

# Medikro Administration Tool

## User Manual

---



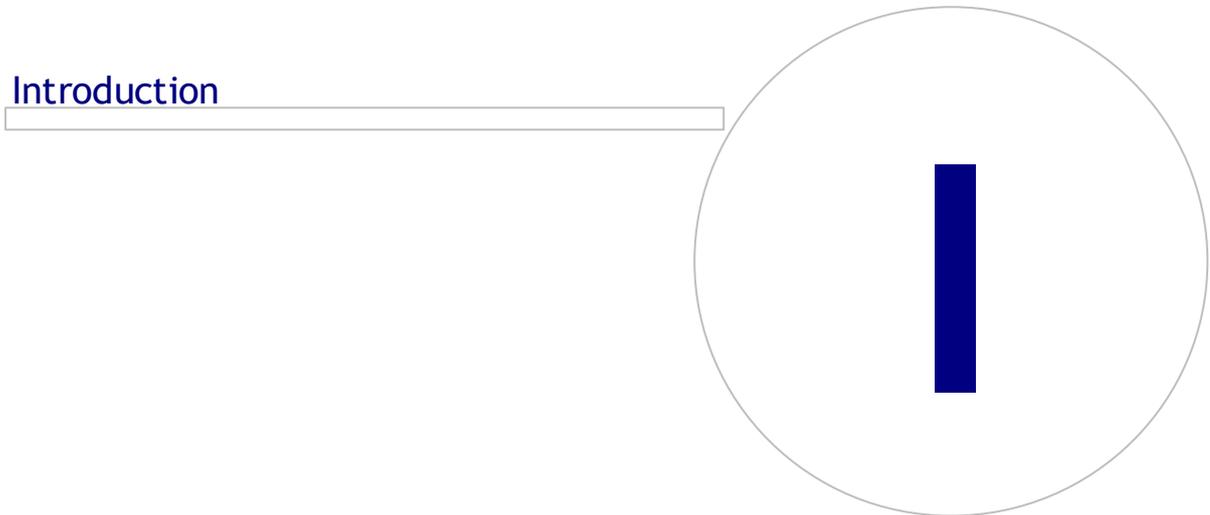


# Table of Contents

<b>1 Introduction</b>	<b>5</b>
1.1 About this Manual.....	6
1.2 Terminology, Acronyms and Abbreviations.....	6
<b>2 General Information</b>	<b>7</b>
2.1 Navigating in Administration Tool.....	8
2.2 Sign in .....	8
2.3 How to Access Sections of Administration Tool.....	9
2.4 How Administration Tool Manages Settings.....	12
<b>3 Settings Management</b>	<b>15</b>
3.1 Access Control Settings.....	17
3.2 Audit Trail Settings.....	17
3.3 General Storage Settings.....	18
3.4 Database Connection Settings.....	18
3.5 Application Settings.....	19
3.6 Import/Export Settings.....	19
3.7 Person Information Settings.....	21
3.8 Person Search Settings.....	21
3.9 Study Settings.....	21
3.10 Other Settings.....	22
<b>4 Access Management</b>	<b>23</b>
4.1 Manage Access Roles.....	25
4.2 Manage Users.....	27
4.3 Manage Organization.....	27
4.4 Manage Department.....	28
<b>5 Audit Trail Viewer</b>	<b>29</b>
5.1 Using Audit Trail Viewer.....	31



## Introduction



## 1 Introduction

# User Manual

## for Medikro Administration Tool



This document is intended for system administrators. This manual explains configuration options and instructs on how to manage and configure the Medikro software system.

### 1.1 About this Manual

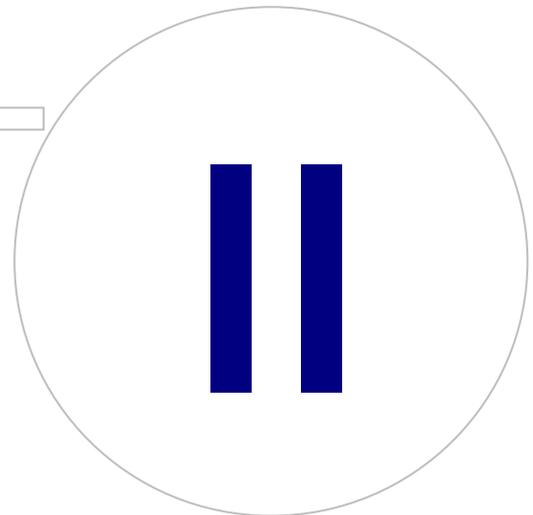
This manual contains instructions for using Medikro Administration Tool. Administration Tool users should be familiar with Medikro Persons and Studies features and functionality (see *Medikro Spirometry Software User's Manual*), and used database configuration (see *Medikro Spirometry Software Installation Guide*).

