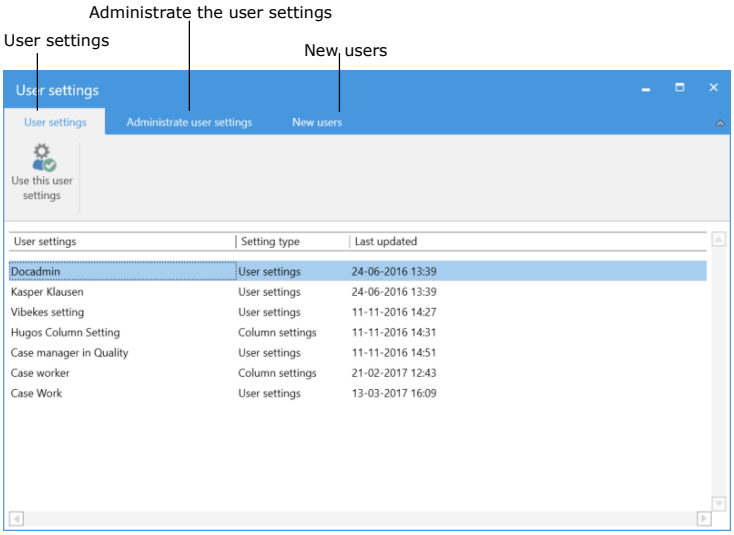


Figure 103: The "User settings" dialogue

The dialogue consists of three tabs:

- "User settings". All users have access to this tab. For further information, see the manual *F2 Desktop – Settings and setup.*
- "Administrate user settings". See below.
- "New users". See the section *New users*.

Administrate user settings

The "Administrate user settings" tab is described below.

On this tab, a user with the "Settings administrator" privilege can create, manage, and assign user settings to other users.

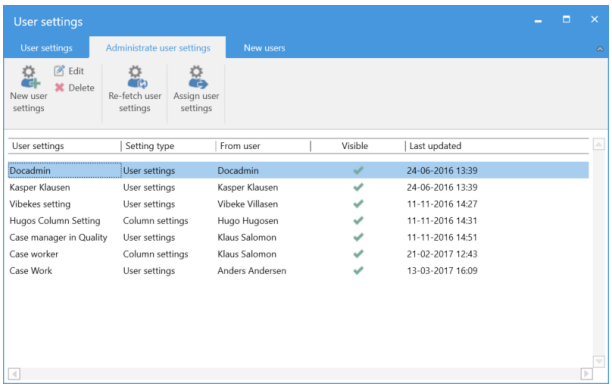
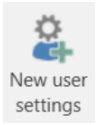
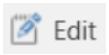
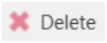
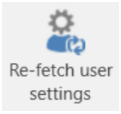


Figure 104: The "Administrate user settings" tab

The tab has the following menu items:

Function	Purpose
	Add a new user setting to the user setting list. Read more in the section *Create a new user setting*.
	Edit the selected user setting. Its name and visibility can be changed.
	Permanently delete the selected user setting from the list.
	Retrieve the user's latest user setup, updating the selected user setting.
	Assign the selected user setting to users or role types. Read more in the section *Assign user settings to users or role types*.

The tab shows the following columns:

Column	Description
"User settings"	Displays the title of the user setting.
"Setting type"	Displays the type of user setting.
"From user"	Displays the name of the user whose user setting has been copied.
"Visible"	Shows whether the user setting is visible and retrievable to other users.
"Last updated"	Displays when the user setting was last updated.

Create a new user setting

The following section describes how new user settings are created and assigned to users. Two types of user settings exist:

- Column settings
- User settings.

Click on **New user settings** on the "Administrate user settings" tab to open the dialogue below.

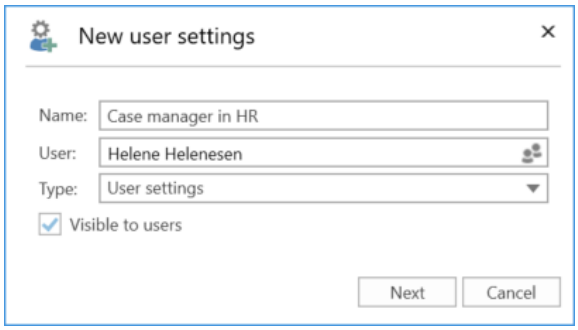


Figure 105: Create a new user setting

A new user setting of the "User settings" type is created and added to the list of user settings by specifying the following:

- The name of the new user setting.
- The name of the user for whom it is set as the standard user setting.
- Select the type.
- Tick the "Visible to users" box to allow other users to retrieve the setting.

