

# Administrator

Created on 26/03/2025 04:04 for F2 version 10

# Introduction to administrative tasks

Setup and administration of F2 is done by a user with F2 administrator privileges. Privileges grant users the rights to handle different administrative tasks and are assigned through roles.

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 [Administrator roles](#) section. They all include special privileges to set up and change the basic functionality of F2.

## Administrator tasks in F2

Many administrative functions can be performed in F2's user interface 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 layout in the result list.
- Setup of the user interface for the record window:
  - Document templates.
  - Keywords.
  - Flags for personal and unit control.
- The administration of various value lists e.g. [progress codes](#) and file plans.

# The user interface for F2 administrators

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

Many administrator tasks are accessed from the “Administrator” tab in F2’s main window. Administrator-related functions for the setup and maintenance of F2 are found in the ribbon.

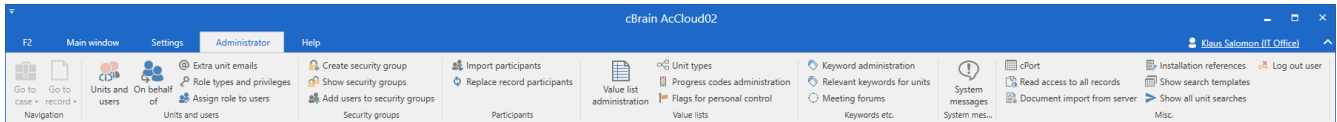


Figure 1. The ribbon of the “Administrator” tab in the main window

## NOTE

The menu items available on the ribbon of the administrator tab depend on the administrator’s privileges and which add-on modules are included in the F2 installation. Users may experience that some functions described or shown here are not available in their F2 installation.

# Installing cBrain F2

Immediately after installation, 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 which is known as the top unit in F2.
- A role of the “Administrator” type. Read more in the [Roles in F2](#) section.

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

# The unit structure in F2

It is important that the user possesses a general knowledge of F2 in order to understand the administrative tasks. For this, refer to the [F2 Basics documentation](#).

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, at least one unit must be defined in the organisation. The reason is that a user's read and write access to records and documents depend on the unit structure. F2's unit structure roughly corresponds 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 created 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.

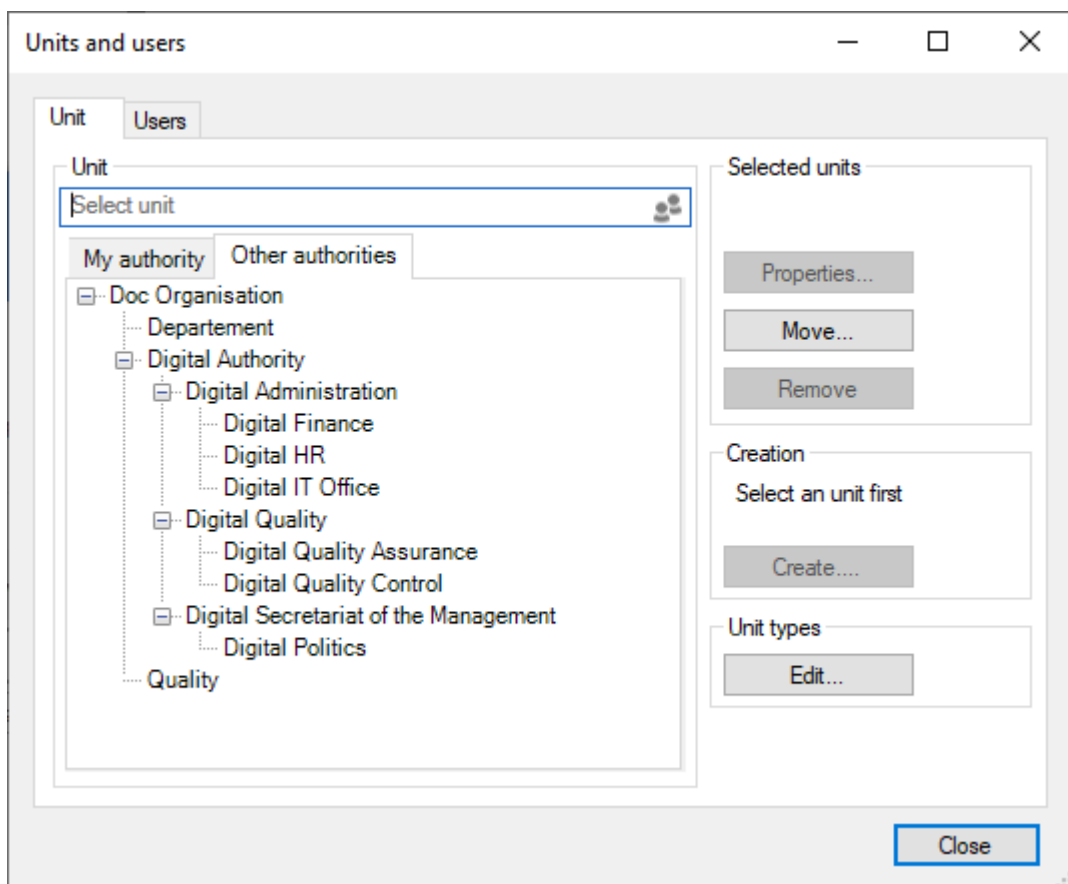


Figure 2. An example of F2's tree structure

**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.

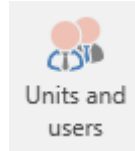


Figure 3. The “Unit and users” menu item

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

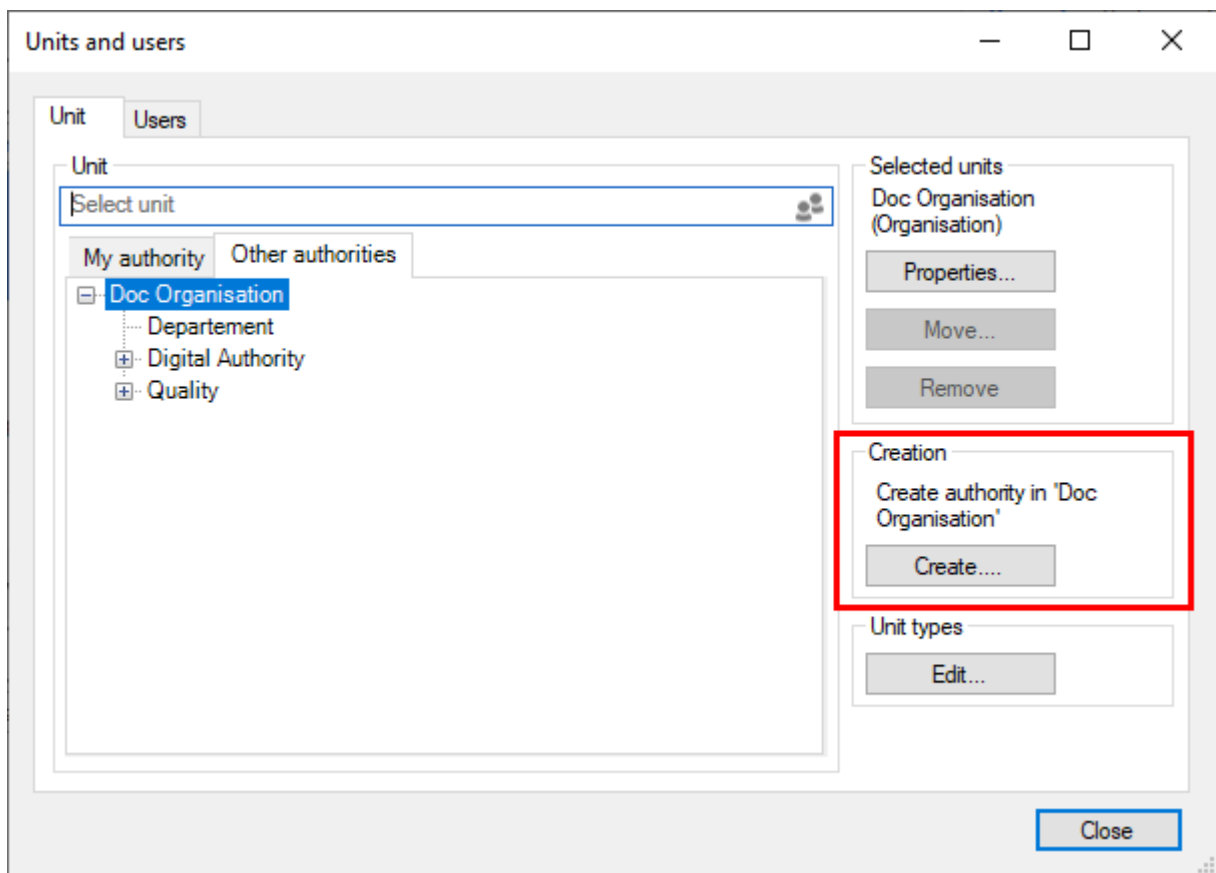


Figure 4. Create a new authority

The dialogue shows an organisation called “Doc Organisation”. This organisation has the authorities: “Departement”, “Digital Authority”, and “Quality”.

The “Doc Organisation” wish to create a new authority with the name “Environmental Department”. Click on **Create** in the “Units and users” dialogue to open the “Create unit” dialogue.

The image shows a 'Create unit' dialog box with the following fields and sections:

- Unit:**
  - Name:
  - Email address:
  - Initials:
  - Unit type:
- Address:**
  - Address 1:
  - Address 2:
  - Post code:
  - City:
  - Country Code:
- Telephone:**
  - Phone:
  - Local No:
  - Mobile:
  - Fax:
- Home page:**
  - Web:
- Synchronisation:**
  - Key:

Buttons: OK, Cancel

Figure 5. The “Create unit” dialogue

Enter the relevant information about the new authority in the dialogue.

- The unit type is set to “Authority”.
- The system provides the location after the unit is created.
- Additional fields can be filled in if needed.

The authority’s email settings can be modified on the “Email settings” tab.

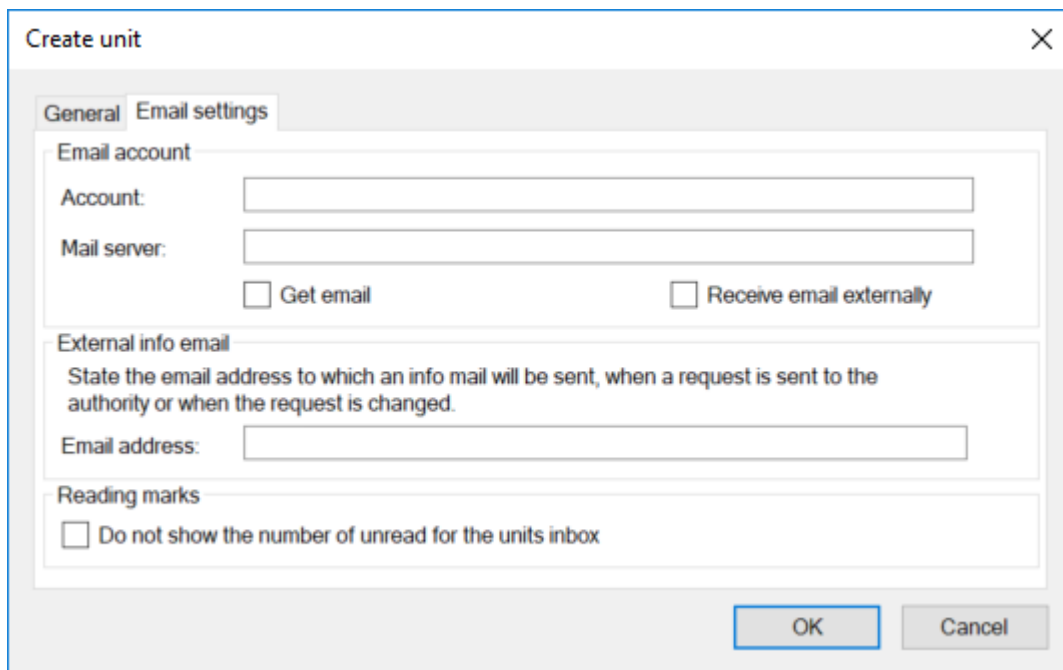


Figure 6. The “Email settings” tab in the “Create unit” dialogue

Read more about [setting up email accounts](#).

When the necessary fields have been filled in, click on **OK**. A warning dialogue appears to inform 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 “Environmental Department” authority is then created, and units and users can now be created within it. View the newly created authority in the figure below.

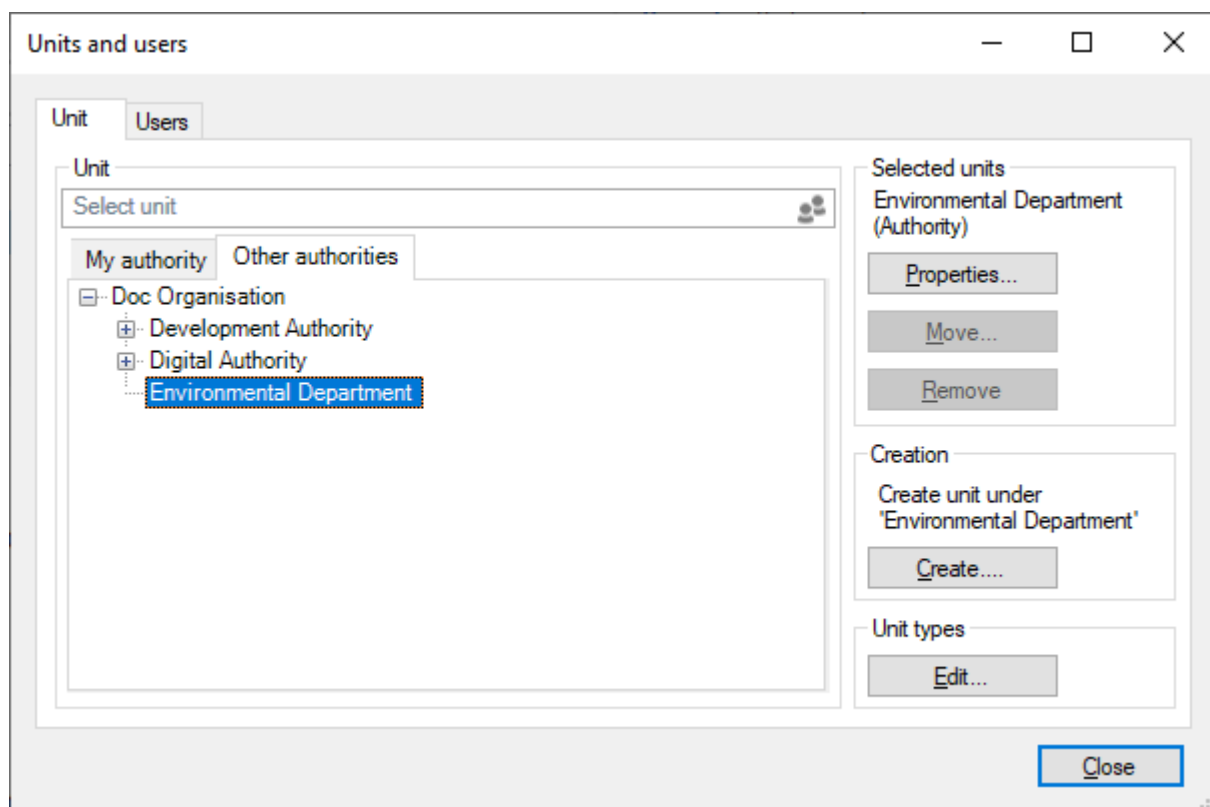


Figure 7. The newly created authority



## Create units within an authority

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

A chief purpose of units is to specify to F2 where to place 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 themselves.

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

An administrator can access units from the ribbon of the "Administrator" tab by clicking on the **Units and users** menu item.

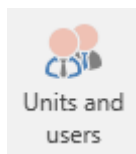


Figure 8. The "Units and users" menu item

In "Units and users" dialogue, a user with the "Unit administrator" privilege can create, edit, move, and deactivate units.

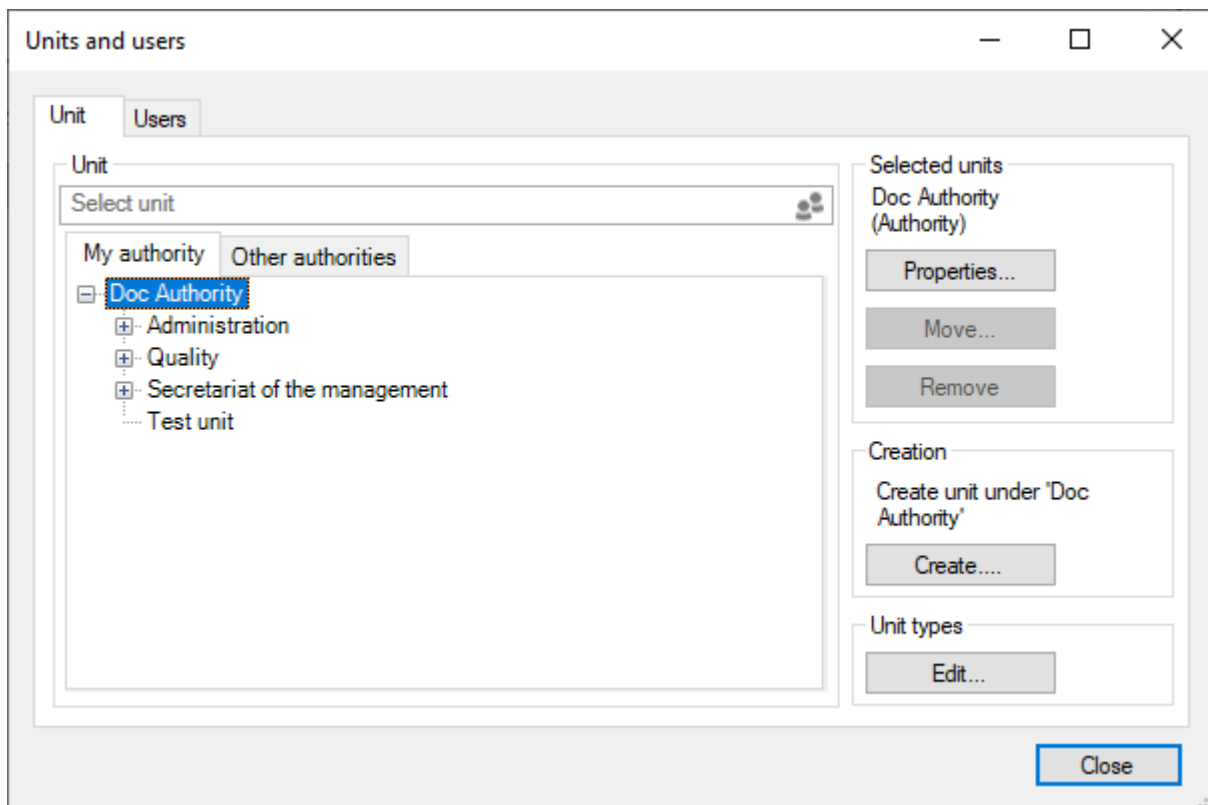


Figure 9. F2 is installed with only one top unit

The "Units" tab shows all units created in F2. They are organised in a tree structure. As mentioned, F2 is installed with one top unit (organisation). The name of the top unit is adjusted to fit the

Expand the top unit node to view all units that have been created in the tree structure. These units can also be expanded to show their subunits.

Create a new unit by selecting a “parent unit” in the directory and clicking on **Create**.

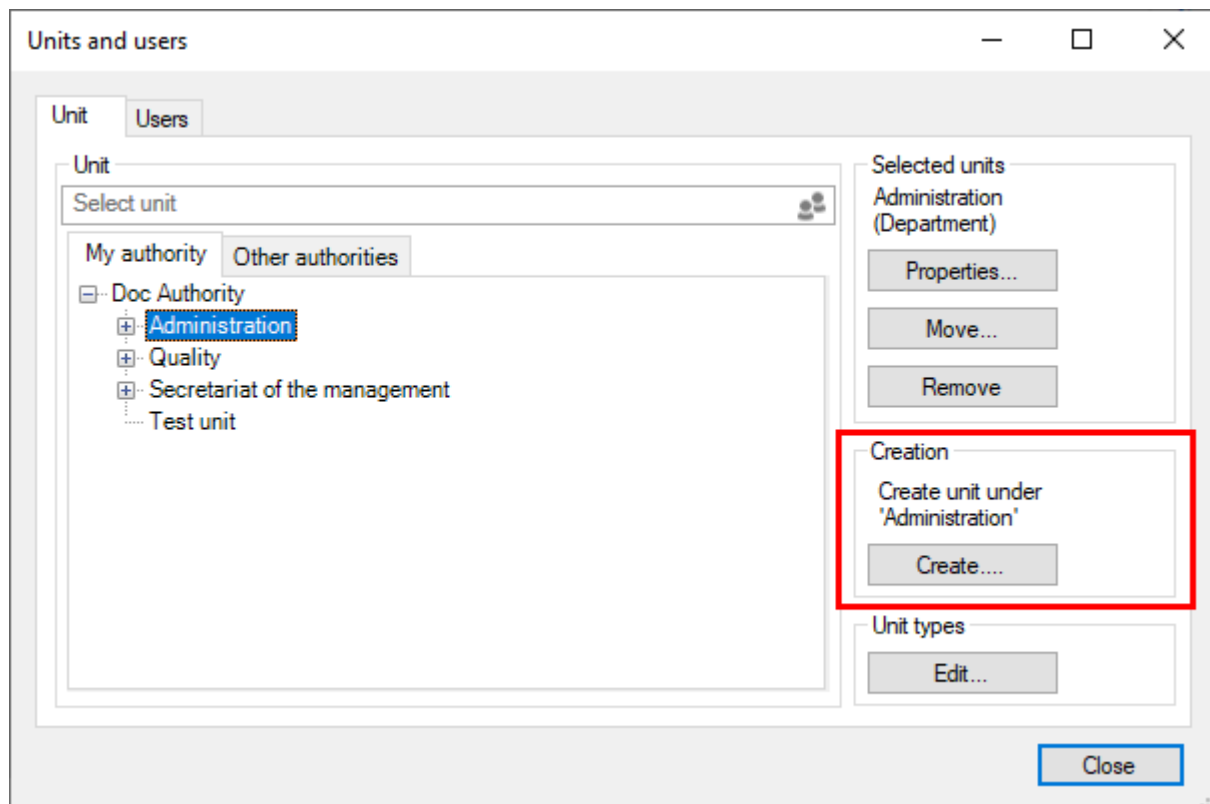


Figure 10. Create units within an authority

The “Create unit” dialogue opens.

Figure 11. The “Create unit” dialogue

Fill in the relevant information in the dialogue.

- In the “Unit type” field, select a representative type for the unit. See below for more information on the management of unit types.
- Units are created in the same dialogue that is used for creating authorities.

The organisational structure within an authority can contain many units.

Read more about [setting up email accounts](#).

## Create unit types for specific units

F2 divides units into types. F2 contains definitions of certain fixed unit types that are created during installation.

Some unit types cannot be deleted 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 the **Unit types** menu item in the ribbon on the administrator tab in F2's main window.

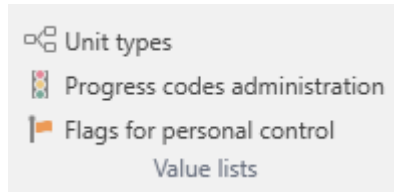


Figure 12. The "Unit types" menu item

The dialogue below opens. From here it is possible to manage unit types.

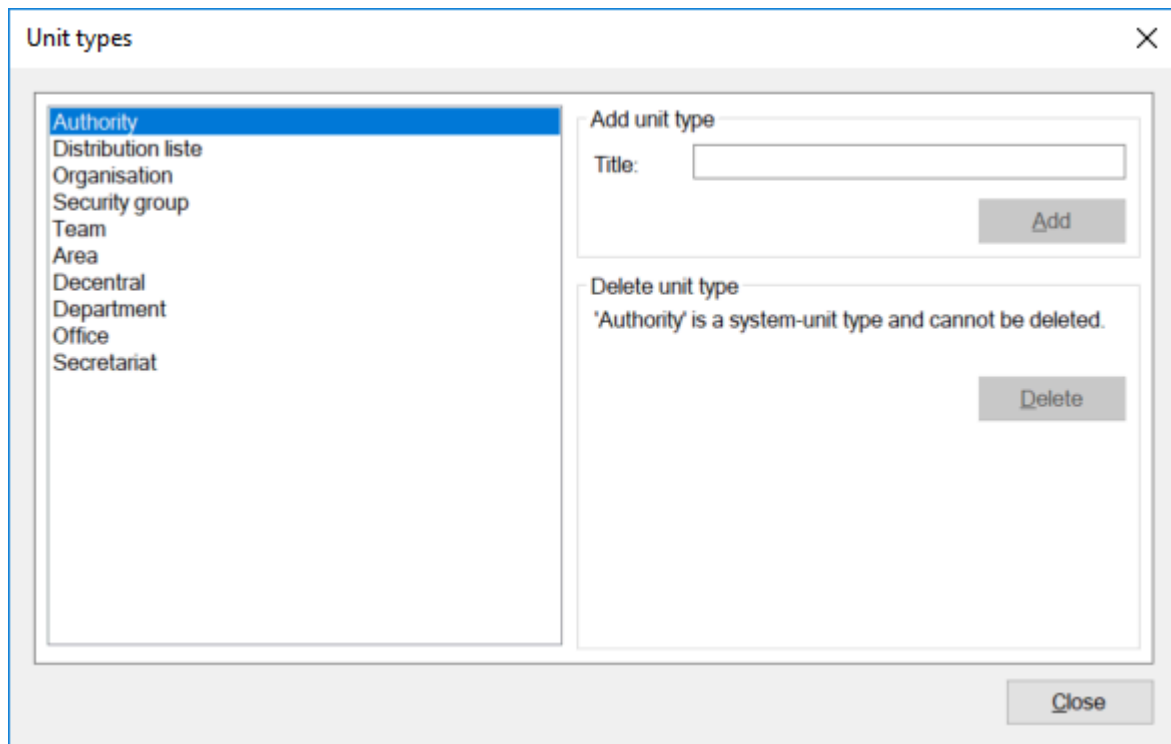


Figure 13. Management of unit types

These are examples of the unit types available:

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

Unit types such as teams and security groups are used to divide 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

The “Decentral unit” type mostly functions as any other F2 unit, but unlike other 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 log in 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.

The following 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 a “job role” before they can log in to F2.

The creation of a new user is described below. Once the user is created, they need 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.

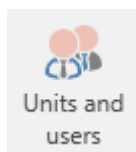
[One or more role types must be defined](#) before a user can be assigned any roles. One role type must be a “job role”.

## 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.

If a user was already created through AD import, the user must be [assigned a role](#).

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



*Figure 14. The “Units and users” menu item*

A dialogue opens in which the user’s master data can be entered.

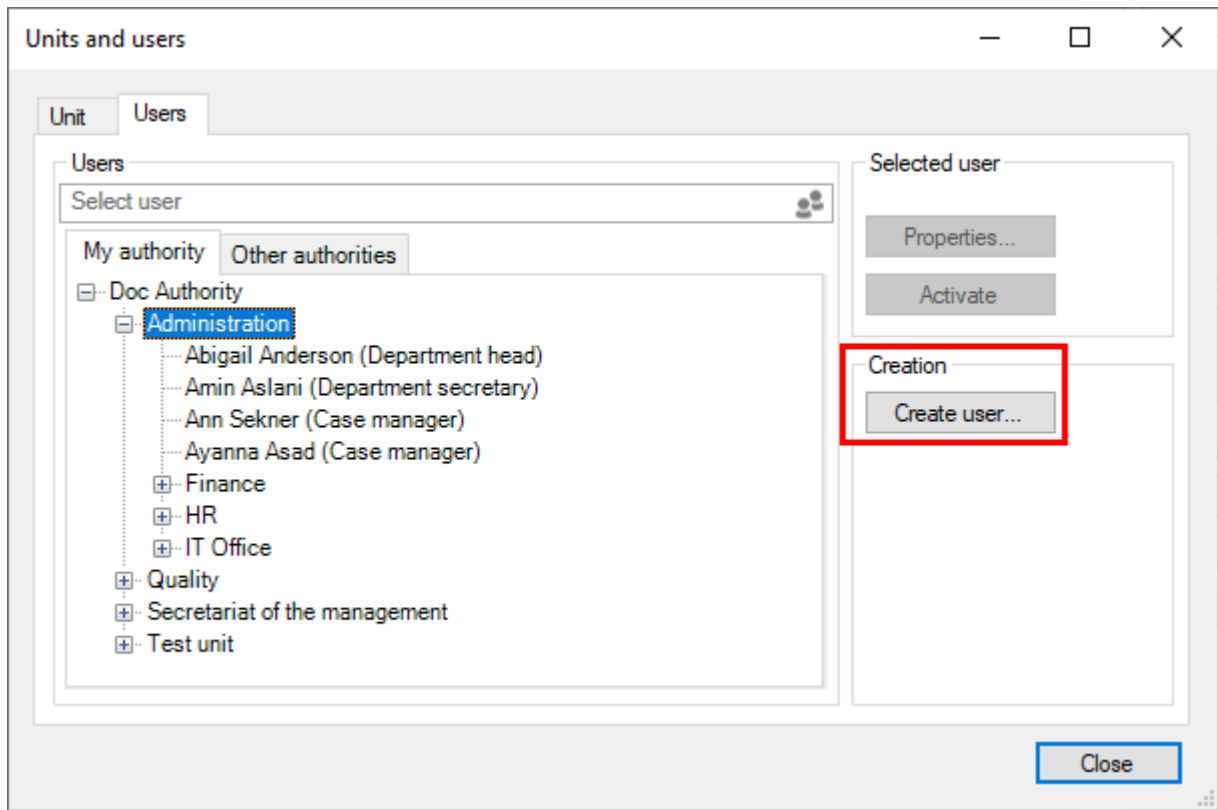


Figure 15. Create user

## 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.

**Create user** [X]

**Information** | Roles

**Name**

Name:

Username:

Initials:

Email address:

Title:

Limited access

SSN:

**Email account**

Account:

Mail server:

Get email       Receive email externally

**Address**

Address 1:

Address 2:

Post code:       City:

Country Code:

**Telephone**

Phone:       Local No:

Mobile:       Fax:

Private phone:

OK      Cancel

*Figure 16. User information*

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



Field	Description
"Limited access"	<p>Ticking the "Limited access" box restricts the user's access to records or cases in F2. The user only gains access when added to a record's or case's access restriction either by username or by being in a security group, unit or team. The user must also have access to the record, e.g. as a supplementary case manager.</p> <p>A user with limited access can access any record they create. The user will lose access to a record if it is added to a case with an access restriction. If the user creates a case, they are automatically added to its access restriction.</p>
"Get email"	<p>Tick the checkbox to automatically import emails from Outlook to F2 for this user. This is only relevant if F2 is set up with manual email import. With this setup a user must manually move emails from Outlook to the "Move to F2" folder if the checkbox is unticked.</p> <p style="text-align: center;"><b>NOTE</b> This field has no effect if F2 is set up with full email import. Full email import means that F2 transfers all emails from the user's Outlook inbox to F2 and creates a record for each.</p>
"Receive email externally"	<p>If this box is ticked, the user will only receive emails in Outlook. This also applies to emails sent internally in F2.</p> <p>Any other communication channels are not affected by a tick in the "Receive email externally" box. For example, chats, approvals and records that are either sent or for which the responsibility is allocated internally will still be found in F2 only.</p>

**NOTE** "Get email" and "Receive email externally" cannot both be ticked. "Receive email externally" lets the user receive email in another email client. These emails must be manually moved 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 in all the relevant fields on the "Information" tab in the "Create user" dialogue and click on **OK**. F2 will then automatically shift to the "Roles" tab. Here, assign a job role to the user in either the top unit or in a subunit.

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

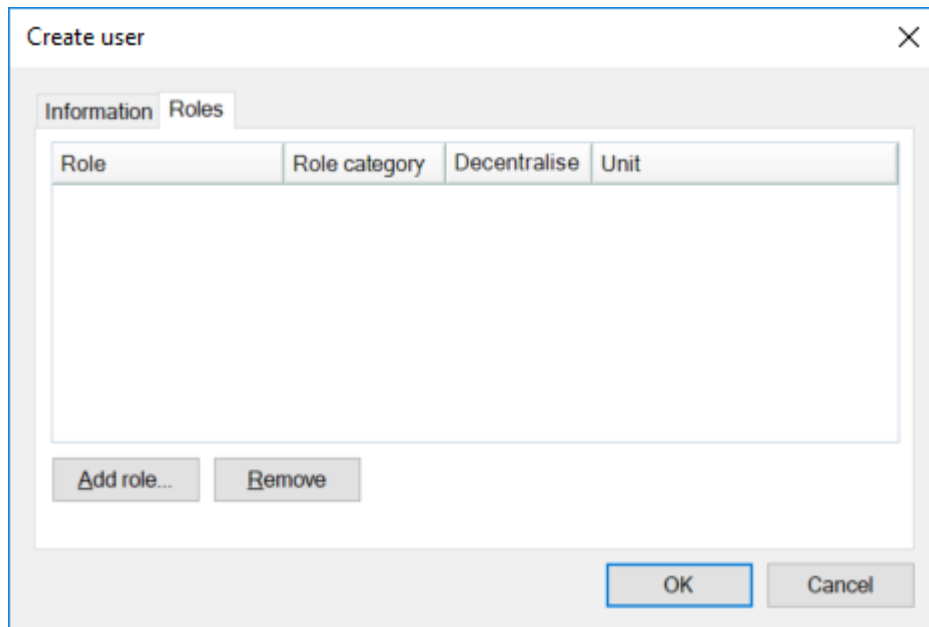


Figure 17. The “Roles” tab in the “Create user” dialogue

**NOTE** An administrator can check which roles are in the "job" category in [the "Role types and privileges" dialogue](#), which is accessed from the ribbon of the "Administrator" tab.

The “Add role to [user]” dialogue opens. Assign the user to an authority or unit. Then select a role type in the “Role type” drop-down menu.