### 1.2 Terminology, Acronyms and Abbreviations

Table: Terminology, acronyms and abbreviations

Term	Description
GDT	Device data transfer. A format to transfer data among medical devices and software systems.
TCP/IP	Set of protocols to communicate over internet.
ODBC driver	Open Database Connectivity driver for accessing database management systems.
SQL	Structured query language for database queries.
INI file	Configuration file.
Plugin	Software component that adds a feature to a program.
Custom field	Configurable person information field.

## General Information



## 2 General Information

This chapter provides basic information how to authenticate and navigate on Medikro Administration Tool and how to access different parts of the application. This gives more detailed information on how the settings are managed and distributed to workstations.

### 2.1 Navigating in Administration Tool

In Medikro Administration Tool, the user can:

- Customise Medikro Persons and Studies appearance and functionality (see chapter [Settings Management](#)<sup>[16]</sup>)
- Manage Medikro Software users and their roles (see chapter [Access Control Management](#)<sup>[24]</sup>)
- View Medikro Software actions (see chapter [Audit Trail Viewer](#)<sup>[30]</sup>)

These tasks can be accessed by selecting a corresponding button (see Table 1).

Table 1: Medikro Administration Tool Buttons

Button	Description
	<b>Home</b> button. Opens Administration Tool Main view.
	<b>Settings Management</b> button. Opens Settings Management view.
	<b>Access Management</b> button. Opens Access Management view.
	<b>Audit Trail</b> button. Opens Audit Trail Viewer.

### 2.2 Sign in

Windows administrators can sign in to Administration Tool. Windows administrators are granted with full privileges and can access all sections of Administration Tool. Because of this it is not advised to install the Administration Tool to such a workstation where all Windows users have administration rights.

Other users are allowed to sign in to the Administration Tool only if they have a Medikro Spirometry Software user account configured in Access Control Management. (See chapter [Access Control Management](#)<sup>[24]</sup>) Note that local access control system cannot be used to authenticate Administration Tool sign in. In such systems only Windows administrators are allowed to sign in.

**Sign in as Windows administrator:** If user has currently logged in to Windows as a Windows administrator then it is possible to sign in without entering credentials by choosing to login as current user. It is always possible to use any Windows administrator account by choosing to sign in as other user and entering credentials.

**Sign in as authenticated user:** Users with Medikro Spirometry Software accounts are authenticated using information from the support database. Therefore connection to the database must be established. If the account type is Windows user based or Windows group based then user should sign in as Windows user. If the account type is internal then user should sign in as internal user and enter credentials.

## 2.3 How to Access Sections of Administration Tool

### Administration Tool Sections

Different sections in Administration Tool require different privileges. Additionally, some of the sections require connection to a database to be established. Some of the sections are free to access by all logged in users. Access to sections is illustrated in Figure 1, the sections that require connection to a database are illustrated in Figure 2.

**Settings Management:** All users can load settings from local Persons and Studies application, import settings from a file or export settings to a file. Most of the settings can be freely read and modified by all users. The following sections in Settings Management are restricted only to users with corresponding privileges:

- Access control settings can only be written by a user with privilege to manage access control.
- Audit trail settings can only be written by a user with privilege to access Audit Trail Viewer.
- Connection settings to person, study and support databases can only be written by a user with privilege to write database settings locally.
- Connection settings to action database can only be viewed and written by a user with privileges to access Audit Trail Viewer.
- Loading settings configurations from online database can only be done by a user with privileges to download settings. Connection to a support database containing settings needs to be established when entering the section. Connection can be established using administrative credentials that were set in Database Creator installer (See chapter *Creating Databases in Medikro Spirometry Software Installation Guide*) or any database server user with SQL-select rights to support database.
- Saving settings configurations to online database can only be done by a user with privileges to distribute settings. Connection to a support database containing settings needs to be established when entering the section. Connection can be established using administrative credentials that were set in Database Creator installer (See chapter *Creating Databases in Medikro Spirometry Software Installation Guide*) or any database server user with SQL-select, SQL-insert and SQL-update rights to support database.