Then click on **Next**.

If "User settings" is chosen as the type, the "Setup" dialogue opens. See the section *New user setting*. If "Column settings" is chosen as the type, the "Choose column settings" dialogue opens. See the section *New column settings*.

New user setting

If "User settings" is chosen as the type, the "Setup" dialogue opens. Here the different options for the new user setting can be selected.

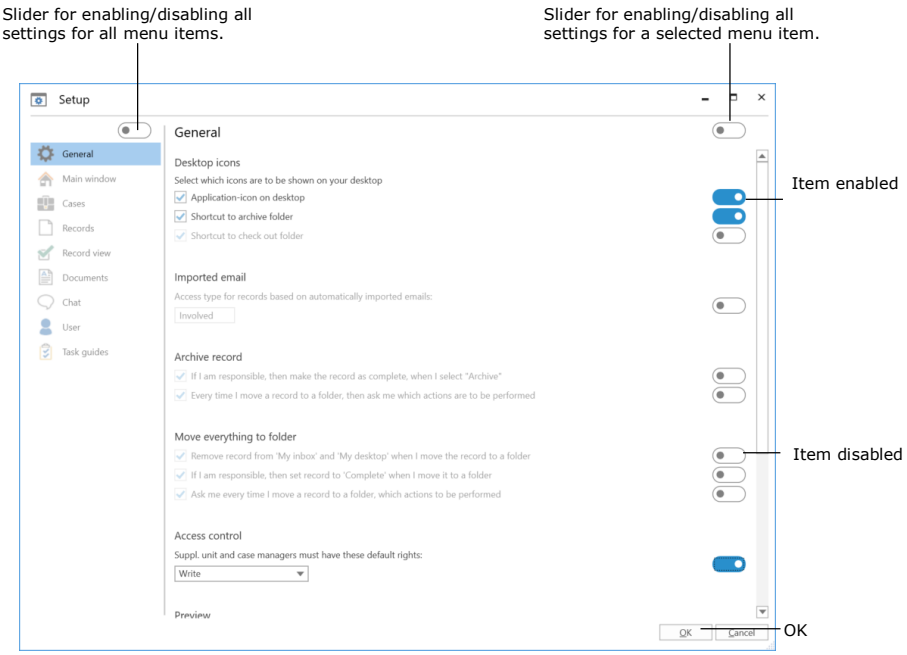


Figure 106: The "Setup" dialogue with sliders

It is possible to include the entire setup in a new user setting. To do this, click on the slider above the tabs in the upper left corner of the "Setup" dialogue. Once the slider is blue, the entire setup is chosen. If the slider is white, none of the user's setup options are chosen.

It is also possible to include the configuration of a single menu item in a new user setting. To do this, first click on the relevant tab on the left side and then click on slider in the upper right corner of the dialogue. All sliders for that menu item will then turn blue, indicating that all configuration options are included in the new user setting.

In addition, it is possible to include individual configuration settings on a given tab in a new user setting. Click on the relevant tab and then click on the sliders next to the settings to be included in the new user setting. The sliders for the selected settings will turn blue.

Once the wanted settings are chosen, click on OK at the bottom of the dialogue to save the settings for the user setting. The new user setting is then added to the list off available user settings which may be retrieved by users or an administrator can assign to certain users and role types.

Note: When a new user setting is retrieved or assigned, F2 must be restarted for it to take effect.

New column settings

Selecting the "Column settings" type will open the "Choose column settings" dialogue. Here it is possible to select which lists, folders, etc., to save as column settings.

Only the columns saved by the user whose settings serve as the basis for the new standard settings will be active.

However, all views, i.e. "Show records", "Show cases", "Show documents", and "Show requests" are included. The new user will have no column settings for e.g. "Show documents" or "Show requests", if the user on which the new settings are based did not select any. The new user settings will match the chosen user setup.