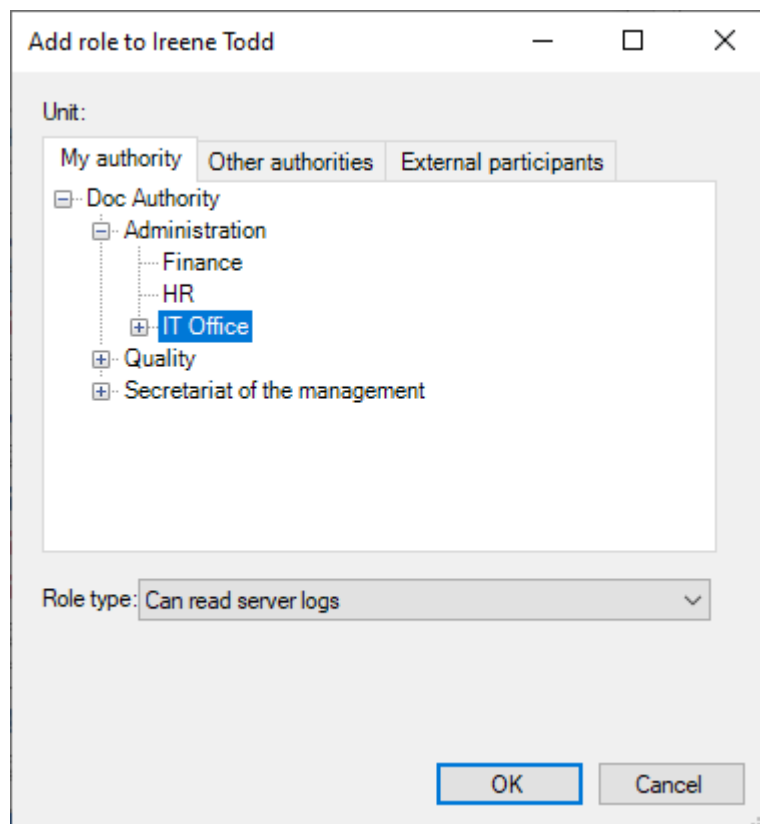


Figure 18. Add a role to a new user

Click on **OK** to apply the changes and close the “Add role to [user]” dialogue.

**NOTE**

It is important to select a unit for the user’s role, since the role and its location determine which rights the user has in the given 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, they can be assigned several roles. Roles have associated privileges that let the user perform different tasks in F2. Read more in the [Roles in F2](#) section.

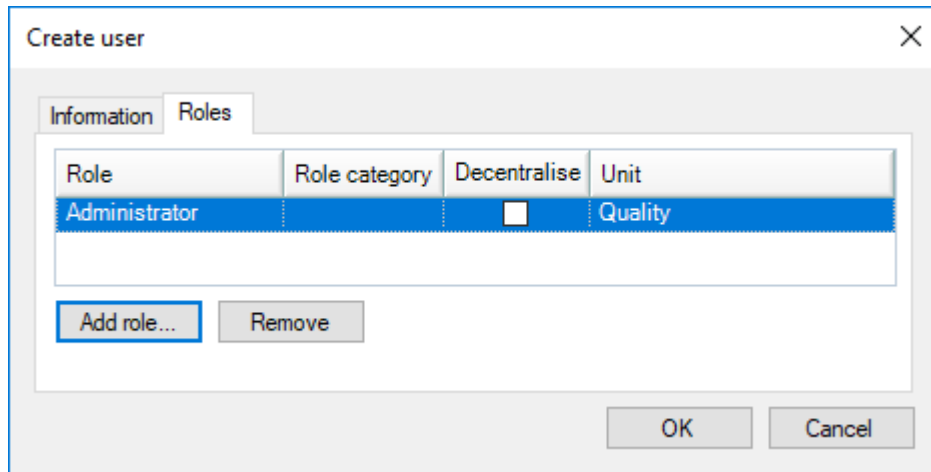


Figure 19. Assign a role to a new user

**NOTE**

New users are always created with the “Addressbook owner” role. Read more about roles in the [Roles in F2](#) section.

## Deactivate user

It is not possible to delete a user in F2. A user can instead be deactivated. In the main window, click on the “Administrator” tab and then the **Units and users** menu item to deactivate a user.

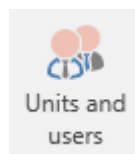


Figure 20. The “Units and users” menu item

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**.

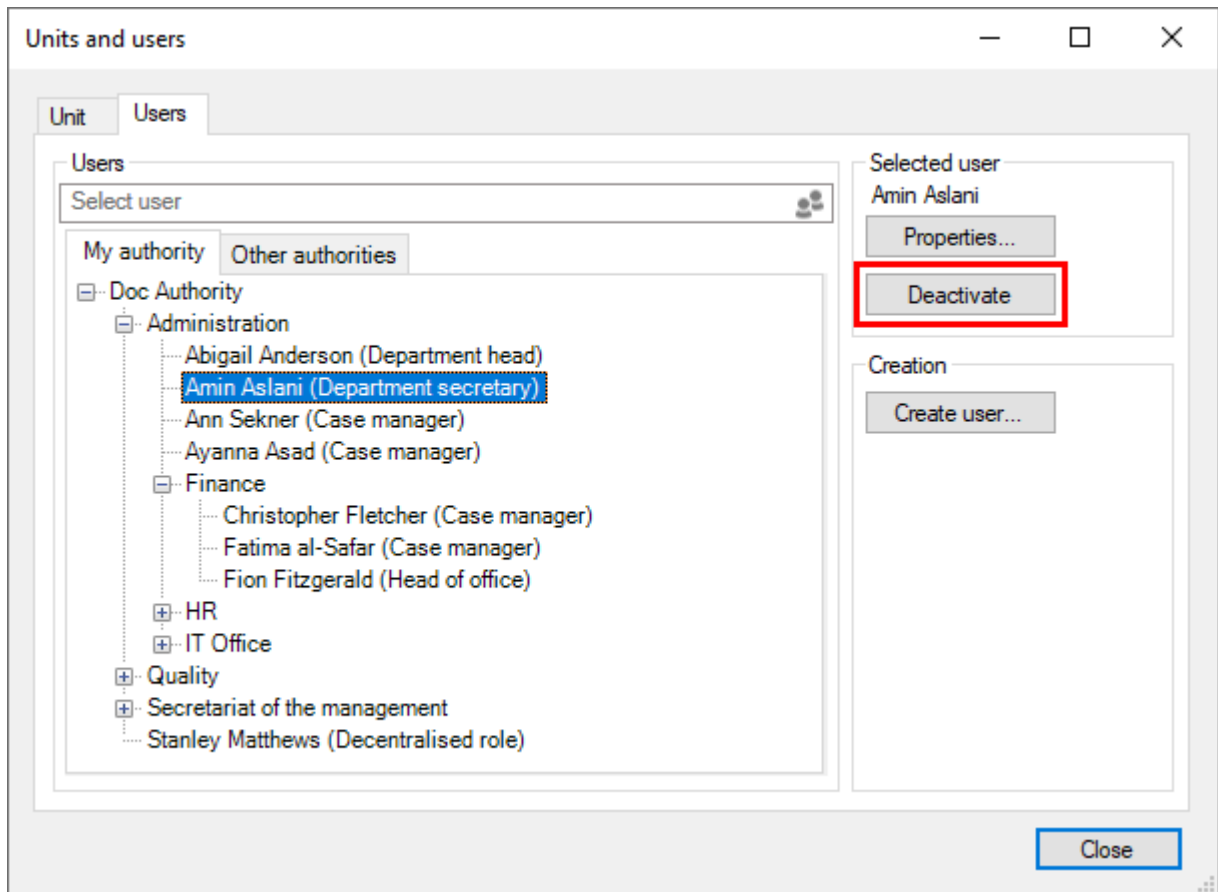


Figure 21. Deactivate a user

F2 asks for confirmation before the user is deactivated. After deactivation the username is shown in italics.

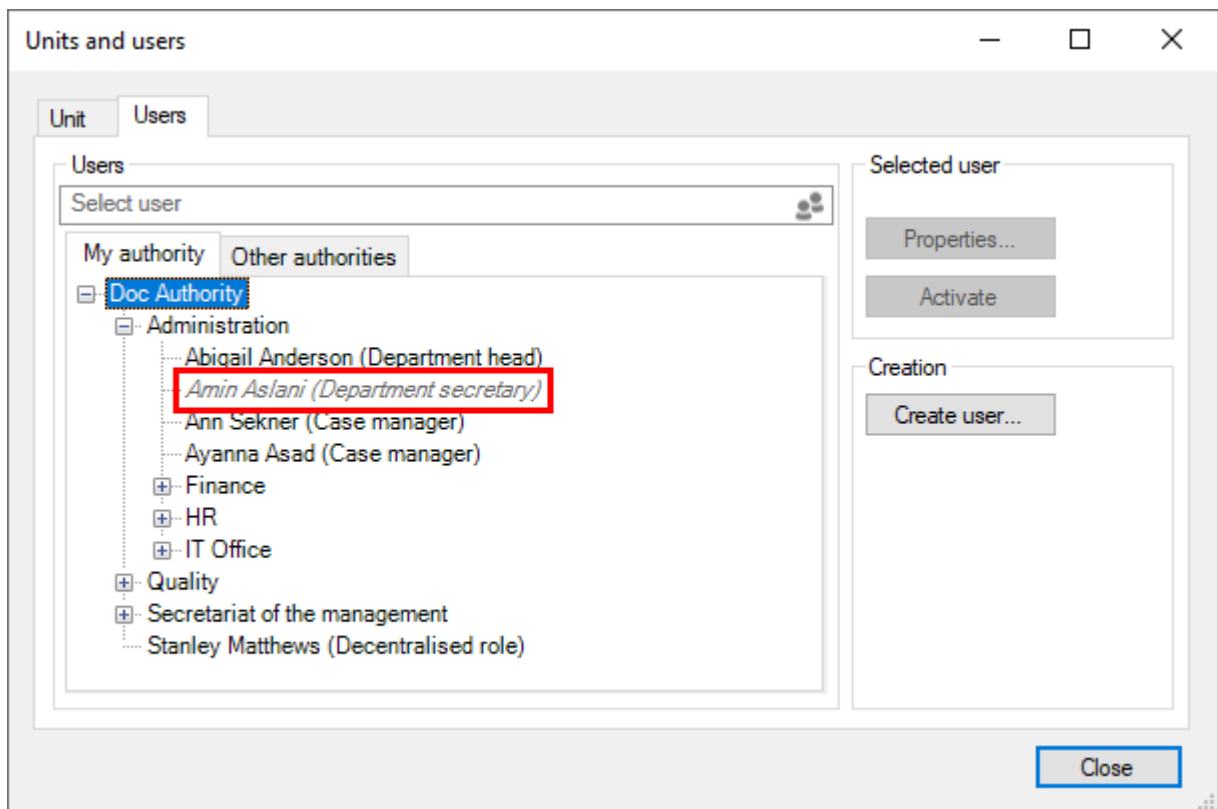


Figure 22. A deactivated user

**NOTE** A user must be deactivated in both F2 and Active Directory to be completely deactivated. If the user is only deactivated in F2, it will be reactivated via AD import.

**NOTE** To immediately block a user's access to F2, it may be necessary to both deactivate them and log them out. The latter is done using the **Log out user** function.

## Log user out of all sessions

You can log a user out of all sessions across all devices if you have the "User administrator" privilege. This function can be relevant in connection with security, e.g. if there is a suspicion that a user password has been compromised.

Go to the **Administrator** tab, and click the **Log out user** menu item.

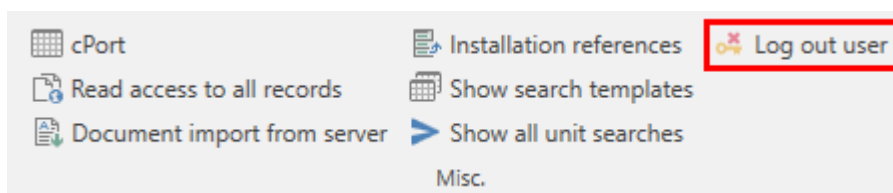


Figure 23. The "Log out user" menu item in the "Misc." menu group

Select the user you wish to log out, and click **Log out user**.

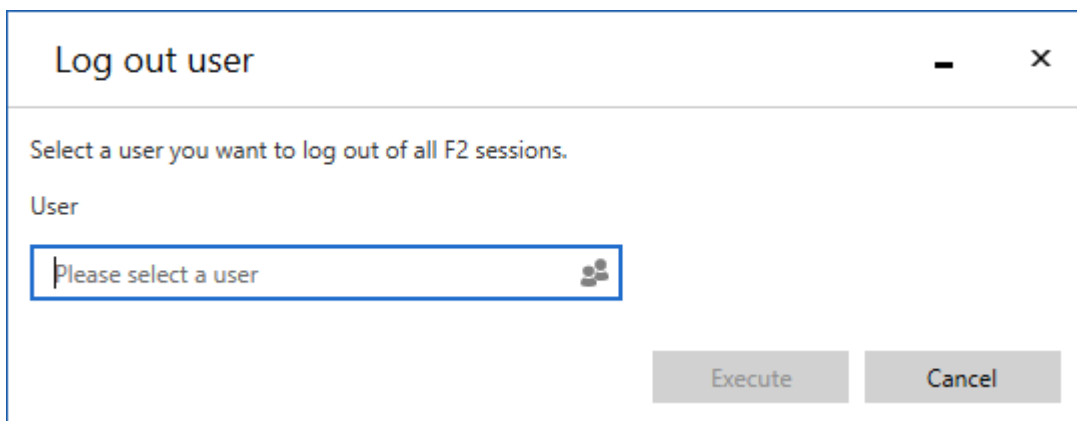


Figure 24. The "Log out user" dialogue

## Activate user

A deactivated user can be reactivated. Click the **Units and users** menu item on the "Administrator" tab in the main window.

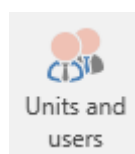


Figure 25. The "Units and users" menu item

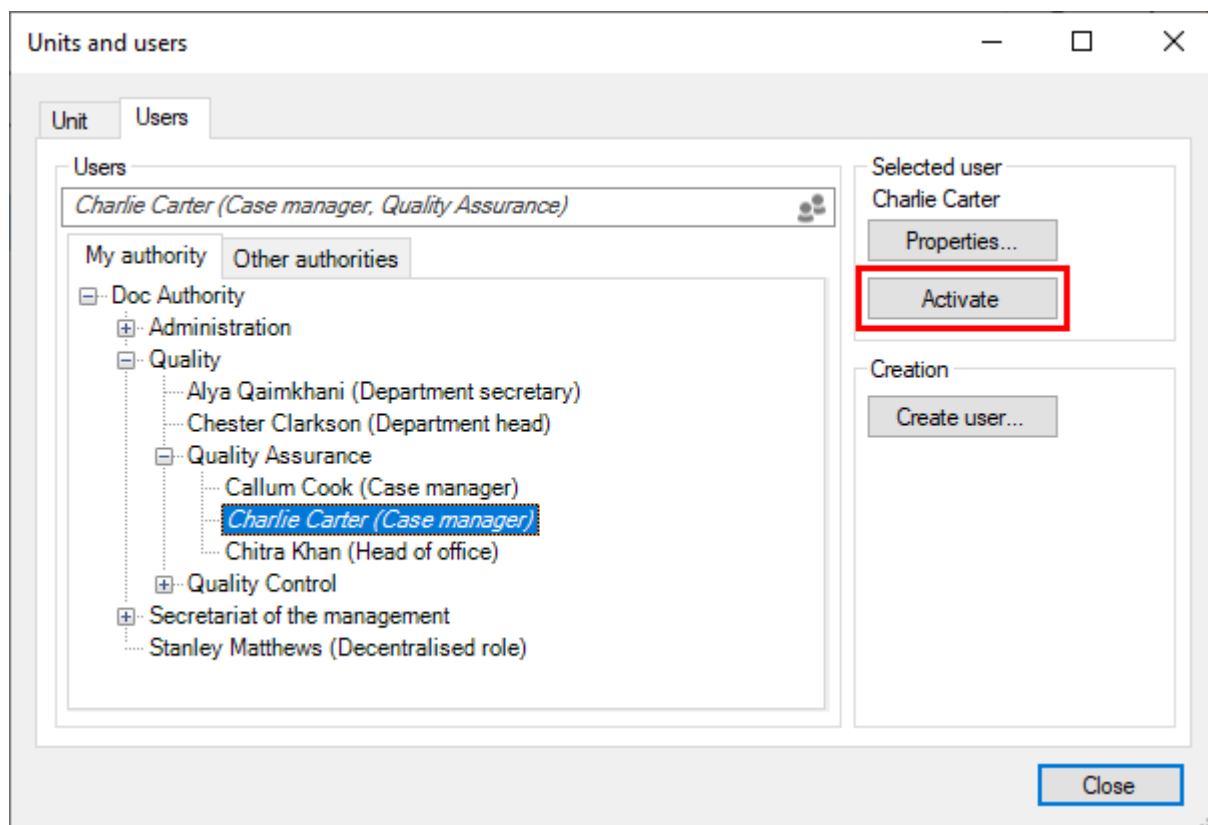


Figure 26. Reactivate a user

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 example Ann Sekner. Either the user's full name or an abbreviated version, e.g. the initials used for login and/or email, must be entered here.

Properties for the user Charlie Carter

Information Roles

Name

Name: Charlie Carter

Username: Not employed

Initials: CCA

Email address: cca@doc.gov.uk

Title:

Limited access

Participant No: 45

SSN:

Email account

Account:

Mail server:

Get email  Receive email externally

Address

Address 1:

Address 2:

Post code: City:

Country Code:

Telephone

Phone: Local No:

Mobile: Fax:

Private phone:

OK Cancel

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** F2 considers the user activated when the “Username” field contains the participant’s username.

**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 their 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 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".

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

**NOTE** It is also possible to go on behalf of a [deactivated user](#) and perform actions as if the user were active.

## Setting up "On behalf of"

On the "Administrator" tab, click on **On behalf of** to open the "On behalf of" dialogue.



*Figure 28. The "On behalf of" menu item*

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.



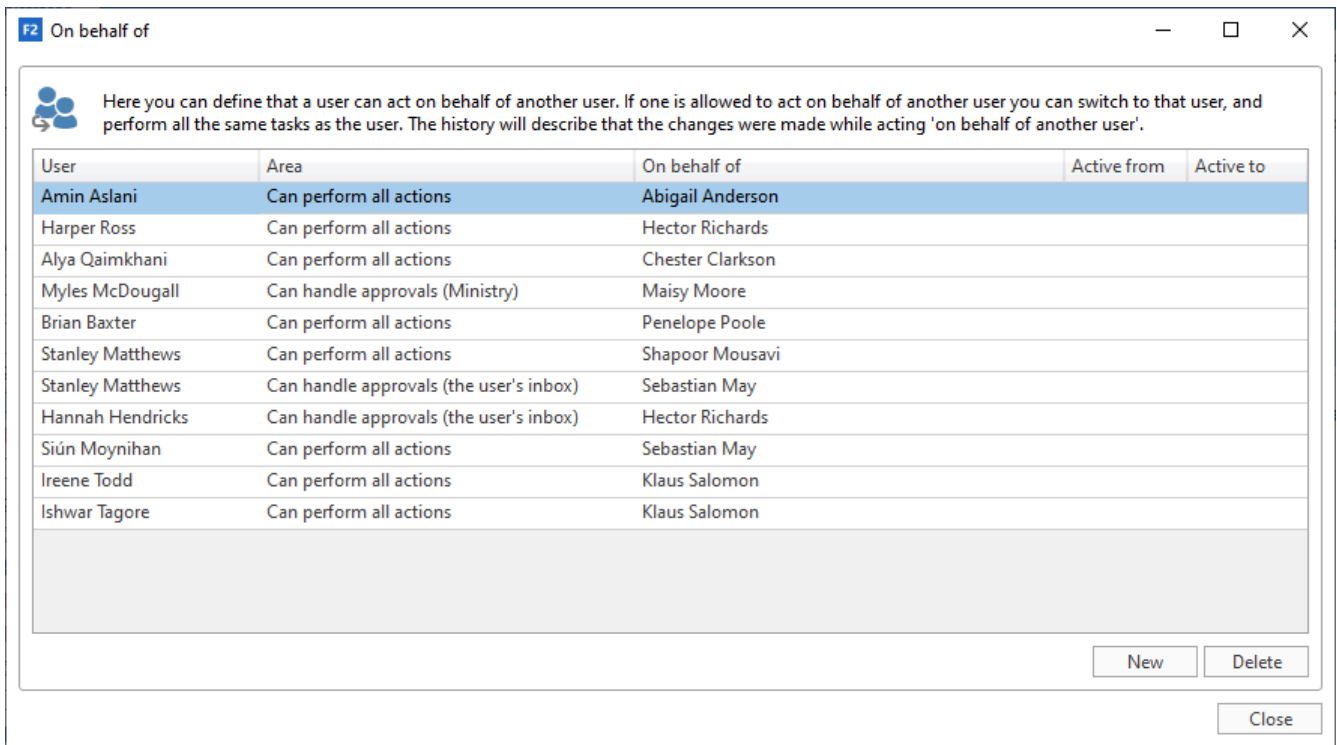


Figure 29. The “On behalf of” dialogue

Click on **New** to assign a new “on behalf of” relation. A dialogue opens in which you can assign a user “on behalf of” rights to another user’s F2.

Choose which type of “on behalf of” rights to assign to the user:

- “Can perform all actions”. These are the full “on behalf of” rights.
- “Can process approvals”. These are partial “on behalf of” rights.

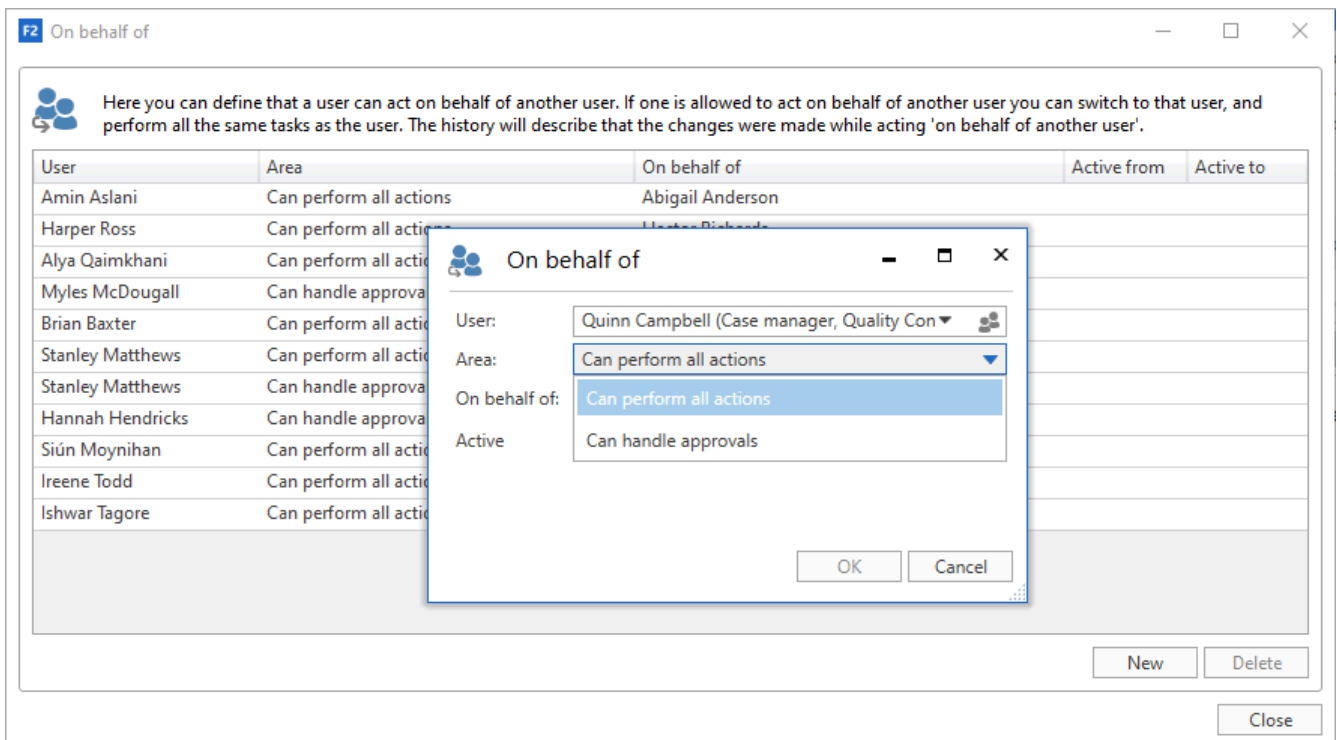


Figure 30. Assigning “on behalf of” rights for all areas

If a user is given rights to process approvals on behalf of e.g. their manager, it is possible to specify in which inbox(es) approval notifications are received.

The notification can be sent to the user's personal inbox, all the user's inboxes, or a specific unit's inbox.

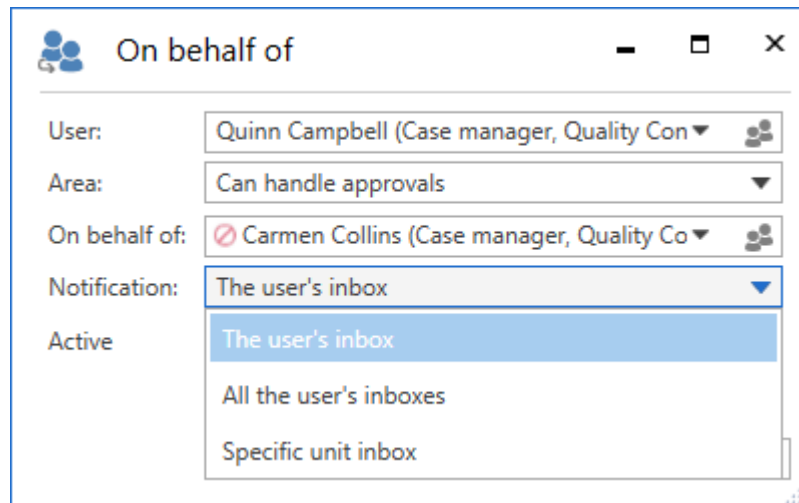


Figure 31. Select the location for approval notifications

When selecting a specific unit inbox, the "Unit" field appears. Here, the relevant unit inbox can be selected.

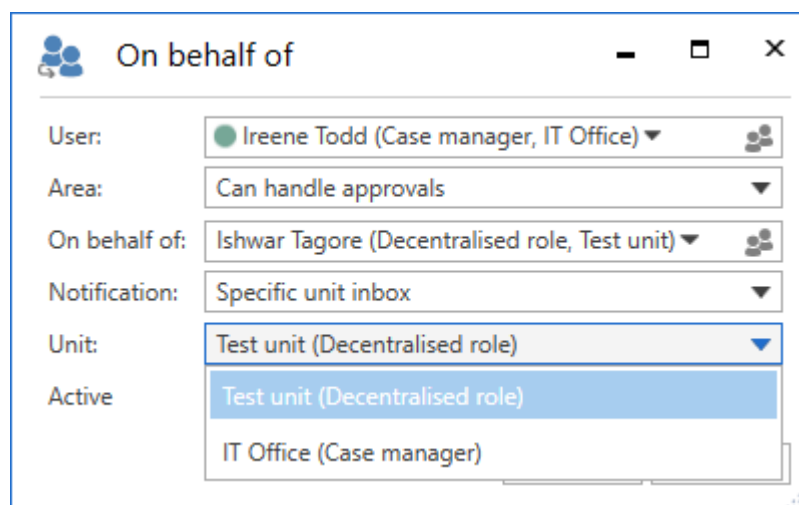


Figure 32. Select a specific inbox

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.

**On behalf of**

User: Ireene Todd (Case manager, IT Office)

Area: Can handle approvals

On behalf of: Ishwar Tagore (Decentralised role, Test unit)

Notification: Specific unit inbox

Unit: Test unit (Decentralised role)

Active: 19/02/2021 - 26/02/2021

OK Cancel

Figure 33. Assign “On behalf of” rights for processing approvals

Click on **OK** to complete.

# 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 F2 Shared Mailboxes add-on module ([documentation available in Danish](#)), it is possible to create and set up shared mailboxes/email addresses for each unit.

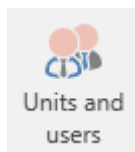
This section describes the administrator's options for setting up emails during installation and during the ongoing work in F2.

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

## Setting 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.



*Figure 34. The "Units and users" menu item*

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

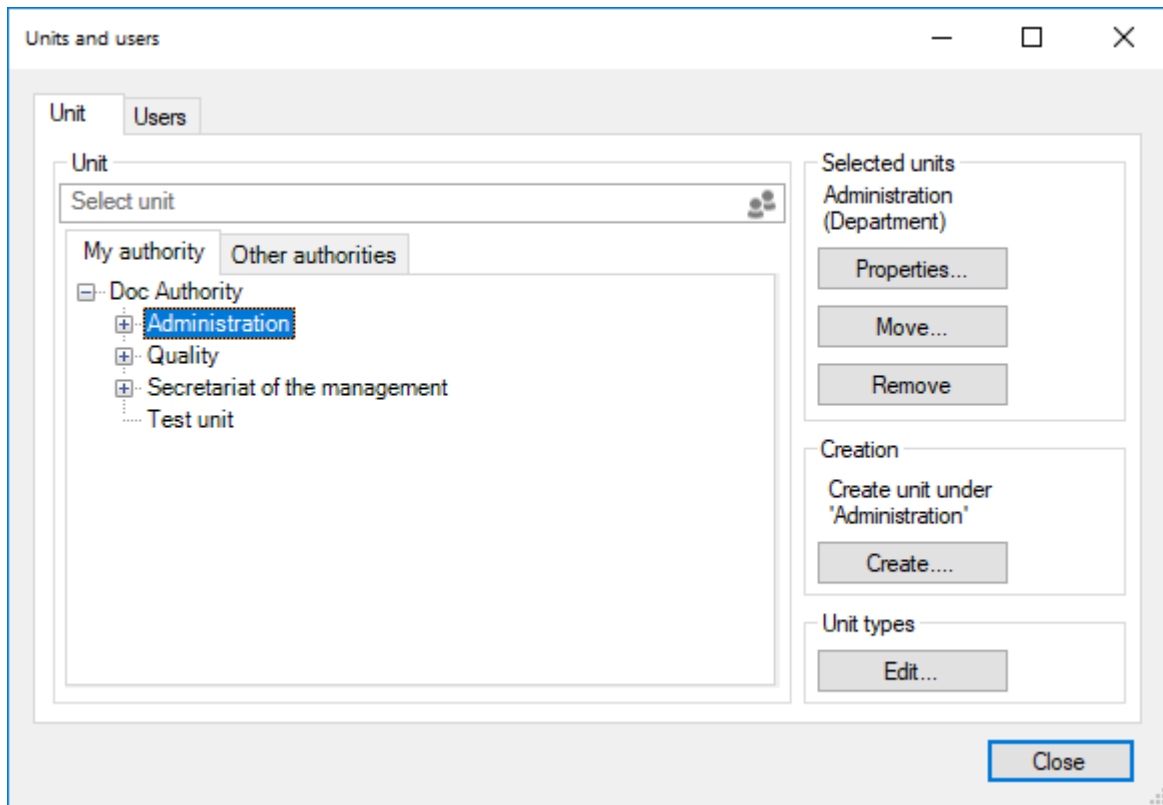


Figure 35. The “Units and users” dialogue

The “Properties for the unit [name of unit or authority]” dialogue opens as shown below.

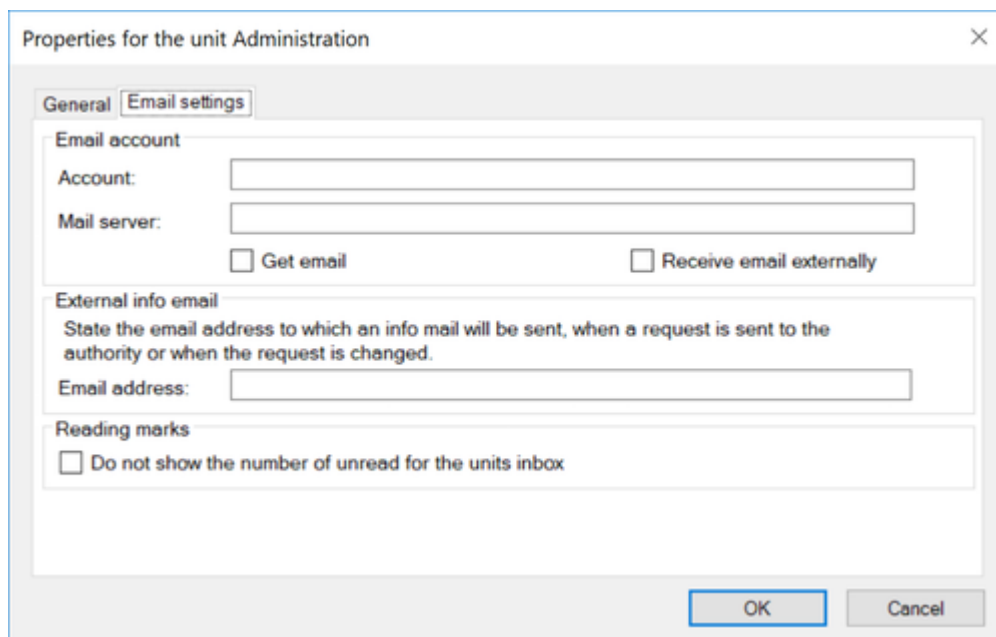


Figure 36. Setting up a unit inbox

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"	<p>Tick this box and all incoming external emails for the unit will be received in an external email system such as Outlook. This includes emails sent to the unit inbox internally in F2.</p> <p>None of the other communication channels are affected by this choice, which means that e.g. chats, approvals and records sent internally exist only in F2.</p>
"External info mail"	<p>Insert a participant from the unit's external email here, and they 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.</p> <p>This allows a third party recipient to receive and respond to requests, e.g. using Outlook. The recipient receives an email with the request as a PDF whenever a request is sent or edited. This external notification email also has a data file attached. The data file is how F2 recognises the reply as a group request reply when it is sent.</p> <p>External notification emails are mainly used in connection with group requests (add-on module). For more information, see <a href="#">Group Request</a>.</p> <p><b>NOTE</b> The data file must be attached to the response, otherwise F2 will be unable to recognise it as a group request reply.</p>
"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” on F2 so everyone in the unit can view them.

## Link email replies to emails sent from F2

When an email is sent from F2, an incoming reply is automatically linked to the original email. The reply is also automatically linked to the case of the original email, just as any following emails will be linked to the case. F2 identifies emails using a unique hidden ID.

By default, email replies are automatically linked to emails sent from F2. An administrator with the “Unit administrator” privilege can change this setting. It is also possible to change the default case association for email replies. This is done on the “Email settings” tab in the “Properties for the unit” dialogue. Open the dialogue by clicking the **Units and users** menu item on the “Administrator tab”, select an authority and click **Properties**.

Here, the relevant options are found in the “Identification of email replies” section:

Field	Description
“Mark imported email as reply to the original record”	Tick this box to automatically link an email reply to the email sent from F2.
“Assign imported email to case”	Tick this box to link an email reply to the same case as the email sent from F2.

