



F2

Administrator

Version 9

Table of contents

Welcome to cBrain F2.....	6
Reading instructions.....	6
Installing cBrain F2	7
The basic installation of F2	7
Introduction to administrative tasks	8
F2 administrator	8
Administrator tasks in F2	8
The user interface for F2 administrators.....	9
The unit structure in F2	10
Create an authority	11
Create units within an authority	13
Create unit types for specific units	15
Decentral units	16
User administration.....	18
Create user	18
Create user – information	19
Create user – roles.....	21
Deactivate user	22
Activate user	23
On behalf of	26
Setting up “On behalf of”	26
Managing emails.....	29
Setting up mailboxes for authorities and units	29
Link email replies to emails sent from F2	32
Add a suffix in the subject field of external emails.....	33

Set up automatic transfer of replies to F2 emails	34
Roles in F2.....	35
Administrator roles.....	35
Other default role types in F2	37
Assigning roles	39
Assign role to several users	40
Assign role to a single user.....	41
Create and assign role types	42
Privileges.....	45
Assign a privilege to a role type	45
Edit or remove privileges from a role type.....	46
Privilege overview	47
Further explanation of selected privileges	52
Administrator read access to all records	52
Archive access	53
Creates cases	53
Distribution list editor	54
Editor of participants	54
Keyword administrator.....	55
No case help for saving or sending records.....	55
Security groups	56
Create a security group	57
Add users to security groups	58
Add user to security group using manual role assignment	59
Show security groups	59
Deactivate security group	61

Import participants and replace record participants	63
Import participants	63
Replace record participants	66
Value lists	67
Value list administration	67
Sorting value lists	68
Create a new value list	69
Value list items	69
Importing a value list item to F2	70
Creating a value list item in F2	71
Setting up flags	73
Keywords	75
Administration of keywords	75
Relevant keywords for units	76
Assign keywords to a unit	77
Remove keywords from a unit	77
System messages	78
The participant register	79
External participants	80
Create external participants manually	80
Create external participant automatically	81
User and participant images	82
Teams	85
Distribution lists	87
Setting up the main window and the result list	88
The main window	88

Setting up fixed searches	88
Shared folders in the main window	92
Setting up standard column layouts for search results and folders.....	92
Setting up a global standard column layout	93
User settings.....	97
Manage user settings	98
Create a new user setting	99
Assign user settings to users or role types	103
New users.....	105
Attach user settings to a role type.....	106
Document templates	108
F2 Settings	110
List of figures	111

Welcome to cBrain F2

cBrain F2 is an electronic document and records management system (EDRMS) based on a fully integrated e-government model. The F2 software is designed to accommodate the user's need for an organised and flexible tool.

The F2 standard system is developed to support full digitisation of the work performed by public authorities, private organisations and companies. In addition to facilitating best practices for digital case and document management as well as communication and knowledge sharing, F2 supports public authorities' special requirements related to administrative tasks, registration and archiving.

Reading instructions

This manual is written for users of F2 Desktop who will be performing administrative tasks for other F2 users. These tasks may include customising the user interface, user administration and assigning roles or creating units and shared distribution lists. All functions available to an administrator through F2's user interface are addressed, with special emphasis on functionality and configuration.

The manual is based on an F2 solution with all available add-on modules installed. Users may notice some differences between their own F2 client and the one presented here depending on the add-on modules included in their organisation's F2 solution.

In this manual, the names of commands are **bolded**. Commands are clickable features such as buttons. The names of fields and lists are placed in "quotation marks".

References to other sections within the document and references to other documentation are *italicised*.

We hope you enjoy using F2.

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. For more information see the section *Roles in F2*.

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

Introduction to administrative tasks

F2 administrator

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

In F2 there are four predefined administrator roles:

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

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

Administrator tasks in F2

Many of the administrative functions can be performed in F2'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 setup in the result list.
- Setup of the user interface for the record window:
 - Document templates.
 - Keywords.
 - Flags for personal and unit management.
- The administration of various value lists e.g. keywords, progress codes (add-on module), file plan and cPort (add-on module).

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

The user interface for F2 administrators

Administrators and standard F2 users share the same user interface. However, administrators 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.

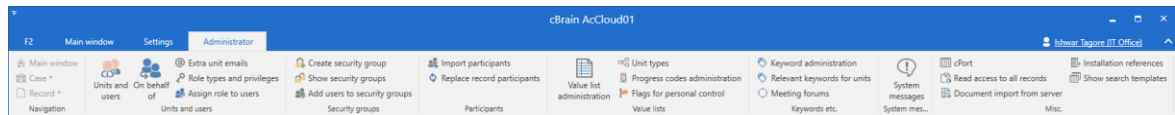


Figure 1: The ribbon on the "Administrator" tab in the main window

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

The unit structure in F2

It is important that the user possesses a general knowledge of F2 in order to understand the administrative tasks. For this, please refer to the F2 Desktop user manuals.

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 reasoning behind this is that F2 generally relates read and write access to documents depending 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.

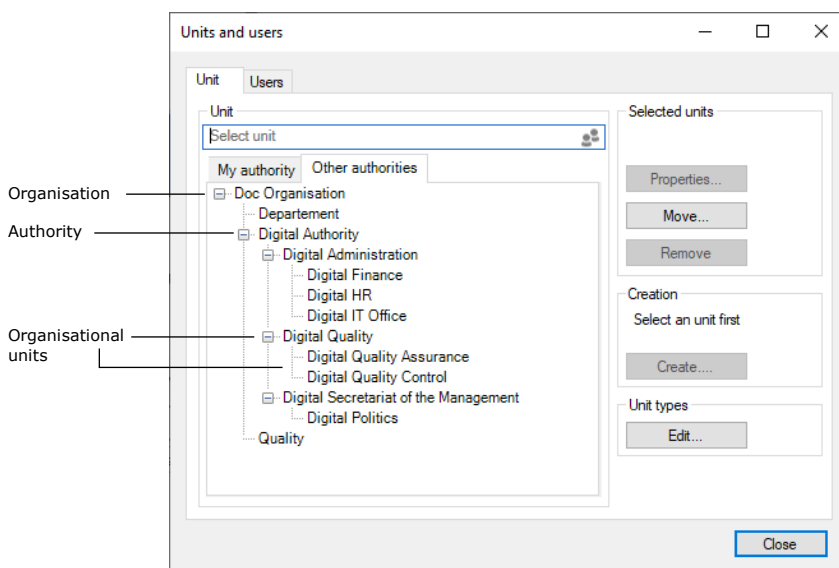
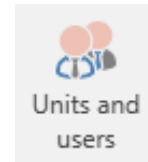


Figure 2: An example of F2's tree structure

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.



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

Figure 3: The "Unit and users" menu item

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.

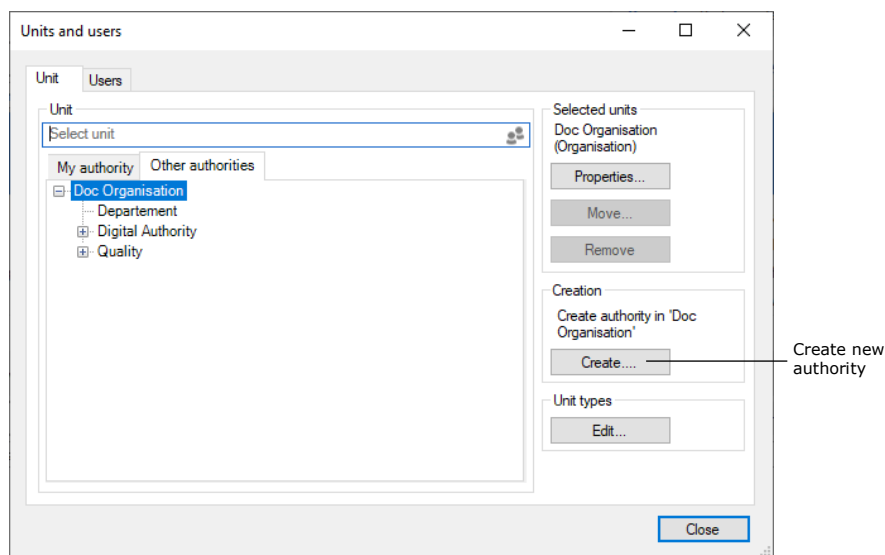


Figure 4: Create a new authority

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.

Figure 5: The "Create unit" dialogue

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

Figure 6: The "Email settings" tab in the "Create unit" dialogue

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

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

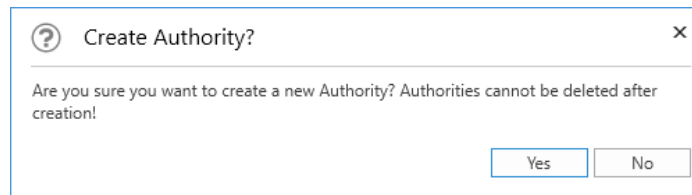


Figure 7: The "Create authority?" dialog

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

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

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.

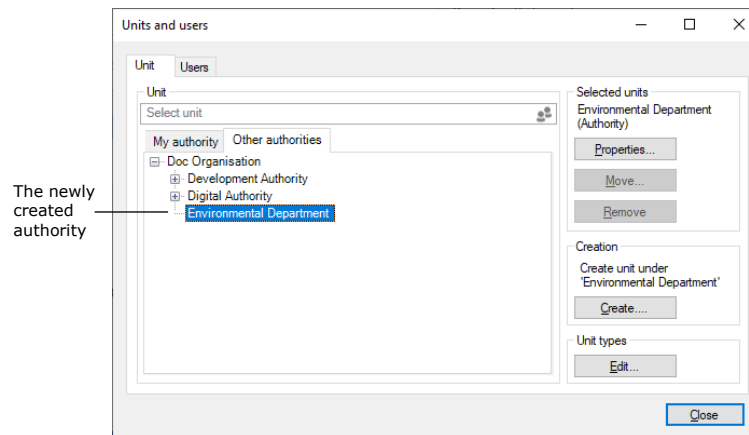


Figure 8: The newly created authority

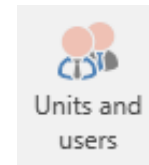
Create units within an authority

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.



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

Figure 9: The “Units and users” menu item

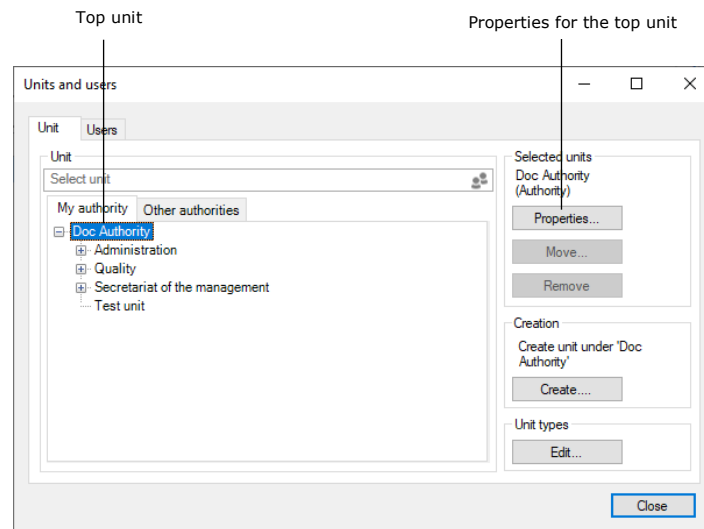


Figure 10: F2 is installed with only one top unit

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 organisation’s name when F2 is installed. In the figure above, “Doc Authority” is the top unit. Edit the name by selecting the unit and then clicking on **Properties**.

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**.

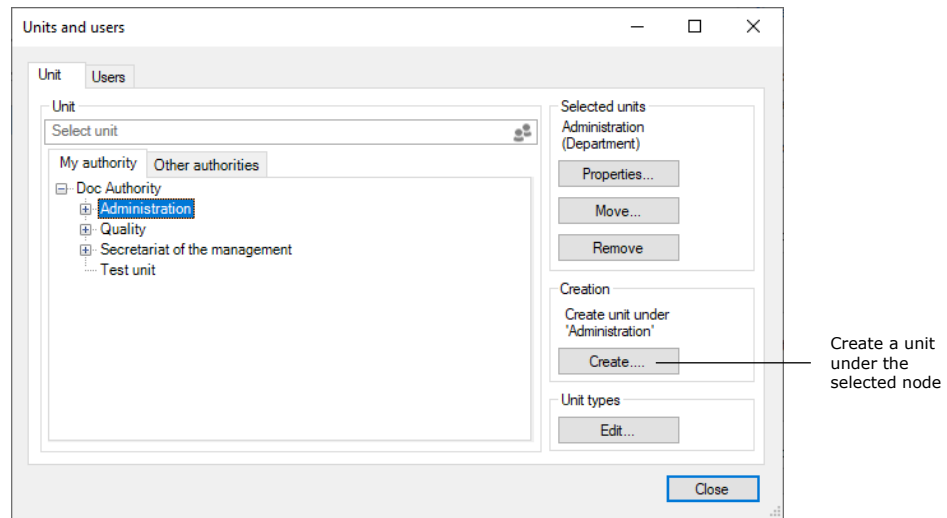


Figure 11: Create units within an authority

The “Create unit” dialogue opens as shown to the right.

Fill in the relevant information in the dialogue.

In the “Unit type” field, select 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.

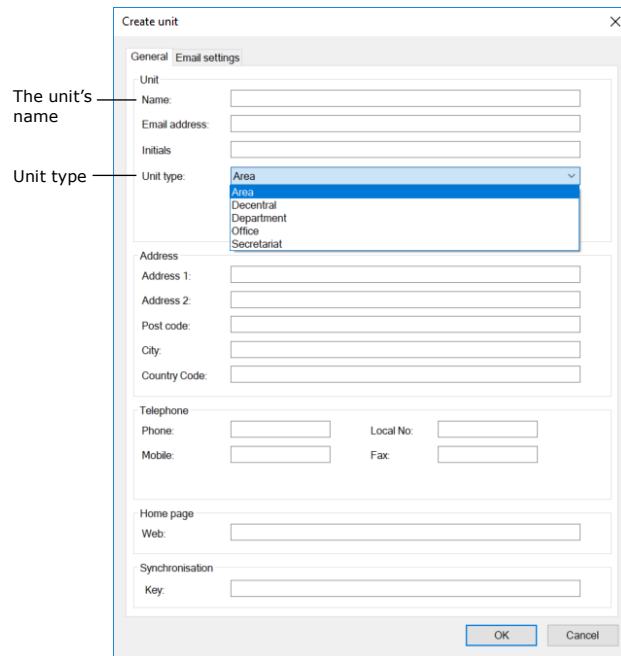


Figure 12: The “Create unit” dialogue

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

Create unit types for specific units

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

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.

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

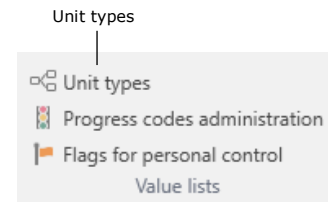


Figure 13: The "Unit types" menu item

These are examples of the unit types available:

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

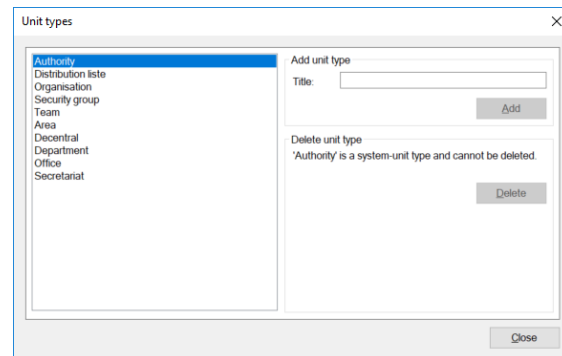


Figure 14: Management of unit types

Unit types such as teams and security groups are used to 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

A unit of the "Decentral unit" type 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 given a role. One role type must be a “job role”. Read more about the creation of role types in the section *Create and assign role types*.

Create user

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

If a user was already created through AD import, the user must be assigned a role. For further information on assigning roles, see the *Assigning roles* section.