**Access Control Management:** Entering Access Control Management can only be done by a user with privileges to manage access control. Connection to a support database containing access control information needs to be established when entering the section. Connection can be established using administrative credentials that were set in Database Creator installer (See chapter *Creating*

Databases in Medikro Spirometry Software Installation Guide) or any database server user with SQL-select, SQL-insert, SQL-update and SQL-delete rights to support database. Alternatively, if local access control is used, a local access database file can be connected instead.

**Audit Trail Viewer:** Entering Audit Trail Viewer can only be done by a user with privileges to manage audit trail. Connection to an action database containing audit trail needs to be established when entering the section. Connection can be established using administrative credentials that were set in Database Creator installer (See chapter Creating Databases in Medikro Spirometry Software Installation Guide) or any database server user with SQL-select rights to action database. If an offline audit trail is wanted to be viewed, a local audit trail database file can be connected instead.

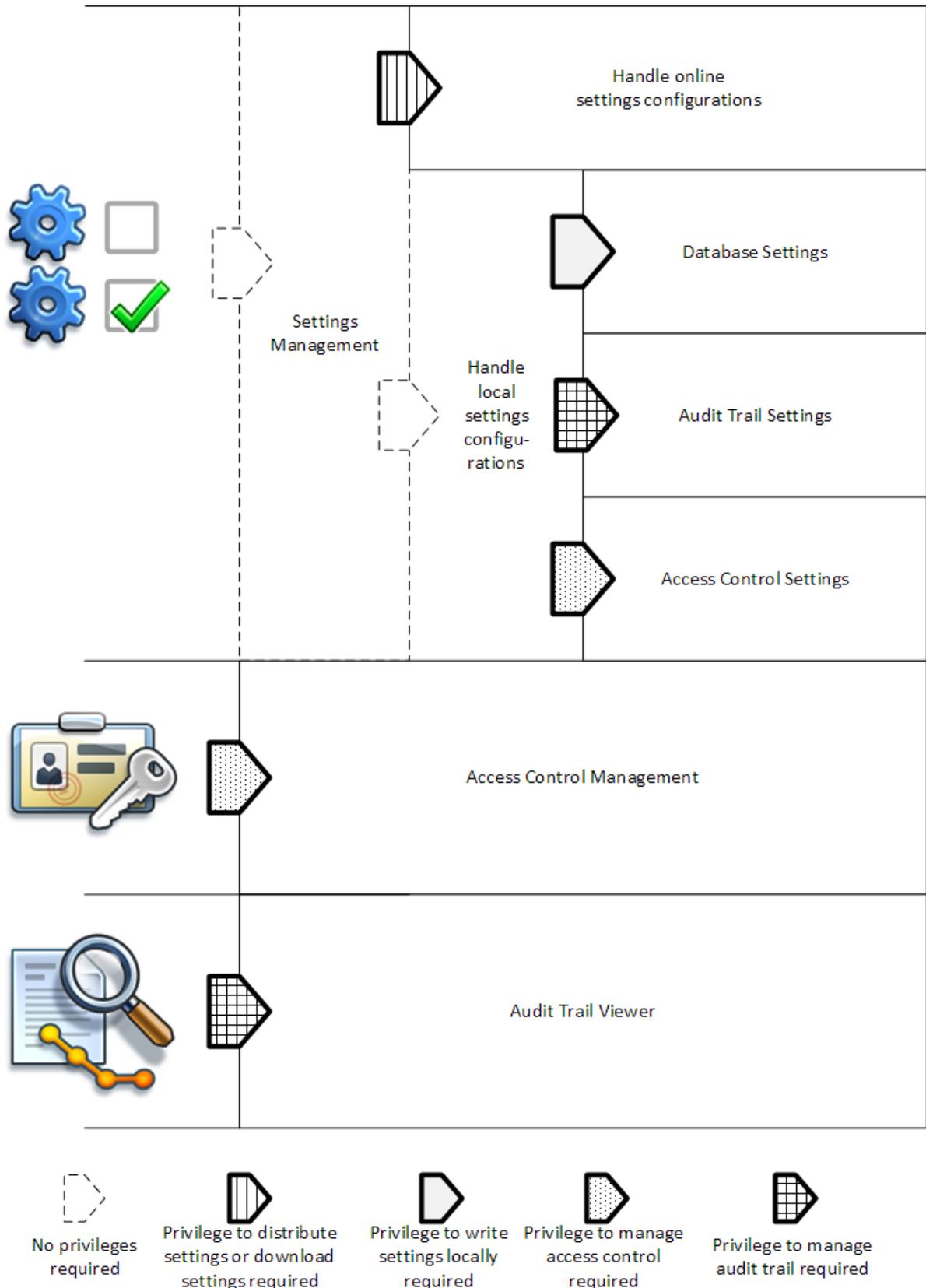


Figure 1: Administration Tool sections that need privileges to enter.