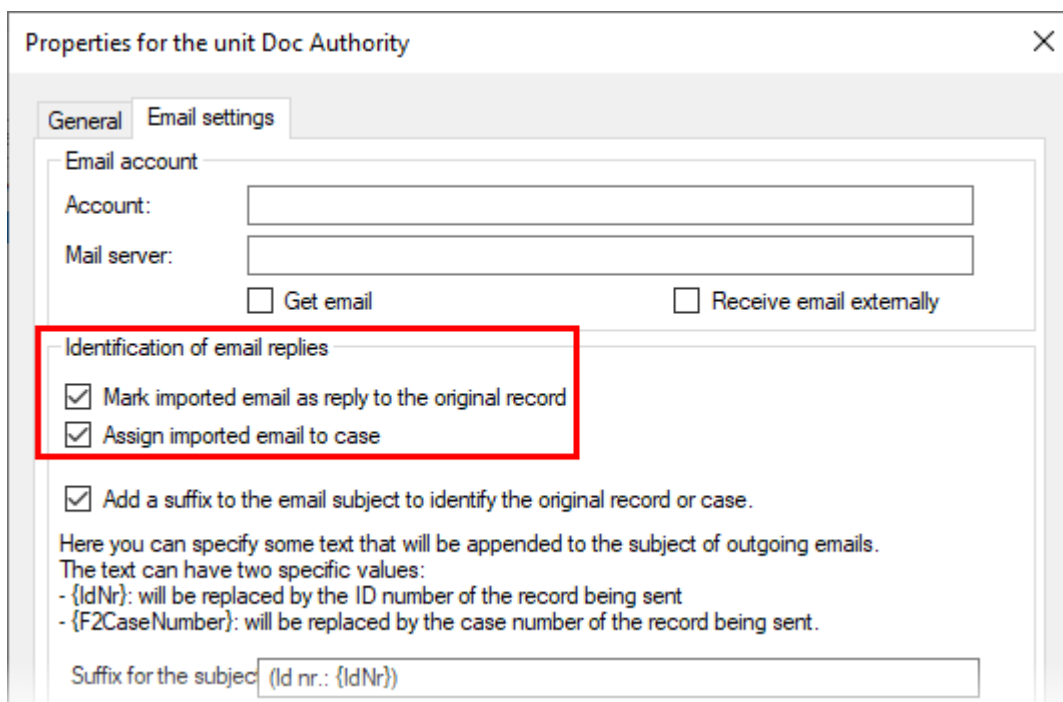


Figure 37. Identification of email replies

**NOTE** Linking emails sent to or from F2 systems older than 6.2 is not possible.

## Add a suffix to the subject field of external emails

F2 can be set up to link incoming emails that are replies to emails sent from F2. This is done by adding a unique ID to the subject field of an outgoing email. An administrator with the "Unit administrator" privilege can set up the subject field of all outgoing emails to include record ID, case number, or both.

To add a suffix to the subject field of the authority's outgoing emails, go to the "Email settings" tab in the "Properties for the unit" dialogue. Click on the **Units and users** menu item on the "Administrator" tab to open the dialogue. Choose an authority from the list and click on **Properties**.

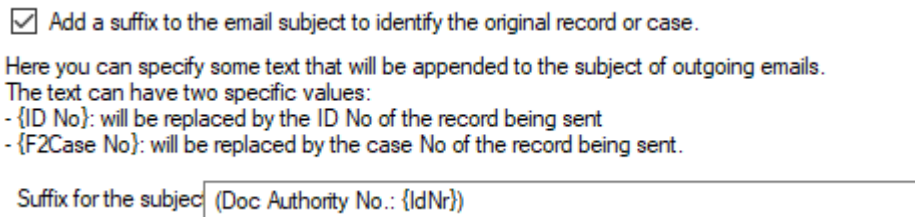


Figure 38. Configure the subject field for emails

Tick "Add a suffix to the email subject to identify the original record or case" to use this method to identify emails.

The "Suffix for the subject" field is used to specify the text and values that make up the subject added to outgoing emails.

The following values can be added to the field:

- Insert "{IdNr}" to add the record ID of the outgoing email to the subject field.
- Insert "{F2CaseNumber}" to add the case number of the outgoing email to the subject field.
- Insert "{IdNr}{F2CaseNumber}" to add both the record ID and the case number of the outgoing email to 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 also be inserted in the subject field. This text is added to all outgoing emails together with the record ID or case number. The static text may be an abbreviation of the authority's name.

For example: "FM - ID No. {IdNr}, case No. {F2CaseNumber}"

The text outside of 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.

F2 can be configured to remove the administrator's option of adding a suffix to outgoing emails. Configurations are performed in cooperation with cBrain.



## **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 that are replies 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](#) let a user perform different tasks in F2. They are given to a user through the assignment of roles. For example, if a user must be able to delete notes, the user must be assigned a role with the “Can delete notes” privilege.

**NOTE** In F2’s user interface, roles are sometimes referred to as “role types”.

F2 comes with a number of roles, including four administrator roles. An administrator with the “User administrator” or “Administrator” role can also create new roles.

The default roles 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. Read more about [assigning privileges to roles](#).

The administrator roles and their privileges are listed below.

The “Administrator” role has the following privileges:

- Access to cPort (add-on module, [documentation available in Danish](#))
- 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
- Can import parties
- Meeting forum administrator (add-on module, [documentation available in Danish](#))
- Editor of participants
- Privilege administrator
- On behalf of administrator
- Result list administrator
- Security group administrator
- Template administrator
- Progress codes administrator
- System messages administrator
- Search administrator
- Team administrator
- Team creator
- Value list administrator.

The above privileges cannot be removed from the “Administrator” role. However, additional privileges may be added.

The “User administrator” role comes with the following privileges. These privileges may be removed, or additional privileges may be added, by a user with the “Privilege administrator” privilege:

- User administrator
- Extra email administrator
- Keyword creator
- Unit administrator
- Unit type administrator
- Flag administrator
- Settings administrator
- Can import documents from the server
- Can import parties
- Meeting forum administrator (add-on module, [documentation available in Danish](#))
- Editor of participants

- Privilege administrator
- On behalf of administrator
- Security group administrator
- System message administrator
- Team administrator
- Team creator.

The “Business administrator” role has the following privileges per default. These privileges may be removed, or additional privileges may be added, by a user with the “Privilege administrator” privilege:

- Access to cPort
- Distribution list editor
- Keyword creator
- Unit type administrator
- Flag administrator
- Can import documents from the server
- Meeting forum administrator (add-on module, [documentation available in Danish](#))
- Template administrator
- Progress codes administrator
- Value list administrator.

The “Technical administrator” role has the following privileges per default. These privileges may be removed, or additional privileges may be added, by a user with the “Privilege administrator” privilege:

- Result list administrator
- Search administrator.

The different privileges are described in [Privilege overview](#) section.

## Other default roles in F2

Besides the administrator roles, F2 comes with a number of other roles. Most of these are either [job roles](#) or related to add-on modules. The table below describes these roles.

Role	Description
Access to data cleanup	<p>This role is part of the <a href="#">F2 Data Cleanup add-on module</a>.</p> <p>Users with this role have read access to all cases in the F2 installation and access to delete all cases regardless of their regular access to cases and records. This includes cases and records which otherwise could not be deleted because of e.g. registration status.</p>
Address book owner	<p>This role is automatically assigned to new users created in F2. Allows the user to create and edit private participants in the “Private” node in the participant register. Cannot be assigned manually and may not be removed from users.</p>
Can delete everything on cases	<p>This role lets the user delete a case regardless of the status of its records. When a case is deleted, a report containing information on the case and its records is sent to the user’s inbox. Read more about <a href="#">deleting cases</a>.</p>
Can use F2 GDPR	<p>This role is part of the F2 Data Protection add-on module.</p> <p>Users with this role can create, delete, and edit GDPR searches and create data protection searches. Using F2 Data Protection, users can access all material in the F2 installation containing personal data. Contact cBrain for further information.</p>
Case manager	<p>This job role lets the user log into an associated unit. The organisation can assign privileges to the role that are relevant to a case manager.</p>
Gated approver	<p>This role is part of the <a href="#">F2 Gateway Approvals add-on module</a>.</p> <p>The role is assigned to users with a gatekeeper (secretariat) who processes approvals on their behalf. The gatekeeper must be assigned “<a href="#">On behalf of</a>” rights for the gated approver.</p>
Head of department	<p>This job role lets the user log into an associated unit. The organisation can assign privileges to the role that are relevant to a head of department.</p>

Role	Description
	the unit's records with the "Unit" access level.
Read and write access to another unit	This role lets the user search for, read, and edit records in the unit with which the role is associated. This means that a user in another unit who is assigned this role has read and write access to all the unit's records with the "Unit" access level.
Team administrator	This role is assigned automatically to users who are specified as <a href="#">team</a> administrators. The role can only be assigned through this dialogue.
Team member	This role is assigned automatically to users who are specified as <a href="#">team</a> members. The role can only be assigned through this dialogue.

## 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 to perform different tasks within.

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

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

**NOTE** F2 can be configured to authenticate F2 users using other LDAP servers than Active Directory, e.g. Oracle Unified Directory. This configuration does not support single sign-on. This means that users must enter their user name and password every time they log into F2. Configurations are performed in cooperation with cBrain.

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

A user with the "User administrator" privilege can assign roles to users in two ways:

- Through the "Assign role to users" dialogue in which it is possible to [assign a role to several users at the same time](#).
- Through the "Properties for the user [name]" dialogue in which it is also possible to remove the user's roles. Read more about this in [Assign role to a single user](#).

Users with the "Decentral unit and user administrator" privilege can use the same dialogue to assign decentral roles.

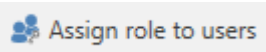


Figure 39. The "Assign role to users" menu item

Add one or more users to the "Users" field. Then select a role to assign to the selected users, and specify the unit in which to assign to role. Click **Assign** to complete the operation.

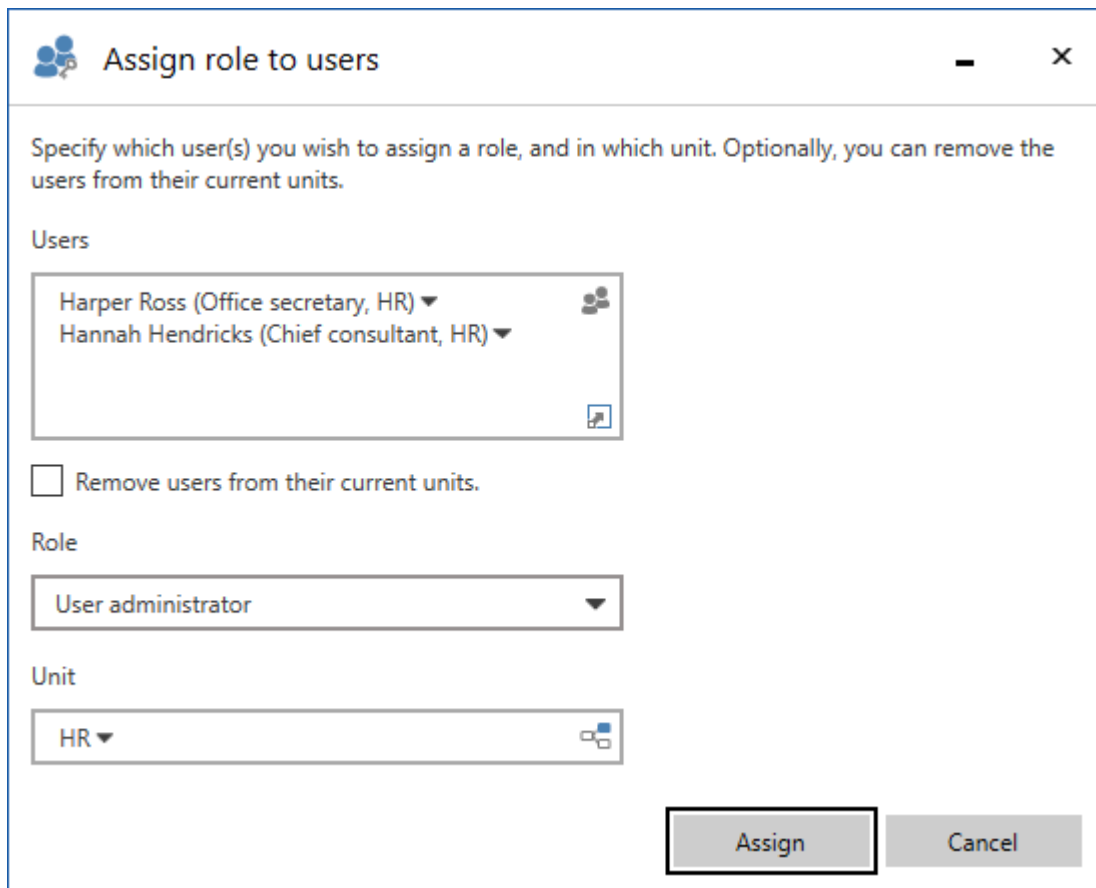


Figure 40. The "Assign role to users" dialogue

In this dialogue, users can also be moved from one unit to another. When the relevant users are added to the "Users" field, tick "Remove users from their current units". Then select a role to assign to the users in the new unit. Click **Assign** to complete the move.

## Assign role to a single user

Roles can be assigned to one user at a time 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 steps below describe how Abigail Anderson from Administration 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.

Select the user who needs a new role, in this case Abigail Anderson.

Click on **Properties**.

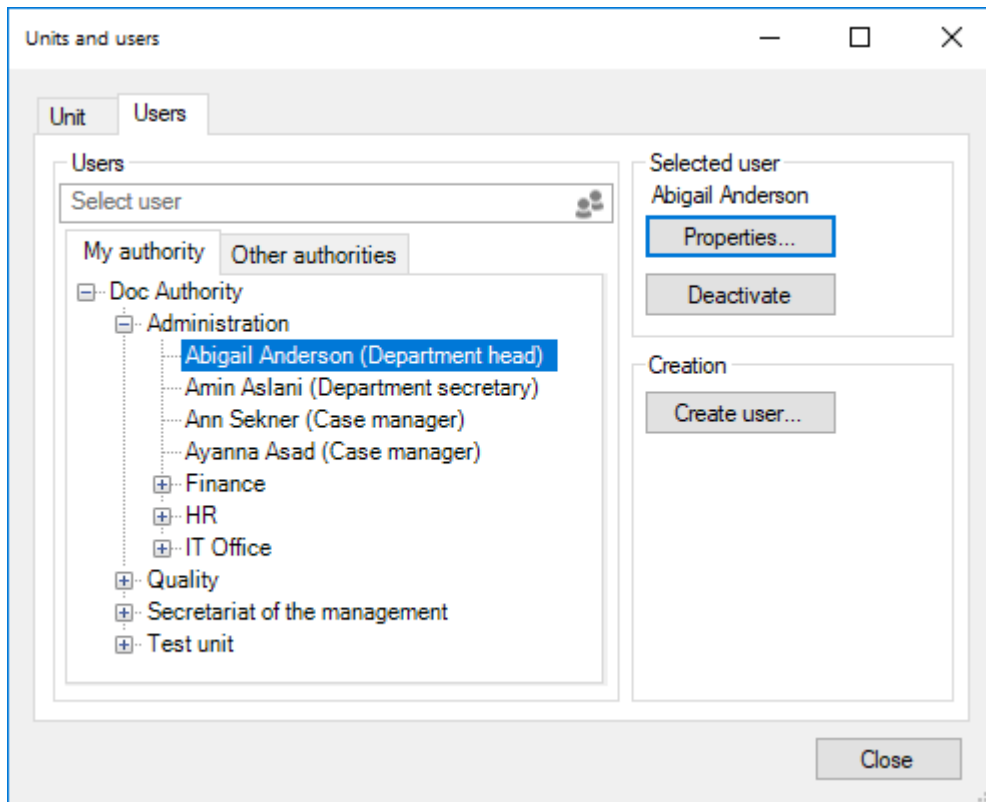


Figure 41. Select user

In the “Properties for the user Abigail Anderson” dialogue, click on the **Roles** tab and then on **Add role**.

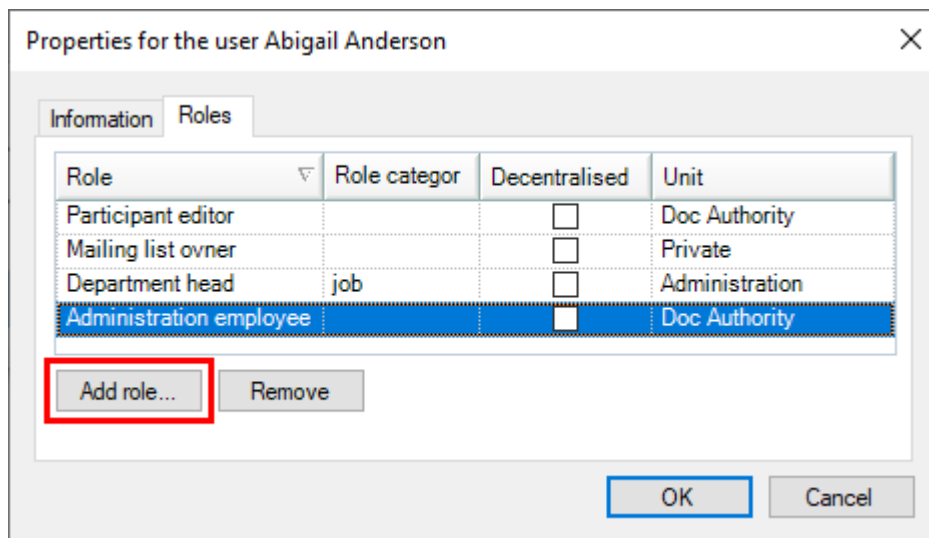


Figure 42. Assign a role to the user

To add a role first select a “Role type”, in this example “Business administrator”. Then select the unit to which the role must be applied. In this example, it is the “Administration” unit.

Click on **OK** to assign the “Business administrator” role for the “Administration” unit to the user Abigail Anderson.



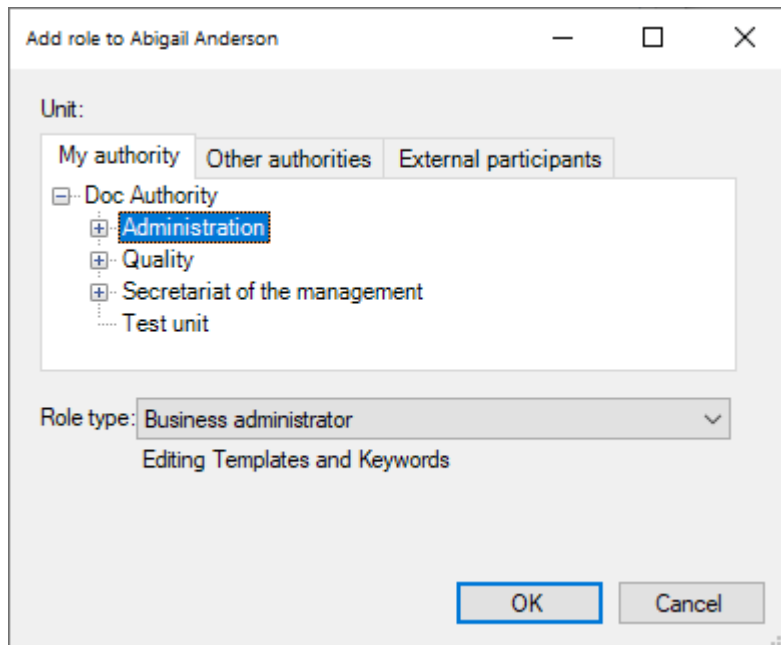


Figure 43. Assign a role type to a user

The role then appears in the overview of the user’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.

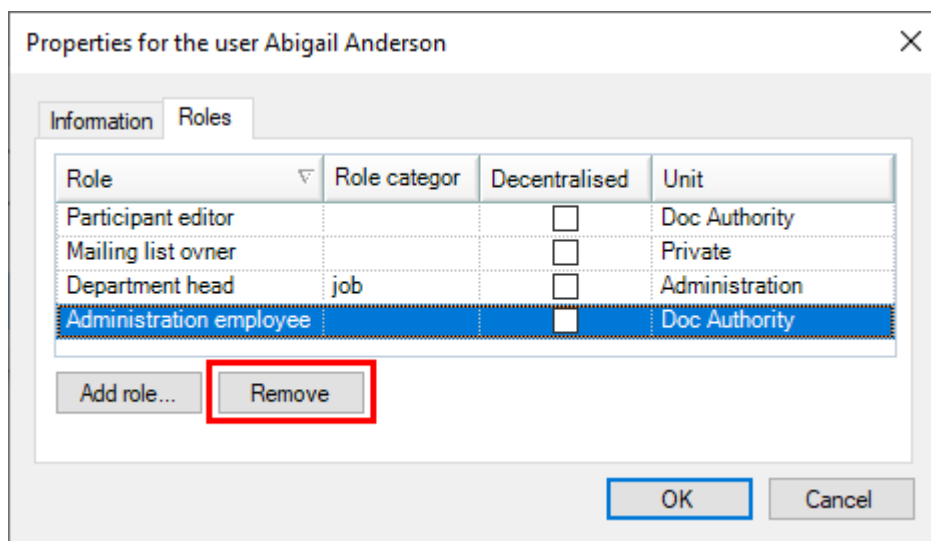


Figure 44. Remove a role from a user

**NOTE**

It is important to select the correct unit for the user’s role. The role and its location determine which privileges the user has in a given unit.

## Create and assign roles

An administrator can create roles as needed. To create new roles, the administrator must have either the “User administrator” or “Administrator” roles.

To view available roles, click on the **Role types and privileges** menu item on the “Administrator” tab.

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

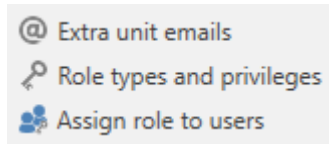


Figure 45. The “Role types and privileges” menu item

In this dialogue roles can also be created and edited by clicking the buttons **New role type** and **Edit role type**, respectively.

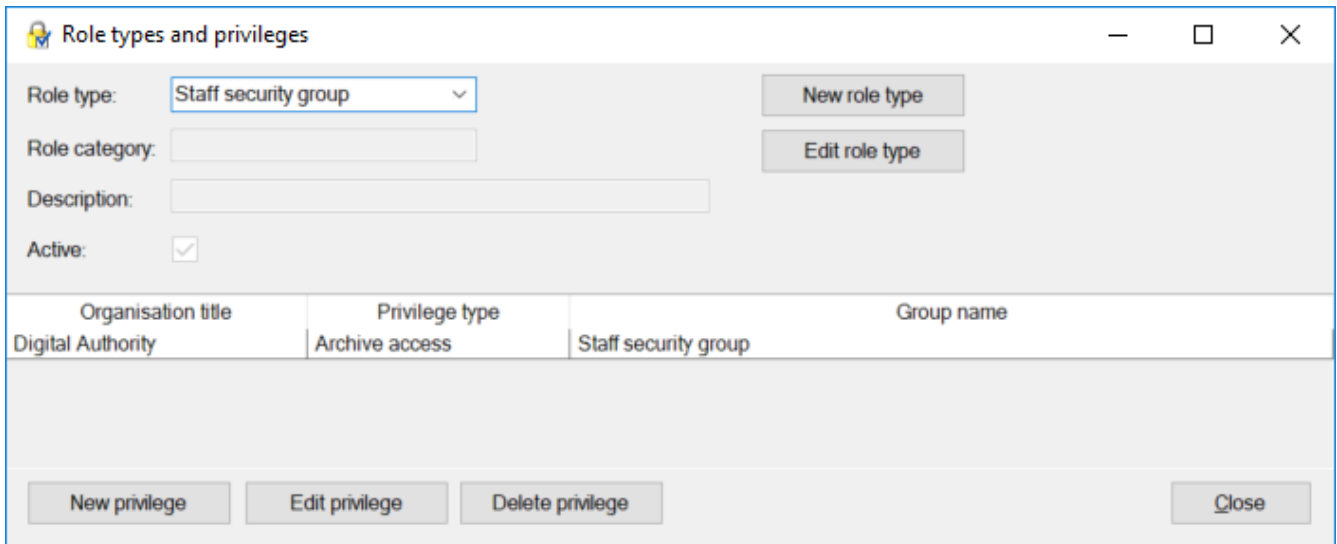
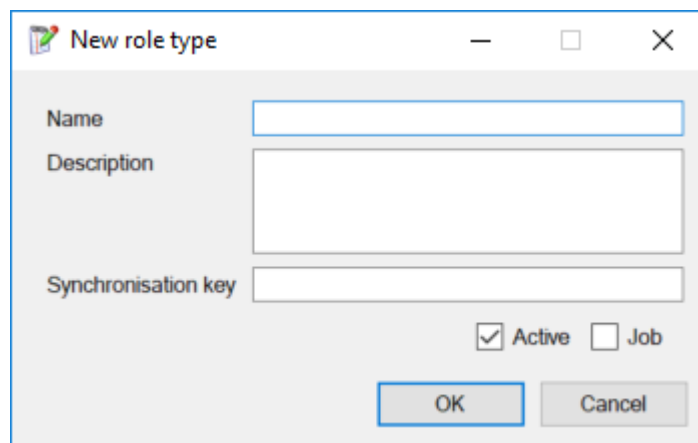


Figure 46. Role types and maintaining them

Click on **New role type** to open the “New role type” dialogue. Add the following information in the dialogue:

- The name of the role.
- A description of the role’s function e.g. “Access to edit templates and keywords”.
- The synchronisation key if using full AD integration.
- Tick the “Active” checkbox to activate the role so it can be assigned to users.
- Tick the "Job" checkbox if the user will use the role to log in to F2. A user must have at least one job role in order to log in. You cannot untick this box later.



*Figure 47. The “New role type” dialogue*

You can then [assign one or more privileges](#) to the role. This lets users with this role perform a number of actions.

**NOTE** A role cannot be deleted, only deactivated.

# Privileges

It is not possible to assign a privilege to a user directly. A privilege must be assigned to a role, which can then be assigned to a user. This means that all users that are assigned a given role type will have its privilege(s).

Assigning privileges to role types requires the “Privilege administrator” privilege.

Privileges, as well as role types, are managed in the “Role types and privileges” dialogue. Click on the **Role types and privileges** menu item on the “Administrator” tab to open the dialogue.

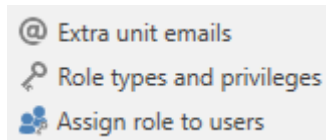


Figure 48. The “Role types and privileges” menu item

The organisation’s appointed privilege administrator can distribute privileges to role types and assign them 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 assigning roles.](#)

## Assign a privilege to a role

In the “Role types and privileges” dialogue, privileges can be assigned to a role. Select a role that needs a privilege assigned in the “Role type” field, e.g. “Access to HR” as shown in the figure below.

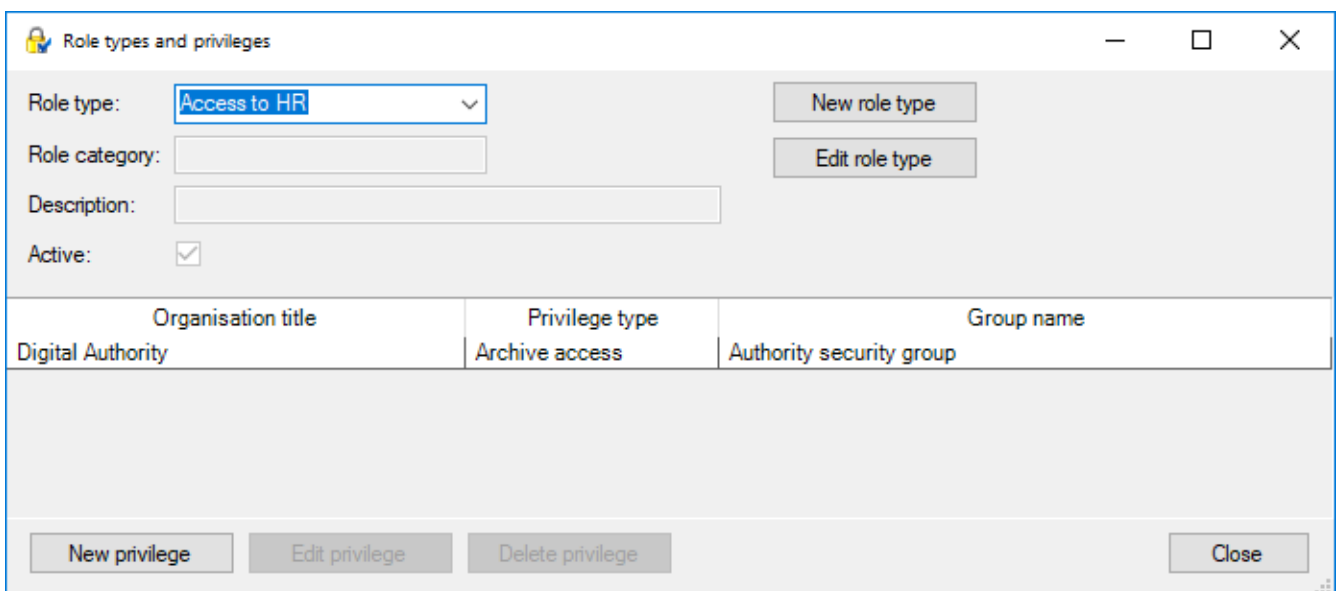


Figure 49. The “Role types and privileges” dialogue

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

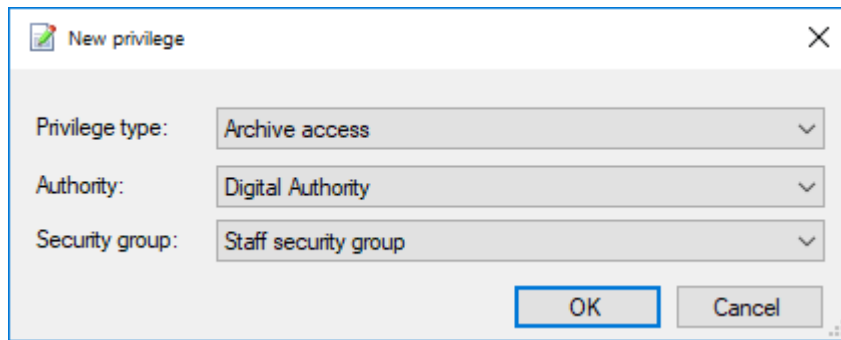


Figure 50. The “New privilege” dialogue

Select a new privilege to add to the role. Then select an authority to which the privilege applies. A security group can also be attached to the privilege.

Click on **OK** to finish.

All users with the “Access to HR” role now have archive access to the security group in the chosen authority.

## Edit or remove privileges from a role

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

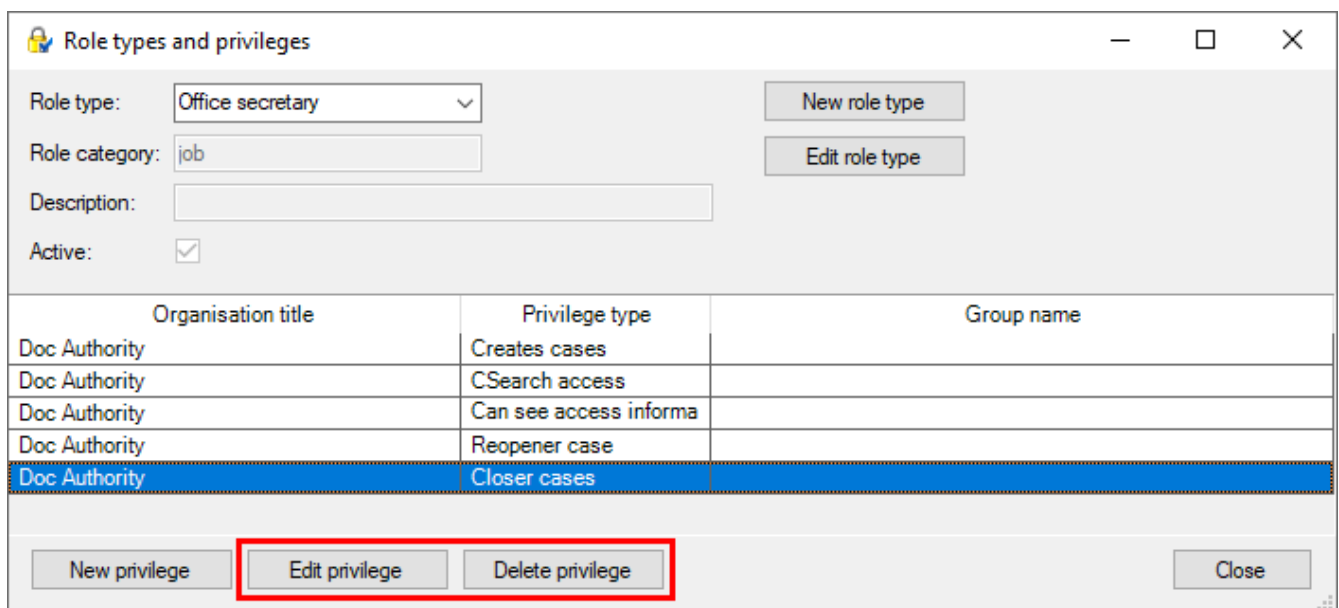


Figure 51. Edit or delete a privilege

Click **Edit privilege** to open the “Edit privilege” dialogue. See the figure below.

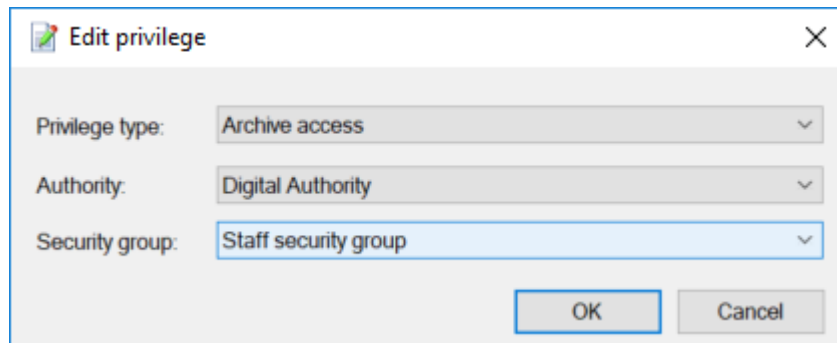


Figure 52. The “Edit privilege” dialogue

Select another privilege, another authority, or another security group.