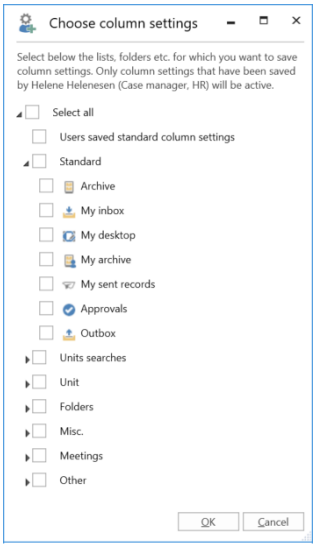


Figure 107: The "Choose column settings" dialogue

Click on **OK** to complete. The column settings will be added to the list of available user settings.

> **Note**: It is not possible to assign/retrieve columns separately. All columns belonging to a list must be collectively assigned or retrieved.

> **Note**: When a new column setting is retrieved or assigned as a user setting, F2 must be restarted for it to take effect.

Assign user settings to users or role types

There are two ways to assign a user setting:

- Assign to users: Used to assign user settings to users, units, distribution lists and/or teams.
- Assign to role types: Used to assign a user setting to users with a certain role type, for example a user with the "Technical administrator" role type in a certain unit, distribution list and/or a team. It can also be assigned to all users with the specific role type.

Select the wanted user setting from the list on the "Administrate user settings" tab. Then click on **Assign user settings**.

A new dialogue opens. Choose between the two options "Allocate to users" or "Allocate to role type".

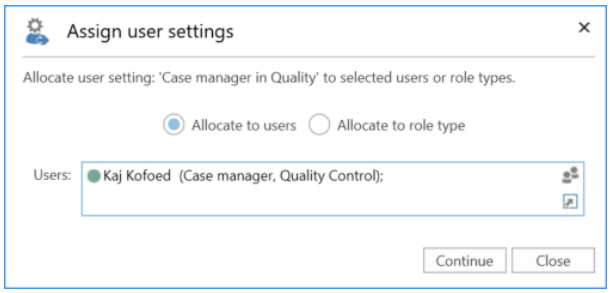


Figure 108: Assign user settings to users

If "Allocate to users" is chosen, enter the users, units, distribution lists and/or teams to receive the user setting in the "Users" field.

If "Allocate to role type" is chosen, select a role type from the drop-down menu in the "Role type" field.

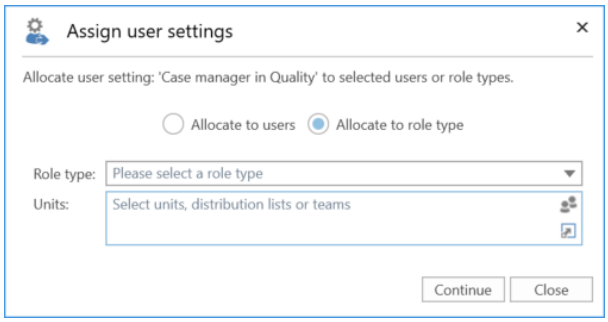


Figure 109: Assign user settings to a role type

Click on **Continue**.

The users that will receive the user setting are displayed. If necessary, a message can be sent to the users added in the dialogue. Complete by clicking on **Allocate**.

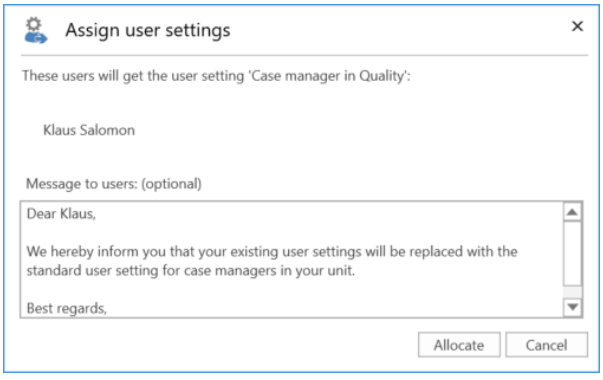


Figure 110: Send a message to the selected users

The user setting is then assigned to the selected user(s). This is shown in the "Assign user settings" dialogue. A green ribbon appears with the text "The default user setting

was pushed to [number] user[s]". See the figure below. From here, more users can be assigned the same user setting. Close the dialogue by clicking on **Close**.