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

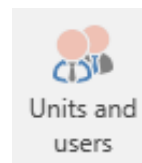


Figure 15: The “Units and users” menu item

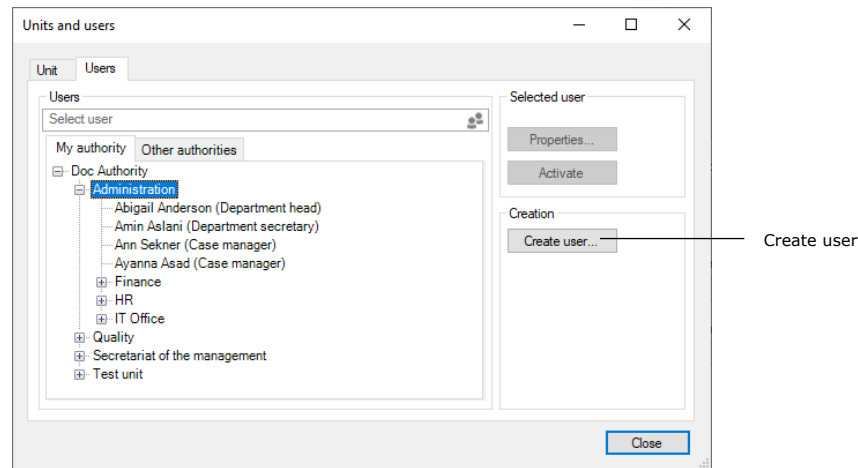


Figure 16: Create user

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

Create user – information

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

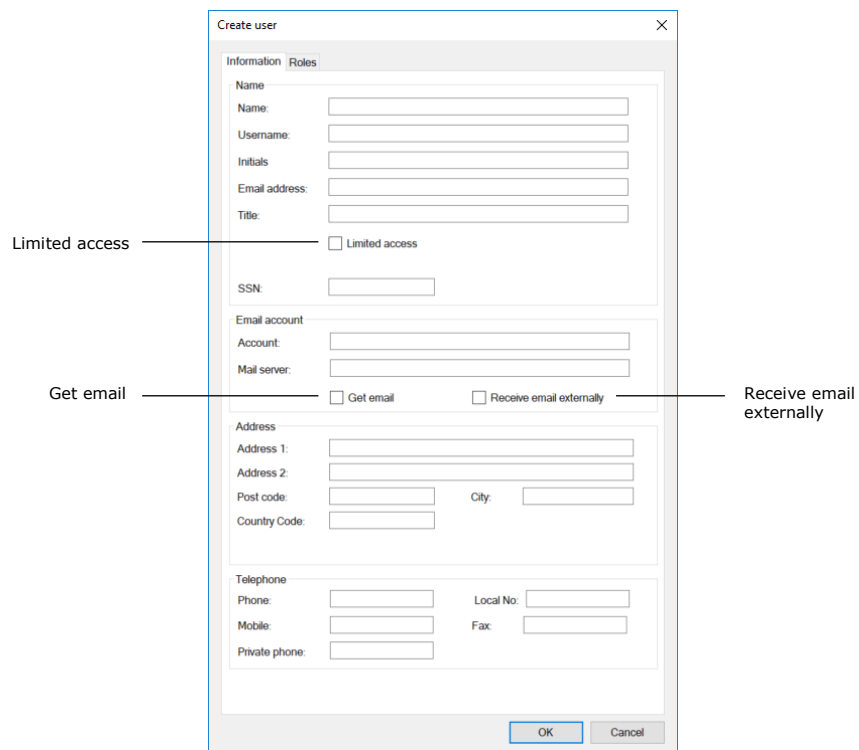


Figure 17: User information

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

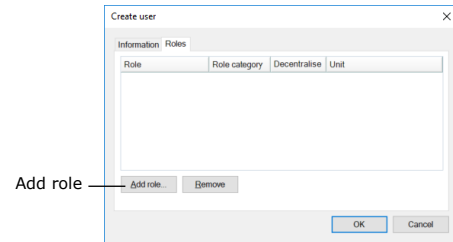
Field	Description
“Limited access”	<p>Ticking the “Limited access” box restricts the user’s access to records or cases in F2. The user only gains access when added to a record’s or case’s access restriction either by username or by being in a security group, unit or team. The user must also have access 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>The consequences of ticking this box depend on F2’s configuration. For installations with full email import, F2 transfers all emails from Outlook’s inbox to the user’s F2 inbox. A record is created for every imported email. With full email import, ticking the “Get email” box is not necessary.</p> <p>If email import is manual, the user must move relevant emails from Outlook using its “Move to F2” folder. The emails will then appear in both the “Moved to F2” folder in Outlook and “My inbox” in F2.</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: The “Get email” and “Receive email externally” boxes cannot both be ticked. Ticking “Receive email externally” lets the user work with a different email client alongside F2. In this case, emails must be manually transferred to F2 using the “Move to F2” folder.

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

Create user – roles

A new user must be assigned a job role. Fill in all the relevant fields on the “Information” tab in the “Create user” dialogue and click on **OK**. Focus 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 18: The “Roles” tab in the “Create user” dialogue

Note: An administrator can see which role types are categorised as “job” in the “Role types and privileges” dialogue which is available on the “Administrator” tab. For more information about role types and privileges see the section *Create and assign role types*.

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

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

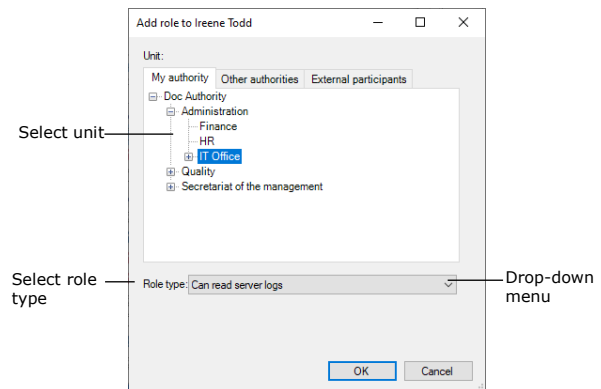


Figure 19: Add a role to a new user

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.

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.

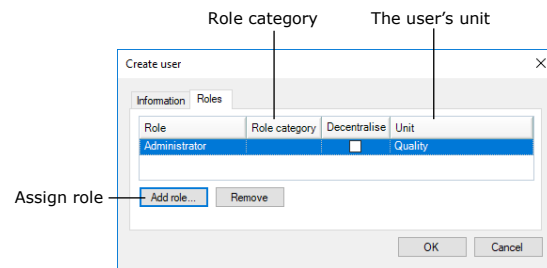


Figure 20: Assign a role to a new user

Note: New users are always created with the “Addressbook owner” role type. 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.

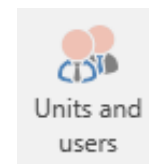


Figure 21: The “Units and users” menu item

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

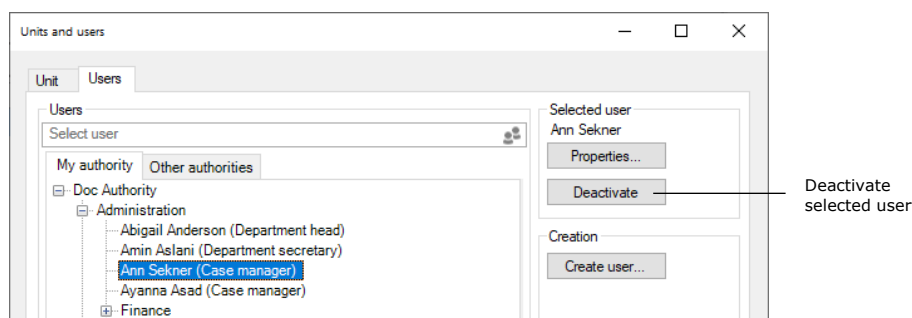


Figure 22: Deactivate a user

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

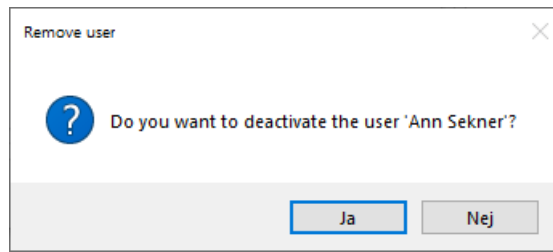


Figure 23: The warning dialogue when deactivating a user

A deactivated user is displayed in italics.



Figure 24: A deactivated user

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

Activate user

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

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

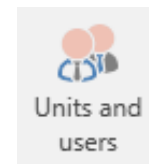


Figure 25: The "Units and users" menu item

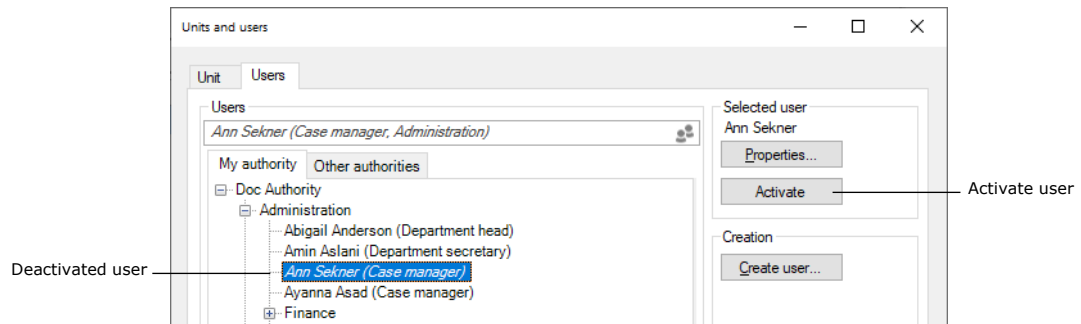


Figure 26: Reactivate a user

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 Ann Sekner

Information Roles

Name

Name: Ann Sekner

Username: Not employed

Initials: ASE

Email address: ase@doc.gov.uk

Title:

Limited access

Participant No: 29

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

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

On behalf of

In a number of situations, a user may need access to another user's inbox for either a fixed time period or on a permanent basis. For example, a secretary may need access to 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" (add-on module).

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 possible to go on behalf of a deactivated user and perform actions as if the user were active. For further information on deactivated users, see the *Deactivate user* section.

Setting up "On behalf of"

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

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

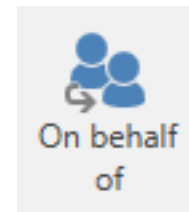


Figure 28: The "On behalf of" menu item

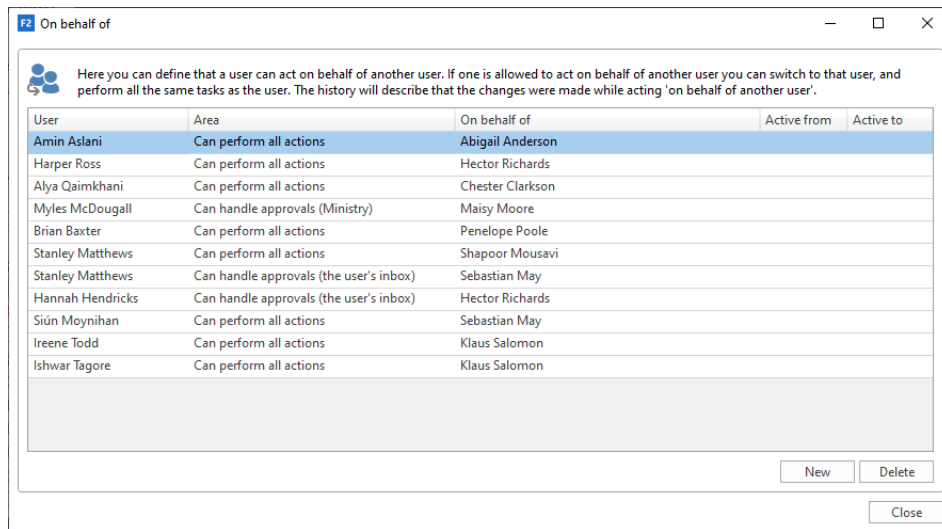
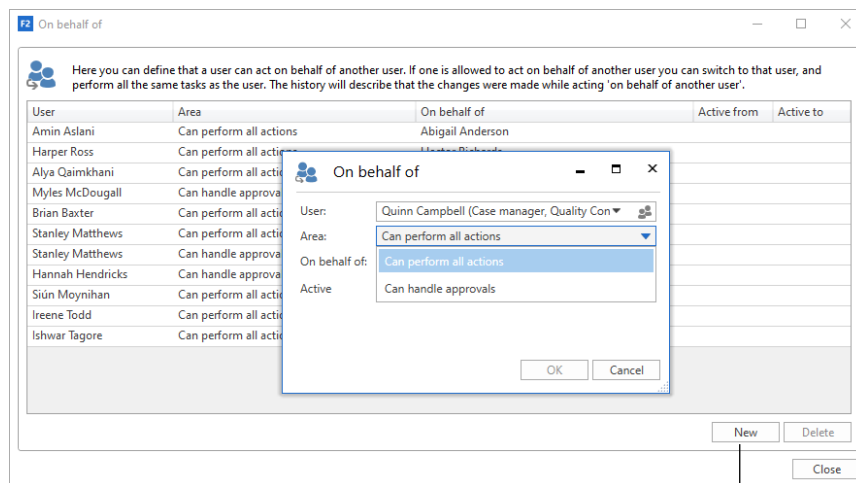


Figure 29: The "On behalf of" dialogue

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

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

- "Can perform all actions". These are the full "on behalf of" rights.
- "Can process approvals" (add-on module). These are partial "on behalf of" rights.



Create new "On behalf of" rights

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

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

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

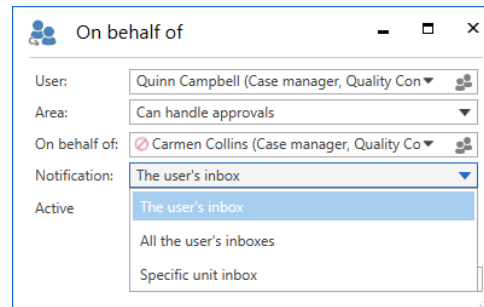


Figure 31: Select the location for approval notifications

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

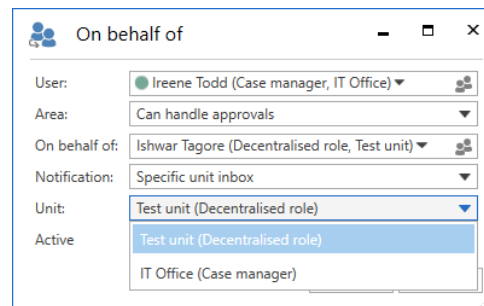


Figure 32: Select a specific inbox

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.

Click on **OK** to complete.

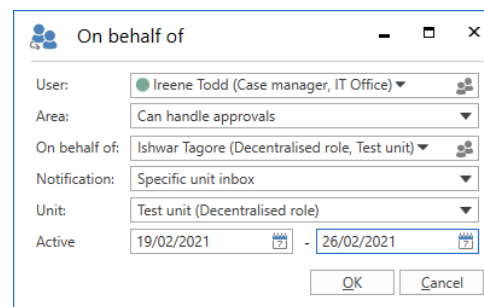


Figure 33: Assign “On behalf of” rights for processing approvals

Managing emails

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

Email settings can be configured in F2 on different levels: authority, unit and user. Using the F2 Shared Mailboxes add-on module 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 as shown in the figure below.

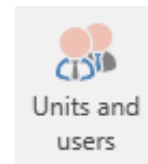


Figure 34: The "Units and users" menu item

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**.

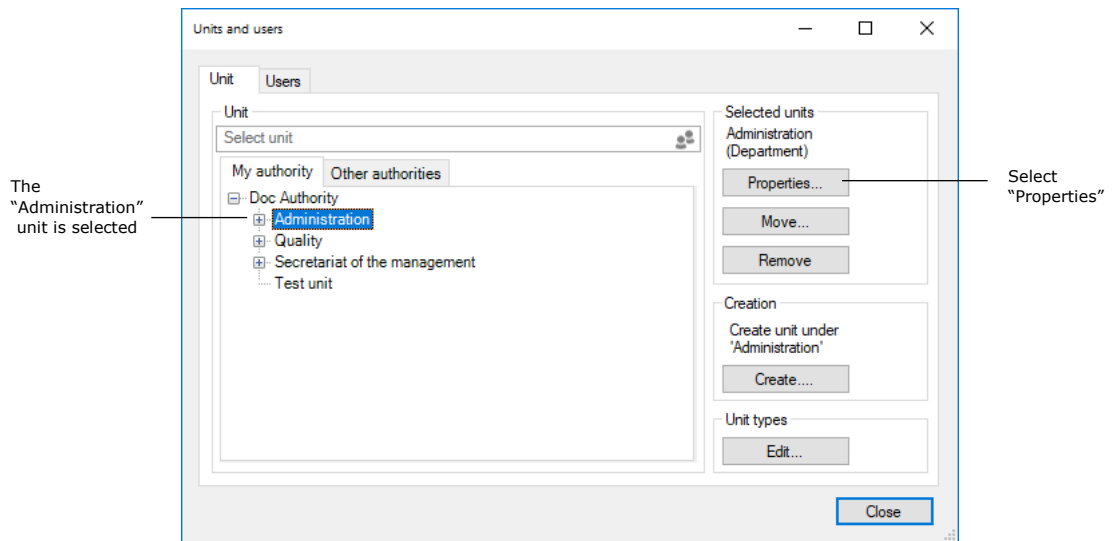


Figure 35: The “Units and users” dialogue

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

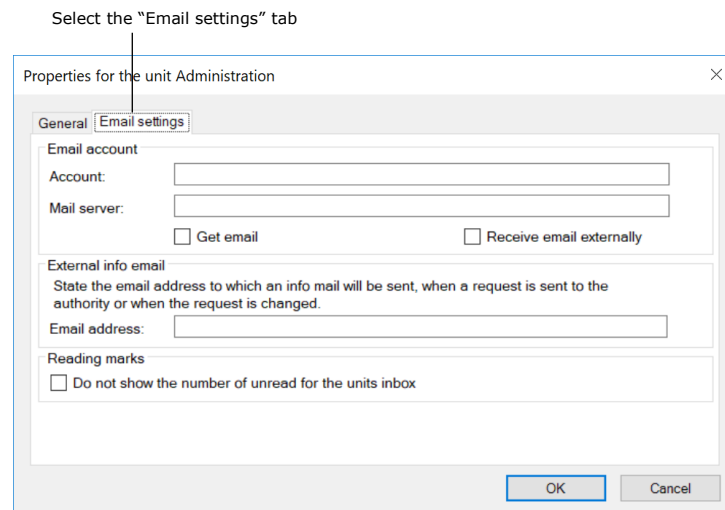


Figure 36: Setting up a unit inbox

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.

Field	Description
"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 for which the responsibility is reallocated are still kept 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 <i>F2 Group Request – User manual</i>.</p> <p>Note: 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" om 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.

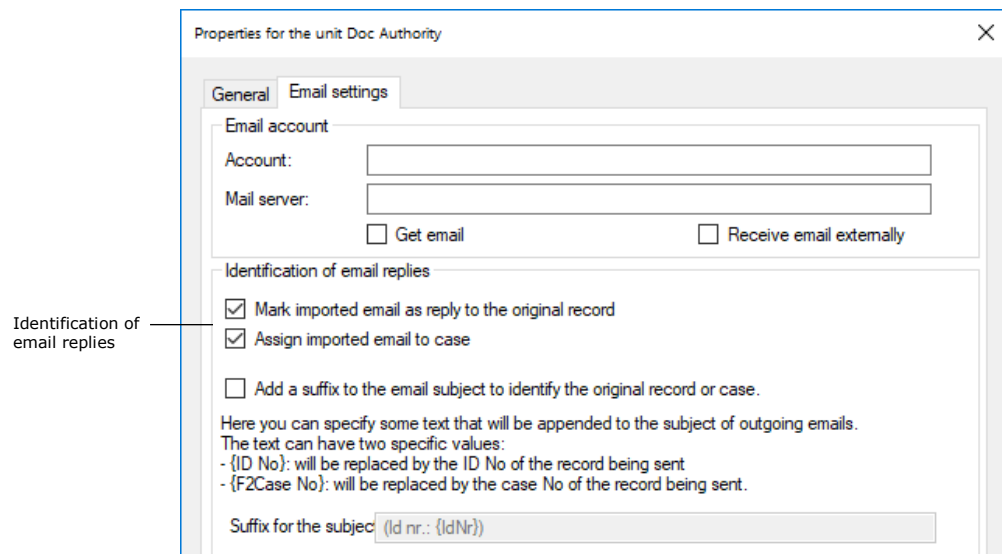


Figure 37: Identification of email replies

Note: Linking emails sent to or from F2 systems older than 6.2 is not possible.