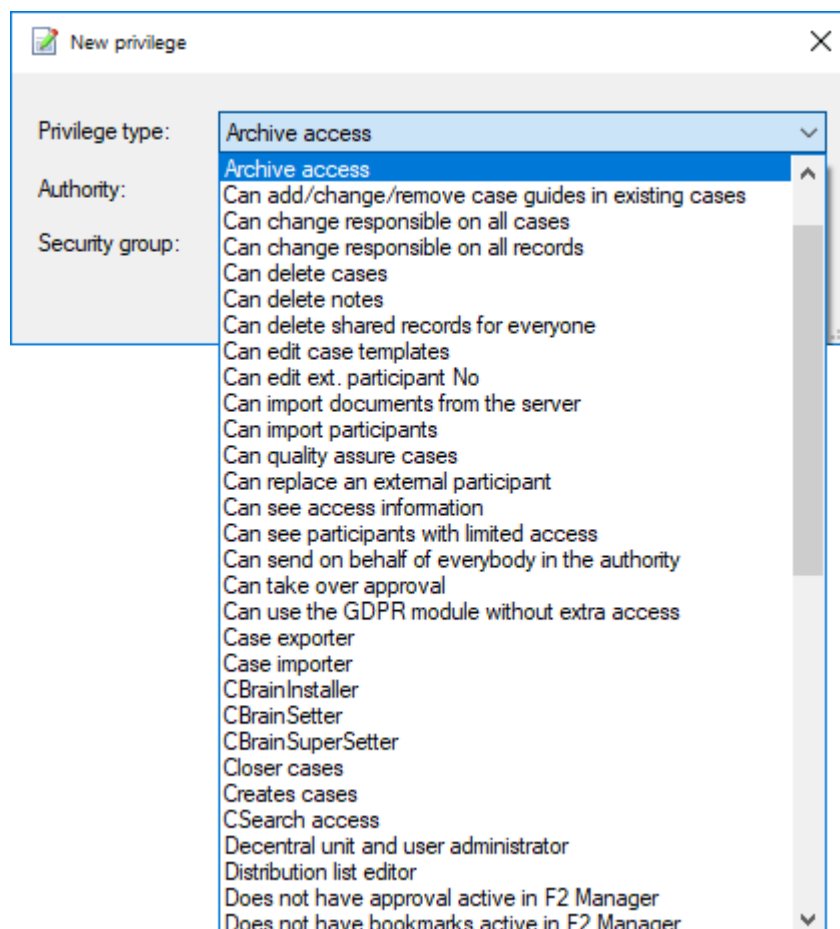
Click on **OK** to finish.

To remove an existing privilege from the current role type, click **Delete privilege**. The action cannot be undone and no warning appears.

## Privilege overview

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.

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.



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
Access to cPort	<p>Provides access to use cPort (<a href="#">documentation available in Danish</a>).</p> <p>Exports are made across access levels and security groups. They do not show content, only titles and records.</p>
<a href="#">Administrator read access to all records</a>	Can read all records in F2 despite their access level.
<a href="#">Archive access</a>	Assigns a role to a <a href="#">security group</a> . This lets an administrator add participants to security groups.
Can add/change/remove case guides in existing cases (add-on module)	Can edit case guides for existing cases.
Can change responsible on all cases	Can change the responsible user/unit on a case.
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 delete cases	Can delete cases under certain conditions. The conditions are listed in <a href="#">Cases</a> .
Can delete notes	Can delete record notes.
Can delete shared records for everyone	Can <a href="#">delete a record for everyone</a> , even if the record is shared.
Can edit case templates ( <a href="#">add-on module</a> )	Can edit case templates. Case templates can be applied by the organisation's users in the "New case" dialogue.
Can edit ext. participant no.	Can edit an external participant's synchronisation number.
Can import documents from the server (add-on module)	<p>Can import documents from the server, if this is configured.</p> <p>The configuration is done in cooperation with cBrain.</p>



Privilege	Description
Can import participants	Can import external participants.
Can quality assure cases (add-on module)	Can quality assure cases on the case tab.
Can see access information	Can see <a href="#">access information for records</a> , i.e. who can view the records, and how they were granted access, using the record context menu.
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.
Can take over approval ( <a href="#">add-on module</a> )	<p>Can take over an approval without write access to the approval record.</p> <p>This allows for urgent processing of an approval when the responsible user/unit or an approver is unavailable.</p> <p>Read more about <a href="#">taking over approvals</a>.</p>
Can use the GDPR module without extra access (add-on module)	<p>Can view existing GDPR searches, but not create, delete or edit them.</p> <p>The user can open GDPR searches, but can only preview cases, records, and documents which they otherwise would be able to see.</p>
CBrainInstaller	<p>Can <a href="#">edit configurations</a> of the F2 installation.</p> <p>cBrain recommends that all configurations are performed in cooperation with cBrain.</p>
CBrainSuperSetter	<p>Can <a href="#">edit configurations</a> of the F2 installation.</p> <p>cBrain recommends that all configurations are performed in cooperation with cBrain.</p>
CBrainSetter	<p>Can <a href="#">edit configurations</a> of the F2 installation.</p> <p>cBrain recommends that all performed are done in cooperation with cBrain.</p>
Closer cases	Can complete cases.

Privilege	Description
cSearch access (add-on module)	Can perform searches using the add-on module <a href="#">cSearch</a> .
Decentral unit and user administrator	Can create decentral units.  Can assign decentral roles to existing users for selected levels in the organisation.
<a href="#">Distribution list editor</a>	Can create and edit shared distribution lists in F2.
Does not have approvals active in F2 Manager ( <a href="#">add-on module</a> )	Cannot see approvals in F2 Manager.
Does not have bookmarks active in F2 Manager ( <a href="#">add-on module</a> )	Cannot see bookmarks in F2 Manager.
Does not have meeting planner active in F2 Manager ( <a href="#">add-on module</a> )	Cannot see the meeting planner in F2 Manager.
<a href="#">Editor of participants</a>	Can create, edit, and delete external participants as well as edit images for external participants.  <b>NOTE</b> The privilege must be attached to a node under external participants.
Extra email administrator	Can create extra emails for units.
F2Setter	Can <a href="#">edit configurations</a> of the F2 installation.  cBrain recommends that all configurations are performed in cooperation with cBrain.
Flag administrator	Can create, edit, and delete <a href="#">flags</a> .
<a href="#">Keyword administrator</a>	Can create, edit, and delete keywords as well as assign keywords to a unit.
Limited access to data cleanup ( <a href="#">add-on module</a> )	Allows the user to clean up and delete cases to which they already have write access using the F2 Data Cleanup add-on module. The user can also access cases to which they have read access in the module, but they cannot delete them.  Read more about <a href="#">Data Cleanup</a> .

Privilege	Description
Meeting forum administrator (add-on module)	Can create, edit, deactivate, activate, and delete meeting forums.
No case help for saving or sending records	<p>Will not see the case help when sending or saving a record.</p> <p>For more information, see the section <a href="#">No case help for saving or sending records</a>.</p>
On behalf of administrator	Can create and delete <a href="#">“on behalf of” rights</a> for all users.
Phrase administrator (add-on, <a href="#">available in Danish</a> )	Can edit phrases for merging documents.
Privilege administrator	Can create new roles and assign, remove, and edit privileges for a role.
Progress code administrator	Can create, edit, and delete <a href="#">progress codes</a> .
Reopener case	Can reopen cases.
Result list administrator	Can create <a href="#">standard column layouts</a> for all users.
Search administrator	<p>Can create <a href="#">fixed searches</a> for all users.</p> <p>If the F2 Search Templates add-on module has been configured, users with this privilege will be able to view search templates. Search templates are configured in cooperation with cBrain.</p>
Security group administrator	Can create, edit and delete <a href="#">security groups</a> .
Settings administrator	Can create, edit, and delete <a href="#">user settings</a> and assign them to individual users, new users, and based on the users' roles.
SSN Synchronizer (add-on module)	Can access the CPR from the properties dialogue for participants and users and update participant information from there.
System message administrator	Can create, edit and delete <a href="#">system messages</a> .

Privilege	Description
Template administrator	Can create, edit, and delete <a href="#">document templates</a> and global approval templates ( <a href="#">add-on module</a> ).
Unit administrator	Can create, edit, move, and deactivate <a href="#">units</a> .
Unit type administrator	Can create and delete <a href="#">unit types</a> .
User administrator	Can create, deactivate, and edit users, including user images. Can also <a href="#">log out a user from all F2 sessions</a> .
Value list administrator	Can create, edit, and delete <a href="#">value lists</a> .

## Further explanation of selected privileges

The following sections describe selected privileges in further detail.

### Administrator read access to all records

Users with this privilege can search and find all records in their authority except for records in users' "My private records" lists or records with an access restriction which they aren't part of. The privilege grants read access to records with the "Involved" and "Unit" access levels which would be otherwise inaccessible to the user.

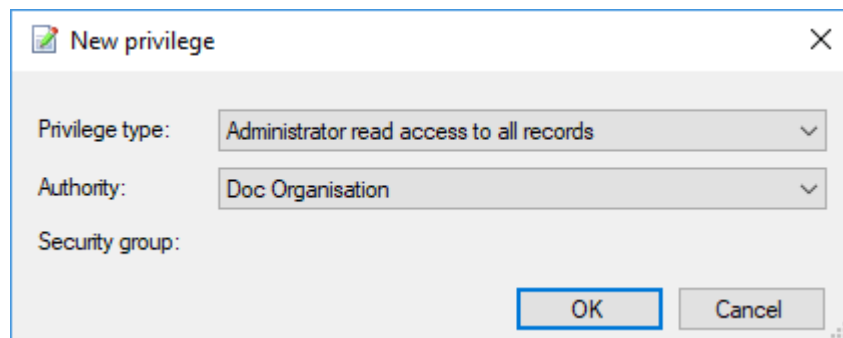


Figure 54. The "Administrator read access to all records" privilege

This privilege can be used e.g. when an employee leaves the organisation and the records for which they are responsible must be reallocated.

Read access to all records is disabled by default. A user with the privilege can enable it via the "Read access to all records" menu item in the "Misc." menu group on the "Administrator" tab.

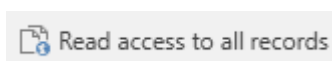
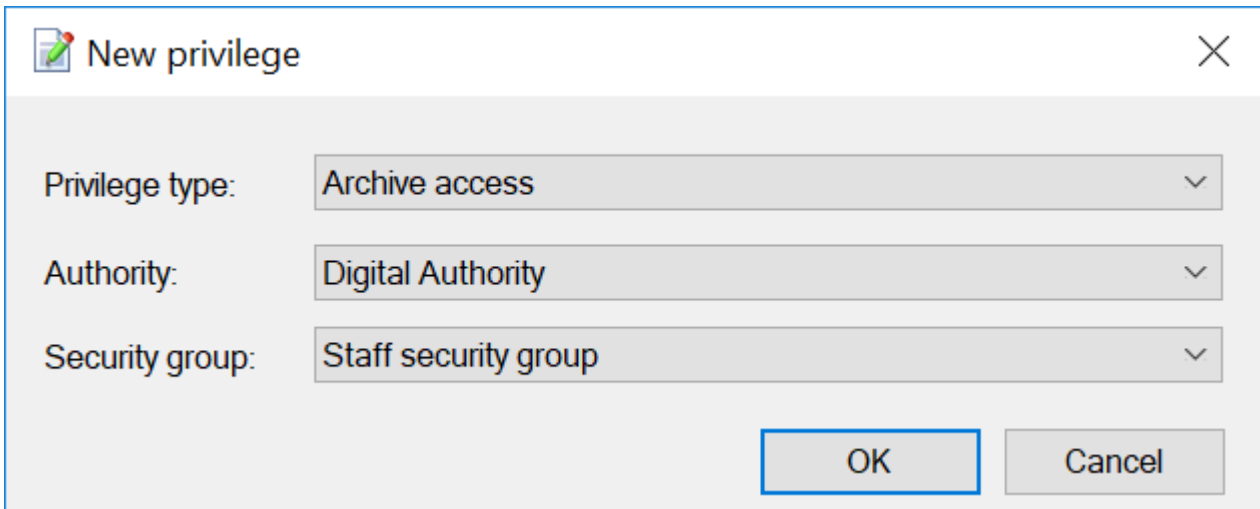


Figure 55. The "Read access to all records" menu item

## 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.



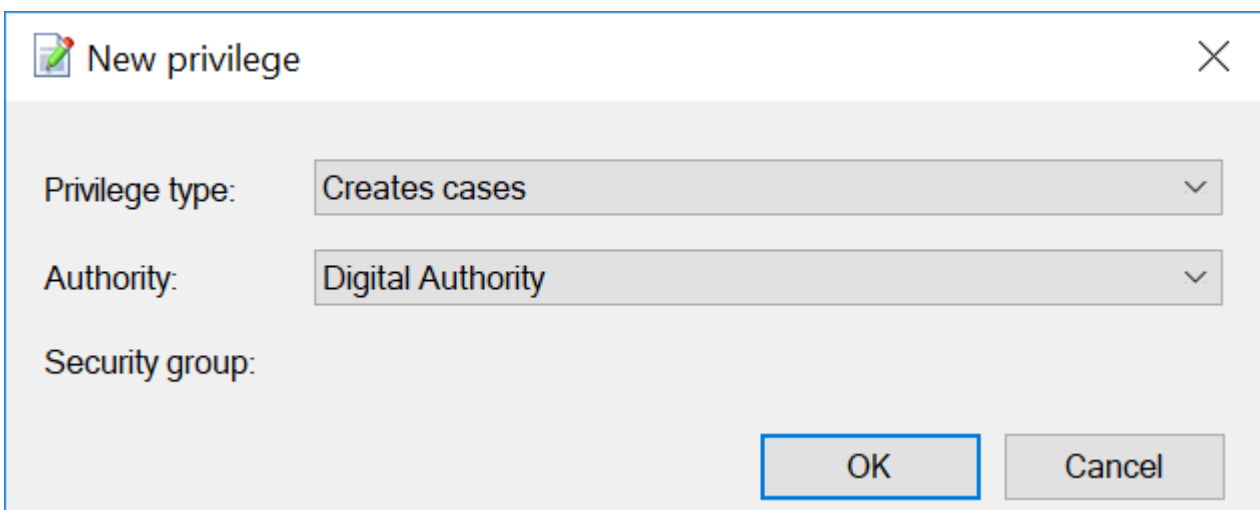
The screenshot shows a dialog box titled "New privilege" with a close button (X) in the top right corner. It contains three dropdown menus: "Privilege type:" set to "Archive access", "Authority:" set to "Digital Authority", and "Security group:" set to "Staff security group". At the bottom right, there are two buttons: "OK" and "Cancel".

Figure 56. 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.



The screenshot shows a dialog box titled "New privilege" with a close button (X) in the top right corner. It contains three dropdown menus: "Privilege type:" set to "Creates cases", "Authority:" set to "Digital Authority", and "Security group:" which is currently empty. At the bottom right, there are two buttons: "OK" and "Cancel".

Figure 57. The "Creates cases" privilege

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

## Distribution list editor

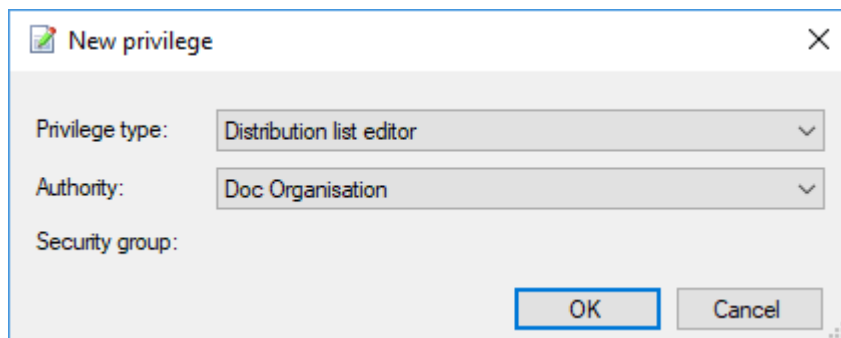


Figure 58. The “Distribution list editor” privilege

Read more about [editing distribution lists](#).

## 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.

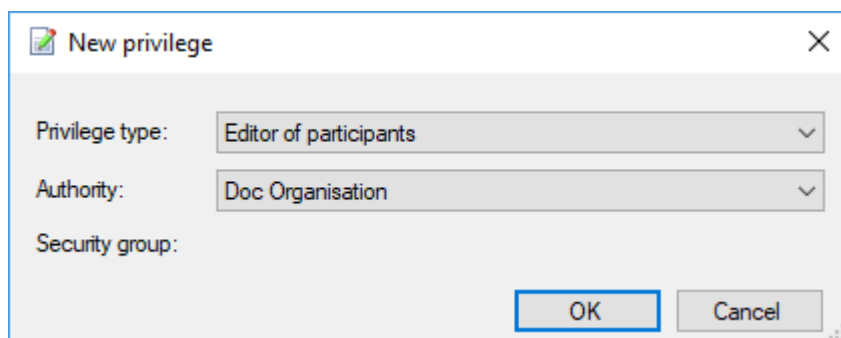


Figure 59. The “Editor of participants” privilege

## Keyword administrator

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 as well as deactivate and edit existing keywords.

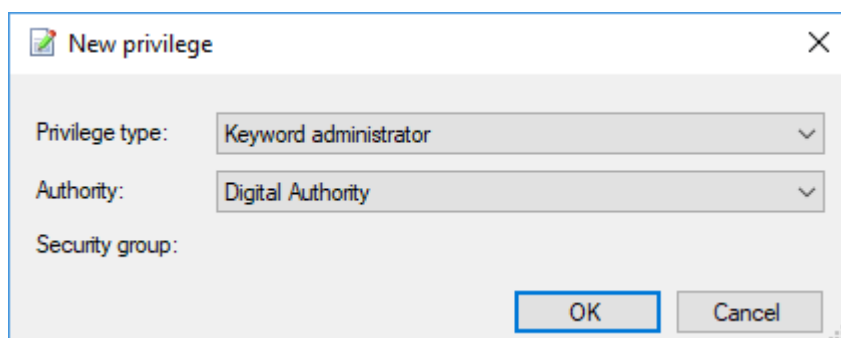


Figure 60. The “Keyword administrator” privilege

Read more about [keywords in relation to departments and authorities](#).

**NOTE** Keywords are shared by all authorities in an F2 installation.

## No case help for saving or sending records

A user with this privilege will not see the case help when saving or sending records. This means that any changes to metadata that are otherwise enforced by the case help will not apply to these actions when performed by said user. Other instances of the case help still apply. Depending on their setup, this means new records created by the user will have the case help box ticked and have the user listed as responsible for the record.

**NOTE** Any user with this privilege may save and send records that do not meet the organisation's guidelines. Use caution when assigning this 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.

Security groups are created in the “Create security group” dialogue. Read more about this in [Create a security group](#).

Users must have a role with a privilege pertaining to a specific security group to be included in that group. Several roles can refer to the same security group. Users can be added to a security group in two ways:

- Automatic allocation of a role in the “Add users to security groups” dialogue. Read more about this in [Add users to security groups](#).
- Manual allocation of a role with a privilege granting access to the security group. Read more about this in [Add user to security group using manual role assignment](#).

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

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

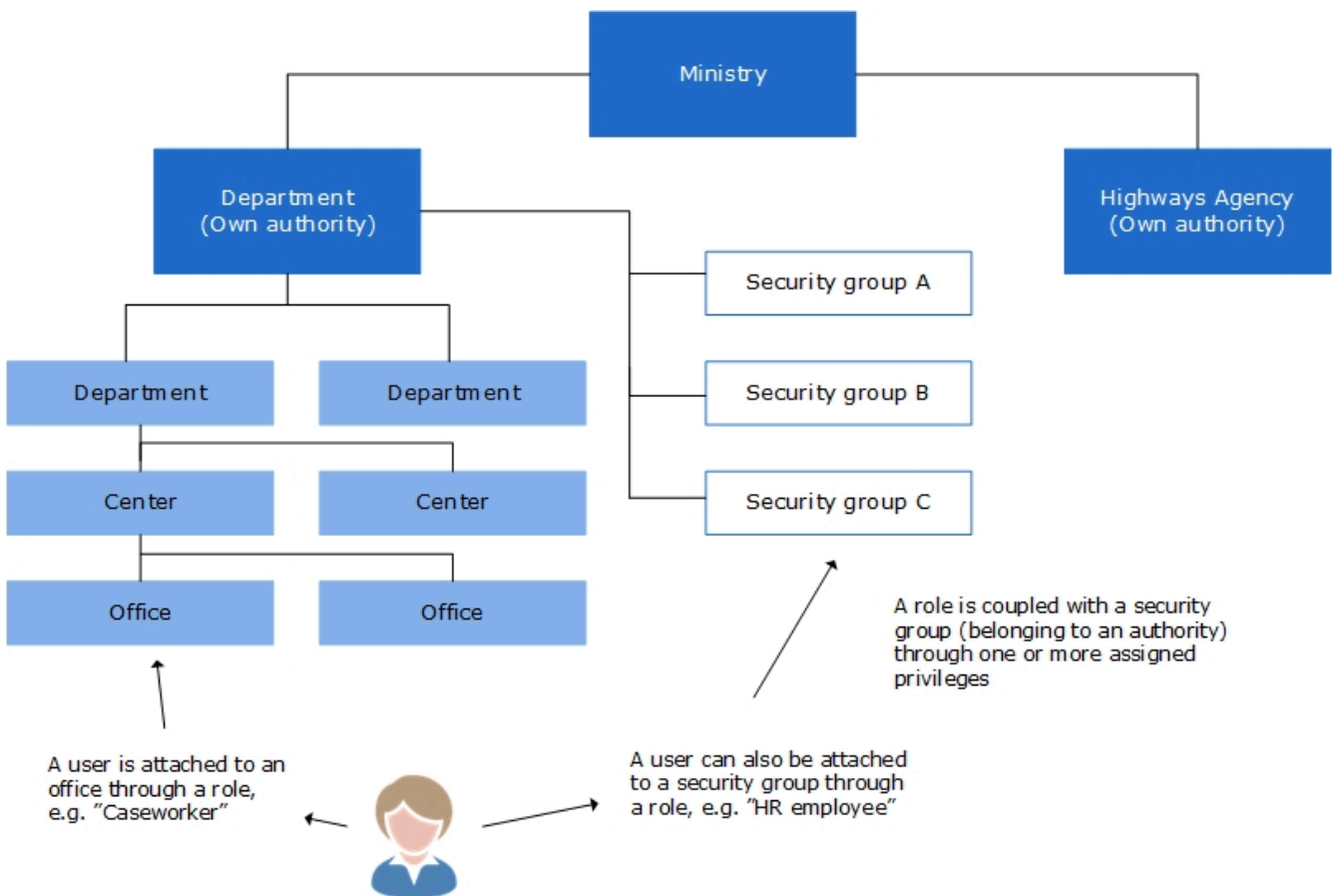


Figure 61. Security groups are created under an authority

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



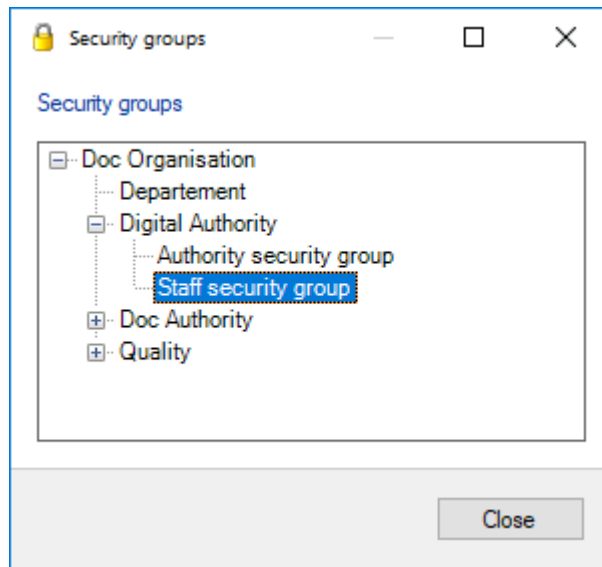


Figure 62. Authorities and security groups

Once a security group is established, users can be assigned to the group. This task is performed by a user with the “Security group administrator” 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.

**NOTE** A user with full write access to a record or a case can remove any security groups added to said record or case. This includes security groups which the user is not a member of.

## Create a security group

To create a security group, click **Create security group** on the “Administrator” tab.

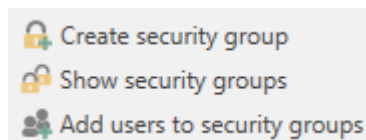


Figure 63. “The “Create security group” menu group

In the “Create security group” dialogue, enter a title for the security group and use the drop-down menu to select the authority under which the security group will be created.

In the “Synchronisation key” field, a synchronisation key can be entered. For example, this key is used when importing security groups to F2.

Enter the title of the new security group and select which authority to add the group to. Only users within this authority can be added to the security group.

Title  
Security group 2

Authority  
cBrain

Synchronisation key  
697589535

Create Cancel

Figure 64. The “Create security group” dialogue

When a security group has been created through the “Create security group” dialogue, F2 automatically creates a role type and a role which can be assigned to users in the “Units and users” dialogue. Read more about this in [Add user to security group using manual role assignment](#).

Alternatively, users can be added to security groups in the “Add users to security groups” dialogue. Read more in [Add users to security groups](#).

## Add users to security groups

Click on **Add users to security groups** on the “Administrator” tab to open the “Add users to security groups” dialogue.

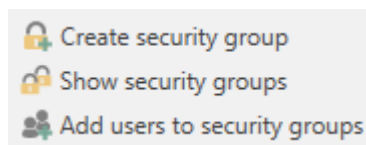


Figure 65. The “Add users to security groups” menu item

In the dialogue, add the relevant users and use the drop-down menu to select the security group to which the users will be added.

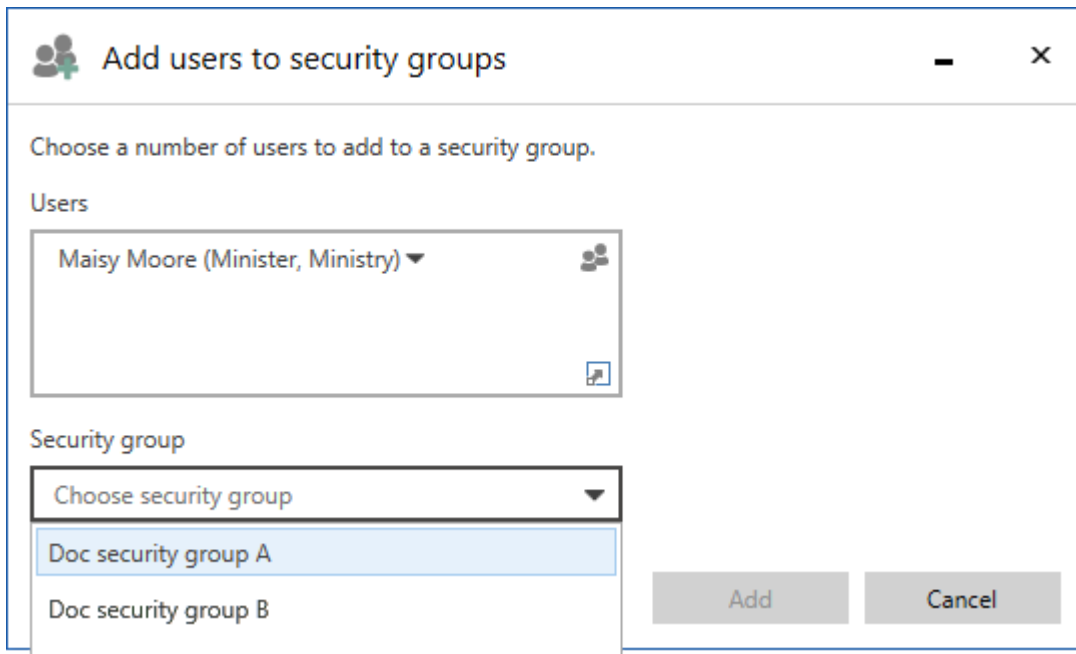


Figure 66. The “Add users to security groups” dialogue

## Add user to security group using manual role assignment

Since 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”. See the [Create and assign role types](#) section.
- 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** A user cannot see the security group if they do not have membership via a role. This means they cannot assign the security group to records or cases.

Privileges for members of security groups are described in the [Archive access](#) section.

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

## Show security groups

To view all security groups, click **Show security groups** on the “Administrator” tab.

Records to which access is limited to a security group can only be accessed by users with roles that include them in said security group. An administrator can add themselves to security groups on a temporary basis if they need 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**.

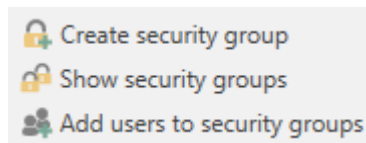


Figure 67. The “Show security groups” menu item

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**.

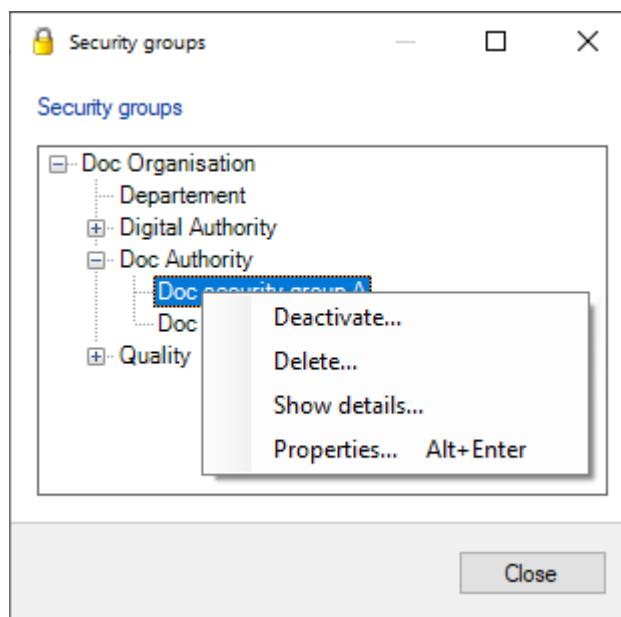


Figure 68. The “Security groups” dialogue

In the example below, Hannah Hendricks, Harper Ross, and Hector Richards are members of the “SG HR” security group.

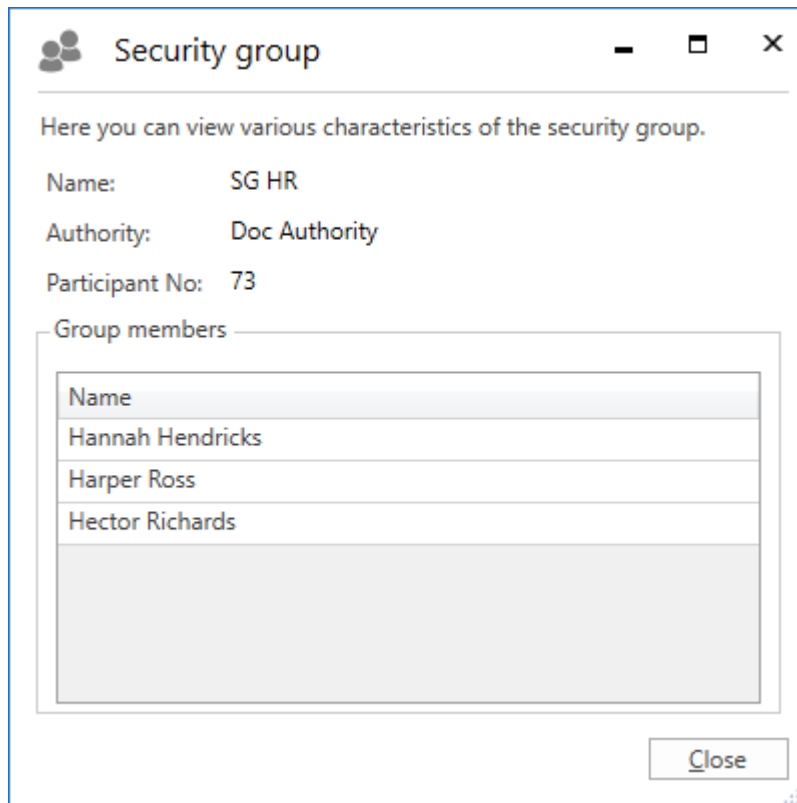


Figure 69. Properties for a security group

## Deactivate security group

A user with the "Security group administrator" privilege can deactivate security groups using the **Show security groups** menu item on the "Administrator" tab.

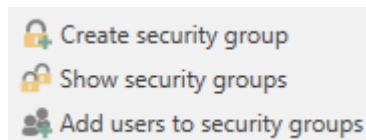


Figure 70. The "Show security groups" menu item

In the "Security groups" dialogue, right-click on the relevant security group and select **Deactivate...** in the context menu.

An inactive security group can be reactivated by right-clicking and selecting **Activate...** in the context menu.

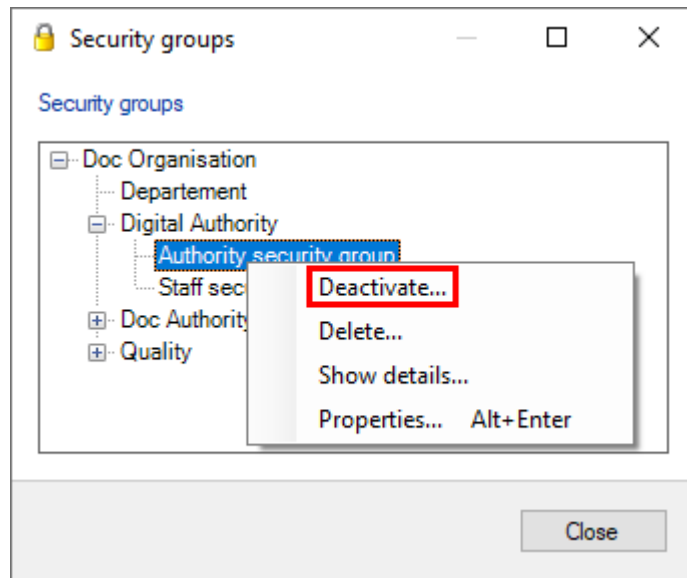


Figure 71. Deactivate security group

An inactive security group cannot be added to a case's or record's access restriction. Deactivating a security group, however, does not affect cases or records on which it is already in use.

Members of an inactive security group can be added or removed as with an active 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.