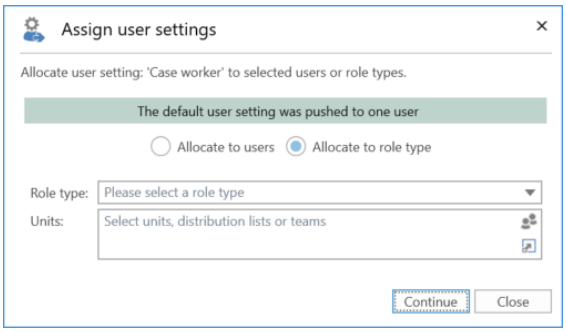


Figure 111: The dialogue after assigning a new user setting

Users will automatically receive a record in their inbox, when they are assigned a new user setting.

The record contains the following information:

- The user's existing configuration has been updated with a user setting.
- The time and date for the update.
- A message from the administrator, if any.

Note: F2 must be restarted for newly assigned or retrieved user settings to take effect. The assigned user settings will overwrite any changes to the user setup performed by the user him/herself.

New users

The following section describes the "New users" tab in the "User settings" dialogue.

Using this tab, a user with the "Settings administrator" privilege can assign a user setting to a role type. As a result, new users are automatically given user settings assigned to their specific role type.

This means that a "Department head" role type can have different user settings than e.g. the "Case manager" role type.

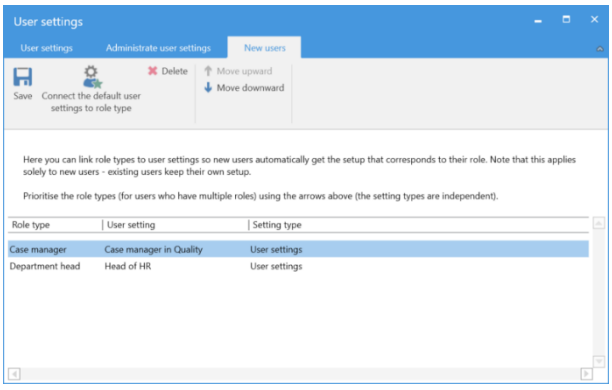
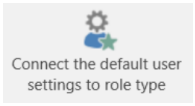
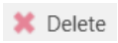
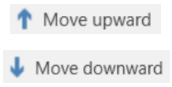


Figure 112: The "New users" tab

The menu items on the "New users" tab are described below.

Function	Purpose
	Saves changes and/or the attachment of role types to a user setting.
	Connects user settings to a role type. Specific user settings are assigned to a specific role type to ensure that all newly created users with this role type receive its user settings.
	Deletes the connection between the user setting and the role type. Users who are assigned this role will no longer receive the formerly attached user setting.
	Moves the role types up/down on the list according to prioritisation. The sequence is crucial as it determines which user setting should be assigned to a user with multiple roles. The higher up on the list a role is, the higher it is prioritised.

The tab has the following columns:

Column	Description
"Role type"	Shows the role type to which the user setting is attached.
"User setting"	Shows the name of the user setting attached to the role type.
"Setting type"	Shows the type of user setting.

Note: The menu items in the ribbon of the dialogue become active once a user setting is selected.

Attach a user setting to a role type

Click on **Connect the default user settings to role type** to attach a user setting to a specific role type.

A dialogue opens in which it is possible to assign a user setting to a role type.