Add a suffix in the subject field of external emails

F2 can be set up to link incoming email replies to emails sent from F2 by adding a unique ID in the subject field of an outgoing email. The subject field in F2 corresponds to the "Title" field on a record. An administrator with the "Unit administrator" privilege can set up F2 so the subject field of outgoing emails contain either its record ID, the case number, or both, which F2 then uses to link the email to any incoming replies.

A subject field suffix that applies to all of the authority's outgoing emails can be set up on 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**.

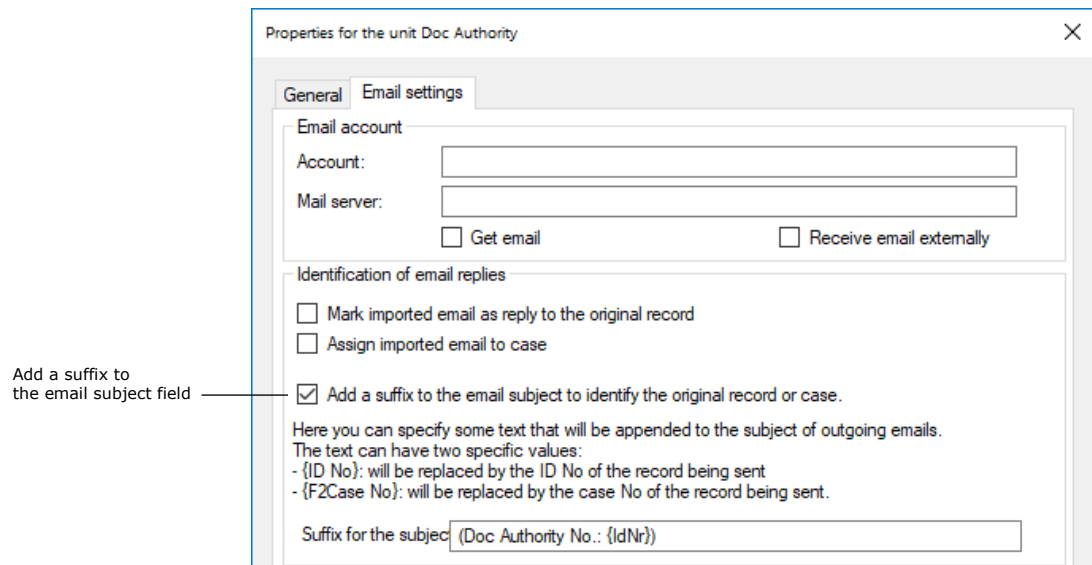


Figure 38: Configure the subject field for emails

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 in the subject field.
- Insert "{F2CaseNumber}" to add the case number of the outgoing email in the subject field.
- Insert "{IdNr}{F2CaseNumber}" to add both the record ID and the case number of the outgoing email in 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 role types. For example, if a user must be able to delete notes, the user must be assigned a role type containing the “Can delete notes” privilege.

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

The default role types in F2 are described below.

Administrator roles

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

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

There are four integrated administrator roles:

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

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

The assignment of the individual privileges is listed below.

The “Administrator” role type has the following privileges:

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

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

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

The "User administrator" role type 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 (add-on module)
- Can import parties
- Meeting forum administrator (add-on module)
- Editor of participants
- Privilege administrator
- On behalf of administrator

- Security group administrator
- System message administrator
- Team administrator
- Team creator.

As a standard, the “Business administrator” role type has the following privileges. 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 (add-on module)
- Meeting forum administrator (add-on module)
- Template administrator
- Progress codes administrator (add-on module)
- Value list administrator.

As a standard, a “Technical administrator” role type has the following privileges. 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 the *Privilege overview* section.

Other default role types in F2

Role type	Description
Access to data cleanup	<p>This role type is part of the F2 Data Clean-up add-on module.</p> <p>Users with this role type 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>

Role type	Description
	For further information, see <i>F2 Data Clean-up – User manual</i> .
Address book owner	This role type 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.
Can delete everything on cases	<p>This role type 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.</p> <p>For further information on deleting cases, see <i>F2 Desktop – Cases</i>.</p>
Can use F2 GDPR	<p>This role type is part of the F2 Data Protection add-on module.</p> <p>Users with this role type 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	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.
Gated approver	<p>This role type is part of the F2 Gateway Approvals add-on module.</p> <p>The role type is assigned to users with a gatekeeper (secretariat) who processes approvals on behalf of the user. The gatekeeper must be assigned “On behalf of rights” for the gated approver. Read more in the <i>On behalf of</i> section.</p>
Head of department	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.

Role type	Description
Read access to another unit	This role type lets the user search for and read 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 access to all the unit's records with the "Unit" access level.
Read and write access to another unit	This role type 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 type is assigned automatically to users who are specified as team administrators in the "Teams" dialogue found on the "Settings" tab in the main window. The role can only be assigned through this dialogue. Read more in the <i>Teams</i> section.
Team member	This role type is assigned automatically to users who are specified as team members in the "Teams" dialogue found on the "Settings" tab in the main window. The role can only be assigned through this dialogue. Read more in the <i>Teams</i> section.

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: Through a configuration, F2 users may be authenticated using other LDAP servers than Active Directory, e.g. Oracle Unified Directory. This configuration does not support single sign-on login, which means that users must enter their username 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. Read more about this in *Assign role to several users* section.
- 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 the *Assign role to a single user* section

Assign role to several users

Users with the “User administrator” privilege can assign roles to one or more users through the “Assign role to users” dialogue, which is accessed on the “Administrator” tab in the main window.



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.

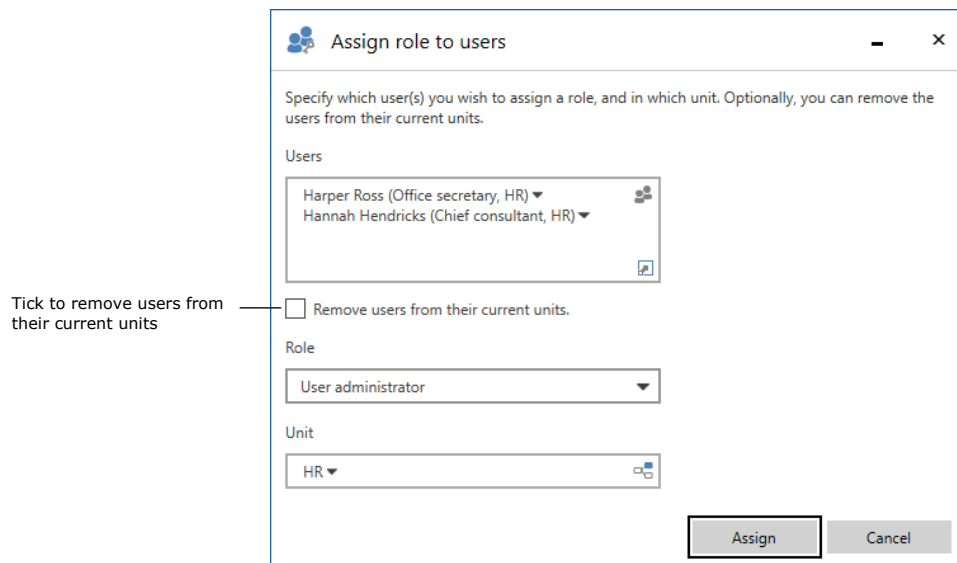


Figure 40: The “Assign role to users” dialogue

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**.

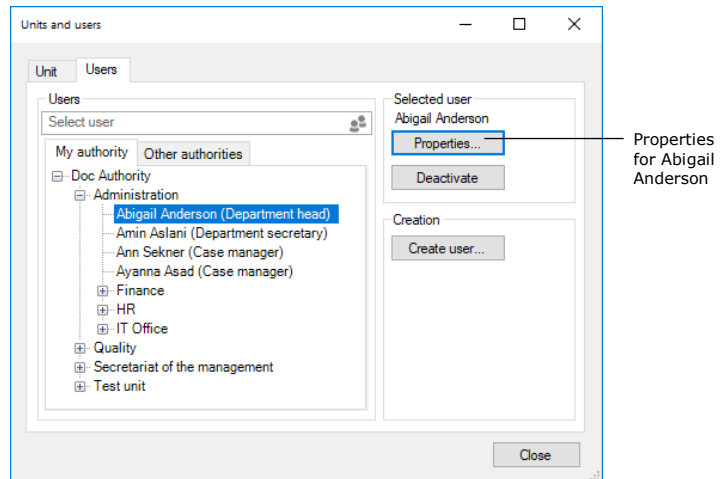


Figure 41: Select user

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

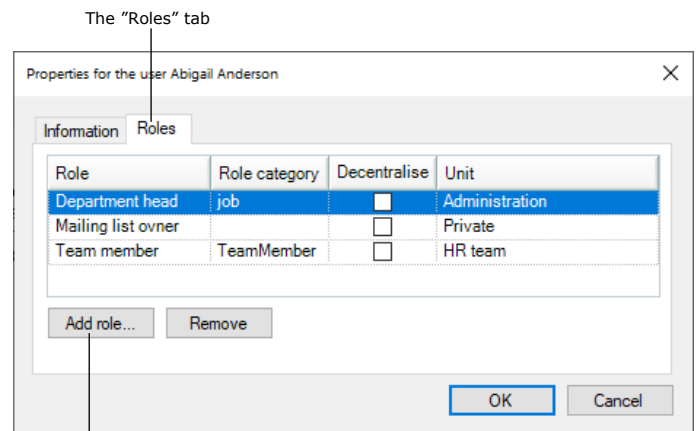


Figure 42: Assign a role to the user

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.

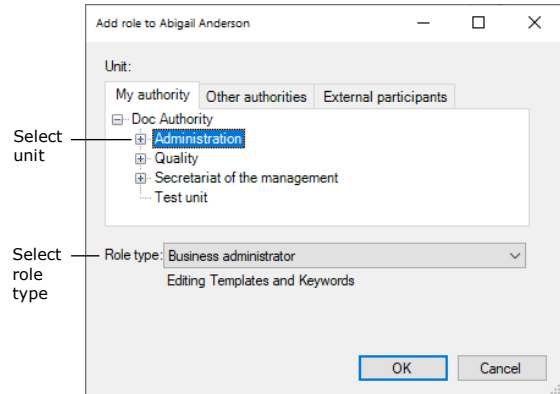


Figure 43: Assign a role type to a user

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.

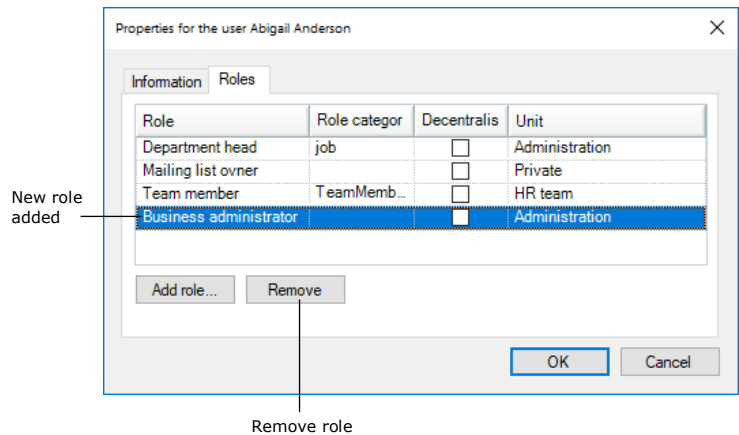


Figure 44: Add or remove a role from a user

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 role types

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

To view available role types, click on the **Role types and privileges** menu item 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.

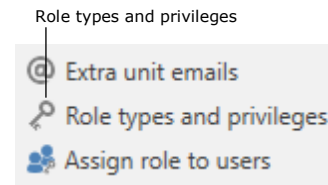


Figure 45: The “Role types and privileges” menu item

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

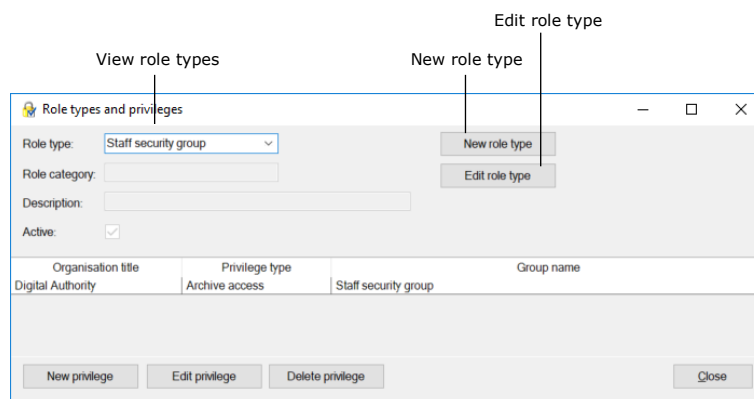


Figure 46: Role types and maintaining them

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

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

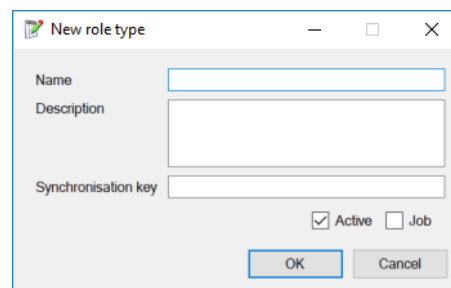


Figure 47: The “New role type” dialogue

Untick the “Active” checkbox to deactivate the role type. This means the role type can no longer be assigned.

Tick the “Job” checkbox to allow users to log into F2 with this role type. A user must have at least one job role to log into F2.

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

Note: A job role must be created with a tick in the "Job" checkbox. The box cannot be ticked after creating the role.

Note: A role type 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 type, 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.

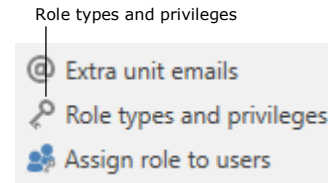


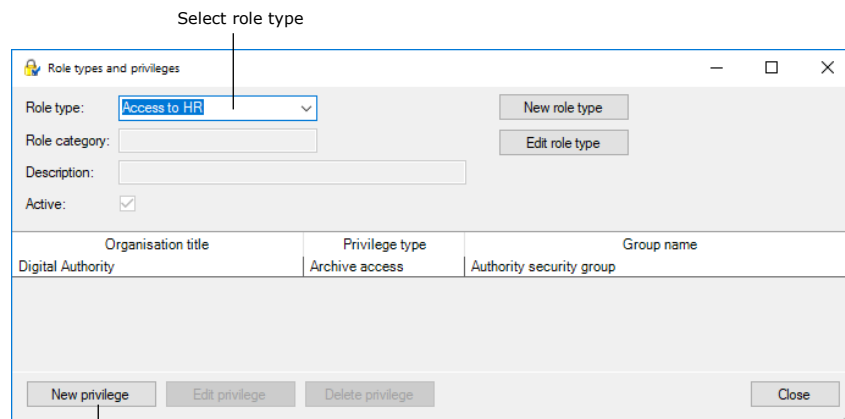
Figure 48: The "Role types and privileges" menu item

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 managing role types in the *Assigning roles* section.

Assign a privilege to a role type

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



Add a new privilege to the selected role type

Figure 49: The "Role types and privileges" dialogue

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

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

Click on **OK** to finish.

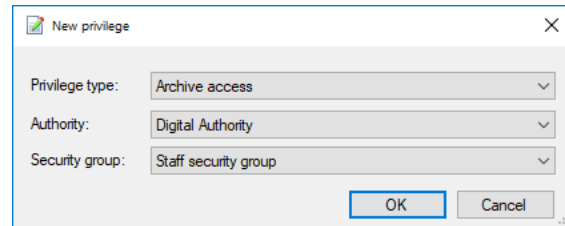


Figure 50: The "New privilege" dialogue

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 type

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.

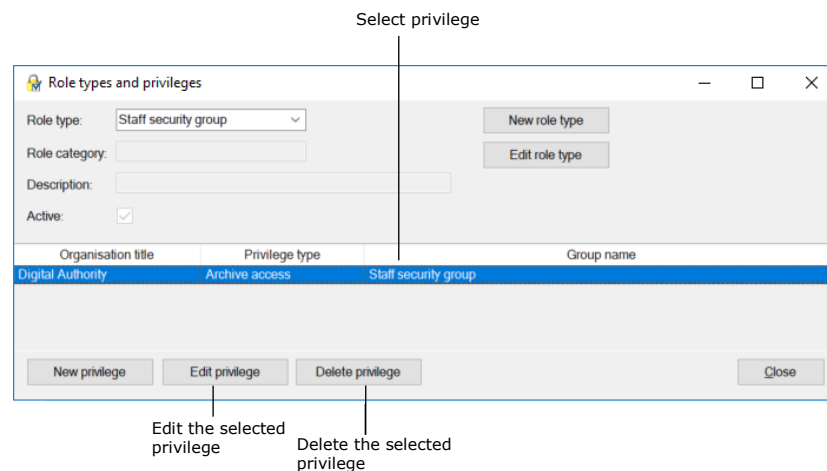


Figure 51: Edit or delete a privilege

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

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

Click on **OK** to finish.

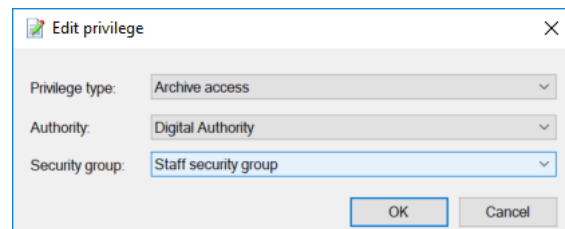


Figure 52: The "Edit privilege" dialogue

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.