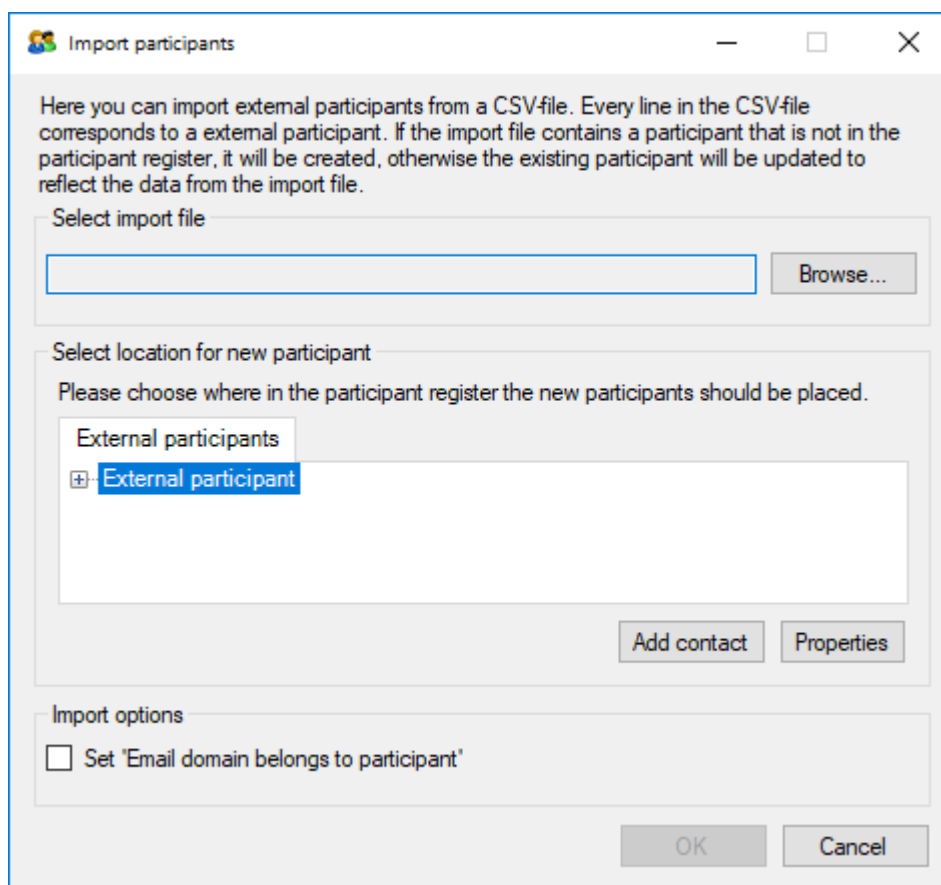


Figure 72. Import participants

Fill in the following fields in the “Import participants” dialogue:

Field	Description
“Select import file”	Click on <b>Browse...</b> to select the file.
“Select location for new participant”	Select a location for newly created participants in the participant register.  If the participants in the import file must be placed in a new node, first create the node by clicking <b>Add contact</b> .
“Add contact”	Opens the “Create unit” dialogue. From here a new node can be added to the participant register. The new unit can then be selected as the location for the new participants.
“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 they correspond 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.

Read more about [the participant register and how to create external participants](#).

## 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.

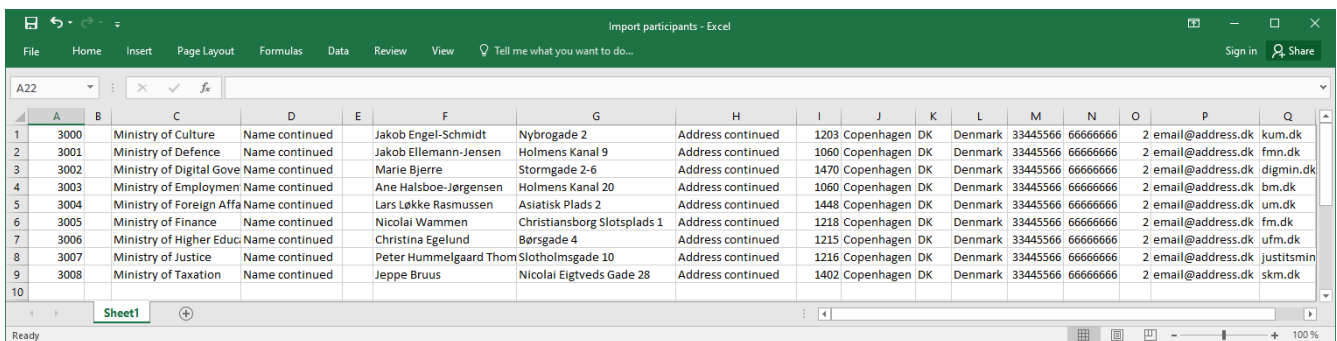


#	Column heading	Description
1	External ID	This ID is saved with the participant. If a participant is reimported, the existing participant with this ID is updated with the new data from the CSV file.
2		This column may be empty, but must be included.
3	Name	Name
4	Name, continued	
5		This column may be empty, but must be included.
6	Contact person	
7	Address	Address
8	Address, continued	
9	Zip code	
10	City	
11	Country code	
12		This column may be empty, but must be included.
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	CVR/SSN number	The participant's CVR or SSN number.
19	CVR P number	
20	Created date	If this field is empty, the current date is used for new participants.
21	Edited date	If this field is empty, the current date is used.
22	Groupcode01	DB07 codes. The codes are saved to the participant. The participant properties dialogue must be configured in order to show the codes. Configurations are performed in cooperation with cBrain.
23	Groupcode02	

#	Column heading	Description
24	Groupcode03	
25	Groupcode04	
26	Groupcode05	
27	Groupcode06	
28	Groupcode07	
29	Groupcode08	
30	Groupcode09	
31	Groupcode10	

**NOTE** The "Private phone" field for the participant's private telephone number can be added through a configuration. Read more in [Communication](#). Configurations are performed in cooperation with cBrain.

Note that the columns above are shown in a table format. In the import file they must be formatted differently. The import file must use a semicolon as a separator between columns. For empty columns, simply do not enter anything between the semicolons. The figure below shows an example of an import file with external participants.



If you create the CSV file as a comma-separated list in e.g. Notepad, a semicolon must be used as a separator between columns. For empty columns, simply do not enter anything between the semicolons.

**TIP**

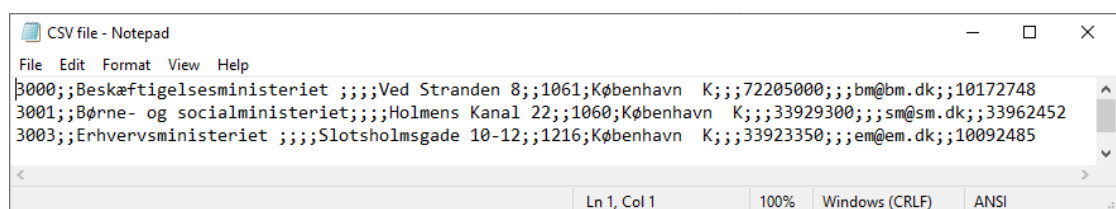


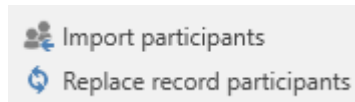
Figure 73. Comma-separated import file

## 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.

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



*Figure 74. 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.

It is possible to restrict access to specific external participants in the participant register using the F2 Access Restriction for Participants add-on module ([documentation available in Danish](#)). An external participant with access restriction can only be seen and found by the unit who 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 are lists that apply to [all authorities in an organisation](#). Each value list represents a group of standardised texts used in connection with different tasks.

An example of a value list is the request types, which may contain text strings such as:

- Office reply
- Report
- Alert
- For information.

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

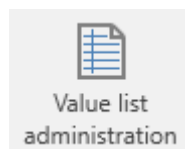
## NOTE

A value list can be used as the basis of data in extension fields through a configuration. The external ID of the value list items are used as the storage value in F2, which means that when a value list item is updated, it is also updated on records and cases where it is already in use. This enables users to search for records and cases using the current value of the value list item. Configurations are performed in cooperation with cBrain.

## 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, select the "Administrator" tab and click on **Value list administration** in the ribbon.



*Figure 75. 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 below shows examples of value lists that are available in an F2 installation.

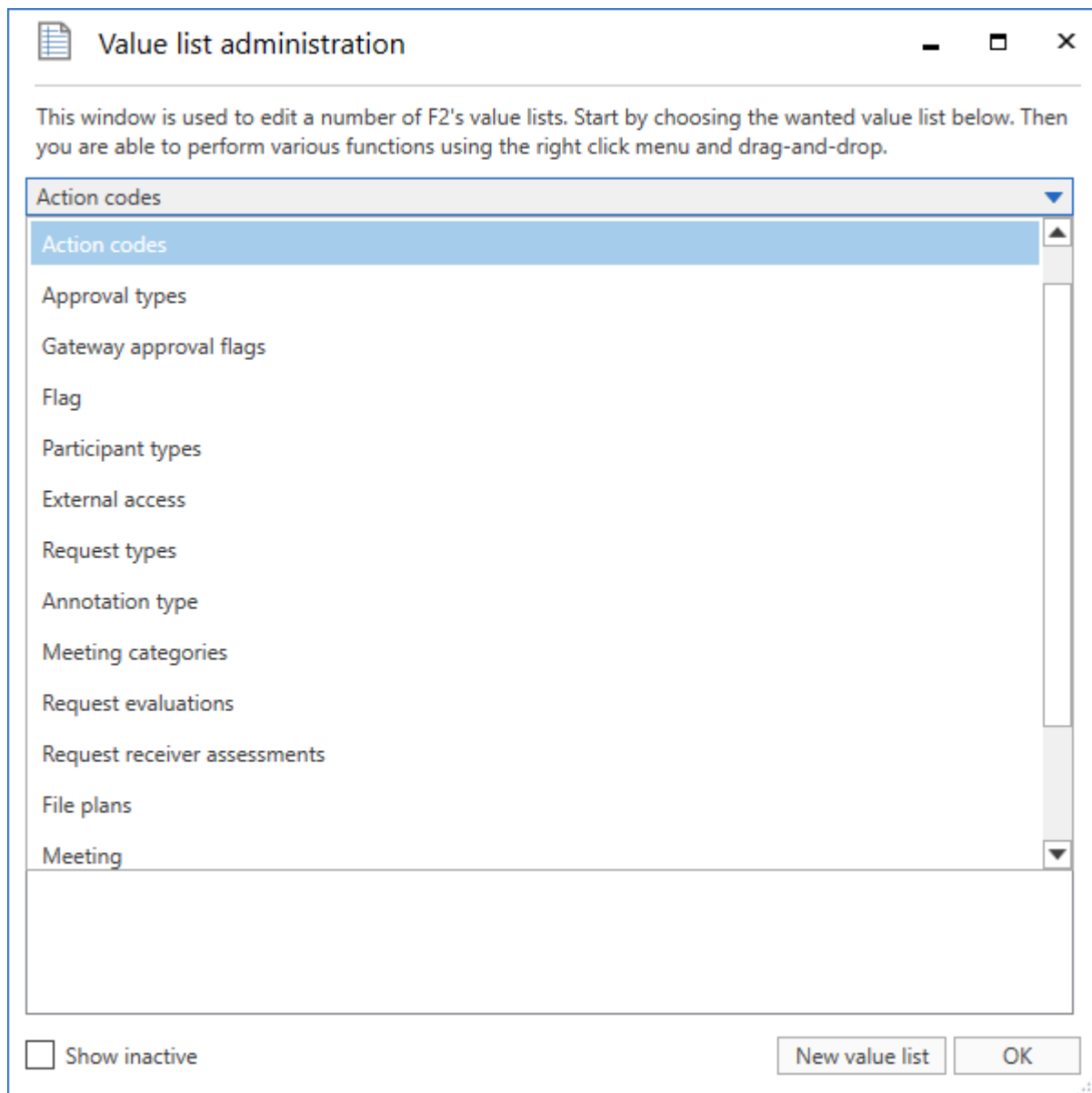


Figure 76. The “Value list administration” dialogue

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

Once a list is chosen, its values are displayed in the window. Values are created as subitems for each list.

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

- Create item
- Rename value list
- Sort item
- Check for inconsistent deactivation
- Import value list
- Export value list.

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

- Create item
- Rename item
- Deactivate item
- Selectable item
- Sort item
- Import/Export item
- Item properties.

Tick “Selectable” to make the the text (type) selectable where it appears. Untick “Selectable” to make the text visible, but not selectable.

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

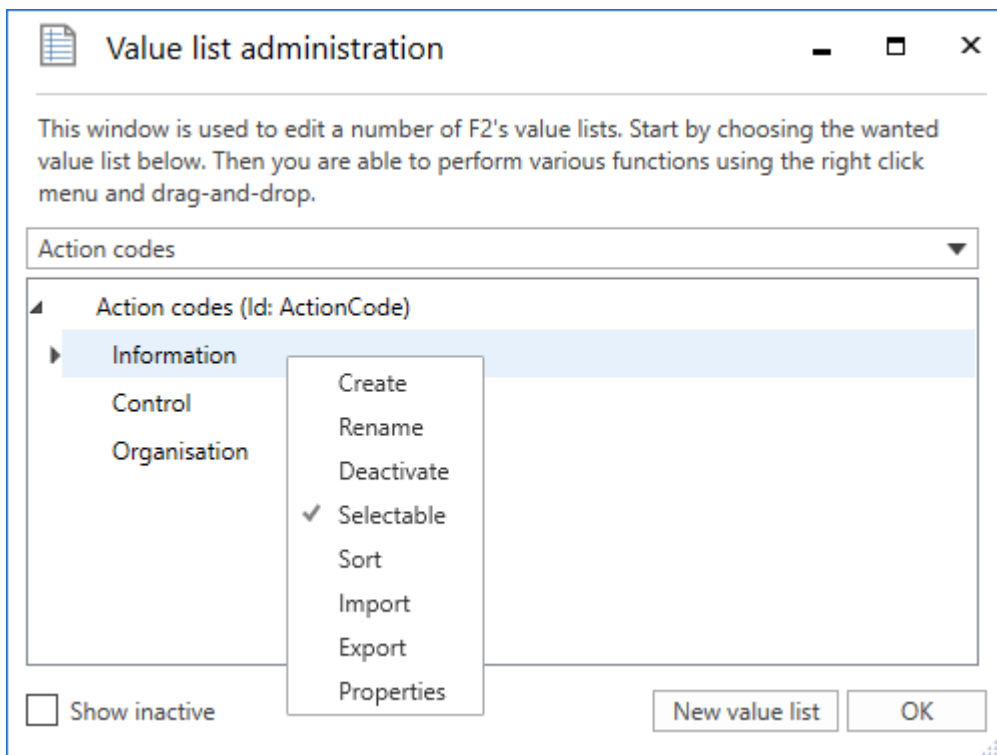


Figure 77. The context menu of a value list item

**NOTE** A value list item cannot be deleted, only deactivated. Deactivating a node in the item tree will also deactivate all value list items it contains.

## Sorting value lists

In the “Value list administration” dialogue it is possible to sort value list items on any level alphabetically. Right-click on a list, and select **Sort** in the context menu. F2 then sorts the selected list alphabetically. Only the selected level will be sorted. Any sublevels will not be affected.

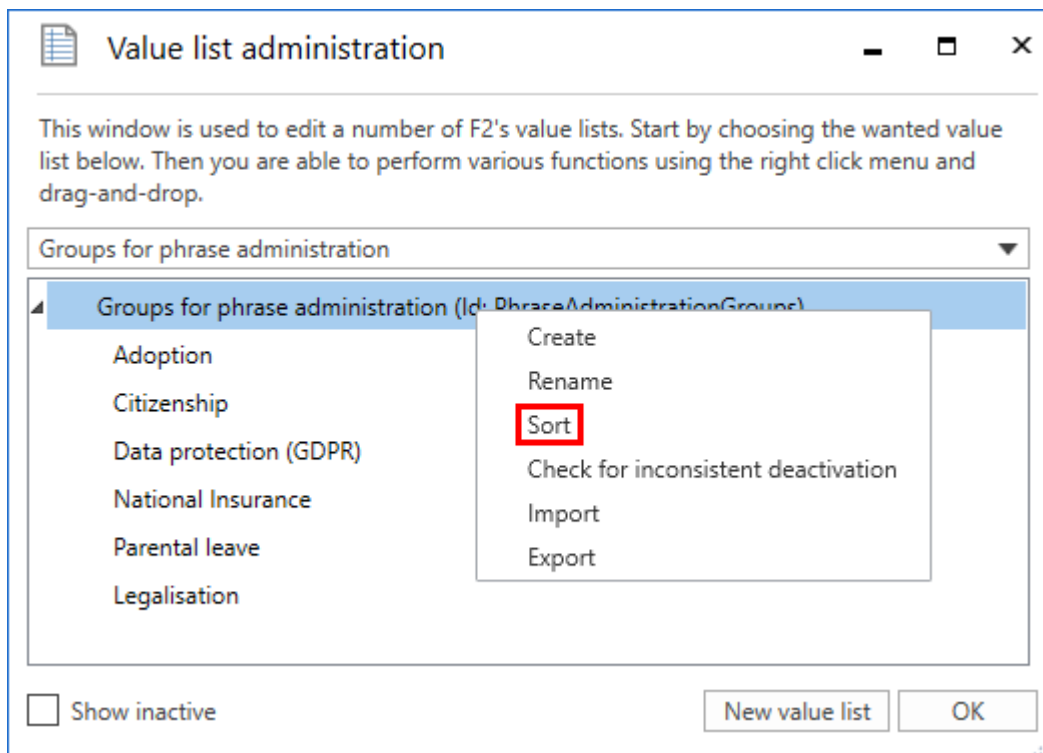


Figure 78. Sorting a value list

## Create a new value list

Users with the "Value list administrator" privilege can create new value lists in the "Value list administration" dialogue. Open the dialogue and click on **New value list**.

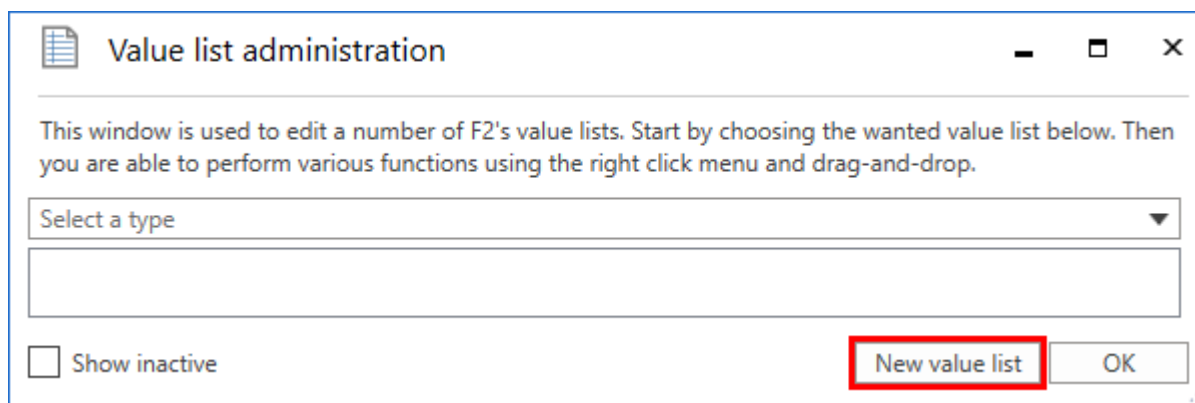


Figure 79. Value list administration

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

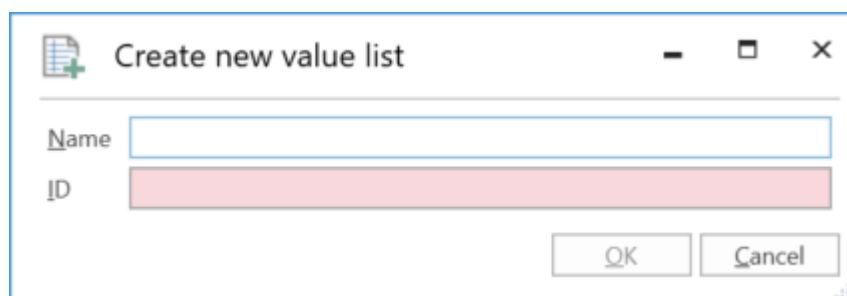


Figure 80. Create a new value list

**NOTE**

New value lists will most likely be created in connection with the add-on modules F2 Management Dashboards, F2 Search Templates, and F2 Task Guides. For these modules the value list ID is used in connection with the customisation of F2.

## Value list items

Users with the “Value list administrator” privilege can import value list items via an XML file or create them directly in F2. Each value list item is defined from certain parameters which vary depending on the type of list. Three obligatory parameters exist which are shared by all value lists:

- Type
- Name
- External ID.

These are described in detail in the table below.

Parameter	XML code	Description
Type	TypeId	Denotes the value list to which the item belongs.  Example: “Flag”.
Name	Title	The name of the value list item determined by its creator.  Example: “Urgent”.
External ID	ExternalId	An ID that must be unique for each value list item.  Example: “Flag_Urgent”.

The figure below shows an example of a value list item’s XML code, in this case the code for the “Urgent” flag.

```
<EnumTypeImportExportItem>
  <TypeId>DossierFlag</TypeID>
  <Title>Urgent</Title>
  <Description />
  <ExternalId>Flag_Urgent</ExternalId>
  <Applicable>>false</Applicable>
  <RelatedColor>#FFFF0000</RelatedColor>
  <Items />
  <Details />
</EnumTypeImportExportItem>
```



## Importing a value list item to F2

Value list items can be imported to F2 via an XML file. Depending on the file's content, existing value list items in F2 will be either moved or updated, and any new items will be created.

Click the **Value list administration** menu item on the "Administrator" tab. The "Value list administration" dialogue opens. Choose a list from the **Select a type** drop-down menu.

Right-click on the top node in the list and select **Import** from the right-click menu. On the figure below, the "Flag" value list has been chosen.

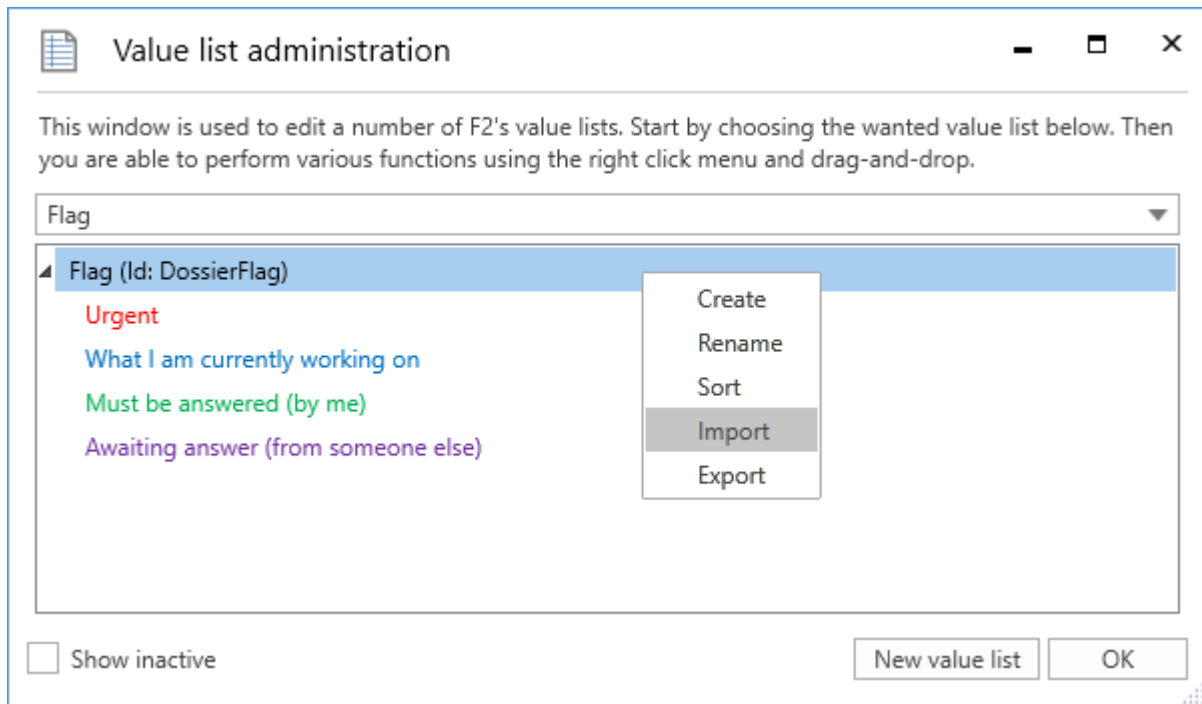


Figure 82. Context menu for the "Flag" value list

Before F2 imports the file with value list items, a message is displayed informing the user of the effects of the import.

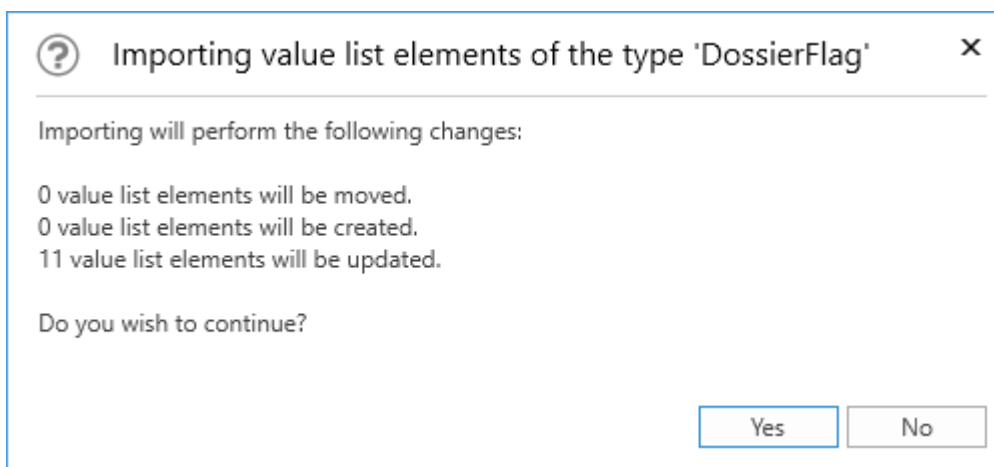


Figure 83. Importing value list items

Click **Yes** to execute the import and have F2 move, create, and update the value list items based on the content of the imported file.

**NOTE** Files with value list items must be in XML format and contain the correct formatting. The formatting appears in F2's existing value lists which can be exported and then accessed in a programme compatible with XML files.

## Creating a value list item in F2

It is possible to create value list items in F2 by clicking **Value list administration** on the "Administrator" tab. The dialogue "Value list administration" opens from which a list can be selected from the **Select a type** drop-down menu.

The name of the selected list type and any items that already exist are then displayed. Right-click on **the list's name** and select **Create** to open the "Create value list element" dialogue. On the figure below, the dialogue has been opened from the "Flag" value list.

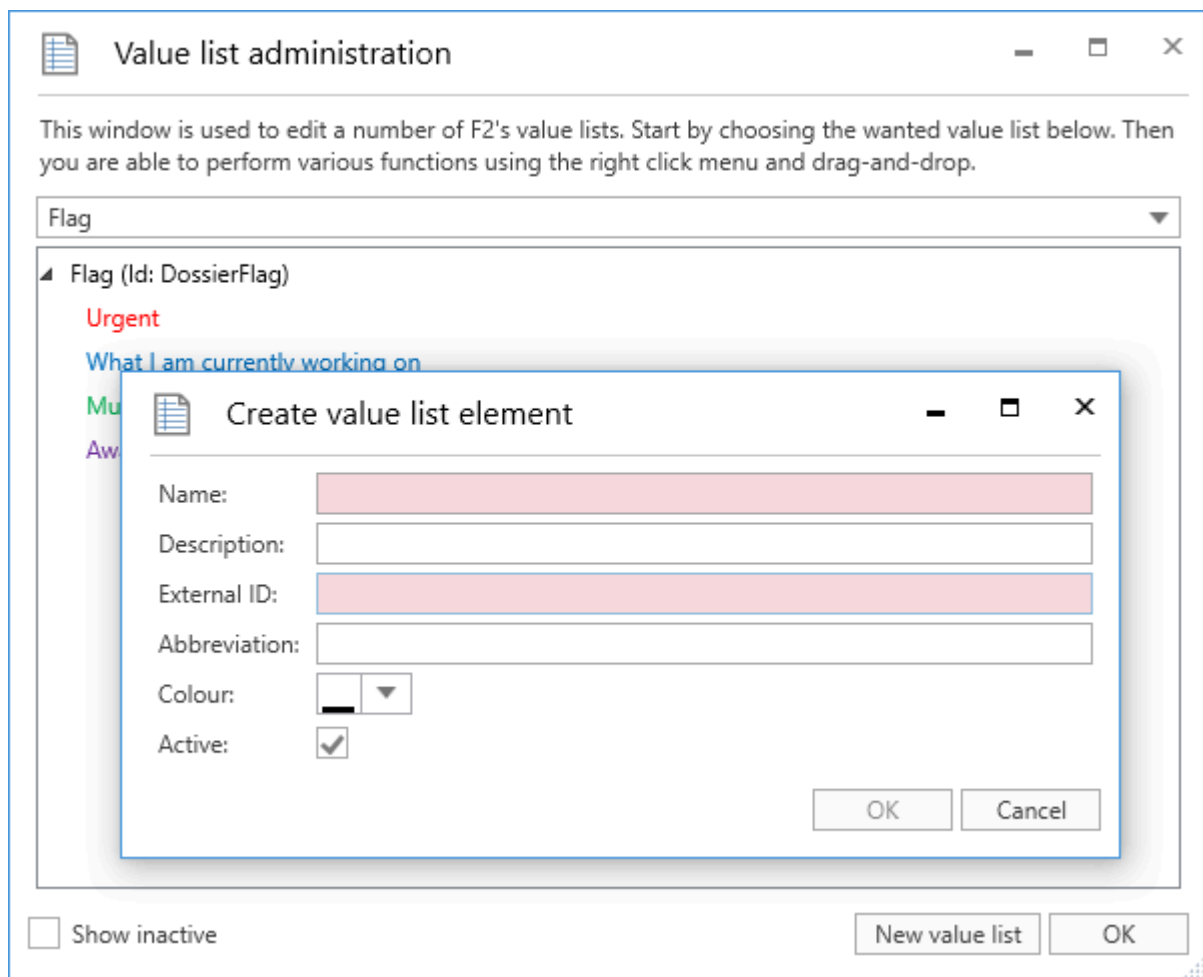


Figure 84. Create a value list item from the "Flag" list

Enter a name for the new value list item. F2 automatically suggests an external ID when a name has been entered. For example, a new flag with the name "Urgent" will be assigned the external ID "Flag\_Urgent". However, the user may overwrite the suggested external ID.

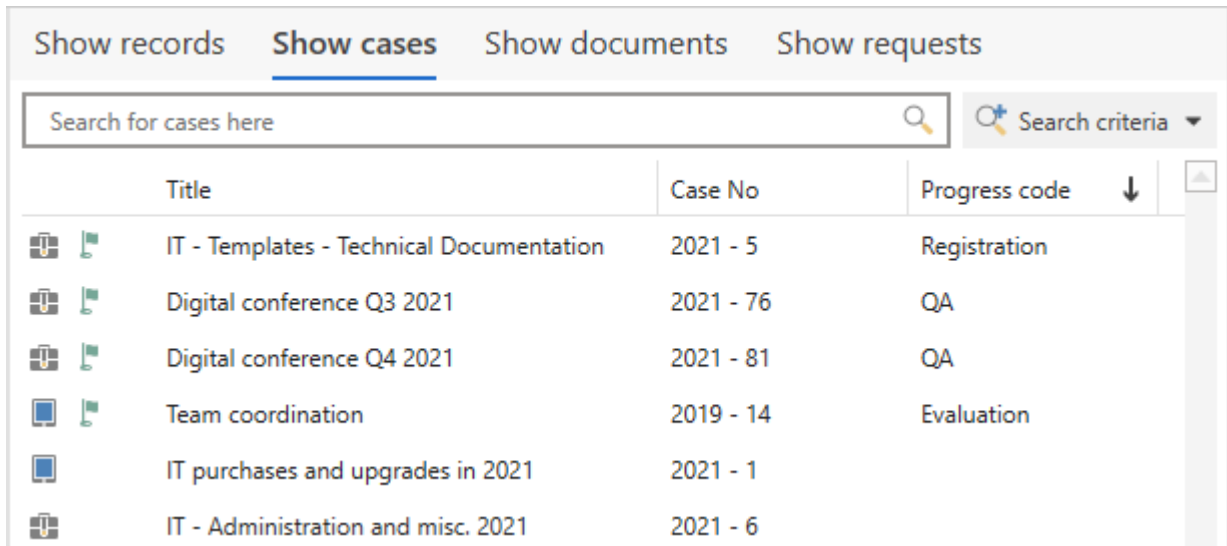
**NOTE** A system cannot have two value list items with the same external ID. Each value list item must have a unique external ID.

In this dialogue it is also possible to add a description and an abbreviation to the value list item if necessary. In order to use the item, tick the "Active" box.

The above figure contains an additional field, "Colour". This field is specific to the "Flag" value list. Use this to select a colour for the newly created flag. Other value lists may have fields that are specific to them also.

# Progress codes

Progress codes are a set of tools used to tag cases. By [tagging a case with a progress code](#), the case is identified as being on a certain step in a process. Progress codes are shown both in the main window's result list and in a case metadata field. This makes it easy to keep track of your cases at a glance.



The screenshot shows a software interface with a navigation bar at the top containing four tabs: "Show records", "Show cases" (which is selected and underlined), "Show documents", and "Show requests". Below the navigation bar is a search bar with the placeholder text "Search for cases here" and a magnifying glass icon. To the right of the search bar is a "Search criteria" dropdown menu. Below the search bar is a table with the following columns: "Title", "Case No", and "Progress code". The table contains six rows of data, each with a small icon to the left of the title. The "Progress code" column has a downward arrow icon next to the header, indicating it is a dropdown menu.

	Title	Case No	Progress code
	IT - Templates - Technical Documentation	2021 - 5	Registration
	Digital conference Q3 2021	2021 - 76	QA
	Digital conference Q4 2021	2021 - 81	QA
	Team coordination	2019 - 14	Evaluation
	IT purchases and upgrades in 2021	2021 - 1	
	IT - Administration and misc. 2021	2021 - 6	

Figure 85. Progress codes on cases in the main window's result list

Progress codes can be set up to update automatically. You can do this either through a case guide or by specifying a deadline for a progress code. When the deadline expires, F2 automatically switches to the next relevant progress code. For example, your organisation might dictate that all enquiries must be registered within two weeks. A progress code can be created to help meet that deadline.

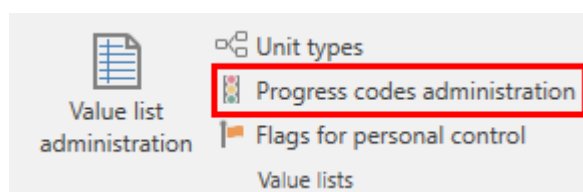
**NOTE** Contact cBrain for further information about using progress codes with case guides.

It is possible to integrate progress codes with the F2 cPort module ([documentation available in Danish](#)) in order to create an overview of deadline compliance for each progress code. F2 cPort is used to extract data from an F2 installation for statistics and analysis.

This article describes how to create, edit, delete, and add deadlines to progress codes.