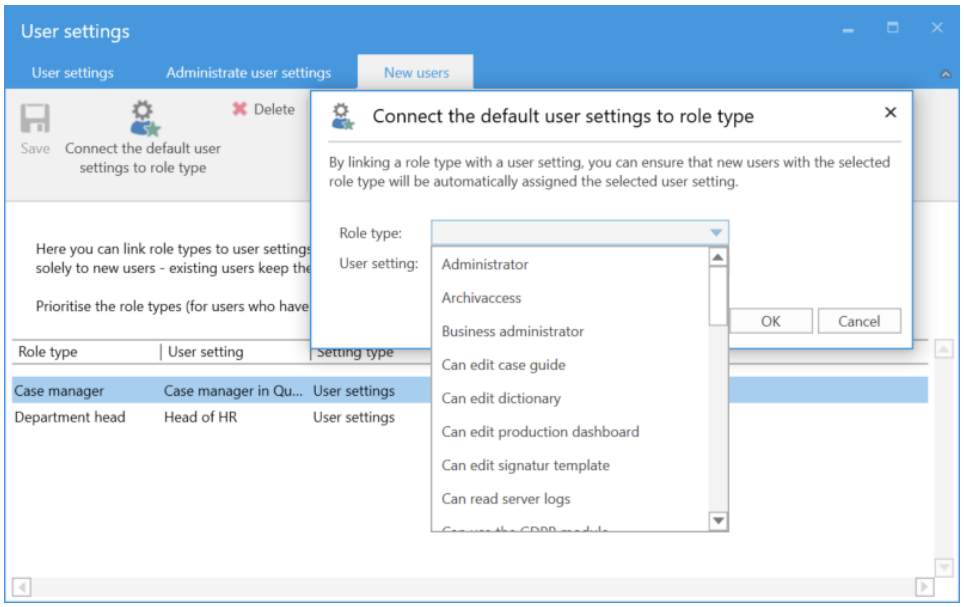


Figure 113: Assign a user setting to a role type

Click on **OK** to complete. The user setting is then assigned to the role type.

The rules for user settings:

- User settings assigned to role types only affect new users. Existing users whose job role is assigned a new user setting are not affected.
- If a new user is assigned a role type, the user automatically receives its user settings, if any.
- If a new user is assigned multiple role types with user settings, the user automatically receives the user settings of the highest ranking role type. It makes no difference with which role the user logs in.
- No matter which user setting was received, the user can always change the setup.

Document templates

All users can create private document templates for use in their everyday work. A user with the "Template administrator" privilege can create, edit and delete shared document templates that are used as standard documents across the organisation.

Document templates are divided into three levels in F2:

- **Standard document templates**
  A standard document template can be used by all users. However, only users with the "Template administrator" privilege can create, maintain and delete them.
- **Document templates on unit level**
  A document template on unit level can be used by all users in the unit or its subunits. Only users with the "Template administrator" privilege can create, maintain and delete them.
- **Personal document templates**
  A personal document template can only be used by the user who created it. Only the user him/herself can create, maintain and delete a personal document template.

F2 supports the following file formats for templates: docm, docx, dot, dotx, dotm, xlsx, xlt, xltx, xltm, pot, potx, odt, ods, odp, ott, ots og otp.

Templates are managed via the "Templates" menu item. The menu item is located in the ribbon of the "Settings" tab in the main window.

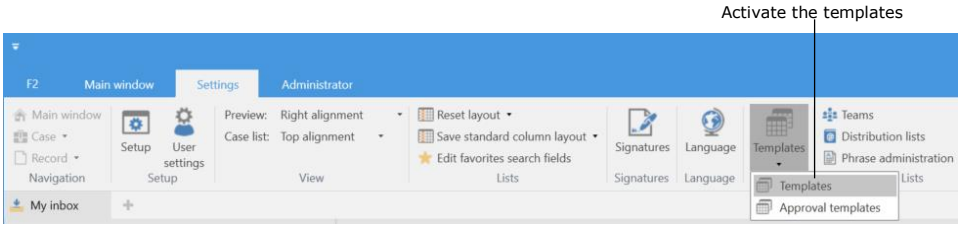


Figure 114: Administration of templates

For an administrator the dialogue window will appear as follows:

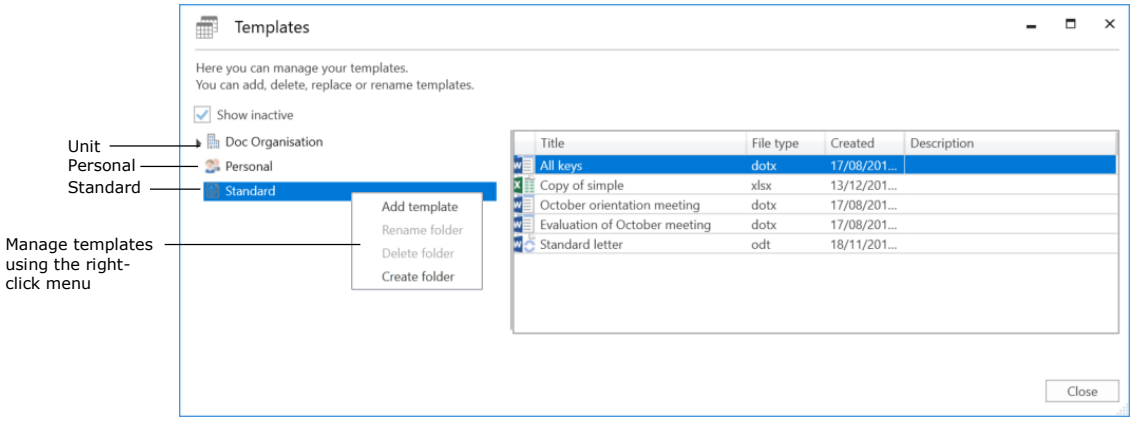


Figure 115: Managing document templates

Managing document templates is described in *F2 Desktop – Settings and setup*.

F2 Settings

In F2 users with special privileges can alter the basic setup and configuration of F2. Users who have special privileges have the "F2 settings" menu item on the "Settings" tab. Access to the "F2 Settings" menu item requires one of the following privileges:

- CBrainInstaller
- CBrainSetter
- CBrainSuperSetter
- F2Setter.

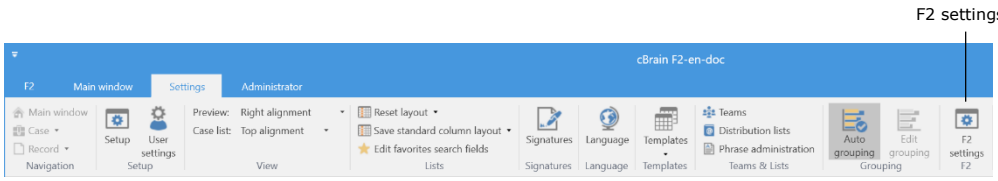


Figure 116: The "F2 settings" menu item

Click on the **F2 settings** menu item to open the "F2 settings" dialogue. From this dialogue it is possible to make changes to the configuration of F2.

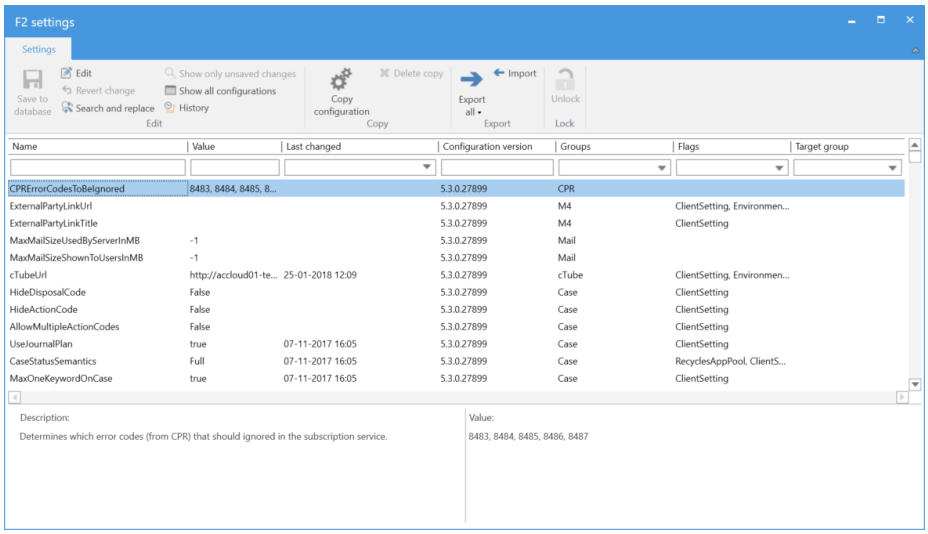


Figure 117: The "F2 settings" dialogue

Note: cBrain recommends that all configurations are performed in cooperation with cBrain. Configuration changes to F2 can have far-reaching consequences for all the users in the F2 installation. Changes should only be performed if strictly necessary and only if the consequences are known.