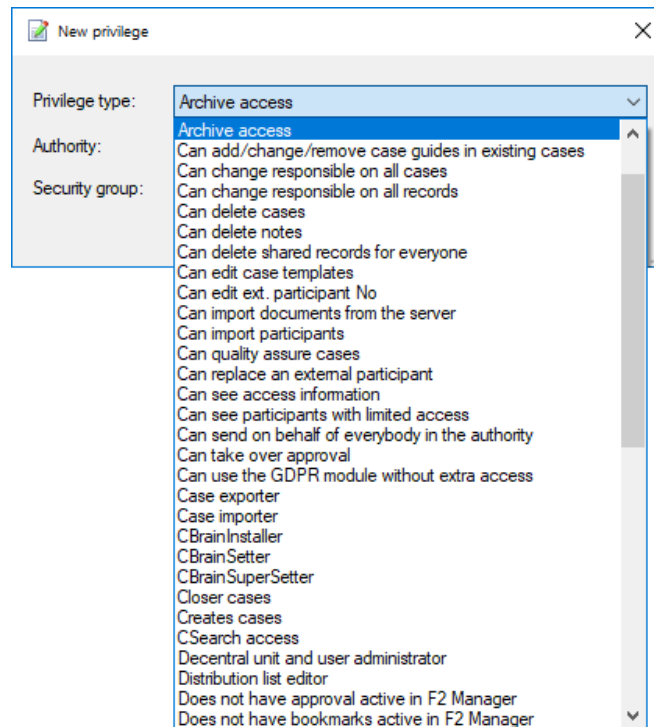


Figure 53: Assignable privileges

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	Provides access to use cPort. Exports are made across access levels and security groups. They do not show content, only titles and records.

Privilege	Description
Administrator read access to all records	Can read all records in F2 despite their access level. For further information, see the section <i>Administrator read access to all records</i> .
Archive access	Assigns a role to a security group. This lets an administrator add participants to security groups. Read more in the <i>Archive access</i> section.
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. These conditions are listed in <i>F2 Desktop – Cases</i> .
Can delete notes	Can delete record notes.
Can delete shared records for everyone	Can delete a record for everyone, even if the record is shared. For further information, see the manual <i>F2 Desktop – Records and Communication</i> .
Can edit case templates (add-on module)	Can edit case templates. Case templates can be applied by the organisation’s users in the “New case” dialogue. Read more in <i>F2 Case Template Editor – User manual</i> .
Can edit ext. participant no.	Can edit an external participant’s synchronisation number.
Can import documents from the server (add-on module)	Can import documents from the server, if this is configured. The configuration is done in cooperation with cBrain.

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 access information for records (right-click function), i.e. who can view the records, and how they received the access. <i>Read more in F2 Desktop – Records and Communication.</i>
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 (add-on module)	Can take over an approval without write access to the approval record. This allows for urgent processing of an approval when the responsible user/unit or an approver is unavailable. <i>Read more about taking over approvals in F2 Approvals – User manual.</i>
Can use the GDPR module without extra access (add-on module)	Can view existing GDPR searches, but not create, delete or edit them. The user can open GDPR searches, but can only preview cases, records, and documents which they otherwise would be able to see.
CBrainInstaller	Can perform configuration changes in the F2 installation. cBrain recommends that all configurations are done in cooperation with cBrain.
CBrainSuperSetter	Can perform configuration changes in the F2 installation. cBrain recommends that all configurations are done in cooperation with cBrain.
CBrainSetter	Can perform configuration changes in the F2 installation. cBrain recommends that all configurations are done in cooperation with cBrain.

Privilege	Description
Closer cases	Can complete cases.
Creates cases	Can create new cases.
cSearch access (add-on module)	Can perform searches using the add-on module cSearch.
Decentral unit and user administrator	Can create decentral units. Can assign decentral roles to existing users for selected levels in the organisation.
Distribution list editor	Can create and edit the shared distribution lists in F2. For further information, see the section <i>Distribution list editor</i> .
Does not have approvals active in F2 Manager (add-on module)	Cannot see approvals in F2 Manager.
Does not have bookmarks active in F2 Manager (add-on module)	Cannot see bookmarks in F2 Manager.
Does not have meeting planner active in F2 Manager (add-on module)	Cannot see the meeting planner in F2 Manager.
Editor of participants	Can create, edit, and delete external participants as well as edit images for external participants. Note: The privilege MUST be attached to a node under external participants. Read more in the <i>Editor of participants</i> section.
Extra email administrator (add-on module)	Can create extra emails for units.
F2Setter	Can perform configuration changes in the F2 installation. cBrain recommends that all configurations are done in cooperation with cBrain.

Privilege	Description
Flag administrator	Can create, edit, and delete flags.
Keyword administrator	Can create, edit, and delete keywords as well as assign keywords to a unit. For further information, see the section <i>Administration of keywords</i> .
Limited access to data cleanup (add-on module)	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 in <i>F2 Data Cleanup – User manual</i> .
Meeting forum administrator (add-on module)	Can create, edit, deactivate, activate, and delete meeting forums.
No case help for saving or sending records	Will not see the case help when sending or saving a record. For more information, see the section <i>No case help for saving or sending records</i>
On behalf of administrator	Can create and delete “on behalf of” privileges for all users.
Phrase administrator (add-on module)	Can edit phrases for merging documents.
Privilege administrator	Can create new roles and assign, remove, and edit privileges for a role.
Process editor (add-on module)	Can access the Process editor tool. This tool is used for editing case guide templates.
Progress code administrator (add-on module)	Can create, edit, and delete progress codes.
Reopener case	Can reopen cases.
Result list administrator	Can create standard column settings for all users.
Search administrator	Can create saved searches for all users.

Privilege	Description
	<p>If the F2 Search Templates add-on module has been configured, users with this privilege will be able to view search templates.</p> <p>Search templates are configured in cooperation with cBrain.</p>
Security group administrator	Can create, edit and delete security groups.
Settings administrator	Can create, edit and delete user settings along as well as assign them to individual users, new users and from the users' roles.
SSN Synchronizer (add-on module)	Can access the SSN register via the properties dialogue for participants and users and update participant information from there.
System message administrator	Can create, edit and delete system messages.
Team administrator	Can create, edit, and delete teams.
Team creator	Can create teams across the authority.
Template administrator	Can create, edit, and delete document templates and global approval templates (add-on module).
Unit administrator	Can create, edit, move, and deactivate units.
Unit type administrator	Can create and delete unit types.
User administrator	Can create and edit users and edit user images.
Value list administrator	Can create, edit, and delete value lists.

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.

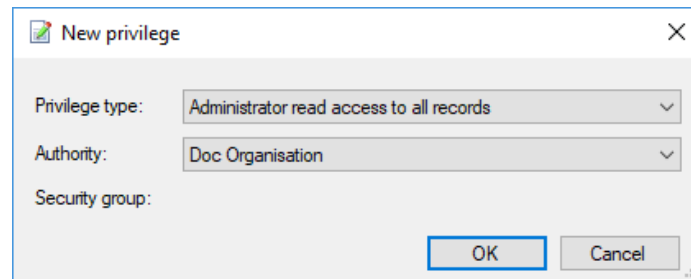


Figure 54: The “Administrator read access to all records” privilege

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.

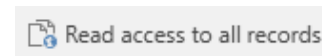


Figure 55: The “Read access to all records” menu item

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.

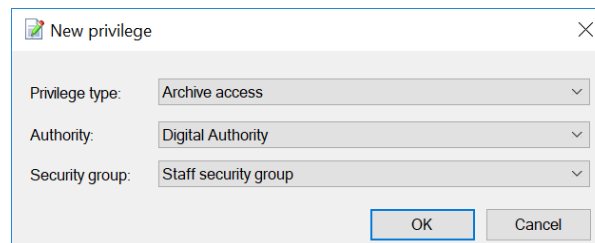


Figure 56: A new privilege type - “Archive access”

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.

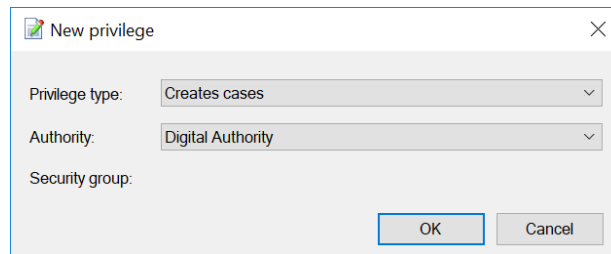


Figure 57: The “Creates cases” privilege

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

Distribution list editor

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

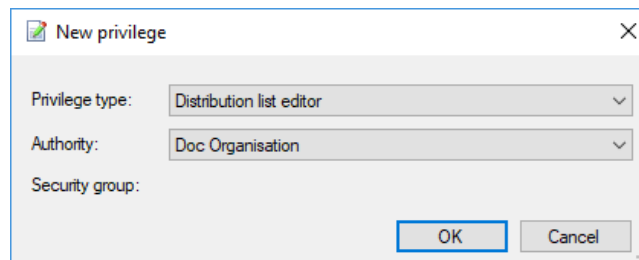


Figure 58: The “Distribution list editor” privilege

How to edit distribution lists is described in *F2 Desktop – Settings and Setup*.

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.

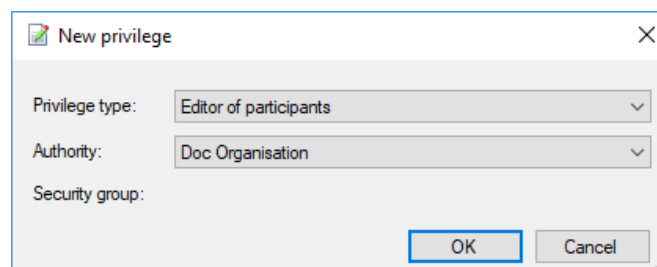


Figure 59: The “Editor of participants” privilege

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.

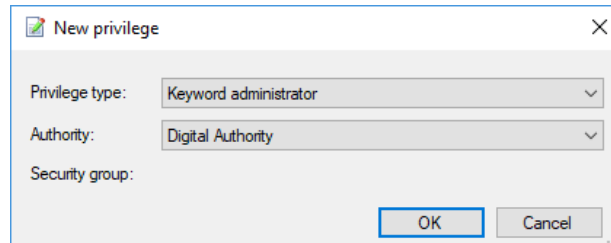


Figure 60: The "Keyword administrator" privilege

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

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.

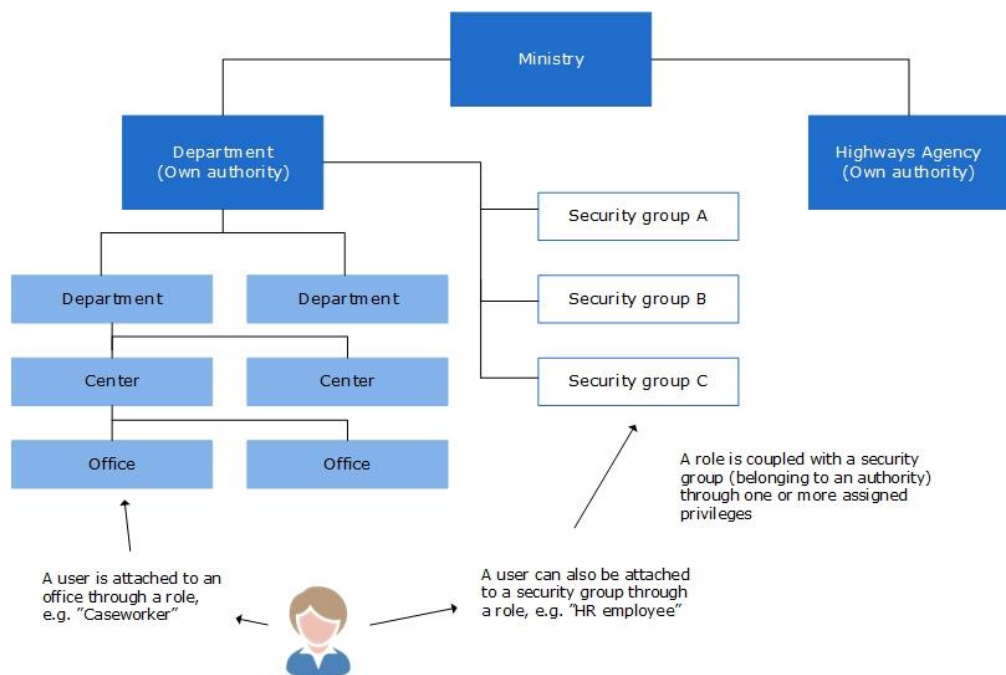


Figure 61: Security groups are created under an authority

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”.

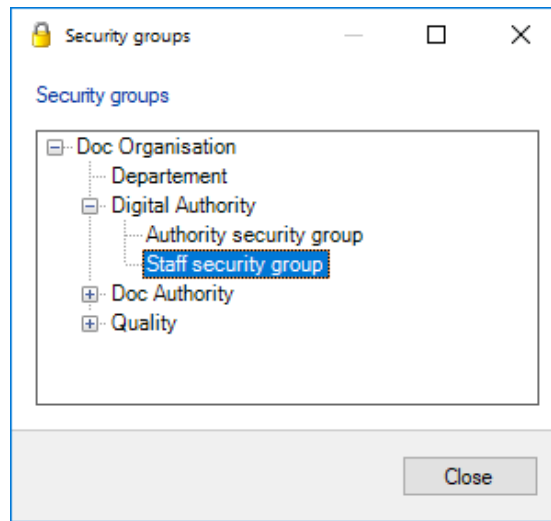


Figure 62: Authorities and security groups

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: If a user has full write access to a record or case and they are included in its access limitation, the user can remove any attached security groups. This includes security group of which the user is not a member.

Create a security group

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

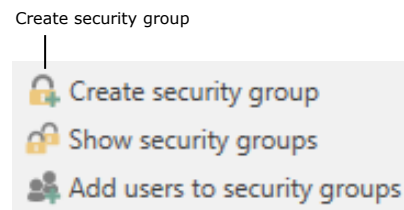


Figure 63: The "Create security group" menu item

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.

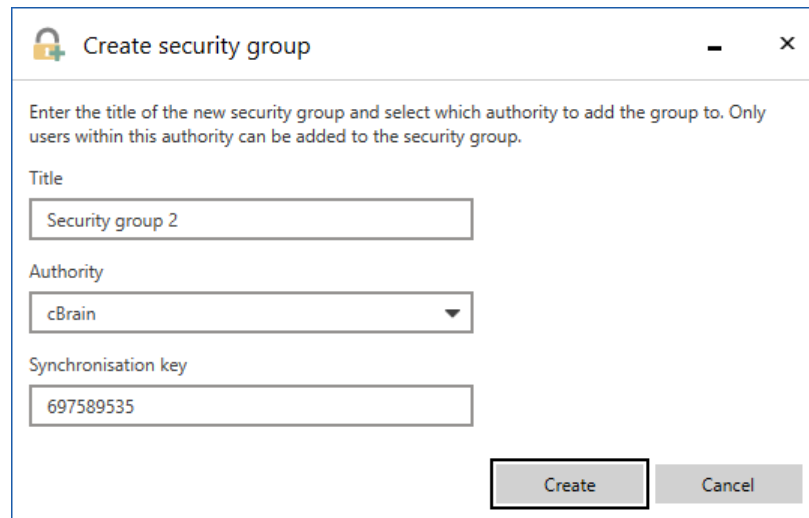


Figure 64: The “Create security group” dialogue

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.

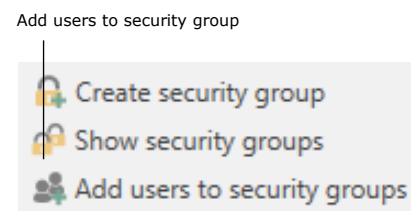


Figure 65: The “Add users to security groups” menu item

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.

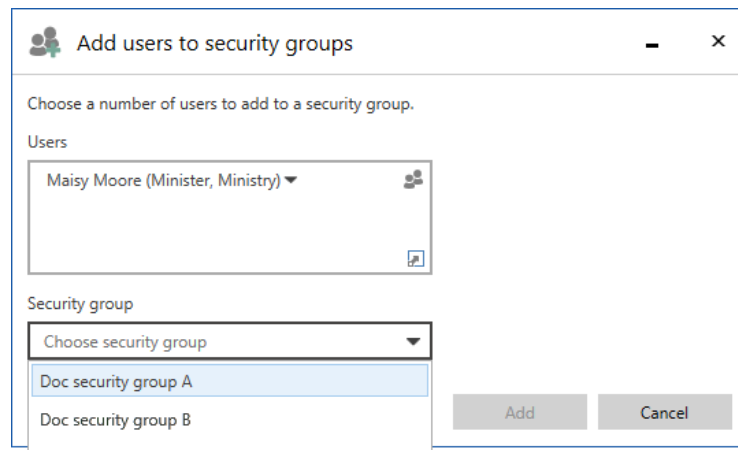


Figure 66: The “Add users to security groups” dialogue

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

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**.

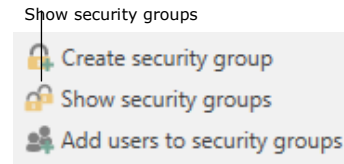


Figure 67: The "Show security groups" menu item

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**.

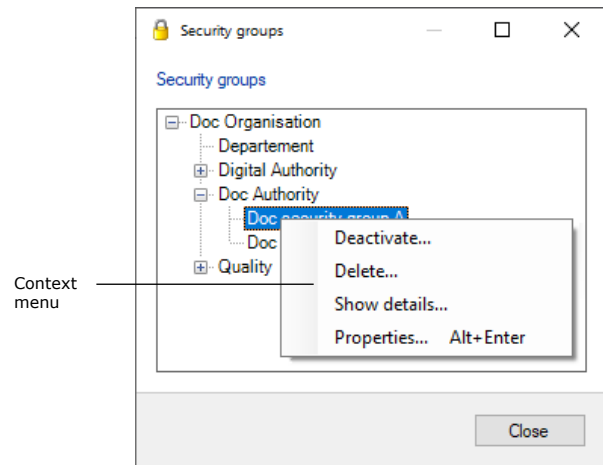


Figure 68: The "Security groups" dialogue

In the example to the right, Hannah Hendricks, Harper Ross, and Hector Richards are members of the "SG HR" security group.