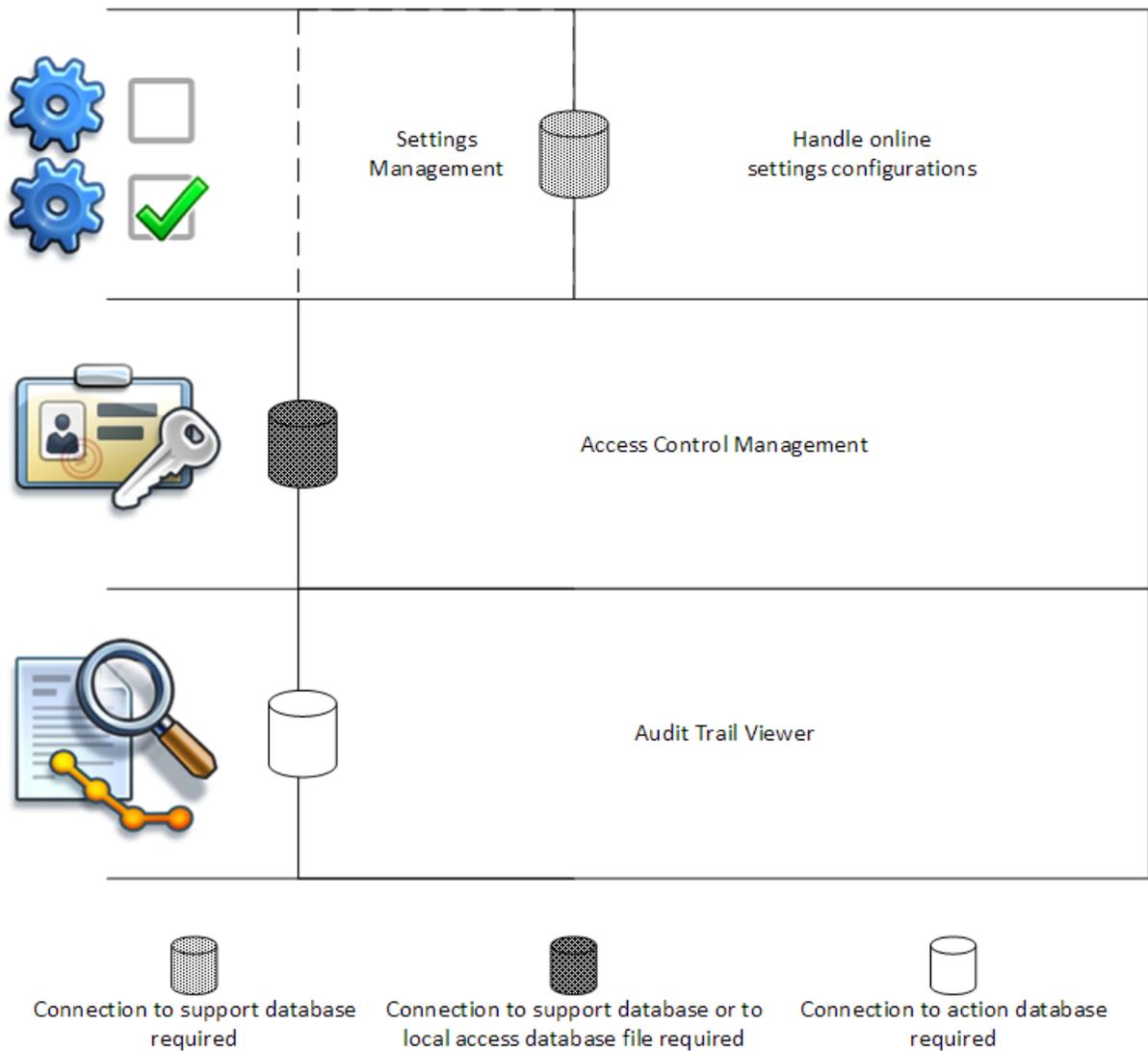


Figure 2: Administration Tool sections that need connection to the database.

## 2.4 How Administration Tool Manages Settings

For more information about settings management see chapter [Settings Management](#)<sup>16</sup>.