Add-on modules

The following section describes how to perform administrator tasks for a number of F2's add-on modules.

F2 Manager (add-on module)

A private office or a similar workplace can use F2's gatekeeper function to determine manage which approvals are sent to the minister's or the head of department's iPad. This requires the add-on modules F2 Manager and F2 Approvals.

The gatekeeper function can only be used by users who have either the "Minister" or "Head of Department" role.

This management is done via unit flags.

In order to use the gatekeeper function, an administrator must perform the following tasks:

- Create a flag using "Value list administration". Further information below.
- Give the private office "On behalf of" rights (either "Can perform all actions" or "Can handle approvals"), so its members can give final approval.

The private office and the minister or head of department must have roles within the same unit. Otherwise the private office cannot use F2's gatekeeper function to support the minister or head of department.

Create flags for F2 Manager

Flags for the gatekeeper function are created and maintained in the "Value list administration" located on the "Administrator" tab.

Open the **Value list administration** menu item and select "Flag" in the drop-down menu for types. Right-click on the **Flag** value list and click **Create** to create a new flag.

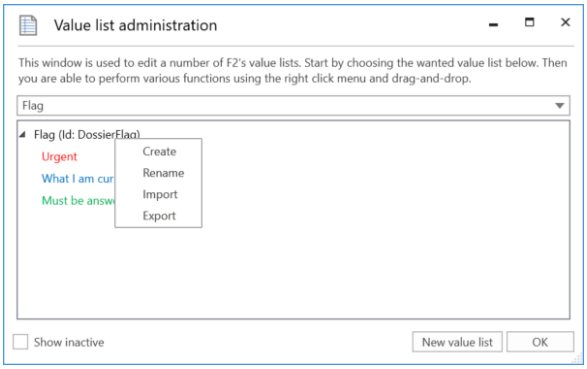


Figure 118: Create a flag

Once created, right-click on the new flag. Select **Properties** and the dialogue below appears. Fill in the name, description, external ID and colour.

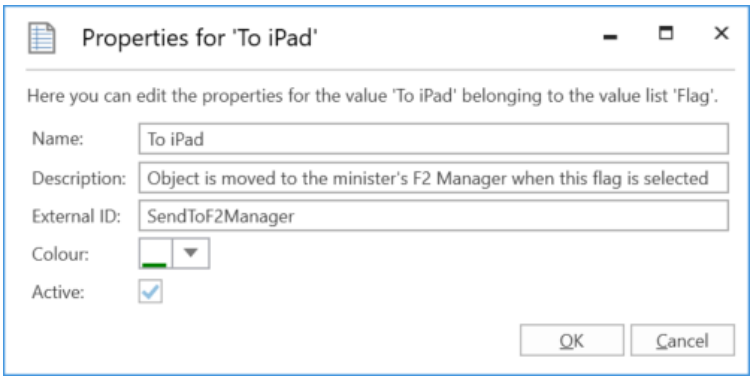


Figure 119: Properties for the flag

The following four flags must be created in order to use the gatekeeper function:

Name	Description	External ID	Colour
To iPad	The approval is moved to the minister's F2 Manager when this flag is selected.	SendToF2Manager	Optional (usually green)
To iPad – urgent	The approval is moved to the minister's F2 Manager and marked as urgent when this flag is selected.	SendToF2ManagerAsImportant	Optional (usually dark red)
From iPad	This flag is automatically put on an approval, once it has been processed by the minister in F2 Manager.	HandledOnF2Manager	Optional (usually purple)
From iPad - sync problem	This flag is automatically put on an approval if there is a synchronisation problem with F2 Manager.	SyncProblemOnF2Manager	Optional (usually blue)

These four flags are created as a standard. However, administrators can create as many flags for the gatekeeper as needed. cBrain can create additional flags to help prioritise approvals. During configuration of each flag, it is possible to select its colour when the approval is moved to the iPad, along with the sorting sequence of the flags.

List of figures