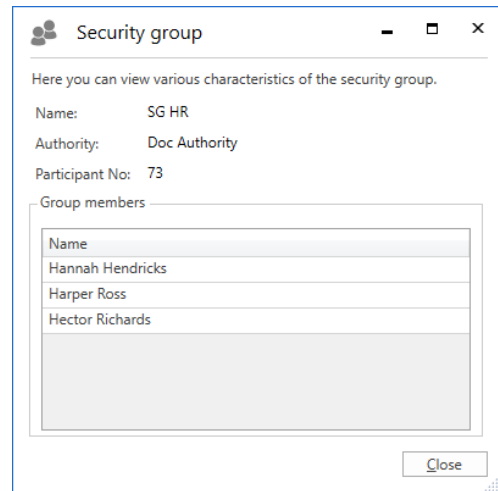


Figure 69: Properties for a security group

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.

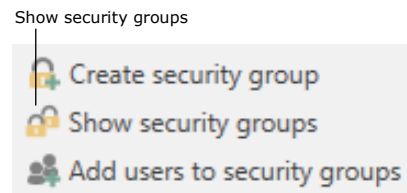


Figure 70: The "Show security groups" menu item

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.

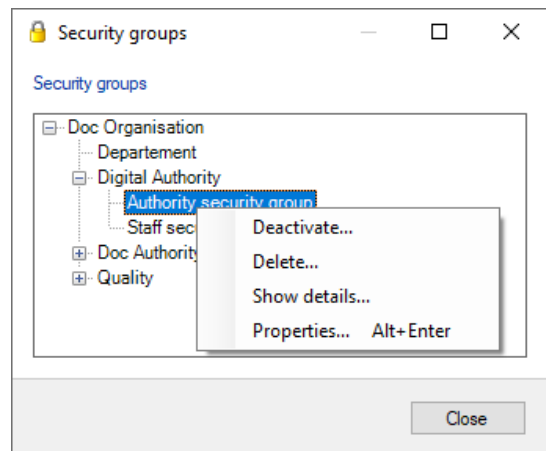


Figure 71: Deactivate security group

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.

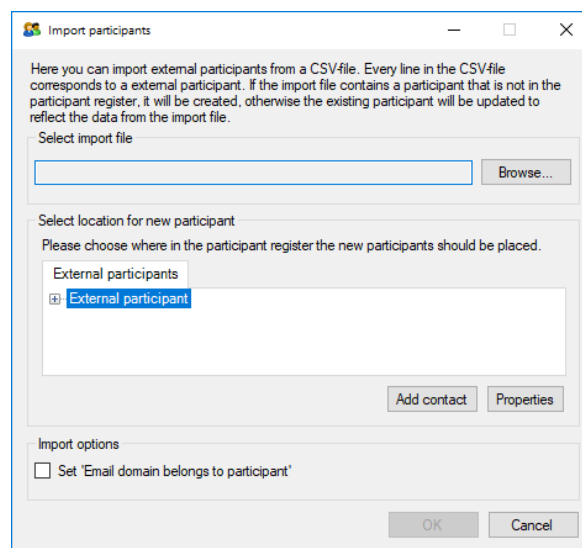


Figure 72: Import participants

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

Field	Description
“Select import file”	Click on Browse... to select the file.
“Select location for new participant”	Select a location for newly created participants in the participant register. If the participants in the import file must be placed in a new node, first create the node by clicking Add contact .

Field	Description
"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.

For further information on F2's participant register and creating external participants, see the section *The participant register*.

CSV file for importing participants

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

#	Column heading	Description
1	External ID	The ID that is saved with the participant. If the participant is reimported, the participant with this ID will be updated with the new data from the CSV file.
2	(Not in use)	
3	Name	Name
4	Name, continued	
5	(Not in use)	
6	Contact person	
7	Address	Address
8	Address, continued	
9	Zip code	

#	Column heading	Description
10	City	
11	Country code	
12	Country name	
13	Telephone	
14	Fax/cell phone	The value in this field is saved as both a fax and a cell phone number.
15	Postage group	The postage group. Displayed on the participant along with the address.
16	Email	
17	Website	
18	CBR number	
19	CBR P number	
20	Created date	If this field is empty, 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	
24	Groupcode03	
25	Groupcode04	
26	Groupcode05	
27	Groupcode06	
28	Groupcode07	
29	Groupcode08	
30	Groupcode09	
31	Groupcode10	

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.

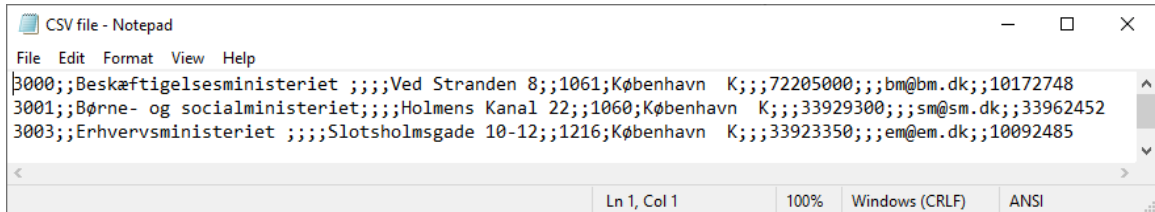


Figure 73: Import file

Note: The import file does NOT contain column headings.

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.

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

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

Value lists

Value lists are lists that apply to all authorities across the organisation. Each individual value list represents a group of standardised texts used in connection with different tasks. For further information on authorities and organisations, see the section *The unit structure in F2*.

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

- Office reply
- Report
- Alert
- For information.

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

Value list administration

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

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

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

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

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

Once a list is chosen, its 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

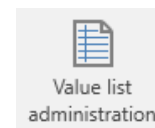


Figure 75: The "Value list administration" menu item

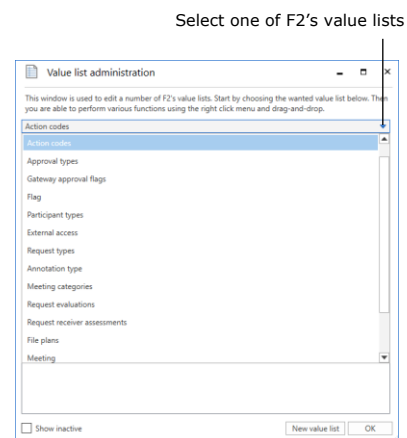


Figure 76: The "Value list administration" dialogue

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

Checking for inconsistent deactivation means that F2 identifies any items that are still active on an otherwise deactivated list.

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

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

If "Selectable" is ticked, the value can be selected where the dialogue appears. If "Selectable" is unticked, the value can be seen, but not selected.

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

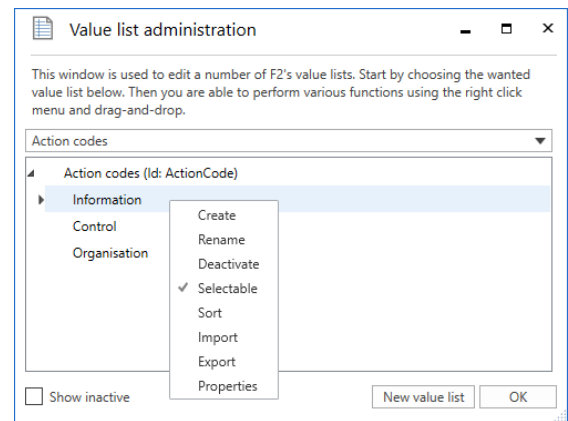


Figure 77: The context menu of a value list

Note: A value list item cannot be deleted, only deactivated. Deactivating a value list node will deactivate all items belonging to that node as well.

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.

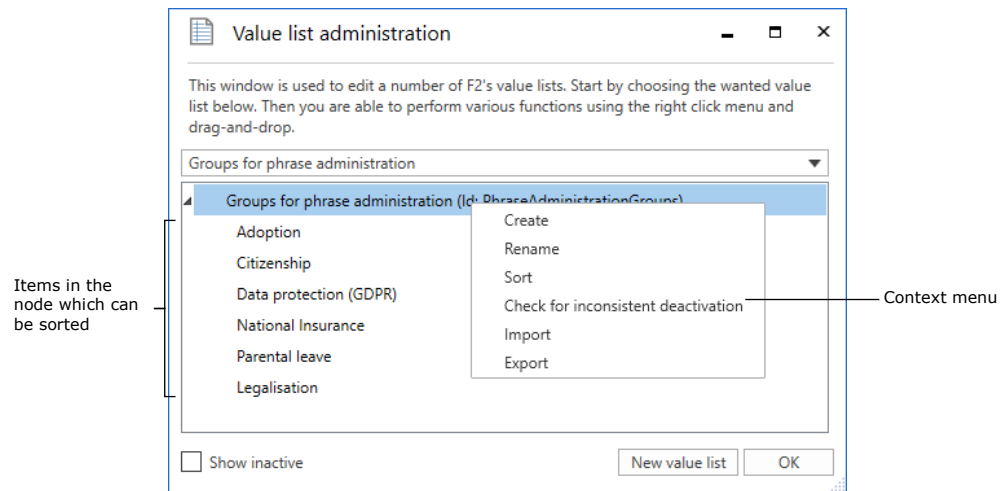
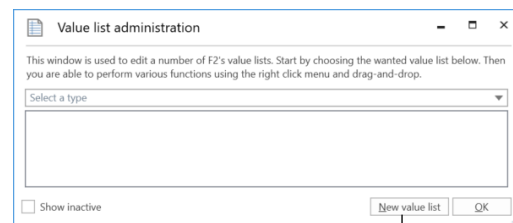


Figure 78: Sorting a value list

Create a new value list

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



Create a new value list

Figure 79: Value list administration

In the “Create new value list” dialogue enter the value list’s name and ID.