The source for managing the settings can be one of three kinds: local application settings, settings from online database or imported settings. Similarly, the settings can be passed out in three ways: saving to local application, saving to online database or exporting to a file. Figure 3 explains this further. In single workstation installations only the local application is usually managed, but in multiple workstation installations it is often possible to use online configurations as well. The usage of online configurations is illustrated in Figure 4.

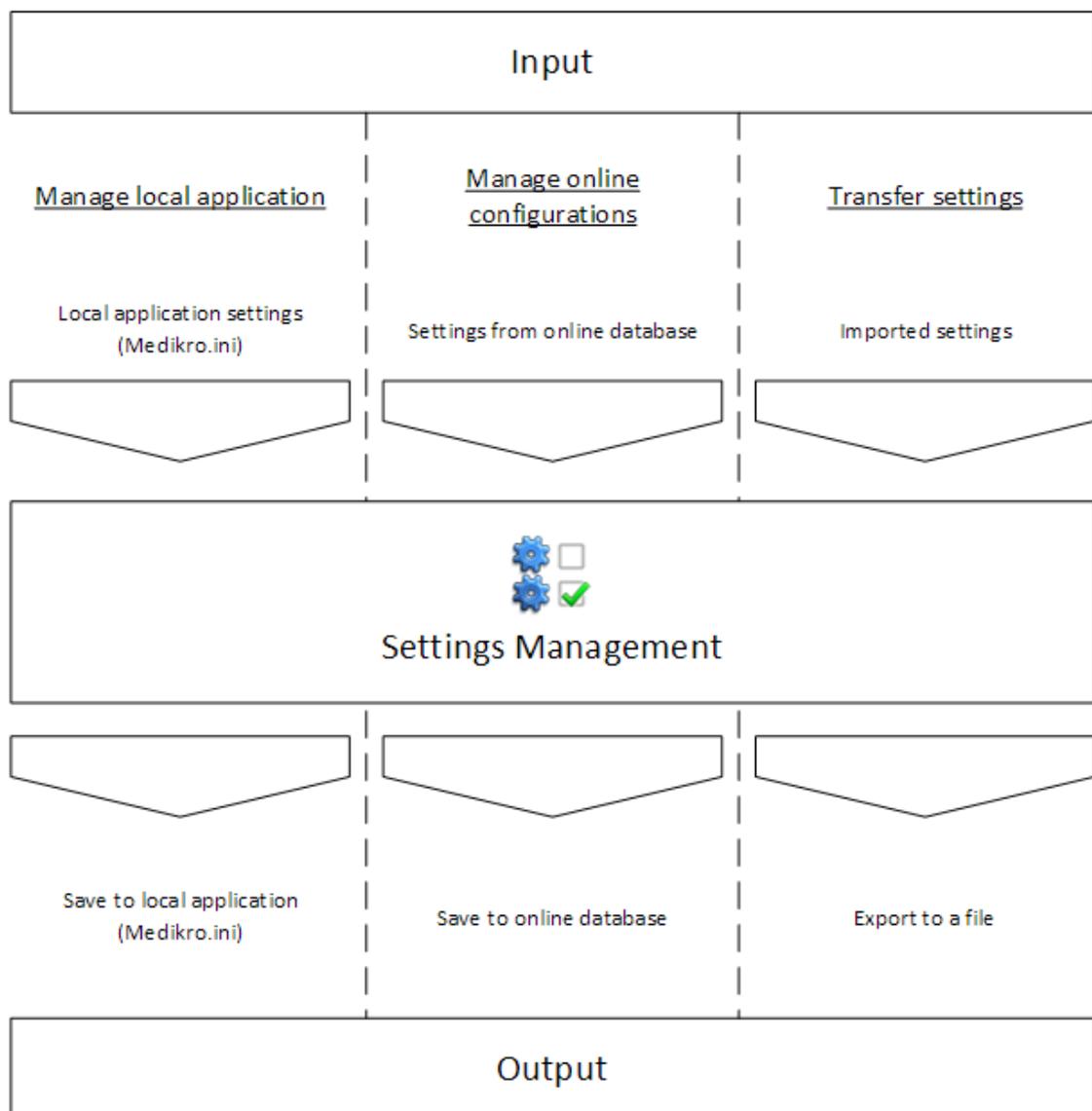


Figure 3: Settings input and output in Administration Tool Settings Management.

Settings can be brought to Settings Management from local Persons and Studies application if it is installed on the same workstation as the Administration Tool. Persons and Studies stores the settings in a configuration file called "Medikro.ini". The file is stored in the program data location in the workstation ("C:\ProgramData\Medikro" by default). Local application settings can be loaded by selecting "*Load settings from local application*" from "*Manage local application*" menu at the bottom of the Settings Management section.