## Create progress code

You can create progress codes if you have the the "Progress code administrator" privilege. Go to the the "Administrator" tab and click **Progress codes administration**.



The "Progress codes" window opens.

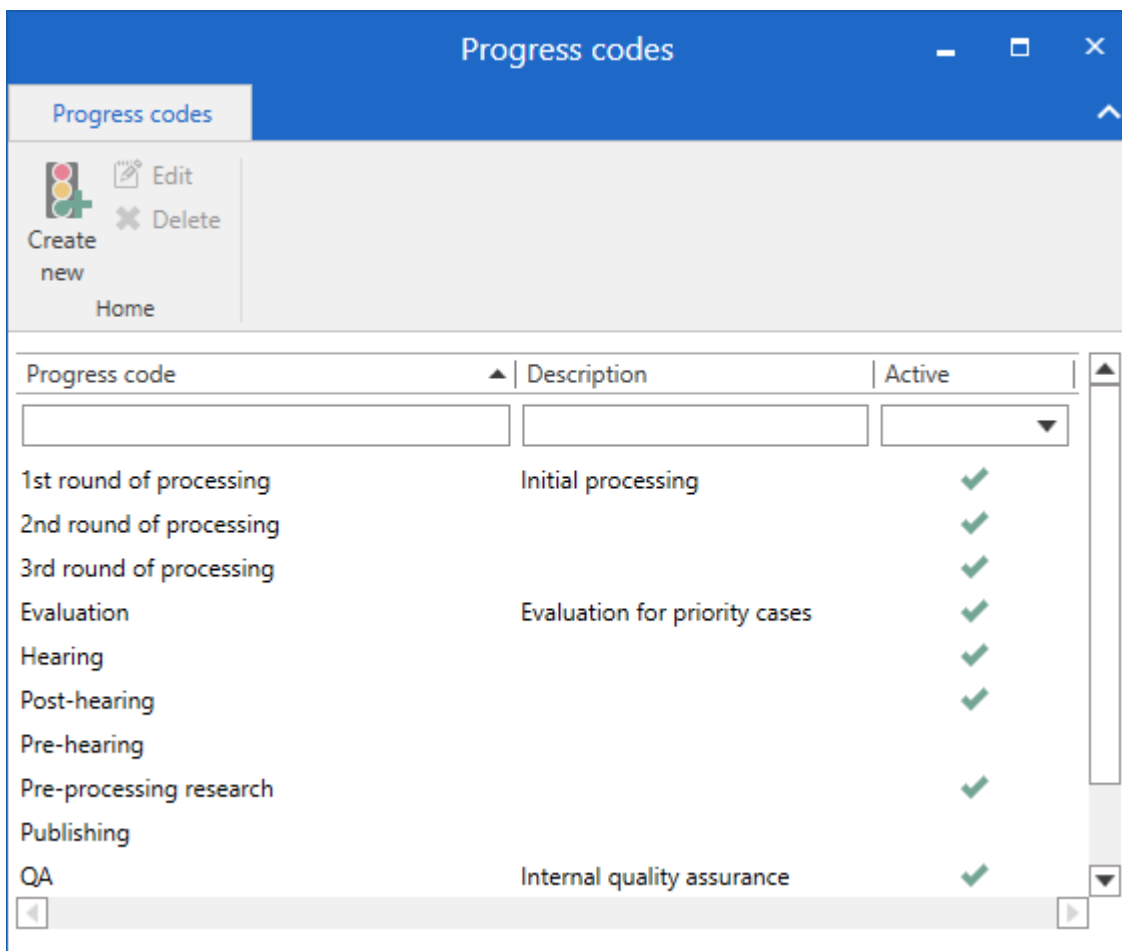


Figure 87. The "Progress codes" window

Click **Create new** to create a new progress code.

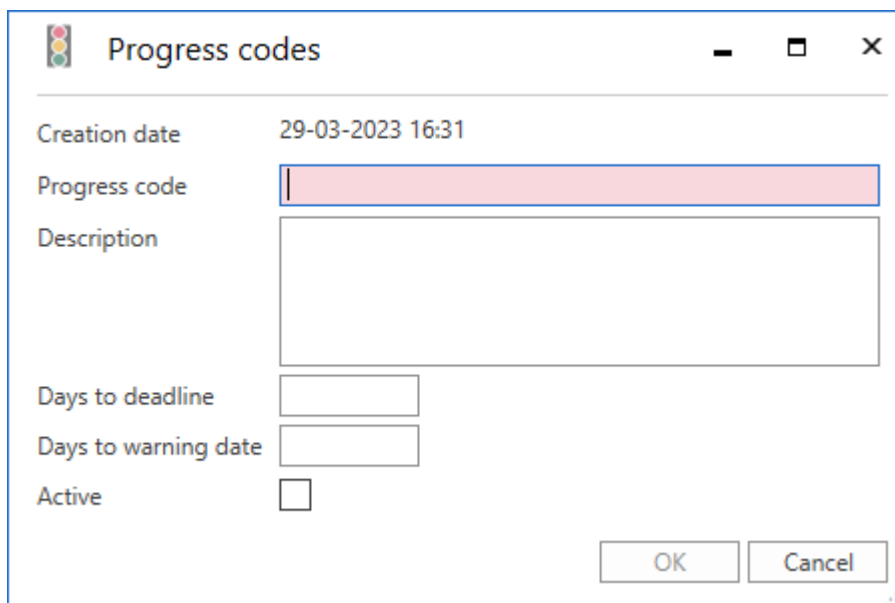


Figure 88. Create new progress code

In the dialogue that opens, enter the relevant information as described in the table below.

Field	Description
"Creation date"	Shows the date and time when the creator clicked <b>Create new</b> .
"Progress code"	Enter the title of the progress code. The title is shown in the "Progress code" column when viewing a list of cases. This field is mandatory and thus coloured red in the figure above.
"Description"	Add a description of the progress code here, e.g. to state its purpose.
"Days to deadline"	When you add the progress code to a case, this deadline is automatically added as well. Enter the number of calendar days until the deadline. The day when the progress code is saved to the case counts as day 0. A progress code doesn't require a deadline, but the progress code icon is only shown in the case result list if a deadline exists.
"Days to warning date"	Enter a warning date to decide when the progress code icon changes from green to yellow. Enter how many days you want the warning period to last, i.e. the period between the warning date and the deadline.
"Active"	Activate the progress code. Inactive progress codes cannot be added to cases, but do appear in searches.

How this information affects the use of progress codes is described in [Cases](#). This includes how the progress code icon changes colour in the result list based on the deadline and the warning date.

Click **OK** to create the progress code.

When using the F2 Task Guides module, progress codes can also be added automatically as part of tasks in a case guide.

## Progress code overview

If you have the "Progress code administrator" privilege, you can see an overview of existing progress code in the "Progress codes" window.

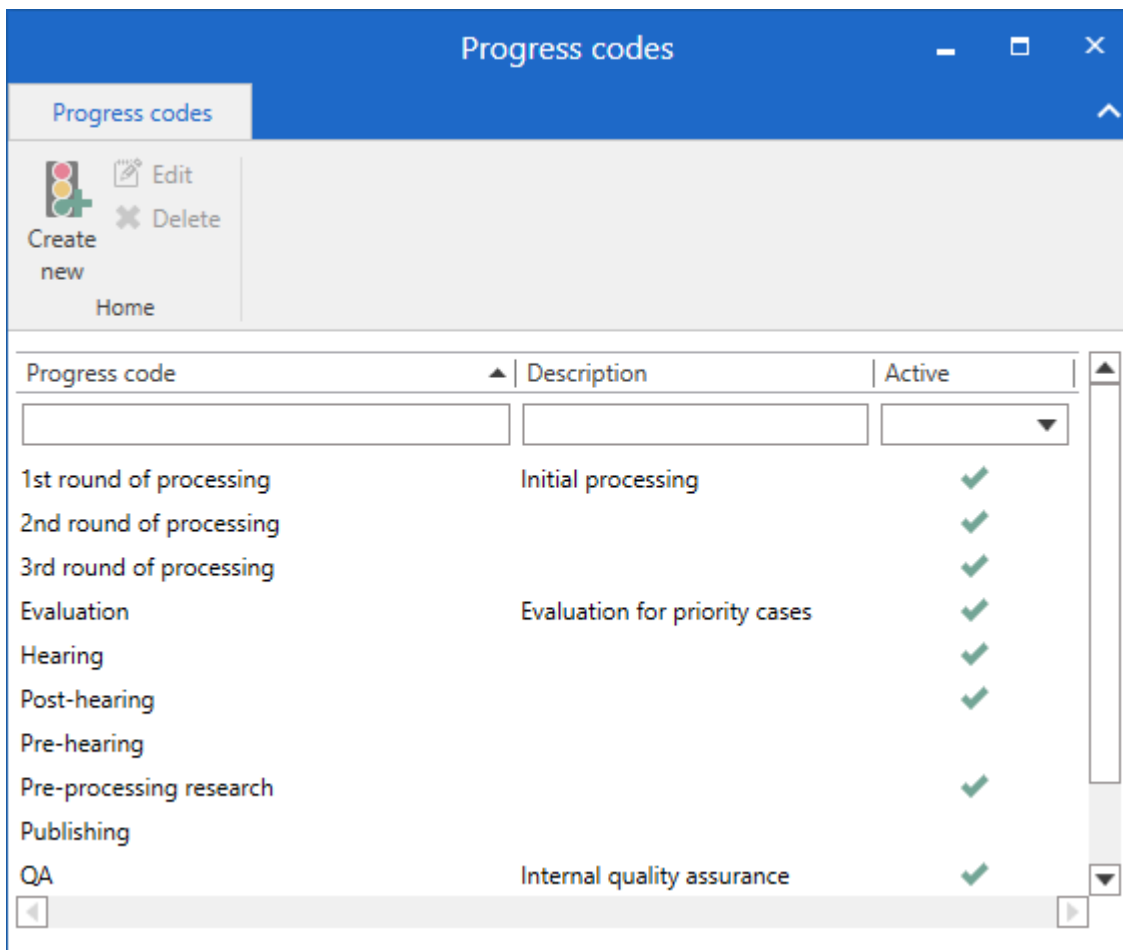


Figure 89. The "Progress codes" window and its ribbon

Progress codes are sorted alphabetically by title in the "Progress code" column. Progress codes can also be sorted by the "Description" and "Active" columns. Under each column title is a field that lets you filter the displayed progress codes.

From this window you can edit, deactivate, and delete progress codes as described in the sections below.

## Edit progress code

Click **Edit** in the ribbon or double-click a progress code to edit it. The dialogue below opens from which you can edit the progress code's information such as title, description, and deadline.

The screenshot shows a dialog box titled "Progress codes". It has a standard Windows-style title bar with a traffic light icon on the left and minimize, maximize, and close buttons on the right. The dialog contains the following fields and values:

- Creation date: 02-07-2021 10:56
- Progress code: Evaluation
- Description: Evaluation for priority cases
- Days to deadline: 7
- Days to warning date: 2
- Active:

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

Figure 90. Edit a progress code

A progress code can also be deactivated in the dialogue. Deactivated progress codes still appear in the progress code overview, but cannot be added to cases.

Click **OK** to save your changes or **Cancel** to discard them.

**NOTE** You must restart to F2 to complete the deactivation of a progress code.

A deactivated progress code still appears on the cases to which it was added before deactivation. This means that you can still use a deactivated progress code in your advanced searches. To do this, go to the "Case related" search group, click the **drop-down arrow** in the "Progress code" search field, and select the deactivated progress code.

If you reactivate a progress code, it can be added to cases again.

## Delete progress code

You can delete unused progress codes from the "Progress codes" window. When deleted the progress code is removed from the list of progress codes in both the case and the "Progress codes" windows.

To delete one or more progress codes, select them and click **Delete** in the ribbon.

**NOTE** You must restart to F2 to complete the deletion of a progress code.

If you attempt to delete a progress code that is currently in use, F2 offers to deactivate the progress code instead.

If a progress code that is in use must be deleted, it must first be manually removed from all cases to which it was added. Read more about [manually removing progress codes](#).



# 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. A user with the “Flag administrator” privilege is able to define which flags are available to the users of a given F2 authority.

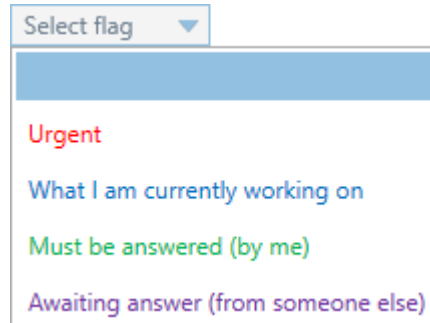


Figure 91. Example of the control flag menu on a record

Control flags are created, edited, and 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.

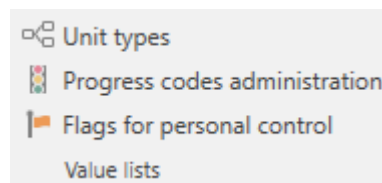


Figure 92. The “Flags for personal control” menu item

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.

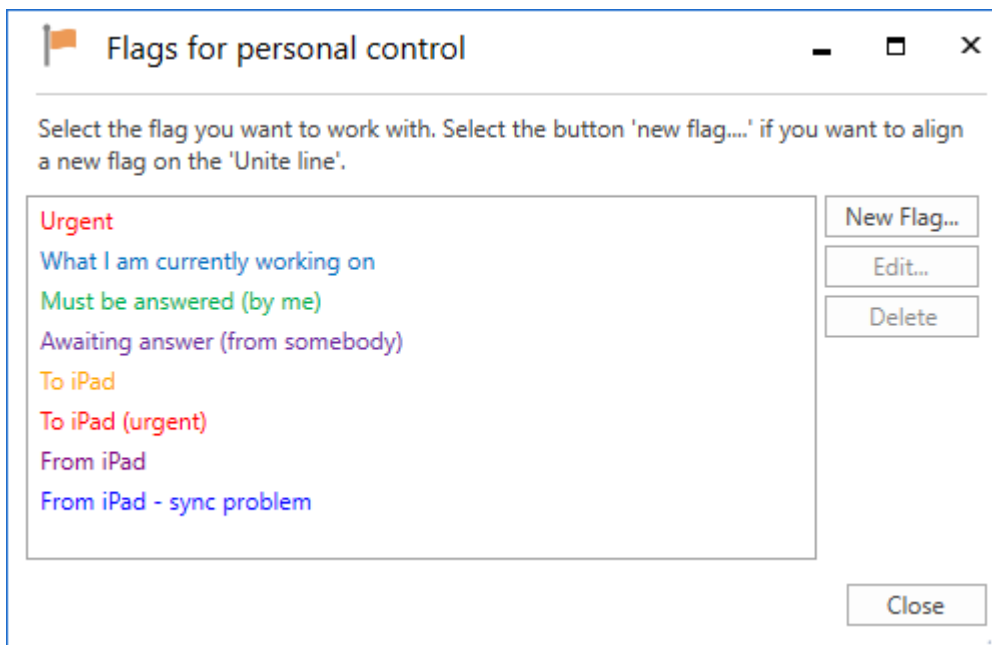


Figure 93. The “Flags for personal control” dialogue

When a new control flag is created it must be given a title, a colour, and a 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.

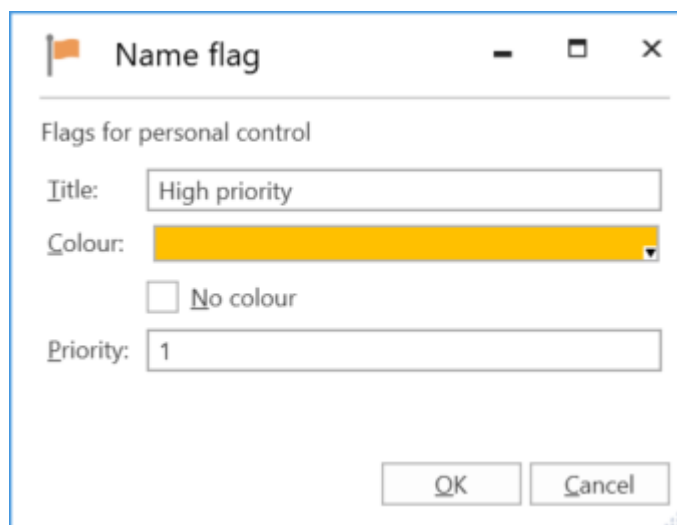


Figure 94. Name the control flag

If the title of a control flag 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 result list immediately by pressing **Ctrl+F5**. The flag’s colour is not updated in the main window ribbon or the context menu 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 “Administrator” tab.

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

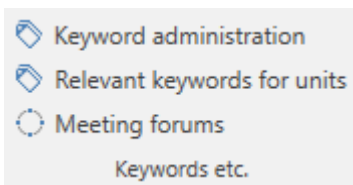


Figure 95. The “Keyword administration” menu item

**NOTE** Keywords are shared by all users in all authorities in an F2 installation.

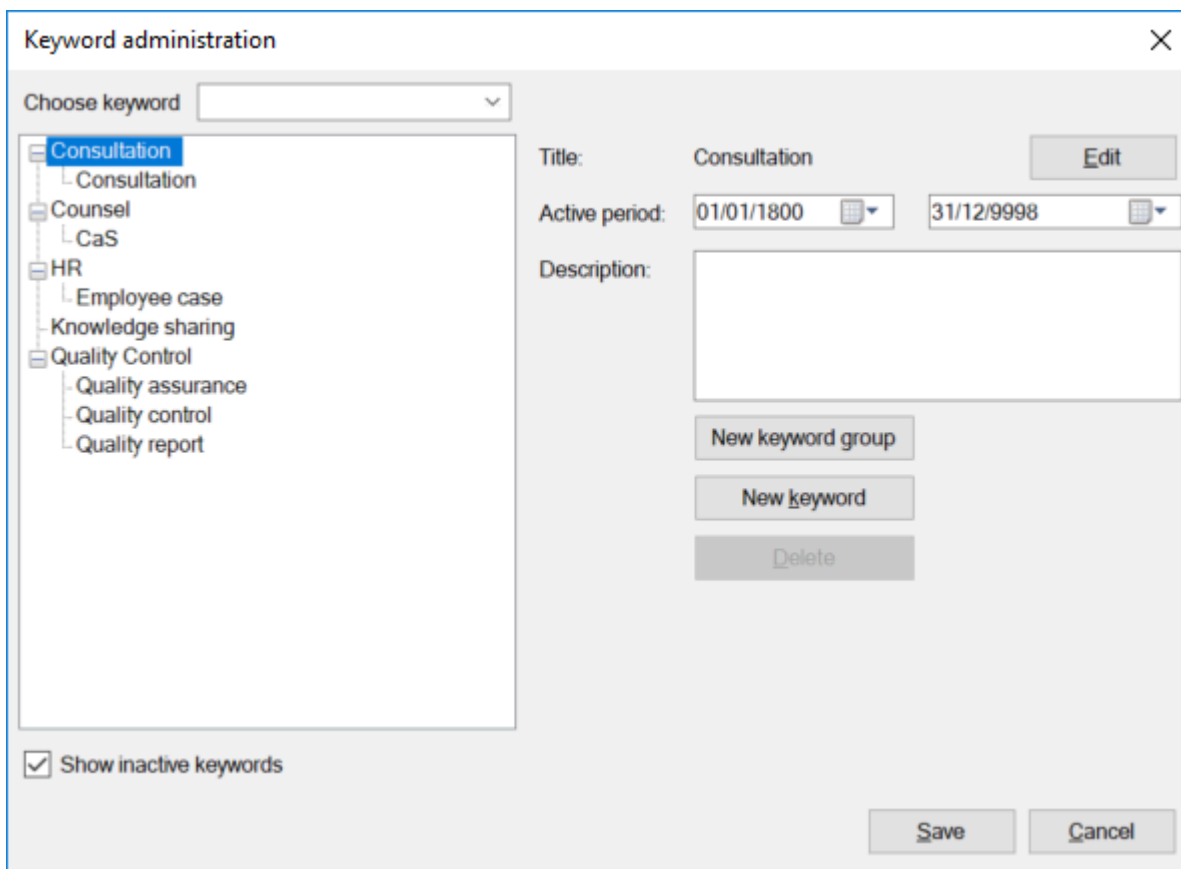


Figure 96. Administration of keywords

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 to records and cases. Deactivated keywords remain on records and cases and can still be used in searches.

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

**NOTE**

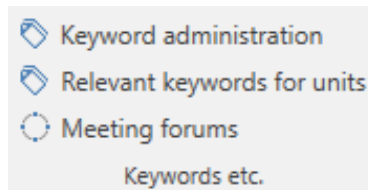
If a keyword is used on a record or a case, it cannot be deleted in the keyword overview. However, it can be deactivated by entering an end date in the “Active period” field. In other words, a keyword cannot be used after the end date, but it can still be used in searches.

**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 97. 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 their records and cases.

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

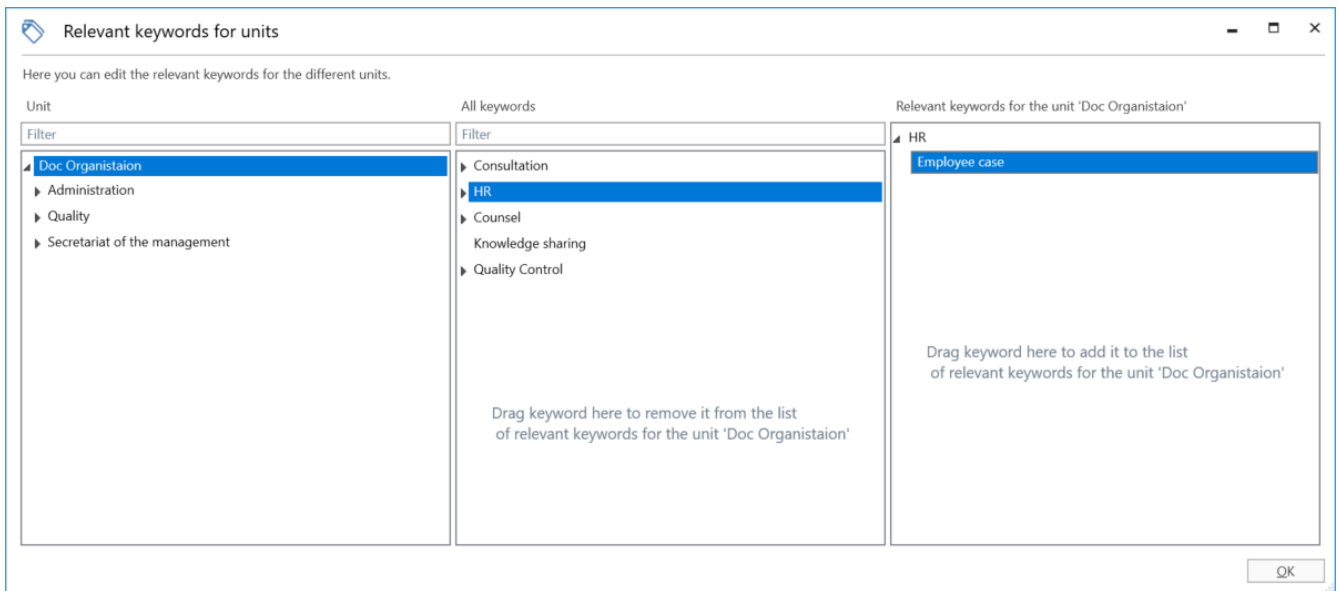


Figure 98. Select keywords

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

Column	Description
“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.

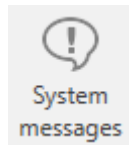


Figure 99. The “System messages” menu item

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.

System messages can be created, edited and 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 users’ screens immediately.

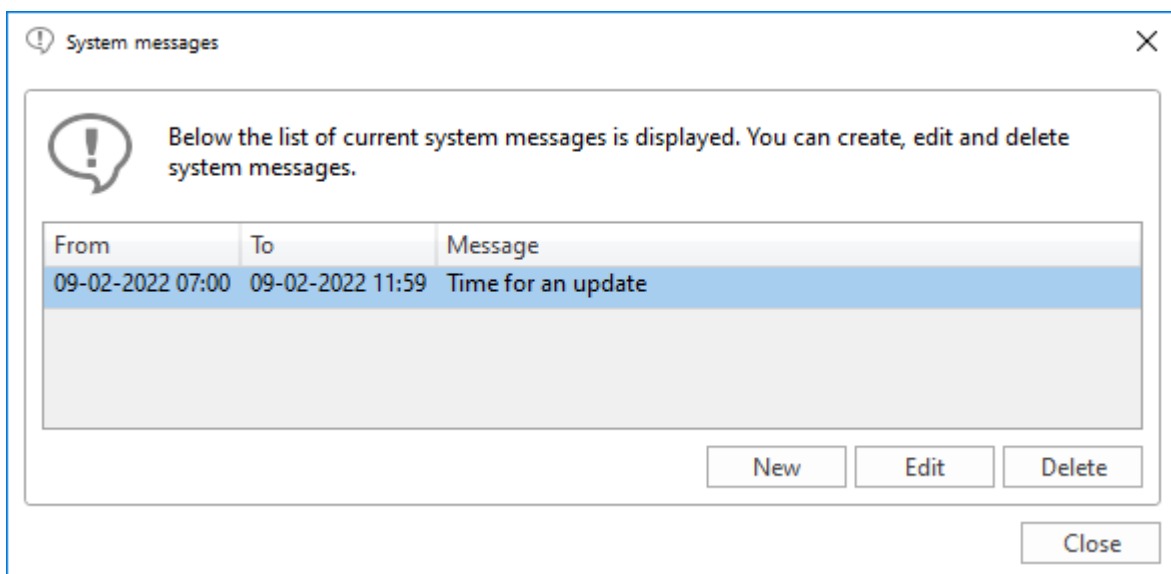


Figure 100. The “System messages” dialogue

The administrator can specify the system message type in the “System messages” dialogue by clicking on **New**. 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.

System message

Type: Push

Title: Time for an update

Shown from: 09/02/2022 07:00

Shown to: 09/02/2022 11:59

Calibri 12 b i u A

Hi everyone,

Your F2 will be updated at 12:00 today.


/IT Office

Save Cancel

Figure 101. 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 accessed by all F2 users regardless of unit.

To open the participant register, click the  **Contact registry** icon 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.

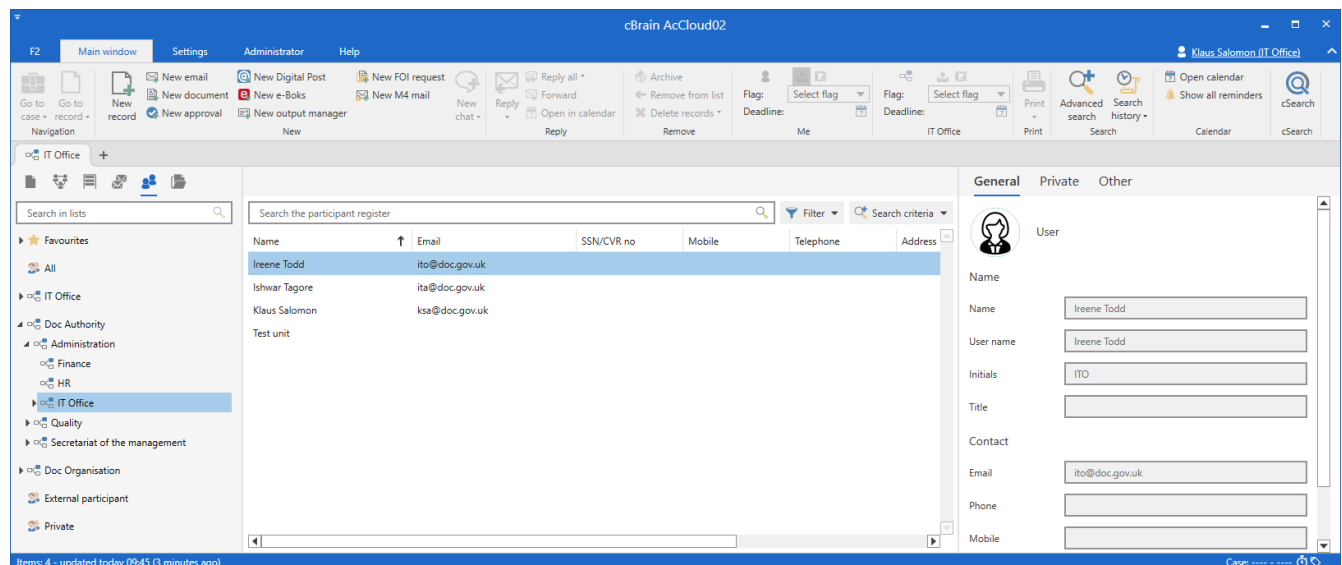


Figure 102. F2's participant register in the main window

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. [Use the “Units and users” dialogue to manage internal participants.](#)
- **External participants:** Participants who are either created manually by a user with the “Editor of participants” privilege or automatically. F2 automatically offers to create 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 “Editor of participants” 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 added to a record or a case, their information is copied from the participant register. However, if the external participant’s information is updated in the participant register, e.g. due to an address change, the updated information is not copied to records or cases to which participant was already added.



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.

Through configurations it is possible to allow all users to create and edit external participants in either the entire participant register or in specific nodes. The configurations are disabled by default. Configurations are performed 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**.

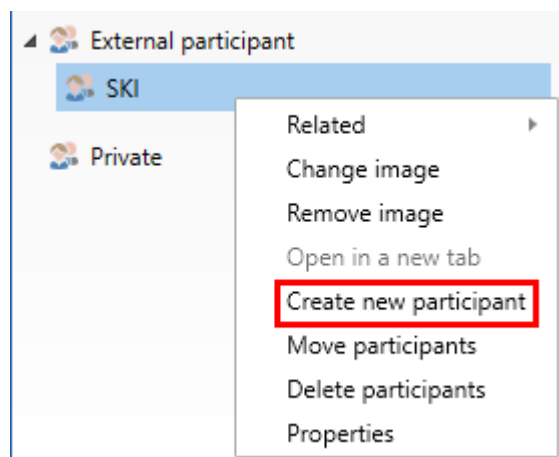


Figure 103. Create external participant

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

Figure 104. The “Create new participant” dialogue

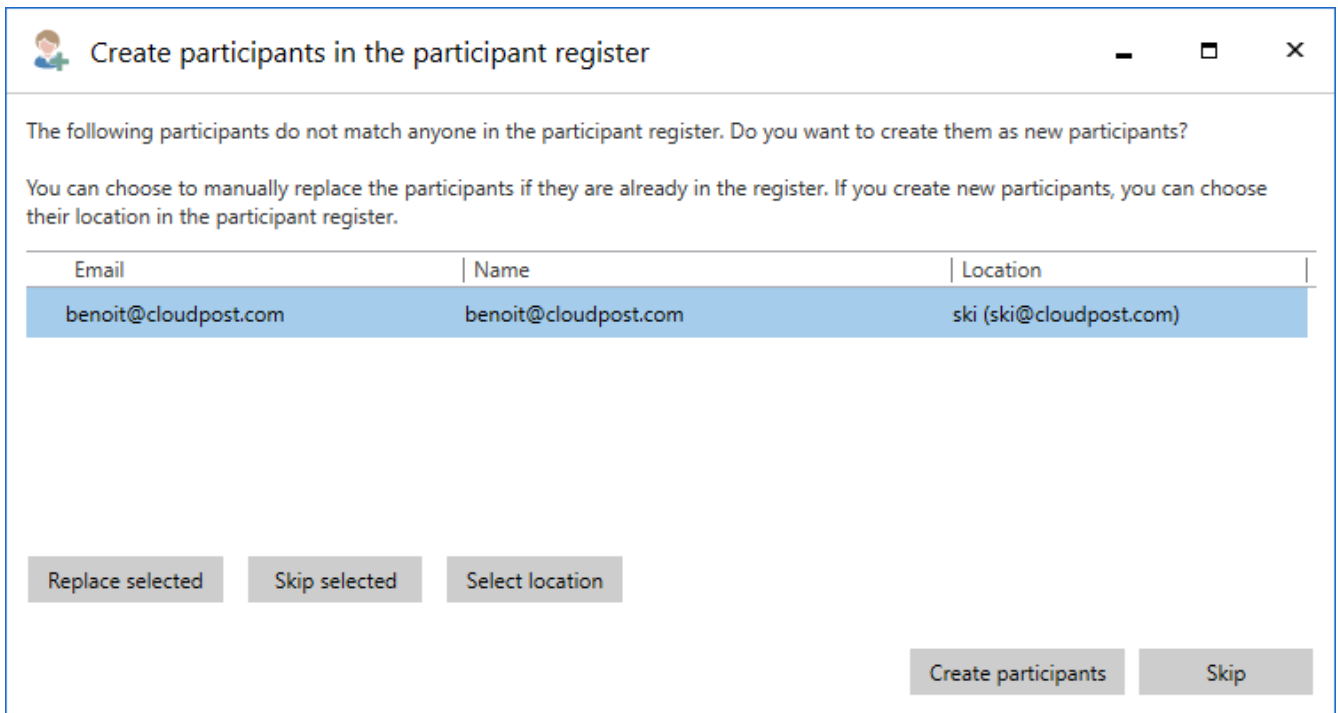
Click on **OK** to register the as an external participant in the selected organisation.

## Create external participant automatically

If an email is sent from or received in F2 and the external sender or recipient is unknown to the participant register, F2 can be set up to automatically suggest creating the unknown participant in the shared participant register. To do this, click on **Setup** on the “Settings” tab in the main window. Go to the “Records” tab and scroll down to the “Create participant” section. Here, tick “Suggest creating participants which don’t currently don’t exist when editing or sending a record”.

The example below shows an email sent to F2 from Benoit. The dialogue informs the user that this participant cannot be found in the participant register. The participant may either be created as a new participant or replaced by an existing participant using the **Replace selected** button, which opens the participant register.

F2 has also registered that that unknown recipient is using the domain @cloudpost.com, and that other known participants have the same domain. Therefore, F2 suggests placing the unknown participant in the same domain group. Using the **Select location** button, it is possible to select a different location.



*Figure 105. F2 suggests placing a new participant under an existing one*

When the email domain is found on an existing participant and the box “This participant is the email domain owner” is ticked, F2 suggests placing the new participant with the same domain under the existing one in the tree structure. For example, the participant SKI owns the @cloudpost.com domain as shown to the right. Click on **OK** in the dialogue above to save Benoit under the same participant as SKI.

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

The screenshot shows a software window titled 'ski' with three tabs: 'General', 'Identification', and 'Other'. The 'General' tab is active. At the top left, there is a circular profile picture placeholder with the text 'SKI' and the label 'External participant' to its right. Below this, the 'General' section contains several input fields: 'Name' (filled with 'ski'), 'Email' (filled with 'ski@cloudpost.com'), 'Phone' (empty), 'Mobile' (empty), 'Address 1' (empty), 'Address 2' (empty), 'Postal code' (empty), 'City' (empty), and 'Country code' (filled with 'DK'). A checkbox labeled 'This participant is the email domain owner' with a question mark icon is checked. An 'OK' button is located at the bottom right of the form.