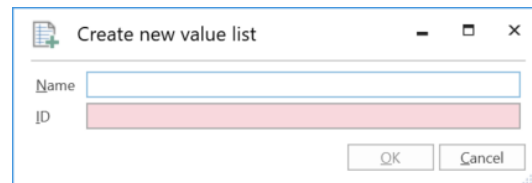


Figure 80: Create a new value list

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

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>
```

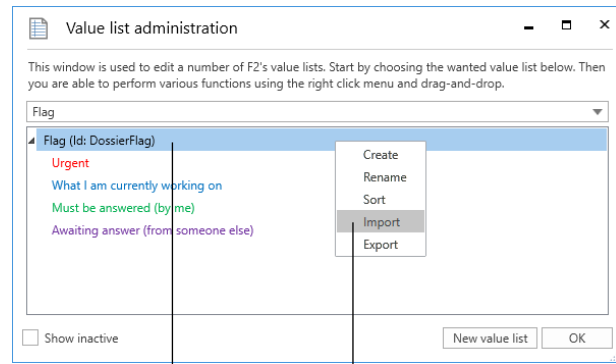
Figure 81: Example of value list item in XML file

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.



The "Flag" value list is selected

Import value list items via the context menu

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. See the figure below.

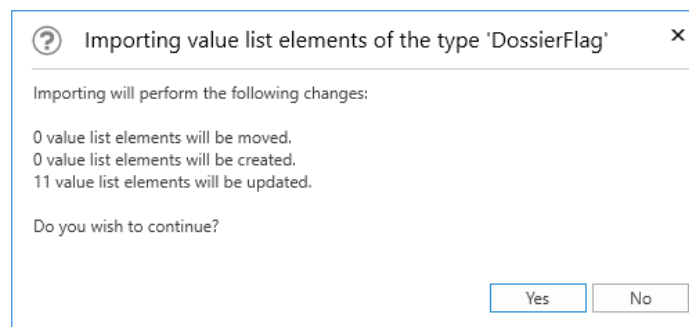


Figure 83: Importing value list items

Clicking **Yes** will execute the import, and F2 will move, create, and update the value list items based on the contents of the imported file.

Note: In order for the import to work, 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 the **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.

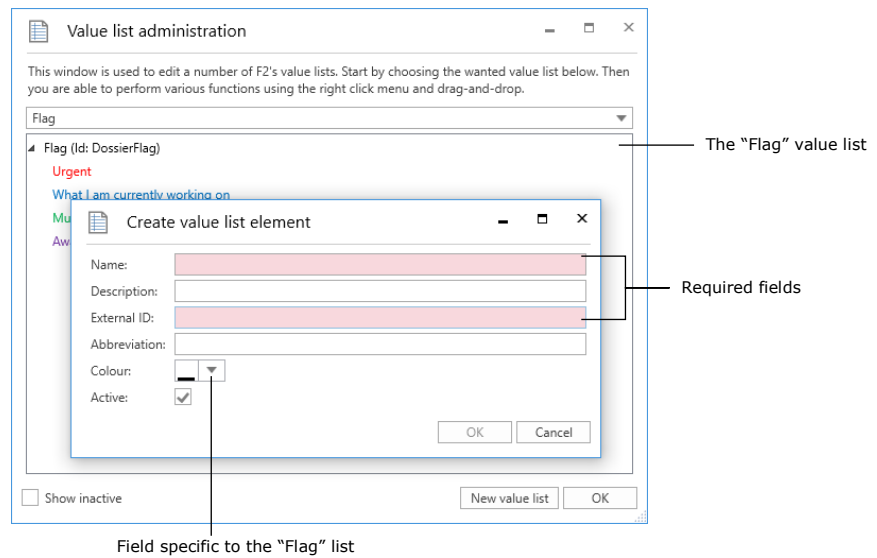


Figure 84: Creating a value list item from the "Flag" list

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 contain two value list items with the same external ID. The external ID must be unique for each value list item.

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.

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.

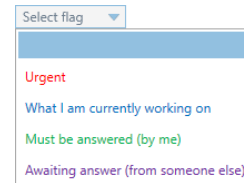


Figure 85: Example of the control flag menu on a record

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.

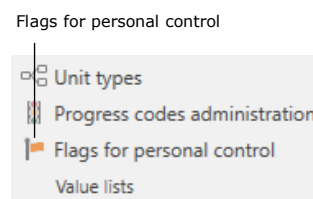


Figure 86: The “Flags for personal control” menu item

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.

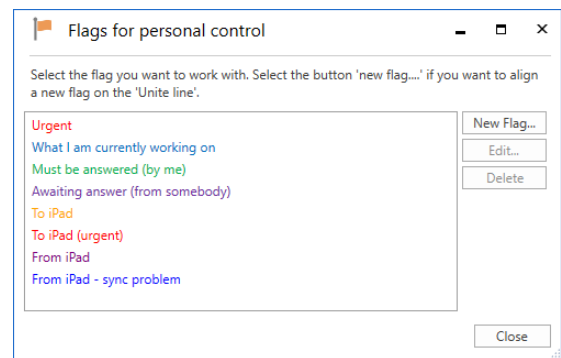


Figure 87: The “Flags for personal control” dialogue

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.

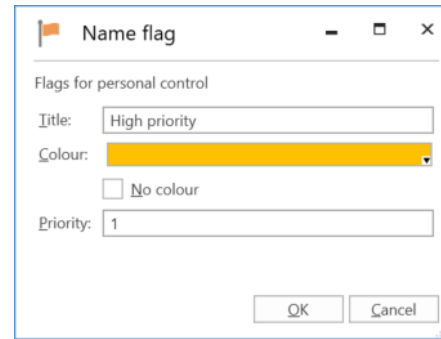


Figure 88: Name the control flag

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.

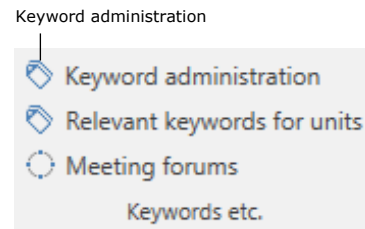


Figure 89: The “Keyword administration” menu item

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

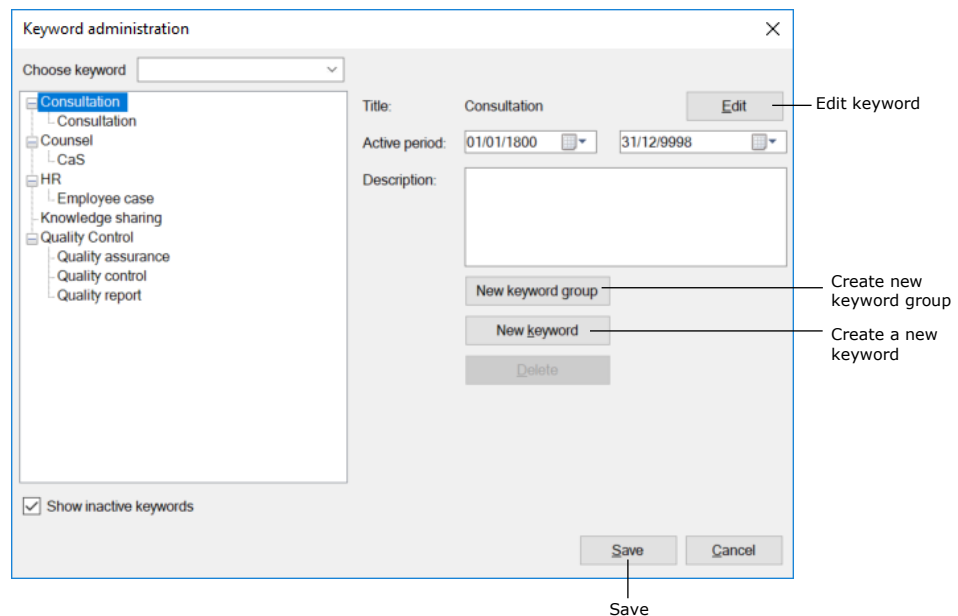


Figure 90: Administration of keywords

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

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

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

Only active keywords can be added 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.

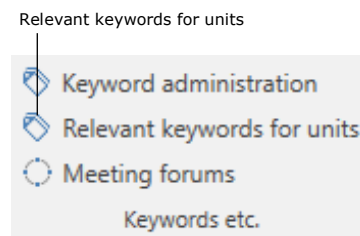


Figure 91: The "Relevant keywords for units" menu item

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.

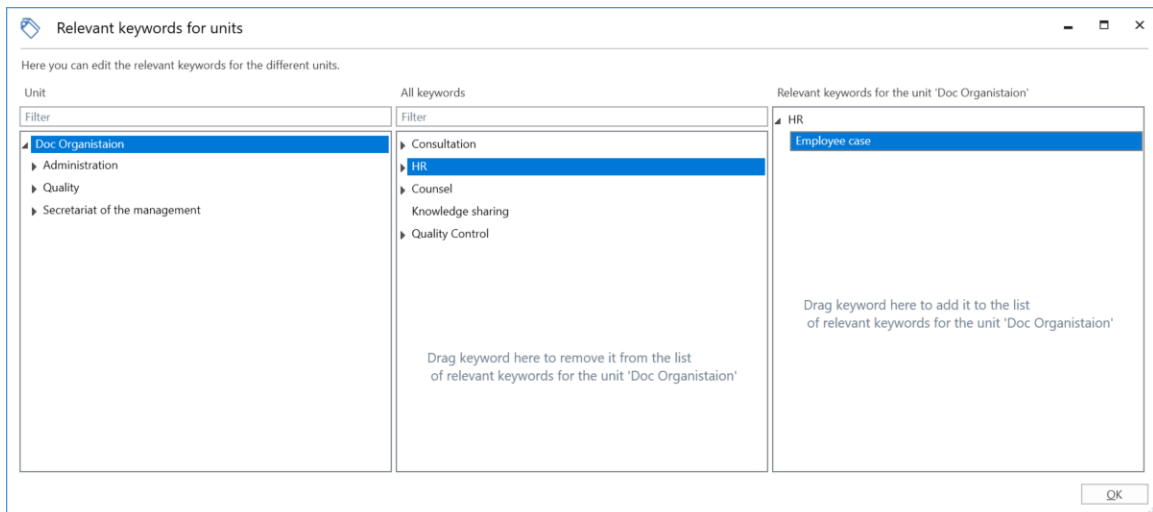


Figure 92: Select keywords

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.

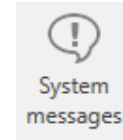


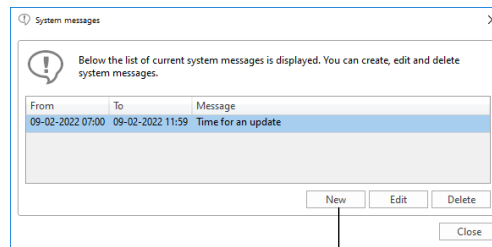
Figure 93: The "System messages" menu item

This can be important messages about unscheduled downtime or other information pertaining to the performance of F2 and which affects all users.

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

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.



Create a new system message

Figure 94: 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.

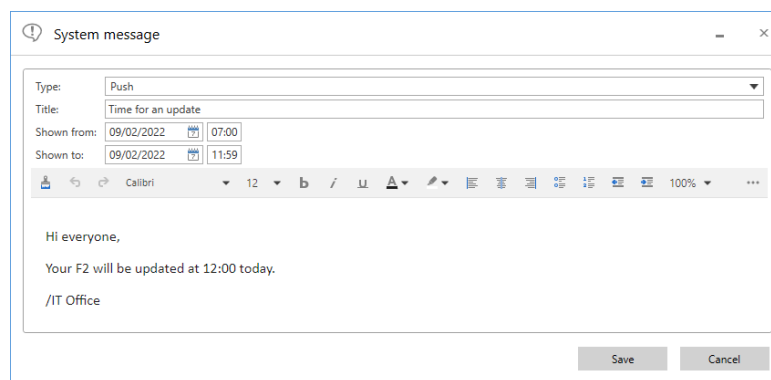


Figure 95: Create a new system message

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 on  **Contacts** above the list view in the left side of the main window.

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

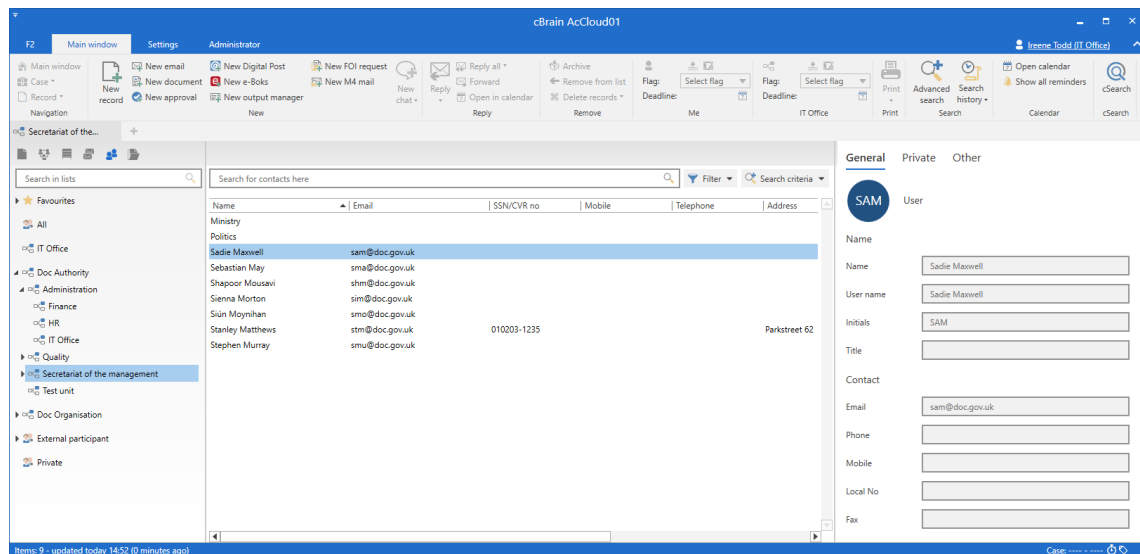


Figure 96: F2's participant register in the main window

The participant register consists of three types of participants:

- **Internal participants:** Users who are created and maintained in F2 via "Units and users". If a user is moved from one F2 unit to another, this change is applied to the participant register as well. The "Units and users" dialogue is used for managing internal participants. For more information, see the section *User administration*.
- **External participants:** Participants who are either created manually by a 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 assigned to a record or a case, their information is copied over from the participant register. However, if the register is updated with new information on the participant, e.g. an address change, the records and cases on which the participant is already added are not automatically updated with the new address.

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

External participants

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

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

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**.

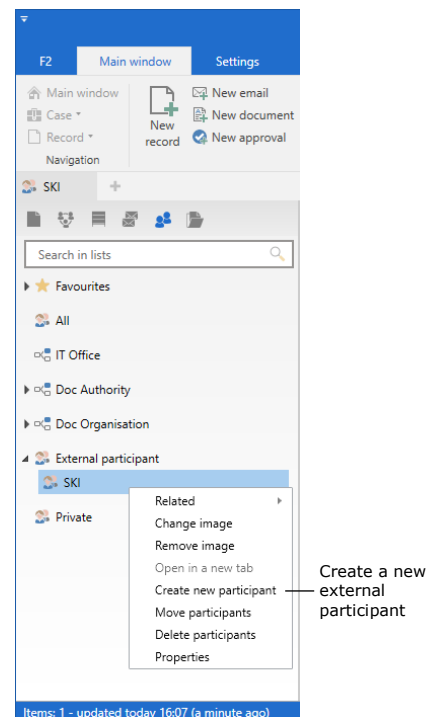


Figure 97: Create external participant

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

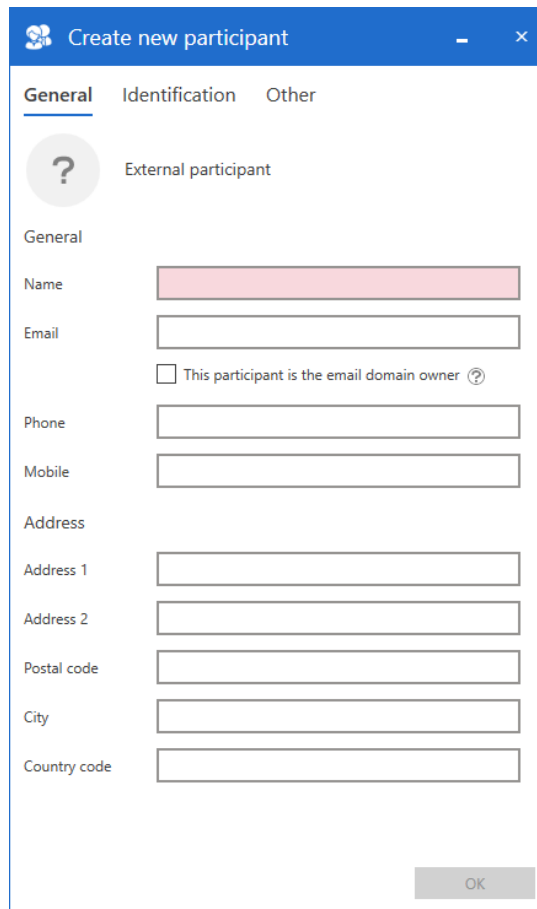


Figure 98: The "Create new participant" dialogue

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 to from the email benoit@cloudpost.com. 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 be 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.

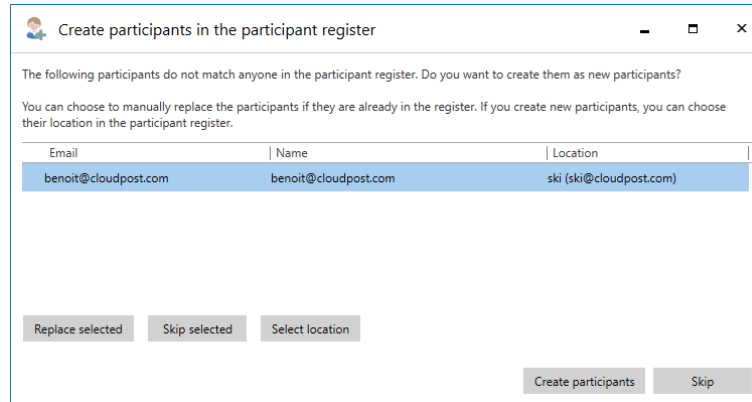


Figure 99: F2 suggests placing a new participant under an existing one

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@cloudpost.com under the same participant as SKI.

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

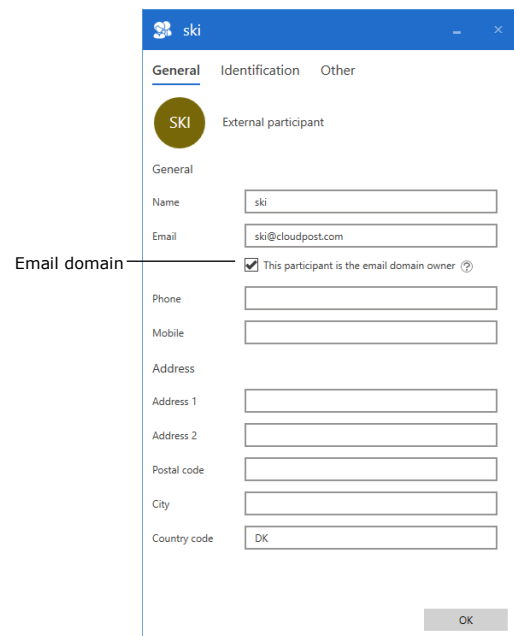


Figure 100: Participant who owns an email domain

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.

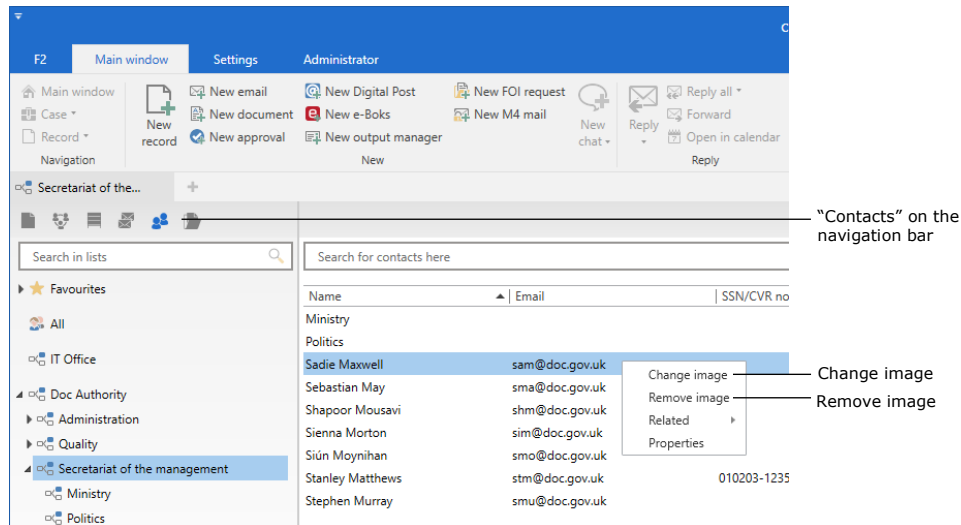


Figure 101: Right-click on a participant in the participant register

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.

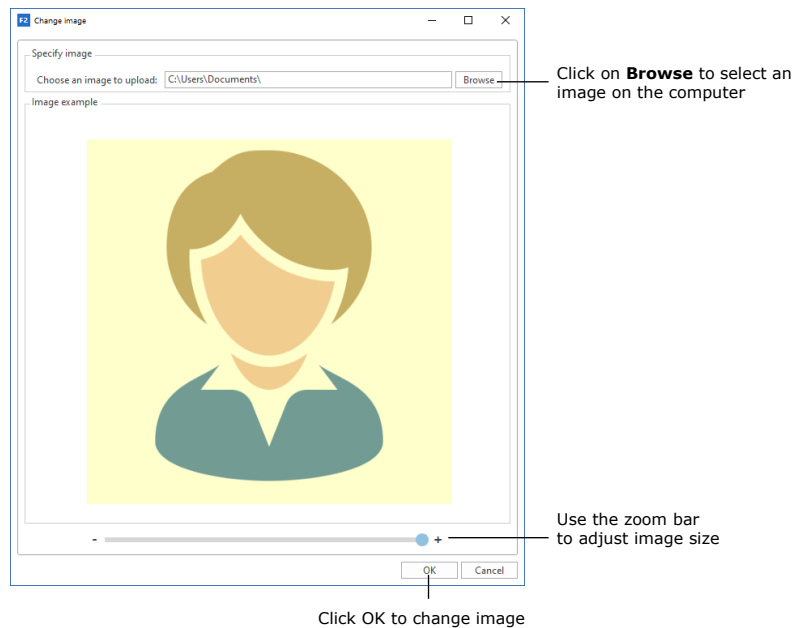


Figure 102: The “Change image” dialogue

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.

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 to open the dialogue.

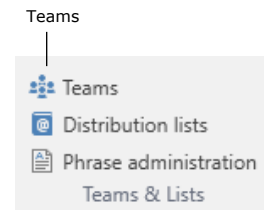


Figure 103: The "Teams" menu item

In the "Teams" dialogue, teams can be created, edited, displayed, and deleted.

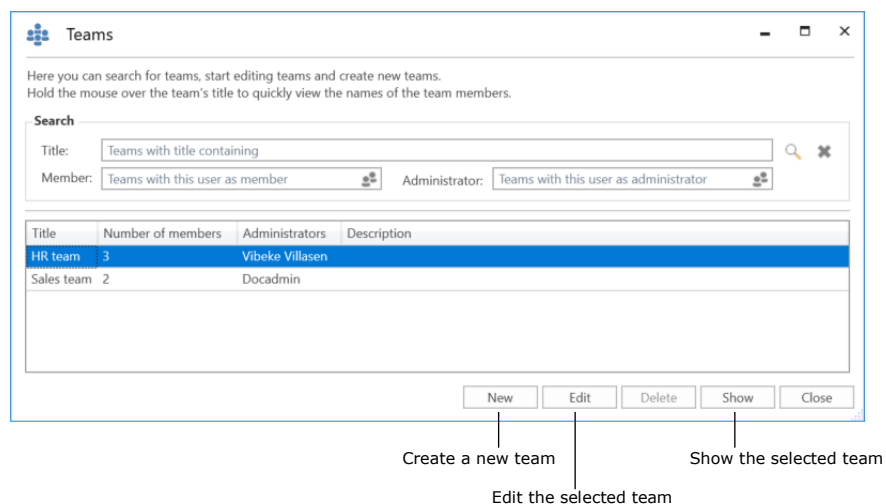


Figure 104: The "Teams" dialogue

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

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

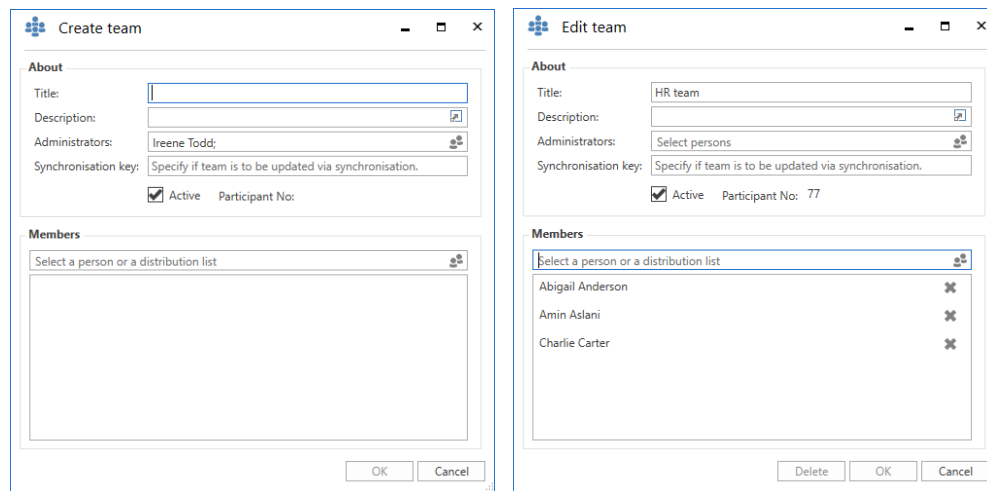


Figure 105: The dialogues in which teams are created and edited

Distribution lists

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

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

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

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

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

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

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

Setting up the main window and the 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 (fixed searches). These are accessed on the left side of the main window. For more information about searches and the use of standard lists, see the manual *F2 Desktop – Searches*.

Fixed searches apply to one of the following:

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

The last two types of fixed searches can only be created by a user 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 by clicking on the “Archive” list from where the search is performed, either as a simple search or as an advanced search.

Click the **Advanced search** menu item in the main window to display the advanced search fields. These are divided into search groups. To see the search fields of a group, hover the cursor over its name or click it.

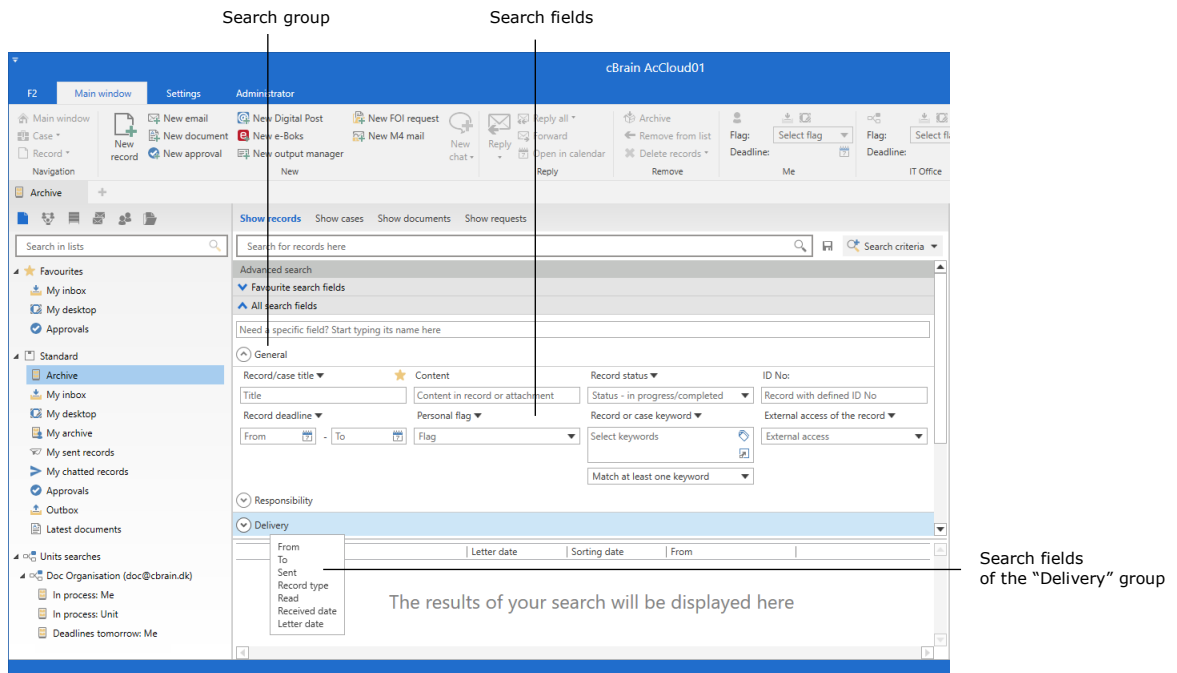



Figure 106: Advanced search

Fill in the relevant fields in one or more search groups, and click the **magnifying glass** or press **Enter** to start the search. Click the **disk icon**  to save the search.

The administrator can make the search visible only to themselves (Personal search), to everyone (Standard), or to selected units (Unit search). For unit searches, a unit must be specified. Give the search a title that correlates with the content of the search.

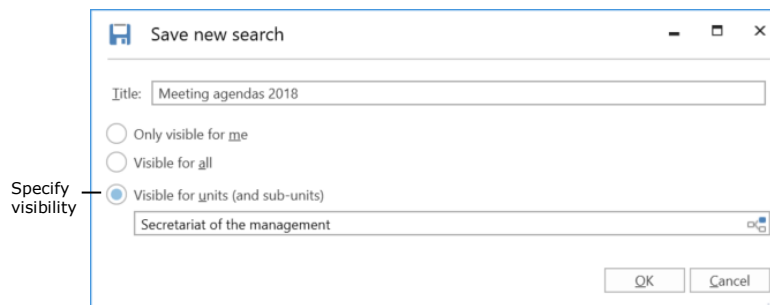


Figure 107: Save a search as a unit search

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

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

Standard searches

F2 comes with a number of standard searches which an administrator may remove or edit. If an administrator creates a fixed unit search, it is available to all users in that unit and any sub-units.

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

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

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

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

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

Title	Description
Inbox ([unit name])	My unit's inbox
Desktop ([unit name])	My unit's desktop
Archive ([unit name])	My unit's archive
In process: Me	Being processed by me
In process: Unit	Being processed by my unit
Deadlines tomorrow: Me	The deadline for me is tomorrow
Deadlines tomorrow: Unit	The deadline for my unit is tomorrow
F2 Requests to unit	F2 Requests to my unit
F2 Requests from unit	F2 Requests from my unit

Title	Description
Post list: Mine – The past 2 days	My post list
Post list: Mine – The past week	My post list, weekly
Post list: The unit’s – The past two days	The unit’s post list the past two days
Post list: The unit’s – The past week	The unit’s post list, the past week

Delete fixed searches

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 “Unit”, it can only be deleted by an administrator.

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

Right-click on the **record icon** on the navigation line in the main window to open the context menu. Then click **Show all** to show all units.

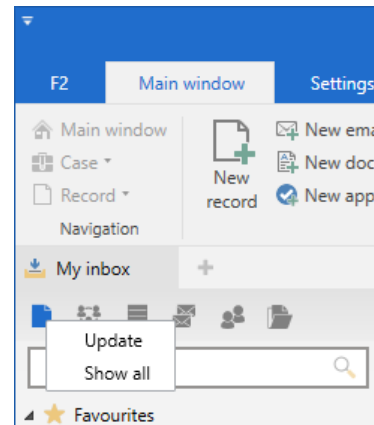


Figure 108: Show all units

The list view expands to display all of F2's units. A search within a unit can then be deleted by right-clicking.

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

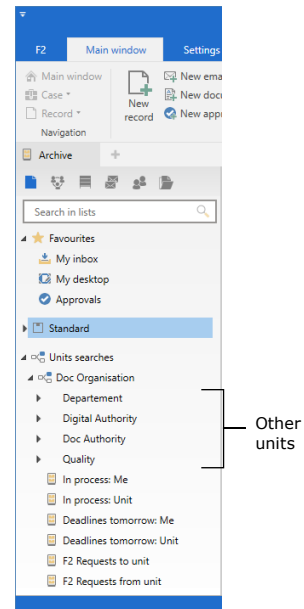


Figure 109: Unit overview

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.

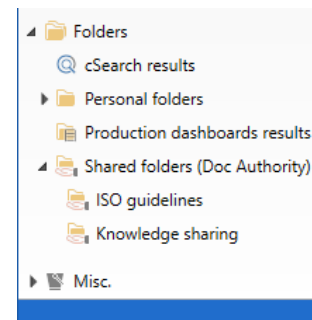


Figure 110: Shared folders in the main window

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

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

Setting up standard column layouts for search results and folders

In F2, the 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 the standard column layout in *F2 Desktop – Settings and Setup*.

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 column layout can reset their column layout to the global standard. Read more about resetting the column layout in *F2 Desktop – Settings and Setup*.

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.

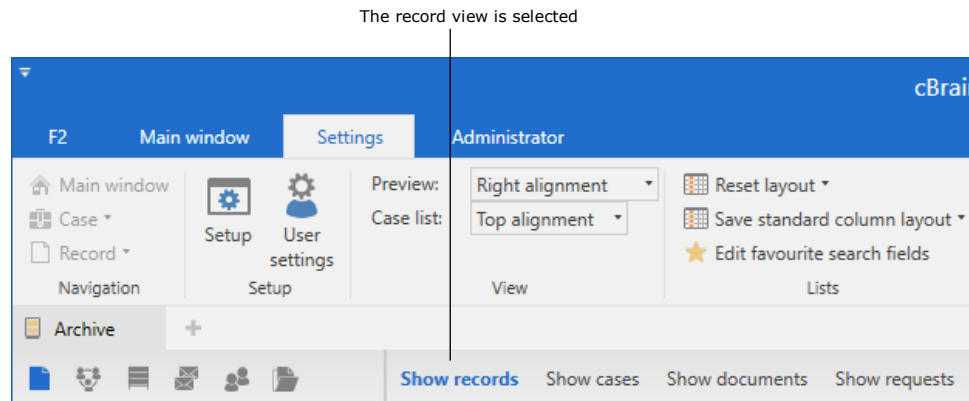


Figure 111: Result list view in the main window

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 **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. In this example, the “From” column is selected.

6) Toggle auto grouping on the "Settings" tab by clicking on **Auto grouping**.

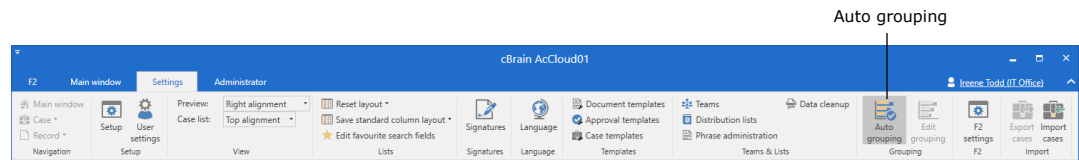


Figure 112: Activate auto grouping

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

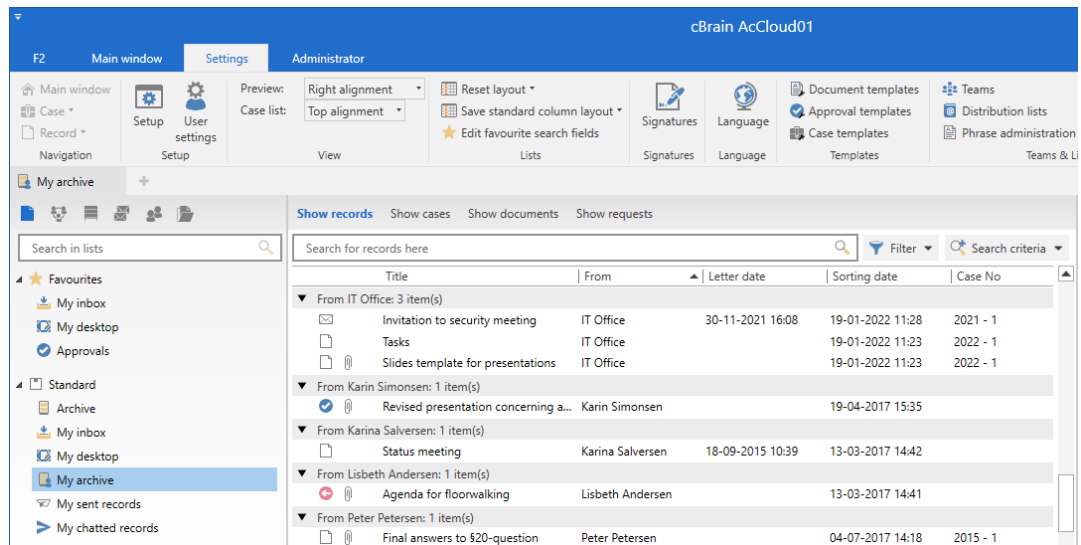


Figure 113: Final global standard column layout for the record view

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**.

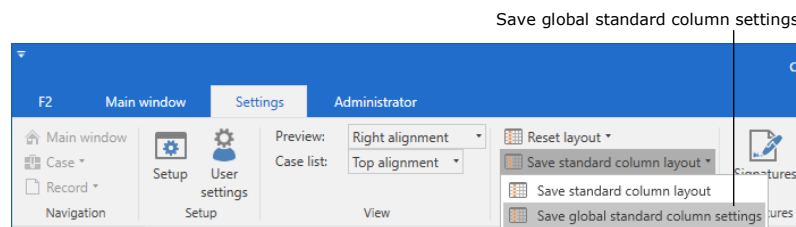


Figure 114: Save global standard column settings

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

Note: Existing global standard column settings will be overwritten when new standard column settings are saved. It is always the most recently saved standard column settings that apply.

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

Note: Fixed standard searches must be checked when metadata fields are changed (added or deleted) when F2 is updated.

User settings

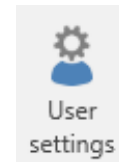
The “User settings” menu item provides access to defining and creating a number of user settings. User settings include user setup, column settings, and list settings.

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.

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.



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

Figure 115: The “User settings” menu item

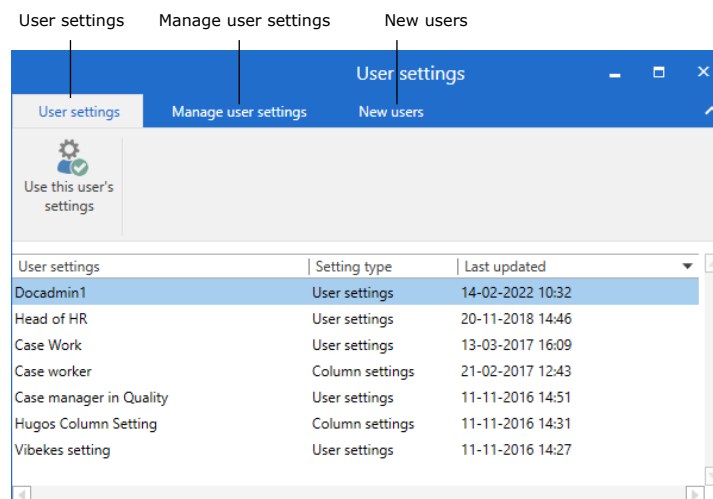


Figure 116: The “User settings” dialogue

The dialogue consists of three tabs:

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

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.

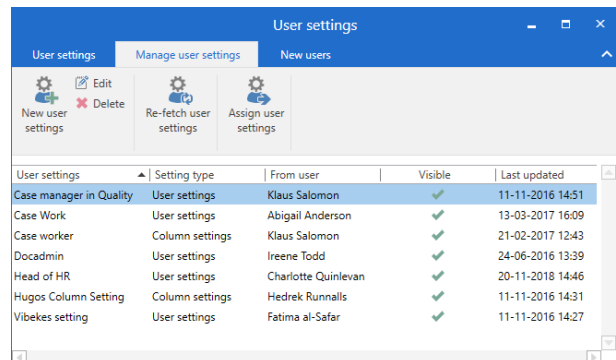
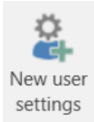



Figure 117: The “Manage user settings” tab

The tab has the following menu items:

Function	Description
	Add a new user setting to the user setting list. Read more in the <i>Create a new user setting</i> section.
	Edit the selected user setting. In the “Edit user settings” dialogue name and visibility can be changed. Click Next to view the individual user settings.

Edit user settings [X]

Here you can change the name and view/edit the configuration details (Next).



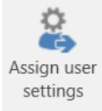
Name:

User:

Type:

Visible to users

Figure 118: The “Edit user settings” dialogue

Function	Description
	<p>Note: When user settings have been edited, they must be reassigned by either the administrator or the user for the changes to be applied.</p>
 Delete	Permanently delete the selected user setting from the list.
 Re-fetch user settings	<p>Retrieve the user's latest user settings, updating the selected user settings.</p> <p>Note: When user settings have been updated, they must be reassigned by either the administrator or the user for the changes to be applied.</p>
 Assign user settings	Assign the selected user settings to users or role types. Read more in the section <i>Assign user settings to users or role types</i> .

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.

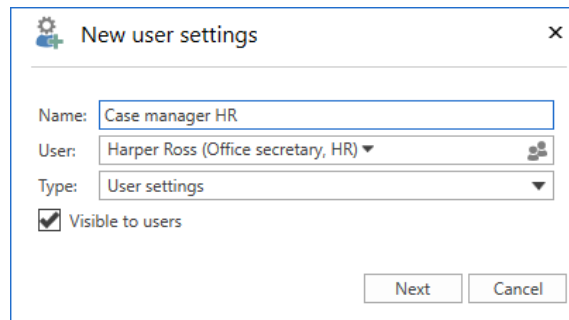


Figure 119: Create a new user setting

Create a new “User settings” type of settings that are added to the list 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 setting* section. If “Column settings” is chosen as the type, the “Choose column settings” dialogue opens. See the *New column settings* section. If “List settings” is chosen as the type, the “Select list settings” dialogue opens. See the *New list settings* section.

New user settings

When “User settings” is chosen as the type in the “New user setting” dialogue, click **Next** to open the “Setup” dialogue. Here, the different options for the new user setting can be selected.

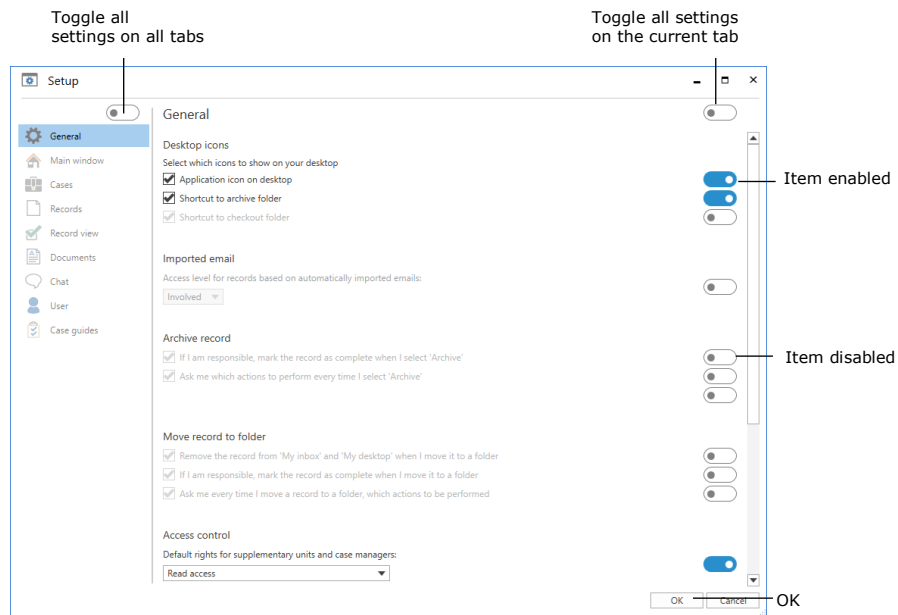


Figure 120: The "Setup" dialogue with sliders

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. Once the slider is blue, the entire setup is chosen. If the slider is white, none of the user's setup options are chosen.

It is also possible to include the all settings of a single tab in a new user setting. To do this, first click on the relevant tab on the left side, then click on the slider in the upper right corner of the dialogue. 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 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 role types.

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

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.

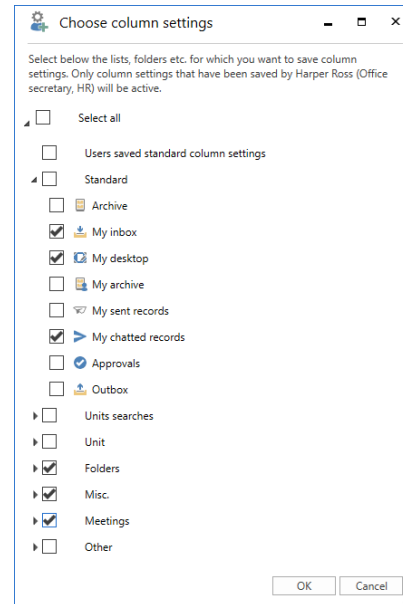


Figure 121: The “Choose column settings” dialogue

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

Note: It is not possible to assign 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.

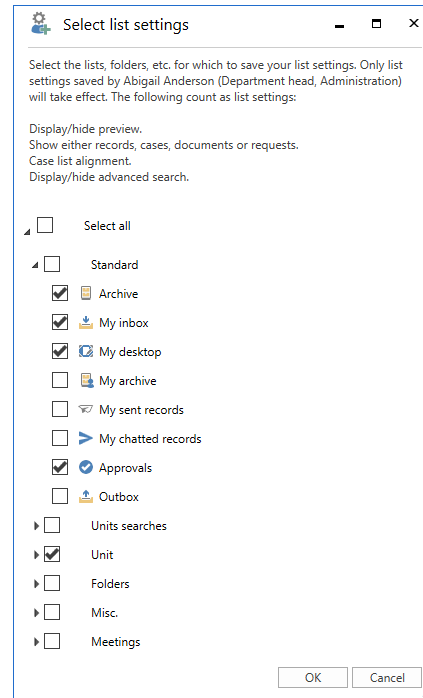


Figure 122: The “Select list settings” dialogue

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”.

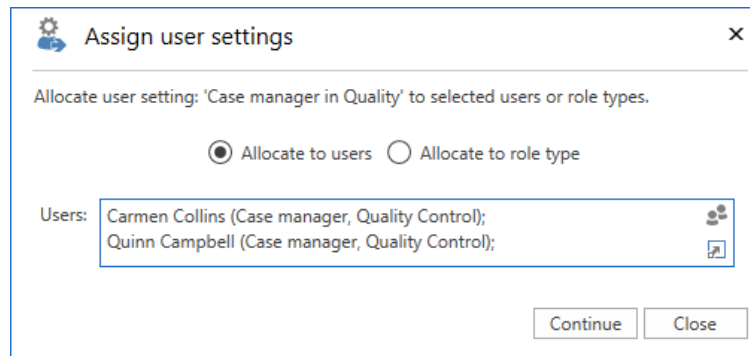


Figure 123: Assign user settings to users

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.

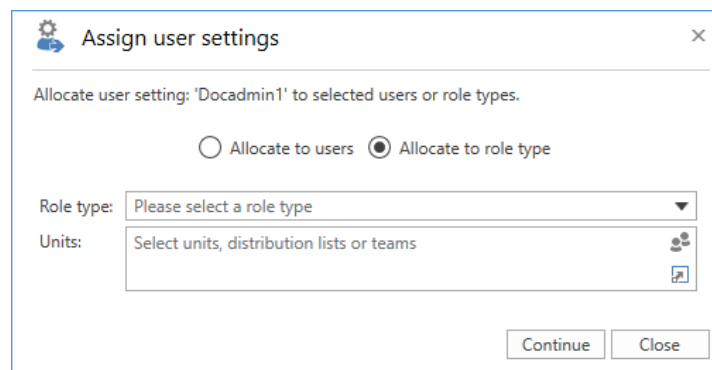


Figure 124: Assign user settings to a role type

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**.

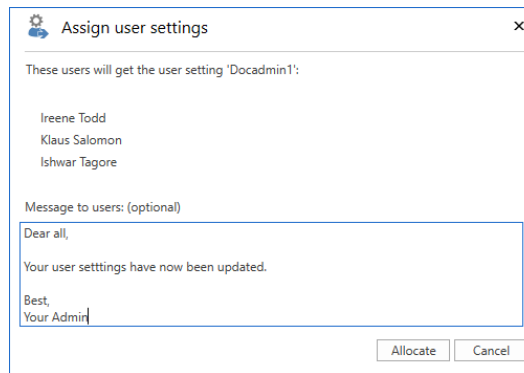


Figure 125: Send a message to the selected users

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 “Department head” role type can have different

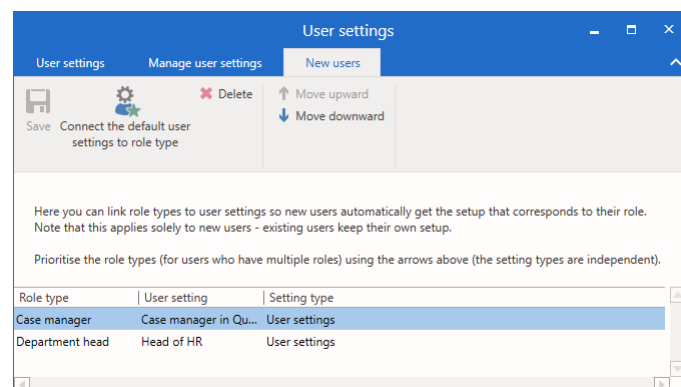

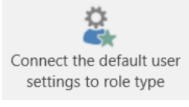
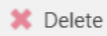
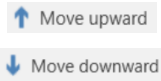


Figure 126: The “New users” tab

user settings than e.g. the “Case manager” role type.

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