Figure 106. 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 a participant’s image, open the participant register by clicking on **Contacts** on the navigation line in the main window. From here, right-click on a participant, and select **Change image** in the context menu.

Search for contacts here		
Name	Email	SSN/CVR no
Ministry		
Politics		
Sadie Maxwell	sam@doc.gov.uk	
Sebastian May	sma@doc.gov.uk	
Shapoor Mousavi	shm@doc.gov.uk	
Sienna Morton	sim@doc.gov.uk	
Siún Moynihan	smo@doc.gov.uk	
Stanley Matthews	stm@doc.gov.uk	010203-1235
Stephen Murray	smu@doc.gov.uk	

- Change image
- Remove image
- Related ▶
- Properties

Figure 107. Right-click on a participant in the participant register

In the “Change image” dialogue, click **Browse** to select an image from either a local or external drive on the computer. Use the zoom bar below the image to adjust the size. Then click on **OK** to add or change the image.

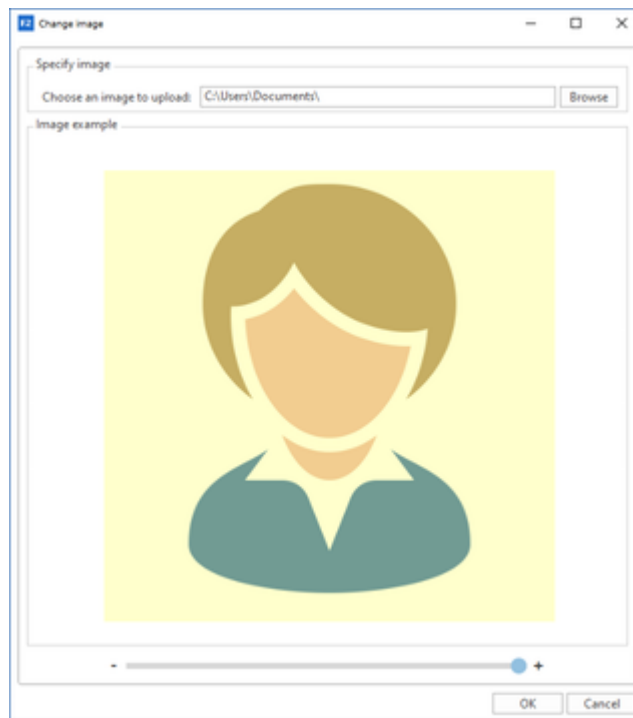


Figure 108. The “Change image” dialogue

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 various purposes:

- As access groups in the “Access restricted to” and “Limited access” fields on records and cases.
- As supplementary units on a record.
- As email, chat and note recipients.
- As participants or stakeholders on meetings that are managed via the add-on modules [F2 Manager \(ad hoc meetings\)](#) and F2 Meetings ([documentation available in Danish](#)).

Teams can be created by users who have roles with the “Team creator” privilege.

Teams are managed in the “Teams” dialogue. Click on **Teams** on the “Settings” tab in the main window.

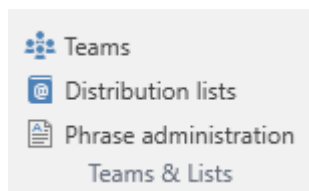


Figure 109. The “Teams” menu item

The “Teams” dialogue opens. Here teams can be created, edited, displayed, and deleted.

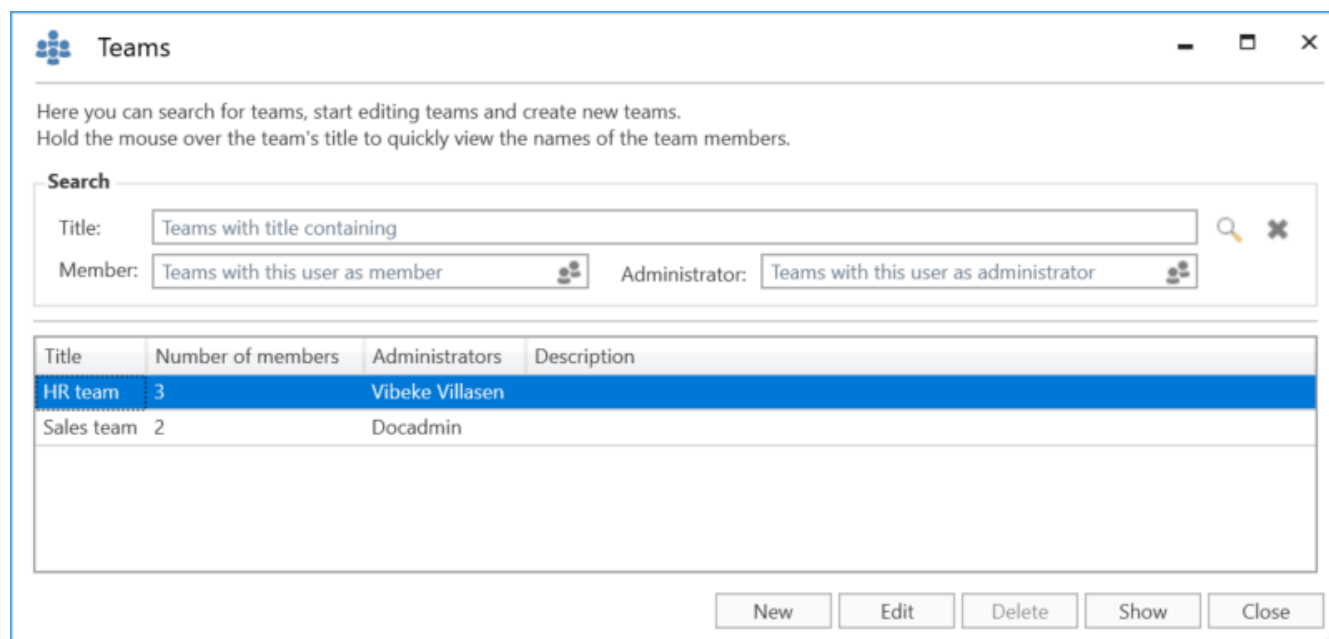


Figure 110. The “Teams” dialogue

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 you want to automatically update the team. Synchronisation is often through AD, but can also be with other systems (e.g. cBrain’s M4 system).
- A tick in the “Active” box to activate the team so it can be used on records and cases.
- Team members, either individual users or distribution lists.

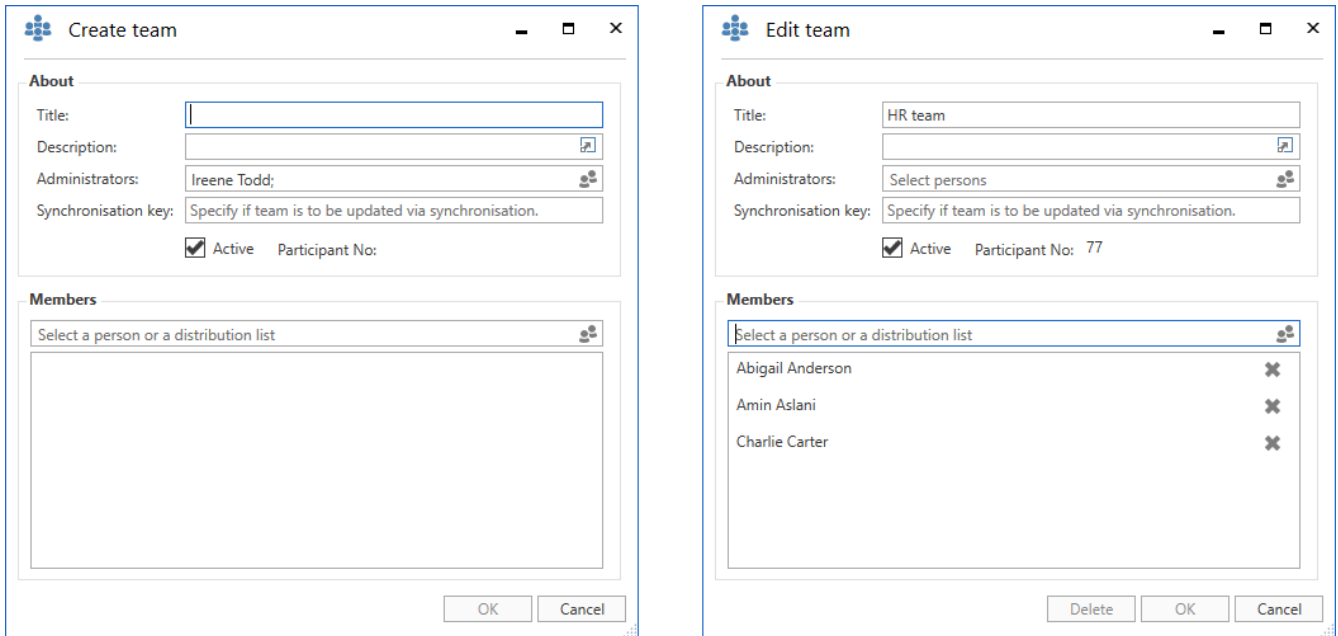


Figure 111. Dialogues for team creation and editing

# 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 [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 result list

## The main window

This section describes how a user with the “Search administrator” privilege can define, create, and manage the fixed or unit-specific searches that are displayed in the main window of the authority’s users.

## Setting up fixed searches

F2 has a number of predefined [standard lists](#). These are accessed on the left side of the main window. New lists can be created by users and administrators when [saving advanced searches](#).

Fixed searches apply to one of the following:

- The individual user (location: “Personal”)
- An organisational unit (location: “Units searches”)
- All (location: “Standard”).

The last two types of fixed searches can only be created by a user with the “Search administrator” privilege, but they can be used by all users in the F2 authority. Fixed searches can also be created from saved search templates (add-on module), if any has been configured. The following sections explain how fixed searches are created.

## Create fixed searches

An administrator can create a fixed search for either a unit or the entire organisation. First perform an [advanced search](#), then click on **Save search**.

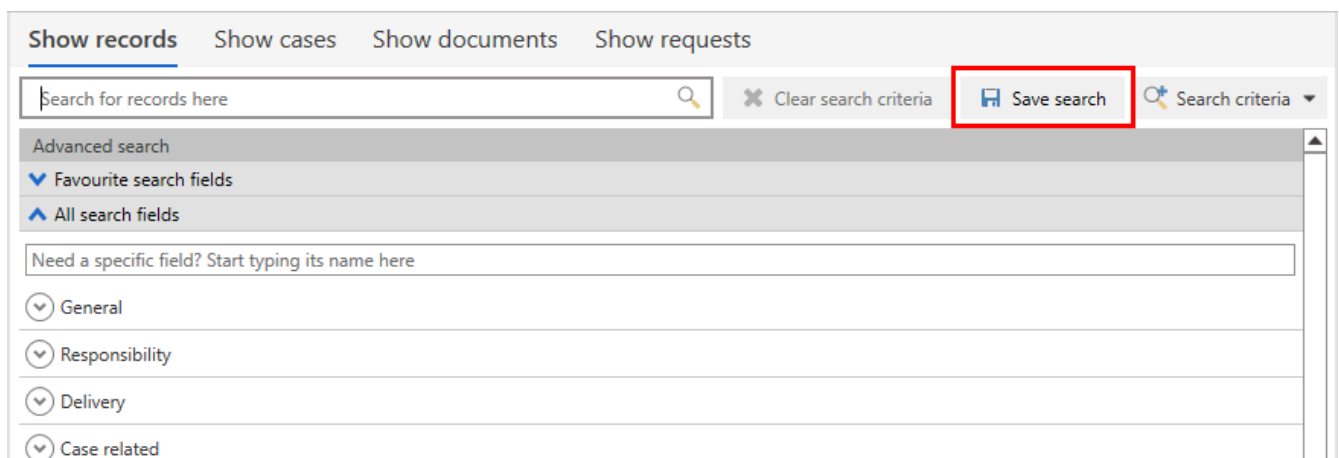


Figure 112. Save search

Give the search an indicative title and determine its visibility. Besides saving it as a [personal search](#), you can make the search available to all users (“Standard”) or specific units (“Units searches”). For the latter, specify the unit(s) to which the search is visible.

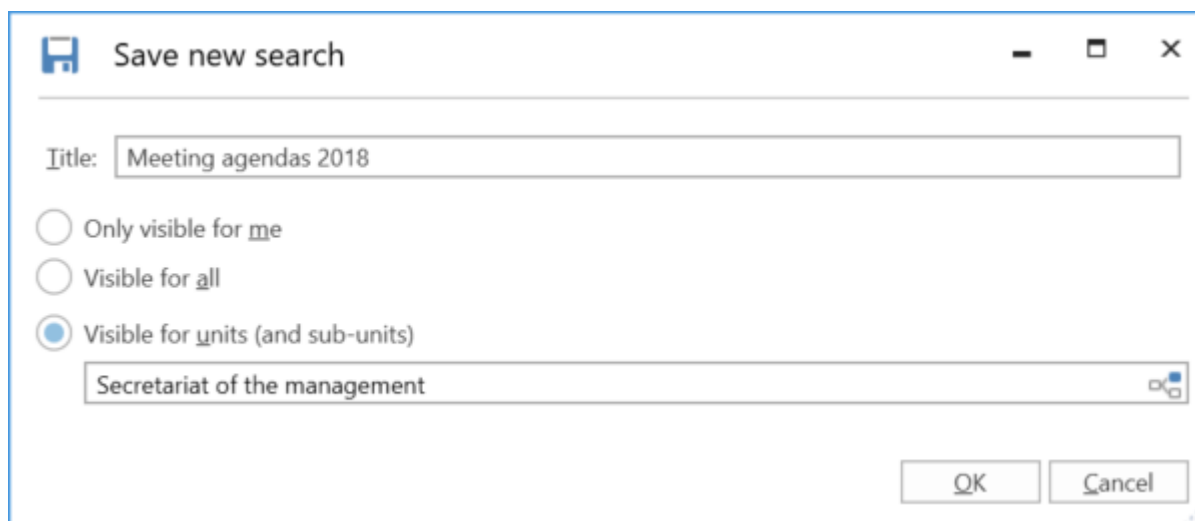


Figure 113. Save a search as a unit search

Click on **OK** to save the search in the main window under either the “Standard” or “Units searches” list node.

Searches can be further qualified by entering more search criteria.

## Standard lists and searches

F2 comes with a number of standard lists and searches defined by cBrain, which an administrator may remove or edit. In addition, an administrator can create fixed searches that are available either to all users in a unit (and any subunits), all users in an authority, or all users in the organisation (multiple authorities)

All users can view standard lists and searches to the left in the main window. They are divided into two nodes, **Standard** and **Units searches**. This division applies to both lists and searches that come with F2 and those created by administrators.

## Delete fixed searches

Any 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 **Units searches**, it can only be deleted by an administrator.

The latter type of fixed search can be deleted as described below.

All unit searches must be shown in the main window before an administrator can access them. Go to the **Administrator** tab and click **Show all unit searches**.

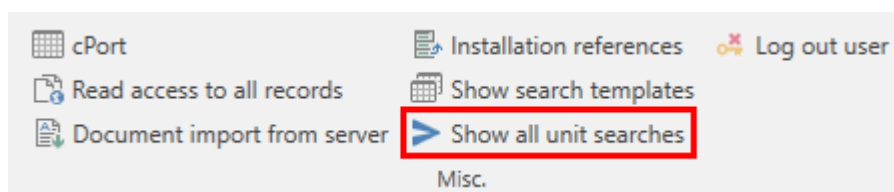


Figure 114. The “Show all unit searches” menu item

The main window’s list view now includes all units across all authorities in F2. The relevant search in any given unit can then be deleted using the context menu.

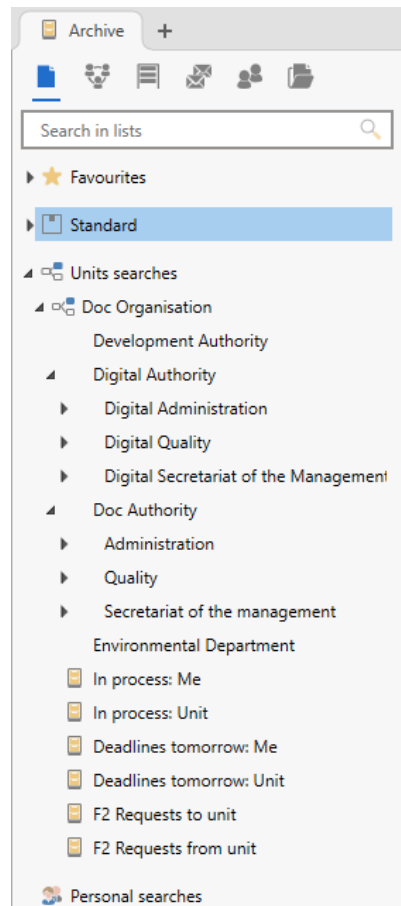


Figure 115. Unit overview

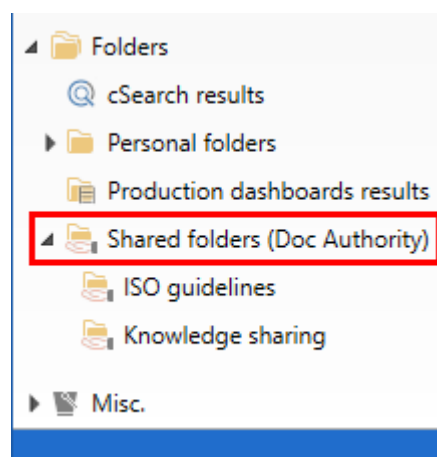
Click **Show all unit searches** again to return to the standard view of the main window.

## Shared folders in the main window

No privilege is needed to create, edit, and delete shared folders. However, it is important that the organisation considers the overall structure or develops guidelines for use of the shared folders.

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.



## Setting up standard column layouts for search results and folders

In F2, the [result list](#) display settings are referred to as the column layout or the column settings. The column layout is used in the main, record, and case windows and contains information on:

- Which columns are show in the result list
- Column sequence
- Column width
- Sorting sequence
- Grouping, if any.

F2 defines the following levels of column settings:

- **Basic column layout:** Predefined column settings that are present in F2 upon installation.
- **Global standard column layout:** Created by an administrator. In F2 also called “Global standard column settings”.
- **Standard column layout:** Created by individual users. In F2 also called “Standard column settings”.

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

- The basis column layout is delivered with F2 and cannot be edited.
- If an administrator creates a new unit search, the current column layout becomes the global standard column layout for the new search.
- If an administrator creates a new global standard column layout, it is applied to all users within the organisation.
- If a user makes changes to their column layout, it can be saved as a standard column layout. If a user changes their column layout without saving it as a standard column layout, F2 remembers the column layout for the current list only.

Read more about [setting up the personal column layout](#).

## Setting up a global standard column layout

A user with the “Result list administrator” privilege can define, create, and maintain the global standard column layout in F2. This layout applies to all users within the organisation who have not created a personal column layout or a standard column layout. The global standard column layout is not applied to the user’s [result list](#) if they have set up a standard column layout or a personal column layout for the list or already accessed the list. Users who want to use the global standard

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

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

- Records
- Cases
- Documents
- Requests.

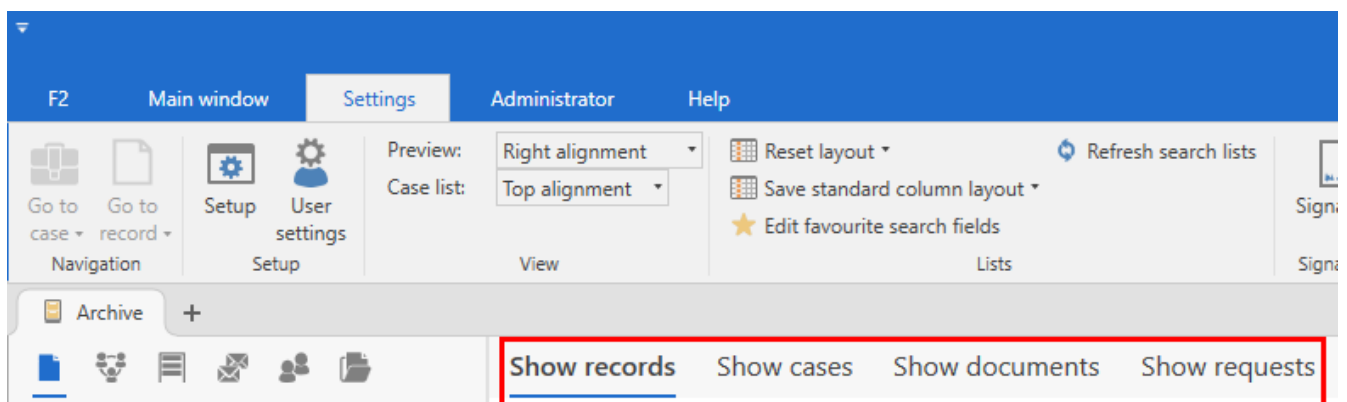


Figure 117. Result list views in the main window

A global standard column layout can be created for each view. The following elements are adjustable:

- 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 any. The administrator can decide whether auto grouping is toggled.

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

1. Click on **Show records** above the result list.
2. Right-click on any column. Then select **Columns** from the context menu.
3. The “Select columns” dialogue opens. Select the relevant columns, then close the dialogue.
4. Rearrange the columns in the result list by dragging one column at a time to the desired location. Adjust the column width by dragging the sides of the column titles.
5. Select the column by which to sort the result list.

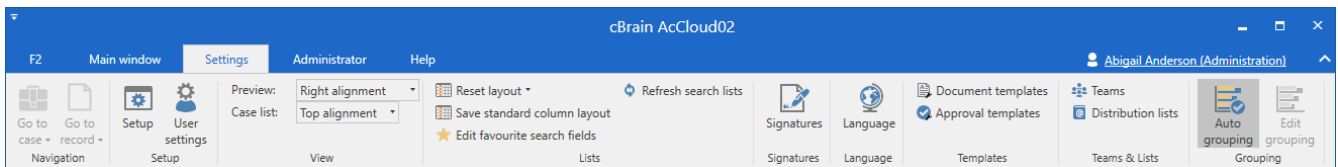


Figure 118. Activate auto grouping

In order to update the new column layout in the database, F2 must be restarted. After a restart, the global standard column layout can be saved by clicking the **drop-down arrow** in the “Save standard column layout” field located on the “Settings” tab. Then click on **Save global standard column settings**.

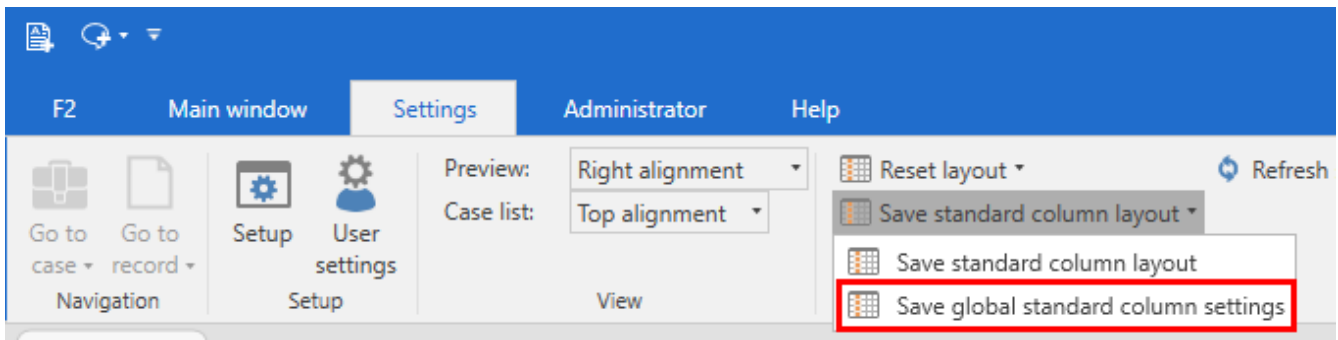


Figure 119. Save global standard column settings

The standard column layout will then be applied to all users without a personal column layout or a standard column layout.

**NOTE** When you save new global standard column settings, you also overwrite the previously saved standard settings. It is always the most recently saved standard column settings that apply.

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

**NOTE** F2 updates can affect metadata fields, i.e. add or delete fields. It is necessary to manually check how updates affect fixed standard searches.

# User settings

The “User settings” menu item provides access to defining and creating a number of user settings. User settings include user setup, column settings, and list settings.

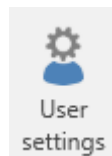
By default, user settings are defined using as a user’s existing setup and settings. It is possible to select all or parts of a user’s setup, column and list settings as content for new user settings. Saved user settings can be obtained by the users themselves. An administrator can also assign certain settings to selected units and role types.

**TIP** Create a dummy user for each type of user in your organisation. This way of creating and pushing settings makes it easier to keep track of the settings that are currently in use.

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 new users are automatically given settings that correspond to their role, while existing users will keep their own settings. 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 are applied. Via the “User settings” dialogue, 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.



*Figure 120. The “User settings” menu item*

This dialogue is used to manage and assign user settings and column settings to users or role types.

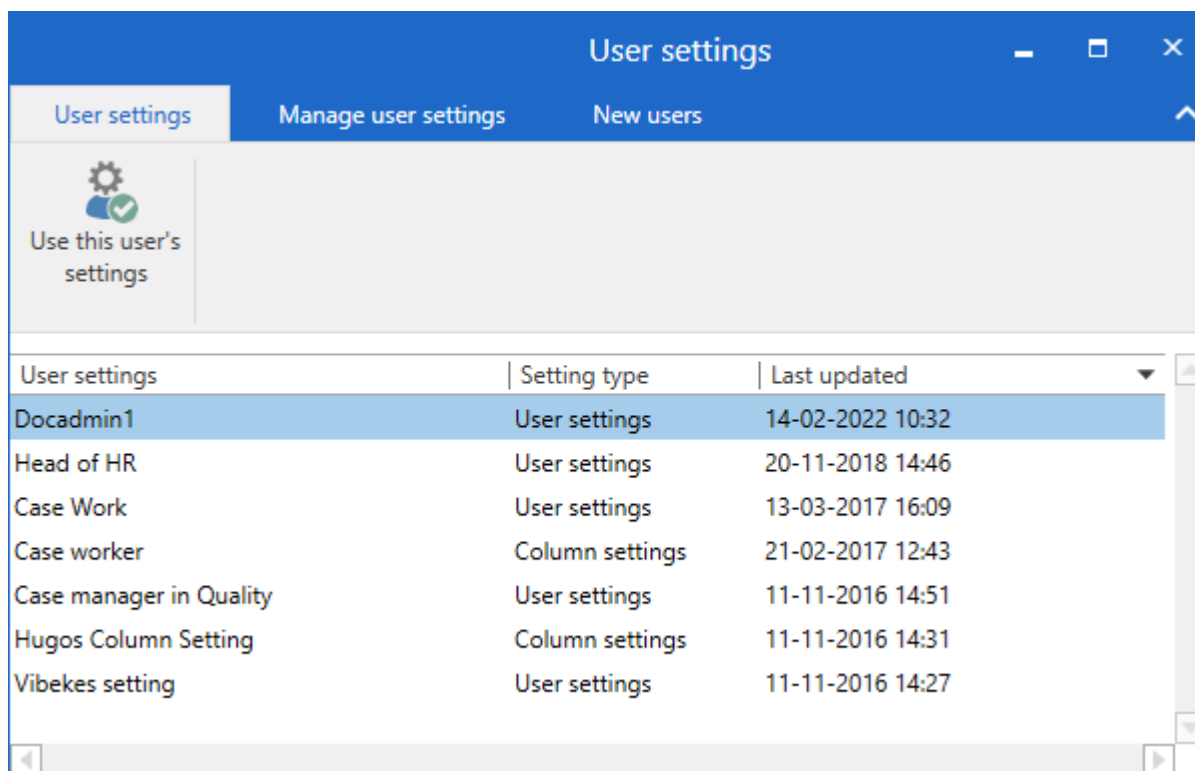


Figure 121. The “User settings” dialogue

The dialogue has three tabs:

- “User settings”. All users have access to this tab. Read more in [Settings and setup](#).
- “[Manage user settings](#)”.
- “[New users](#)”.

## Manage user settings

The “Manage 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.



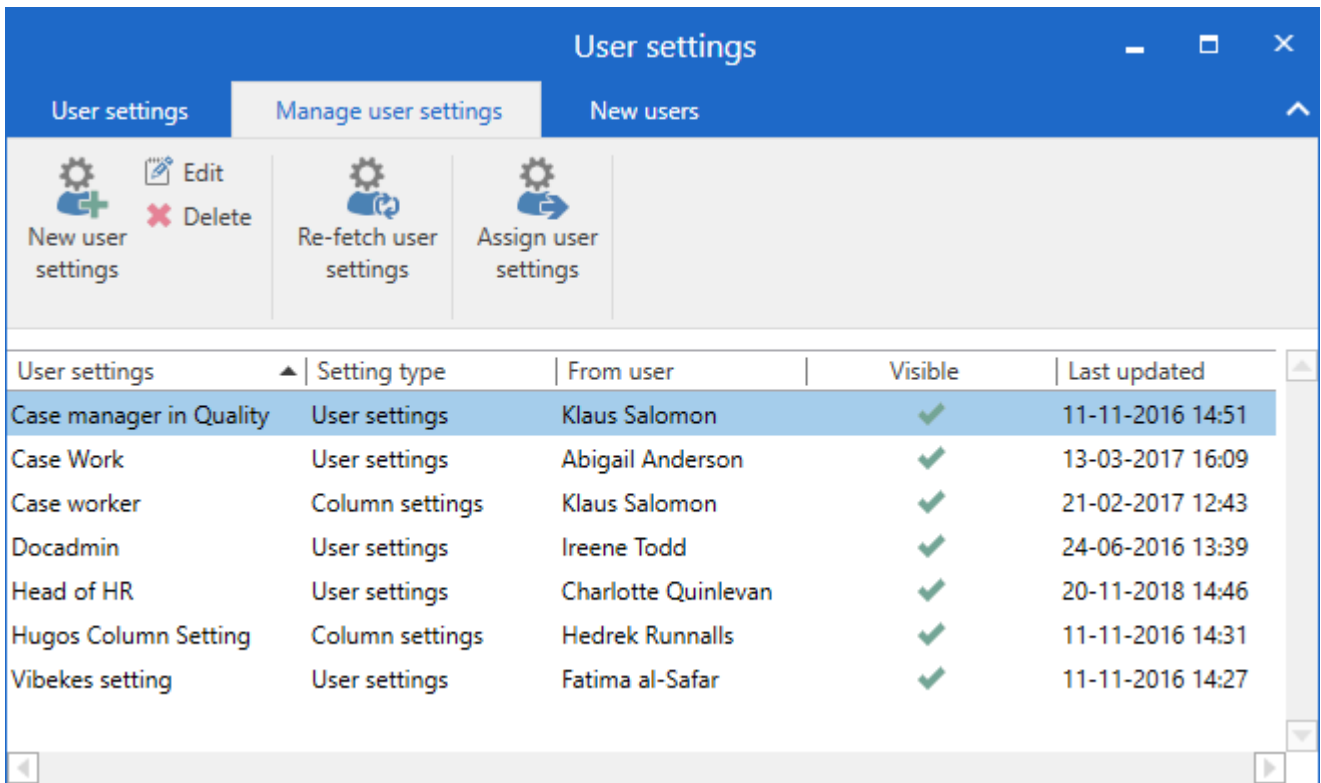
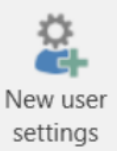

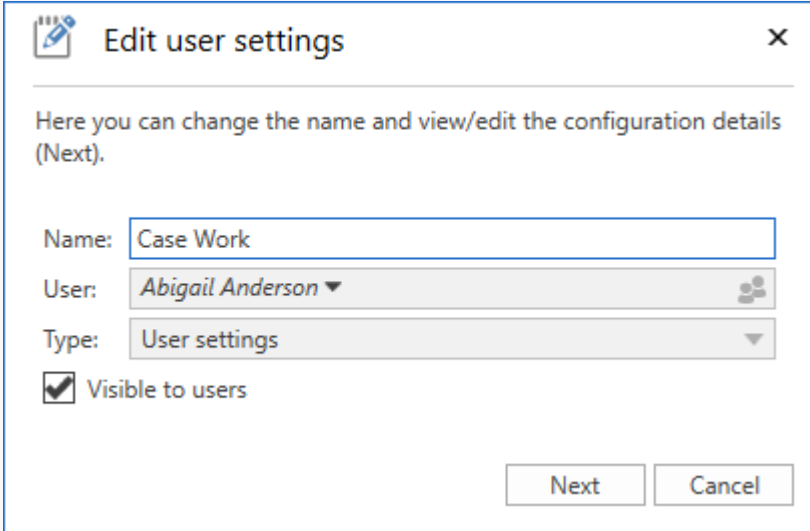
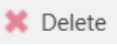




Figure 122. The “Manage user settings” tab

The tab has the following menu items:

Function	Description
	<p>Add a new user setting to the user setting list. Read more in the <a href="#">Create a new user setting</a> section.</p>
	<p>Edit the selected user setting. In the “Edit user settings” dialogue name and visibility can be changed. Click <b>Next</b> to view the individual user settings.</p> <div data-bbox="555 548 1369 1077" style="border: 1px solid #ccc; padding: 10px; margin: 10px auto; width: fit-content;">  </div> <p style="text-align: center;"><i>Figure 123. The “Edit user settings” dialogue</i></p>
	<p>Permanently delete the selected user setting from the list.</p>
	<p>Retrieve the user’s latest user settings, updating the selected user settings.</p>
	<p>Assign the selected user settings to users or role types. Read more in the section <a href="#">Assign user settings to users or role types</a>.</p>

The tab contains the following columns:

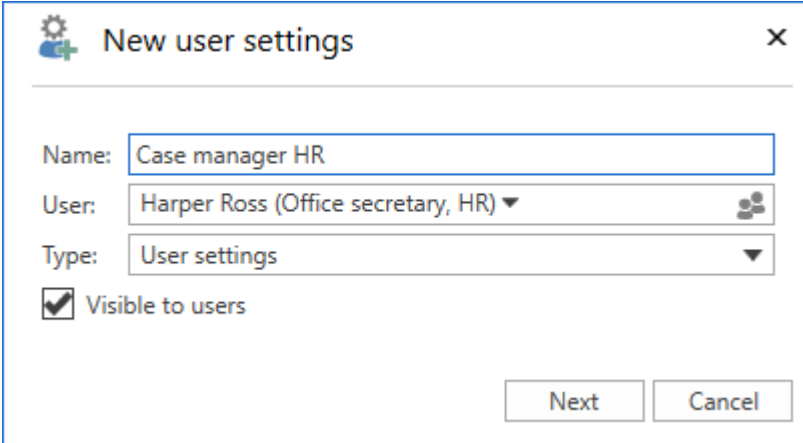
Column	Description
“User settings”	Displays the title of the user setting.
“Setting type”	Displays the type of user setting.
“From user”	Displays the name of the user whose user setting has been copied.
“Visible”	Shows whether the user setting is visible and retrievable to other users.
“Last updated”	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. Three types of user settings exist:

- Column settings
- User settings
- List settings.

On the “Manage user settings” tab, click on **New user settings** to open the dialogue below.



*Figure 124. Create a new user setting*

Add a new set of “User settings” by specifying the following:

- The name of the new user settings.
- The name of the user on whom the settings are based.
- 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 [New user settings](#) section. If “Column settings” is chosen as the type, the “Choose column settings” dialogue opens.

## New user settings

Select “User settings” in the “New user setting” dialogue and click **Next** to open the “Setup” dialogue. Here the different options for the new user settings can be selected.

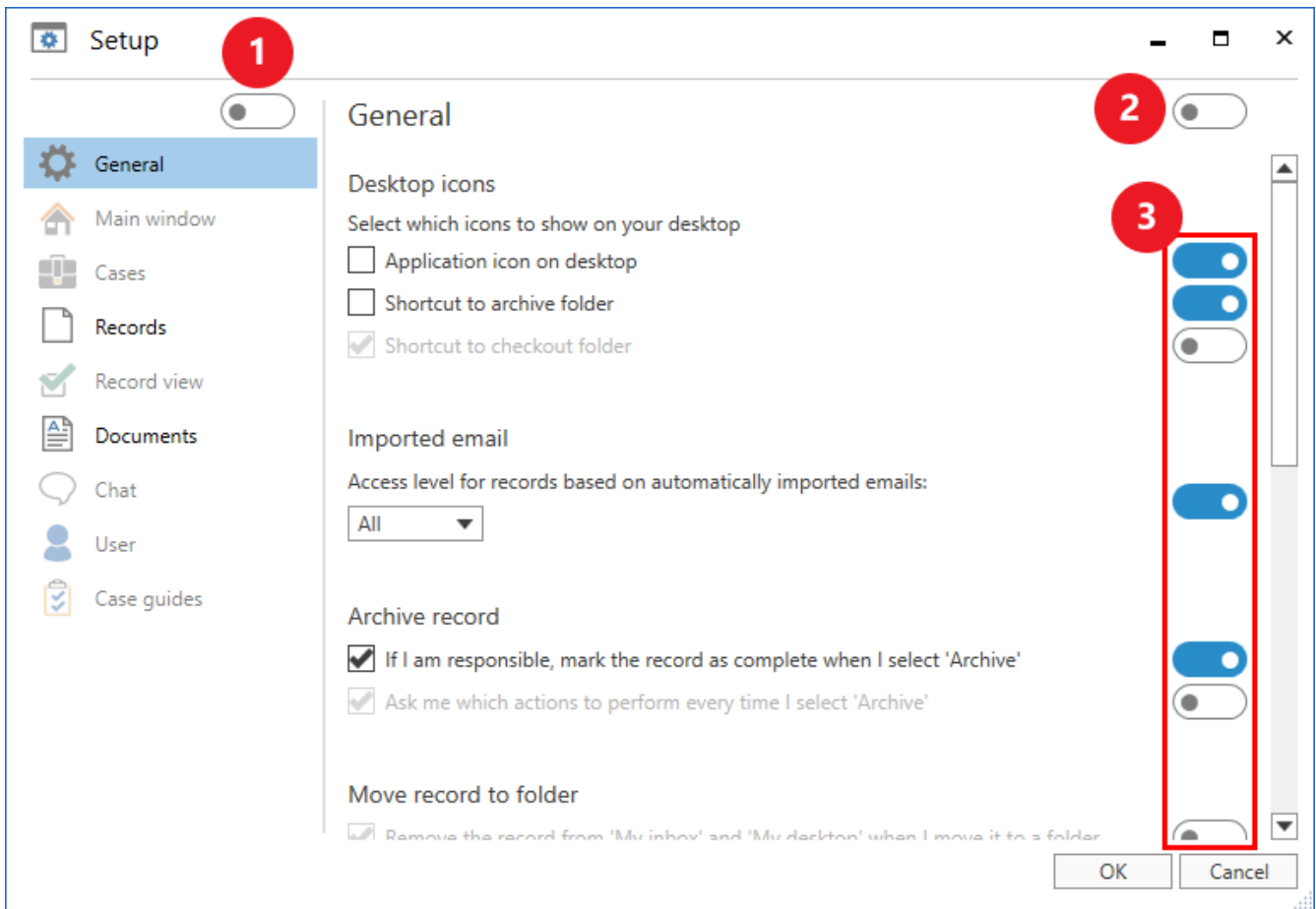


Figure 125. The “Setup” dialogue with sliders

It is possible to include the entire setup of the selected user in a new user setting. To do this, click on the slider above the tabs in the upper left corner of the “Setup” dialogue (1). 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 all settings of a single tab in a new user setting. To do this, first click on the relevant tab to the left, then click on the slider in the upper right corner of the dialogue (2). All sliders for that tab will turn blue, indicating that all the tab’s settings are included in the new user setting.

In addition, it is possible to include individual setting options on a given tab in a new user setting. Click on the relevant tab, then click on the slider for each setting (3) to be included in the new user setting. The sliders for the selected settings will turn blue.

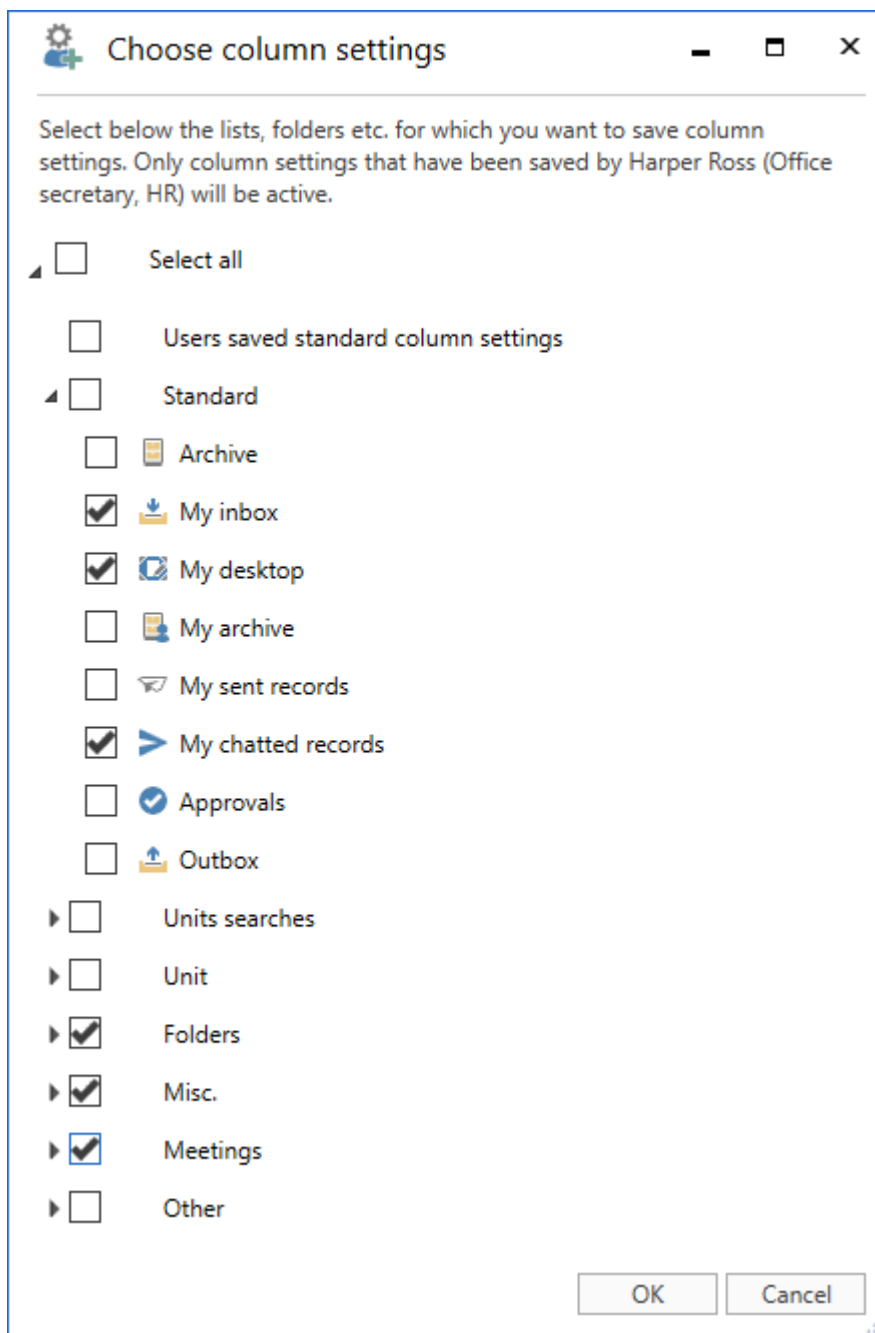
Once the wanted settings are chosen, click on **OK** at the bottom of the dialogue to save the settings for the new user settings. The set of new user settings is then added to the list of available user settings which may be retrieved by users or an administrator can assign to selected users and roles.

## New column settings

When “Column settings” is chosen as the setting type, click **Next** to open the “Choose column settings” dialogue. Here it is possible to select which lists, folders, etc., to include in the new column settings.

The only active columns are those saved by the user whose settings serve as the basis for the new standard settings. The user’s column settings must be updated in the database. That means the user must restart F2 in order to save the column settings in the database.

The column settings include all views of the user on which they are based, i.e. “Show records”, “Show cases”, “Show documents”, and “Show requests”. If the user did not set up any column settings for one of the views, e.g. “Show documents”, no column settings for this view is included in the new column settings.



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 or retrieve columns separately. All columns belonging to a list must be assigned or retrieved collectively.

**NOTE** When a new set of column settings is retrieved or assigned as a user setting, F2 must be restarted for it to take effect.

## New list settings

When “List settings” is chosen as the setting type, click **Next** to open the “Select list settings” dialogue. Here it is possible to select which lists, folders, etc., to include in the new list settings. The settings for the selected lists are included in the saved list settings.

For each selected list, the following settings are saved:

- Whether the preview is shown or hidden and its alignment.
- Whether the result list shows records, cases, documents, or requests.
- Case list alignment.
- Whether advanced search is enabled.

Only list settings saved by the user on whom the settings are based will be shown. The user’s list settings must be updated in the database. That means the user must restart F2 in order to save the list settings in the database.

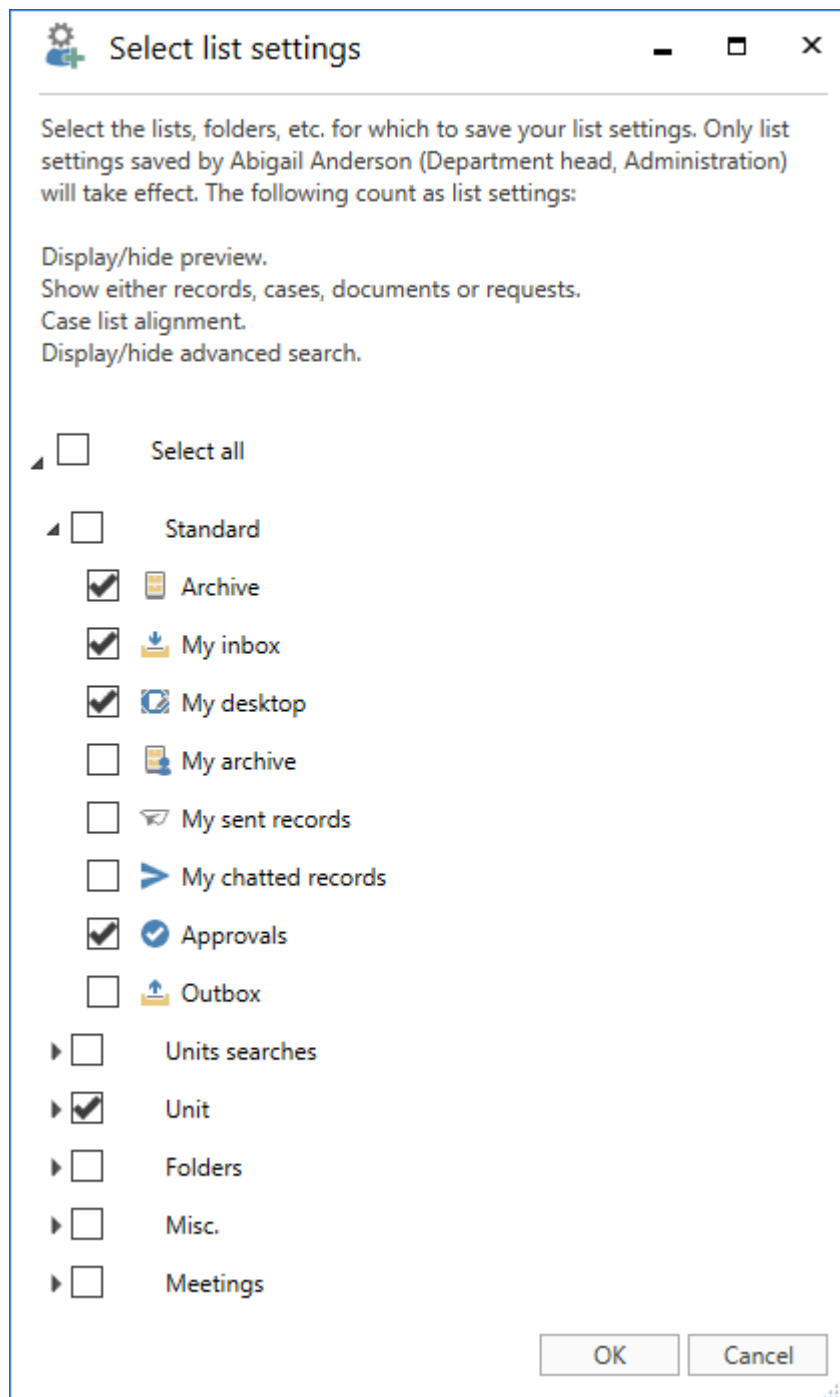


Figure 127. The “Select list settings” dialogue

Click **OK** to complete. The new list settings is then added to the list of available user settings which may be retrieved by users or an administrator can assign to certain users and role types.

**NOTE** When a new list 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 user settings:

- Allocate to users: Assign user settings to users, units, distribution lists, and teams.

- Allocate to role type: Assign user settings to users with a certain role type, for example a user with the “Technical administrator” role type in a certain unit, distribution list, or a team. User settings can also be assigned to all users with the specific role type.

Select the wanted set of user settings from the list on the “Manage user settings” tab. Then click on **Assign user settings**.

A new dialogue opens. Choose either “Allocate to users” or “Allocate to role type”.

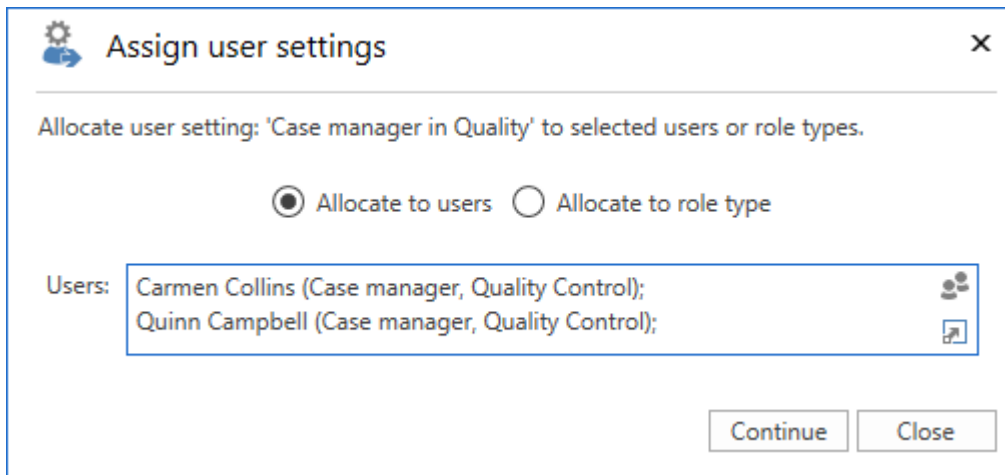


Figure 128. Assign user settings to users

Select “Allocate to users” to enter the users, units, distribution lists, or teams to receive the user setting in the “Users” field.

Select “Allocate to role type” to allocate the user setting to a role type from the drop-down menu in the “Role type” field.

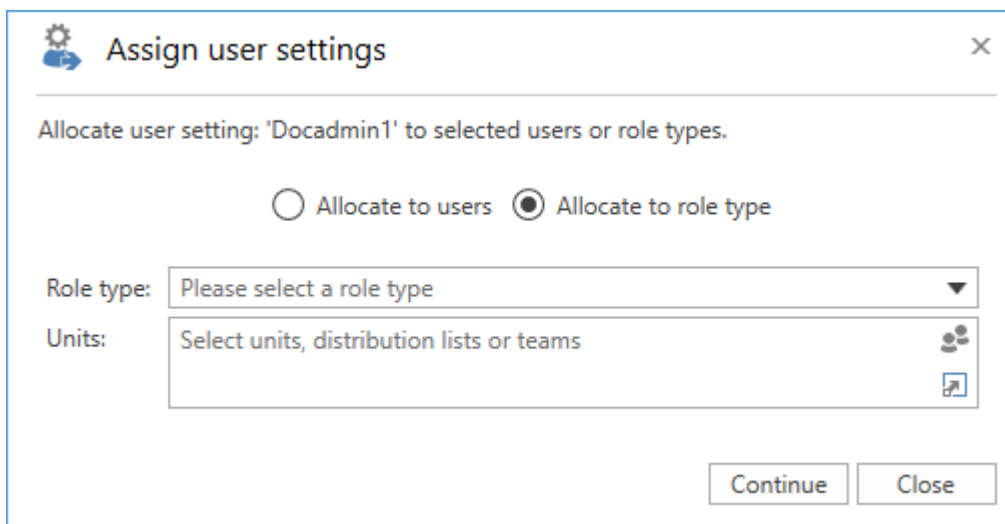


Figure 129. Assign user settings to a role type

Click on **Continue**.

The users that will receive the user settings are displayed in the dialogue. It is possible to add a message to the users. Complete the allocation by clicking **Allocate**.



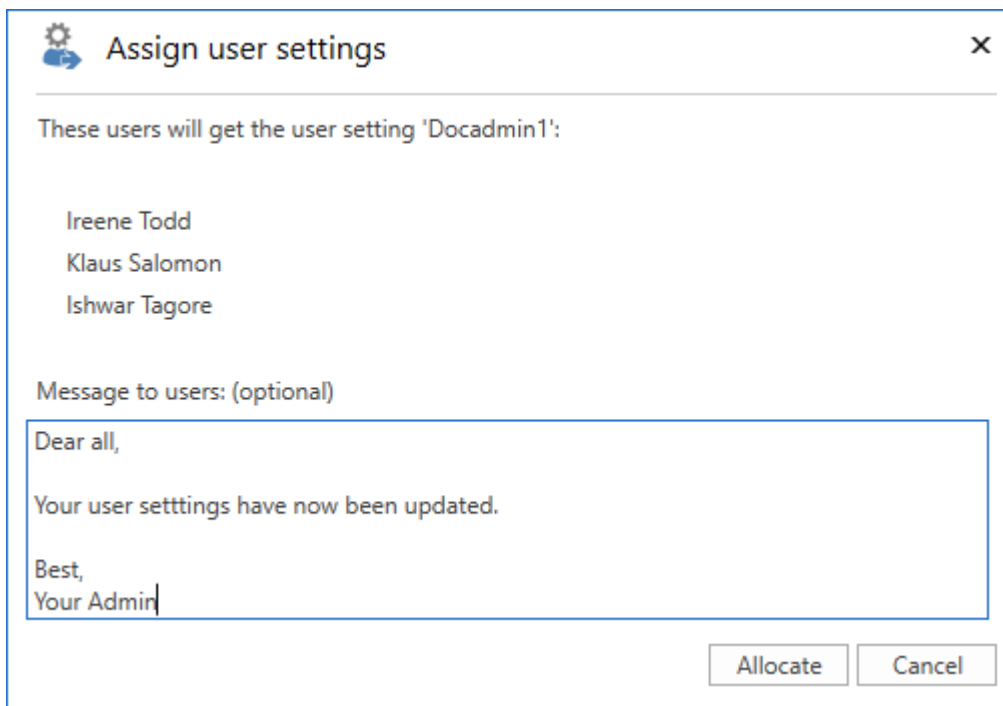


Figure 130. Send a message to the selected users

The user settings are then assigned to the selected user(s). This is shown by a Windows notification that appears at the lower right corner of the screen. When the user settings have been assigned, click the **Close** button.

Users automatically receive a record in their inbox when they are assigned new user settings.

The record contains the following information:

- The user's existing settings have been updated with new user settings.
- 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 settings performed by the users themselves.

## New users

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

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

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

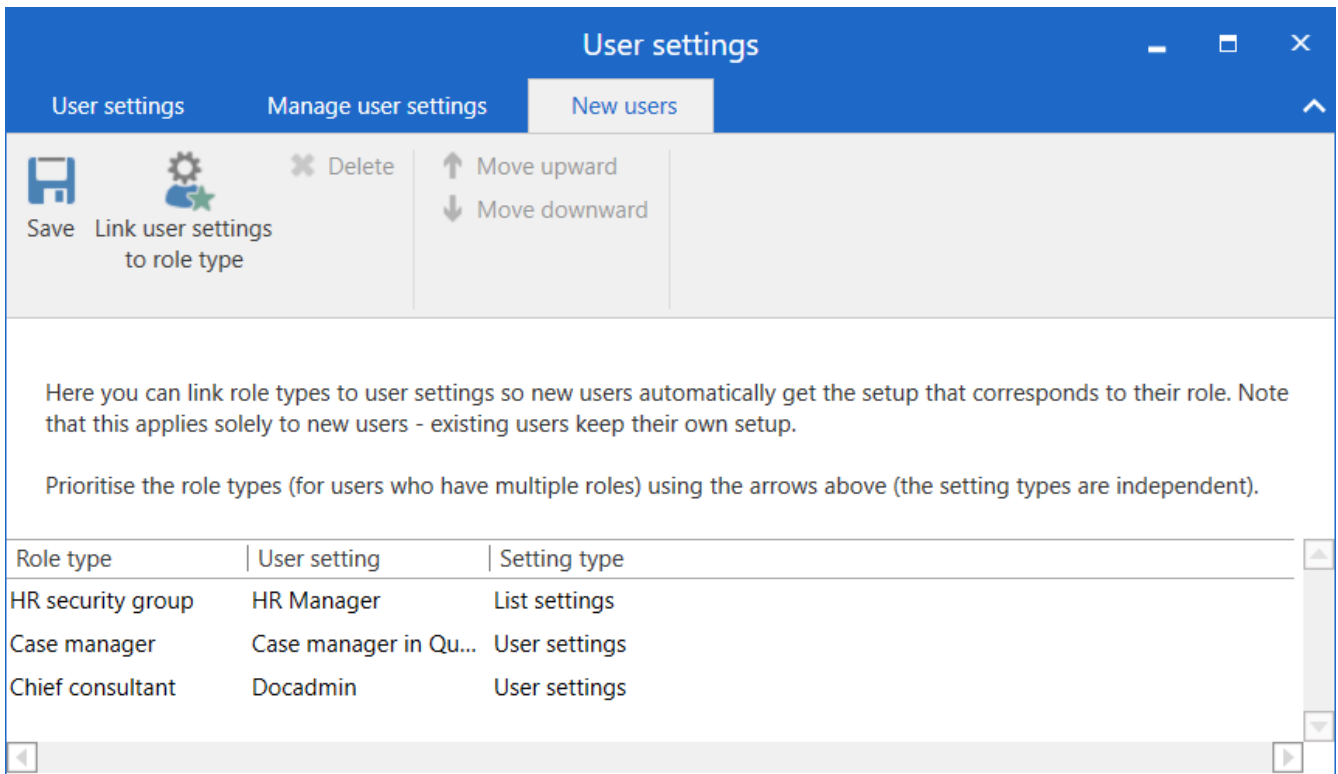

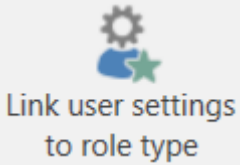
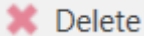




Figure 131. The “New users” tab

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

Function	Description
 Save	Saves any changes, including the association of user settings to a role type.
 Link user settings to role type	Links user settings to a role type. Specific user settings can be assigned to a specific role type to ensure that all newly created users with this role type receive these user settings.
 Delete	Deletes the connection between the user settings and the role type. Users who are assigned this role will no longer receive the formerly attached user settings.
 Move upward  Move downward	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.

## Attach user settings to a role type

Click on **Link user settings to role type** to attach a user setting to a specific role type, linking the two together.

A dialogue opens. Here you choose which user setting and role type you want to link.

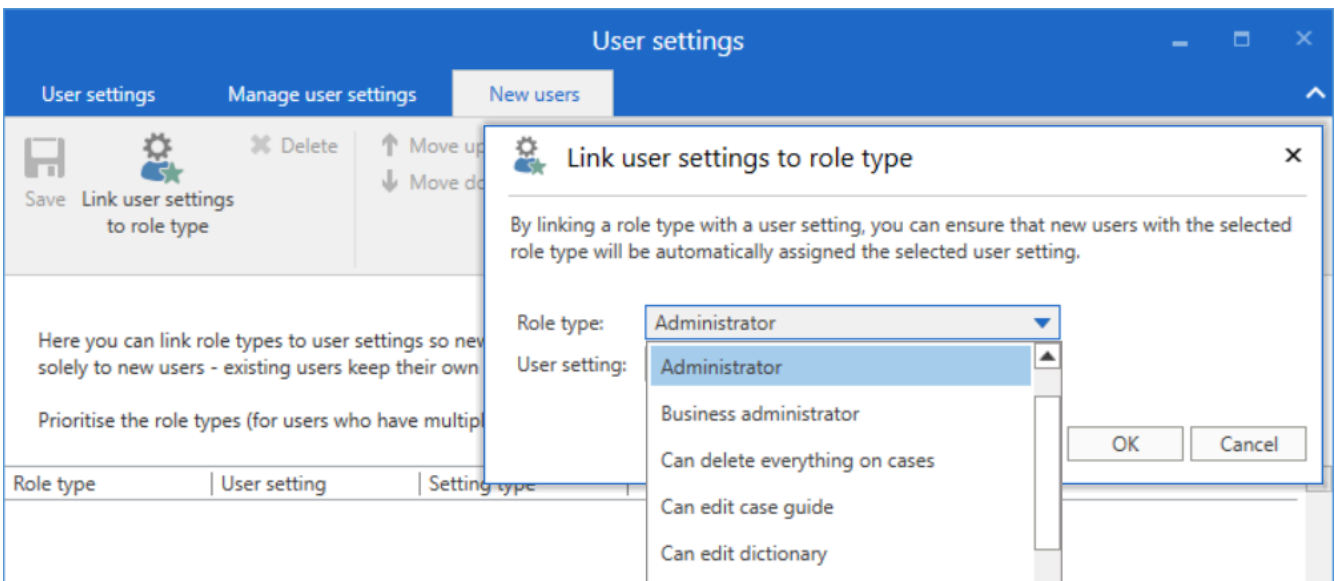


Figure 132. Link user settings to role type

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

The rules for user settings:

- User settings linked to role types only affect new users. Existing users whose job role receives 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 in this dialogue. The role which the user uses for login does not affect this priority.
- No matter which user settings were assigned, the user can always change their settings.

# 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 users themselves can create, maintain and delete a personal document template.

Document templates must be in Office format.

Templates are managed via the “Document Templates” menu item located on the “Settings” tab in the main window.

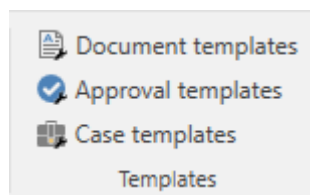


Figure 133. Manage templates

To an administrator, the dialogue window will appear as follows:

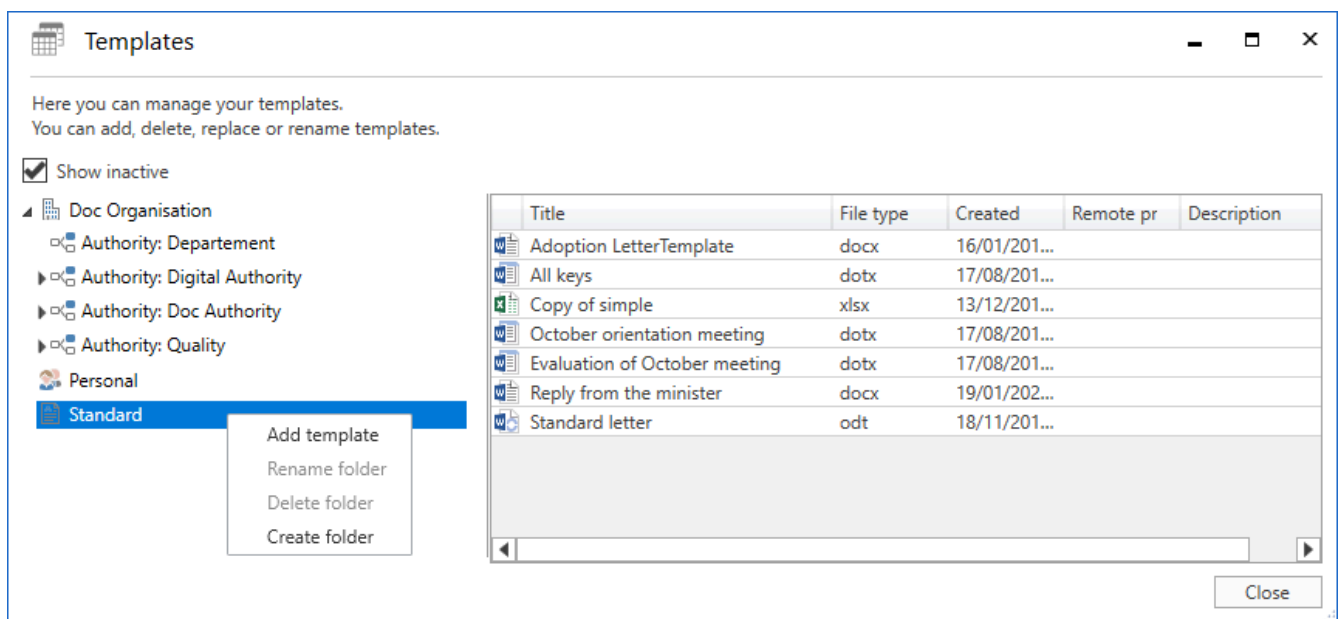


Figure 134. Managing document templates

Managing document templates is described in [Settings and Setup](#).

# Configure F2

In F2 users with special privileges can alter the basic setup and configuration of F2. Users with certain 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.

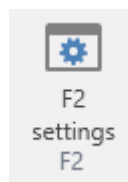


Figure 135. The “F2 Settings” menu item

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.

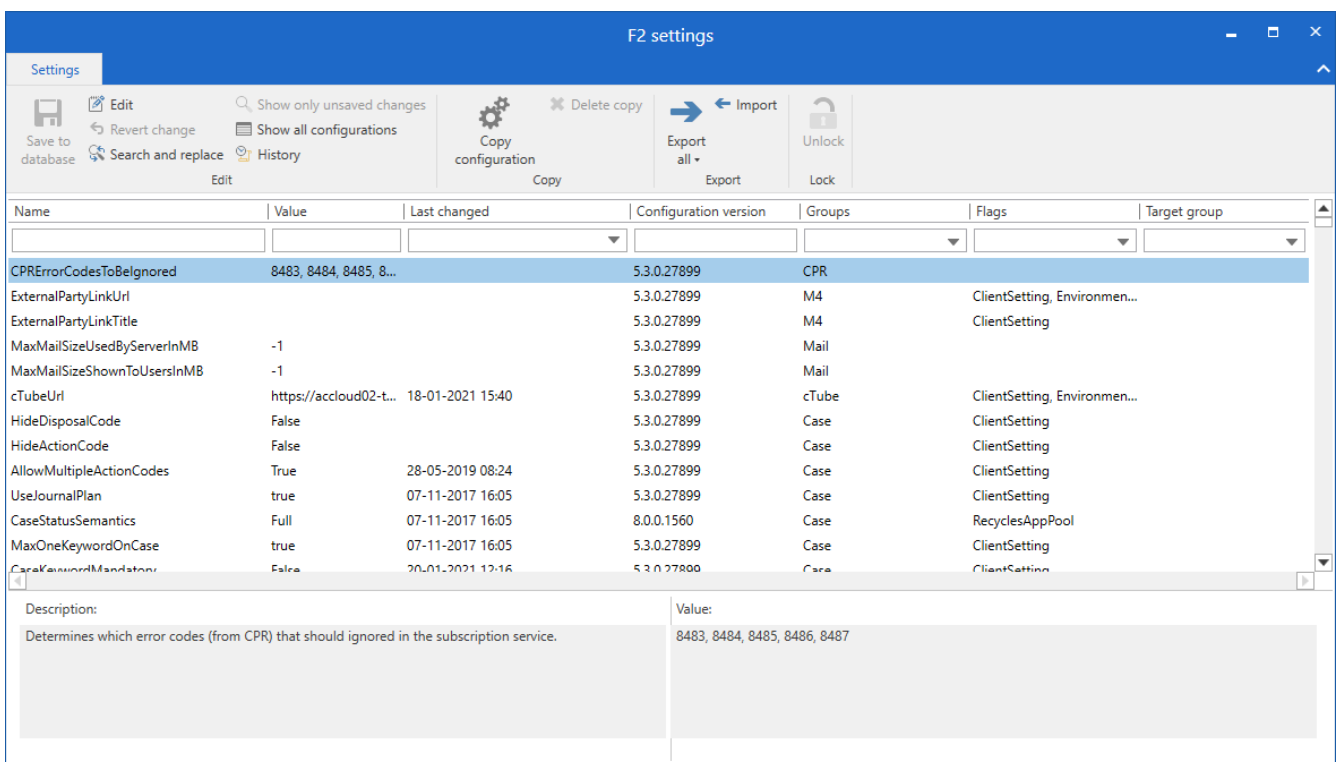


Figure 136. The “F2 settings” dialogue

## 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.