Function	Description
	Saves any changes, including the association of user settings to a role type.
	Connects 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.
	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.
	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 **Connect the default user settings to role type** to attach a user setting to a specific role type.

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

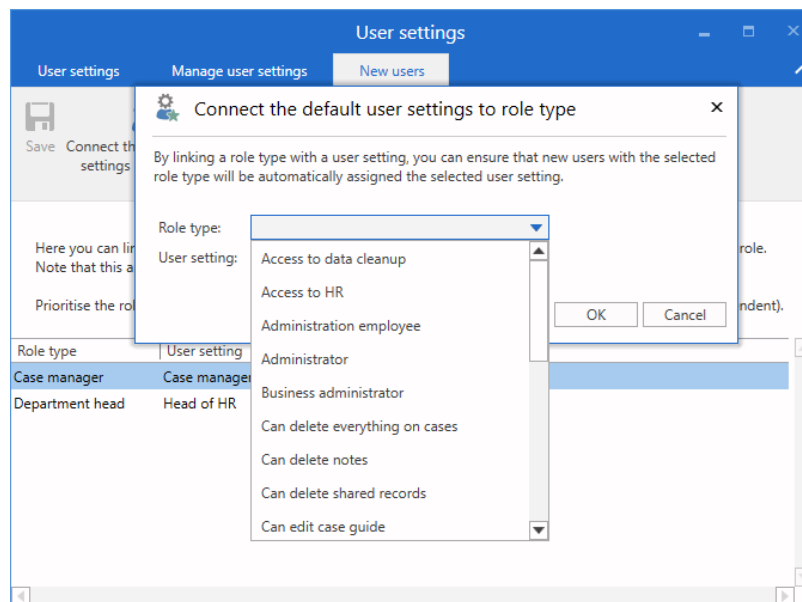


Figure 127: Assign a user setting to a role type

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

The rules for user settings:

- User settings assigned to role types only affect new users. Existing users whose job role is assigned a new user setting are not affected.
- If a new user is assigned a role type, the user automatically receives its user settings, if any.
- If a new user is assigned multiple role types with user settings, the user automatically receives the user settings of the highest ranking role type 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.

F2 supports the following file formats for templates: DOCM, DOCX, DOT, DOTX, DOTM, XLSX, XLT, XLTX, XLTM, POT, POTX, ODT, ODS, ODP, OTT, OTS and OTP.

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

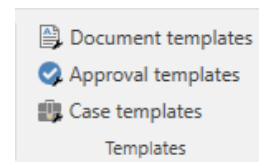


Figure 128: Manage templates

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

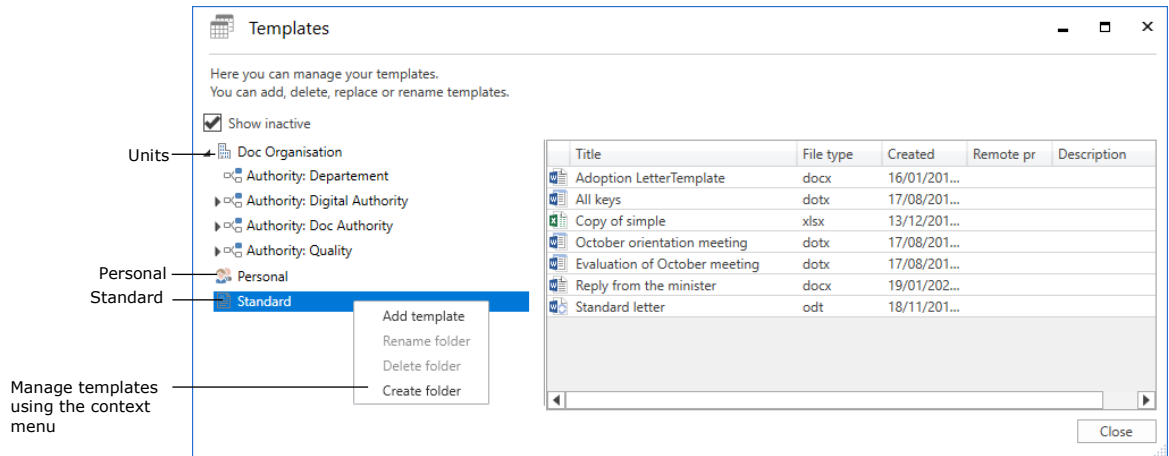


Figure 129: Managing document templates

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

F2 Settings

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

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 130: The “F2 Settings” menu item

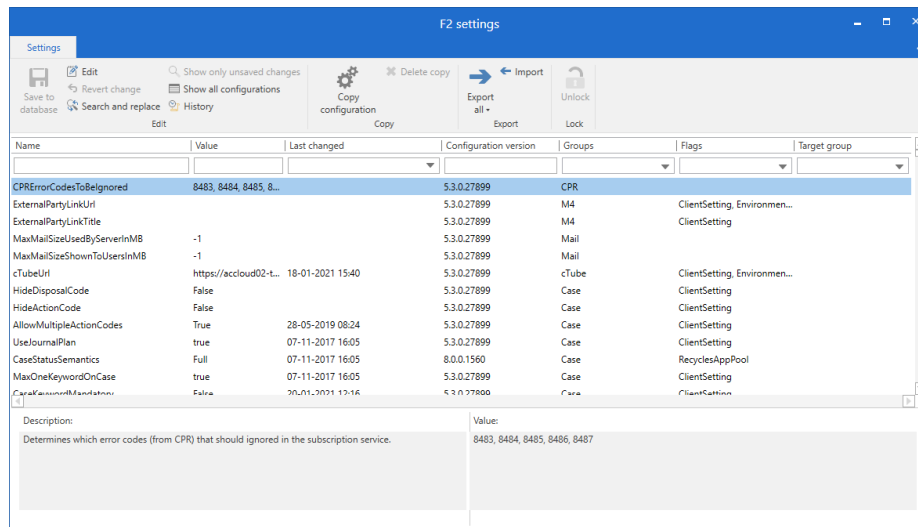


Figure 131: The “F2 settings” dialogue

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.

List of figures

Figure 1: The ribbon on the "Administrator" tab in the main window	9
Figure 2: An example of F2's tree structure.....	10
Figure 3: The "Unit and users" menu item	11
Figure 4: Create a new authority	11
Figure 5: The "Create unit" dialogue	12
Figure 6: The "Email settings" tab in the "Create unit" dialogue.....	12
Figure 7: The "Create authority?" dialogue.....	13
Figure 8: The newly created authority	13
Figure 9: The "Units and users" menu item	14
Figure 10: F2 is installed with only one top unit.....	14
Figure 11: Create units within an authority	15
Figure 12: The "Create unit" dialogue.....	15
Figure 13: The "Unit types" menu item.....	16
Figure 14: Management of unit types	16
Figure 15: The "Units and users" menu item	18
Figure 16: Create user	19
Figure 17: User information	19
Figure 18: The "Roles" tab in the "Create user" dialogue.....	21
Figure 19: Add a role to a new user	21
Figure 20: Assign a role to a new user.....	22
Figure 21: The "Units and users" menu item	22
Figure 22: Deactivate a user	22
Figure 23: The warning dialogue when deactivating a user.....	23
Figure 24: A deactivated user.....	23

Figure 25: The "Units and users" menu item 23

Figure 26: Reactivate a user 24

Figure 27: The "Properties" dialogue for the reactivated user 25

Figure 28: The "On behalf of" menu item 26

Figure 29: The "On behalf of" dialogue 27

Figure 30: Assigning "on behalf of" rights for all areas..... 27

Figure 31: Select the location for approval notifications 28

Figure 32: Select a specific inbox..... 28

Figure 33: Assign "On behalf of" rights for processing approvals..... 28

Figure 34: The "Units and users" menu item 29

Figure 35: The "Units and users" dialogue 30

Figure 36: Setting up a unit inbox..... 30

Figure 37: Identification of email replies 32

Figure 38: Configure the subject field for emails 33

Figure 39: The "Assign role to users" menu item 40

Figure 40: The "Assign role to users" dialogue..... 40

Figure 41: Select user 41

Figure 42: Assign a role to the user 41

Figure 43: Assign a role type to a user 42

Figure 44: Add or remove a role from a user..... 42

Figure 45: The "Role types and privileges" menu item 43

Figure 46: Role types and maintaining them 43

Figure 47: The "New role type" dialogue 43

Figure 48: The "Role types and privileges" menu item 45

Figure 49: The "Role types and privileges" dialogue 45

Figure 50: The "New privilege" dialogue 46

Figure 51: Edit or delete a privilege	46
Figure 52: The "Edit privilege" dialogue	46
Figure 53: Assignable privileges	47
Figure 54: The "Administrator read access to all records" privilege.....	53
Figure 55: The "Read access to all records" menu item.....	53
Figure 56: A new privilege type - "Archive access".....	53
Figure 57: The "Creates cases" privilege	54
Figure 58: The "Distribution list editor" privilege.....	54
Figure 59: The "Editor of participants" privilege	54
Figure 60: The "Keyword administrator" privilege	55
Figure 61: Security groups are created under an authority.....	56
Figure 62: Authorities and security groups	57
Figure 63: The "Create security group" menu item.....	57
Figure 64: The "Create security group" dialogue	58
Figure 65: The "Add users to security groups" menu item	58
Figure 66: The "Add users to security groups" dialogue	59
Figure 67: The "Show security groups" menu item	60
Figure 68: The "Security groups" dialogue	60
Figure 69: Properties for a security group	61
Figure 70: The "Show security groups" menu item	61
Figure 71: Deactivate security group.....	61
Figure 72: Import participants.....	63
Figure 73: Import file	66
Figure 74: The "Replace record participants" menu item	66
Figure 75: The "Value list administration" menu item	67
Figure 76: The "Value list administration" dialogue	67

Figure 77: The context menu of a value list	68
Figure 78: Sorting a value list	69
Figure 79: Value list administration	69
Figure 80: Create a new value list.....	69
Figure 81: Example of value list item in XML file	70
Figure 82: Context menu for the "Flag" value list.....	71
Figure 83: Importing value list items.....	71
Figure 84: Creating a value list item from the "Flag" list	72
Figure 85: Example of the control flag menu on a record	73
Figure 86: The "Flags for personal control" menu item	73
Figure 87: The "Flags for personal control" dialogue.....	73
Figure 88: Name the control flag	74
Figure 89: The "Keyword administration" menu item.....	75
Figure 90: Administration of keywords	75
Figure 91: The "Relevant keywords for units" menu item	76
Figure 92: Select keywords.....	77
Figure 93: The "System messages" menu item.....	78
Figure 94: The "System messages" dialogue	78
Figure 95: Create a new system message.....	78
Figure 96: F2's participant register in the main window	79
Figure 97: Create external participant	80
Figure 98: The "Create new participant" dialogue	81
Figure 99: F2 suggests placing a new participant under an existing one.....	82
Figure 100: Participant who owns an email domain	82
Figure 101: Right-click on a participant in the participant register	83
Figure 102: The "Change image" dialogue	83

Figure 103: The “Teams” menu item	85
Figure 104: The “Teams” dialogue	85
Figure 105: The dialogues in which teams are created and edited	86
Figure 106: Advanced search	89
Figure 107: Save a search as a unit search	89
Figure 108: Show all units	91
Figure 109: Unit overview.....	92
Figure 110: Shared folders in the main window	92
Figure 111: Result list view in the main window.....	94
Figure 112: Activate auto grouping	95
Figure 113: Final global standard column layout for the record view.....	95
Figure 114: Save global standard column settings	95
Figure 115: The “User settings” menu item	97
Figure 116: The “User settings” dialogue	97
Figure 117: The “Manage user settings” tab	98
Figure 118: The “Edit user settings” dialogue	98
Figure 119: Create a new user setting	100
Figure 120: The “Setup” dialogue with sliders	101
Figure 121: The “Choose column settings” dialogue	102
Figure 122: The “Select list settings” dialogue	103
Figure 123: Assign user settings to users.....	104
Figure 124: Assign user settings to a role type	104
Figure 125: Send a message to the selected users.....	105
Figure 126: The “New users” tab	105
Figure 127: Assign a user setting to a role type	107
Figure 128: Manage templates	108

Figure 129: Managing document templates 109

Figure 130: The "F2 Settings" menu item 110

Figure 131: The "F2 settings" dialogue 110