Settings can be loaded from the online support database if one is available. Loading the settings from online database requires the privilege to download settings and the right to SQL-select from the settings table at the database server. Online settings can be loaded by selecting "*Manage settings configurations*" from "*Manage online configurations*" menu at the bottom of the Settings Management section. A dialogue opens where connection information can be inserted when "*Show connection options*" is clicked. Connection is established when "*No connection - connect*" is clicked. After connection is established, the settings configurations are displayed in the drop-down list. The title information displays the configuration ID, creation time and the author of the configuration.

Configuration notes will be displayed when the configuration is selected. The configuration is loaded when the "Load configuration" button is pressed at the bottom of the dialogue.

Settings can be imported from an external file composed by the Administration Tool. Importing can be done by selecting "Import settings" from "Transfer settings" menu at the bottom of the Settings Management section.

In Administration Tool the settings can be managed and passed on in any way regardless of the source of the settings. This makes it possible to transfer settings between local application, online database and a file in file system.

Settings can be saved to local Persons and Studies application if it is installed on the same workstation as the Administration Tool. Settings can be saved to local application by selecting "Save settings to local application" from "Manage local application" menu at the bottom of the Settings Management section.

Settings can be saved to the online support database if one is available. Saving the settings to the online database requires the privilege to distribute settings and the right to SQL-insert and SQL-update to the settings table at the database server. Online settings can be saved by selecting "Distribute settings" from "Manage online configurations" menu at the bottom of the Settings Management section. A dialogue opens where connection information can be inserted at the top of the dialogue. The configuration is saved by clicking "Save to database". The configuration can be distributed and made available to Persons and Studies users by clicking "Distribute to users", note that this also saves the configuration and no additional saving is needed. The configuration ID, creation time and the author of the configuration will be automatically added to the configuration data once the configuration is saved. Release notes may be added to the section below the connection settings. If "Inform user about settings change" is selected the notes will be displayed to Persons and Studies users in Persons and Studies splash screen.

Settings can be exported to an external file by selecting "Export settings" from "Transfer settings" menu at the bottom of the Settings Management section.

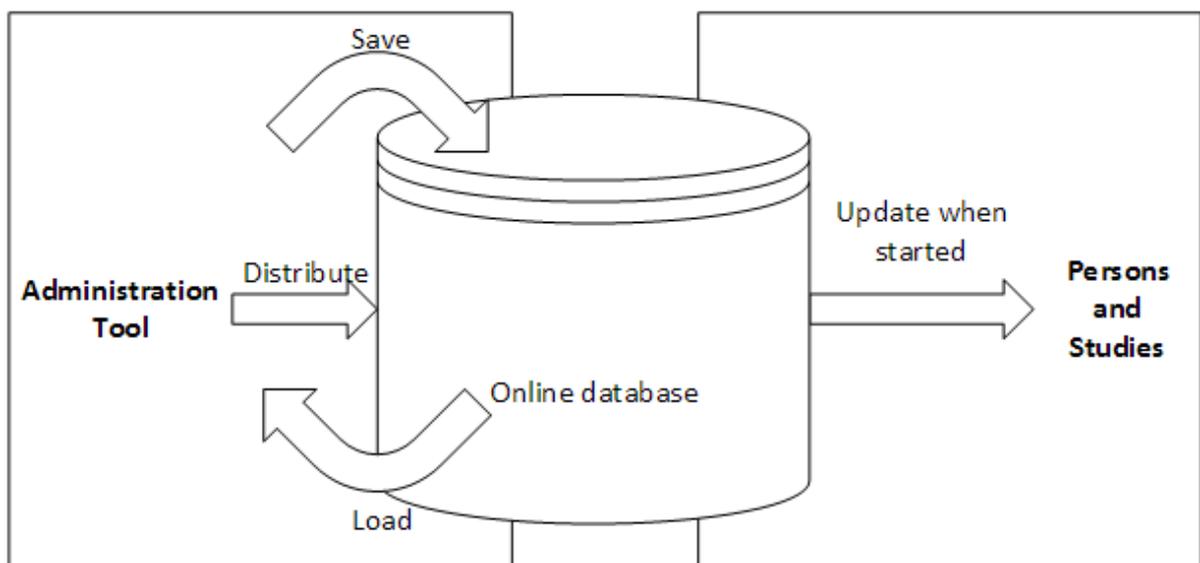
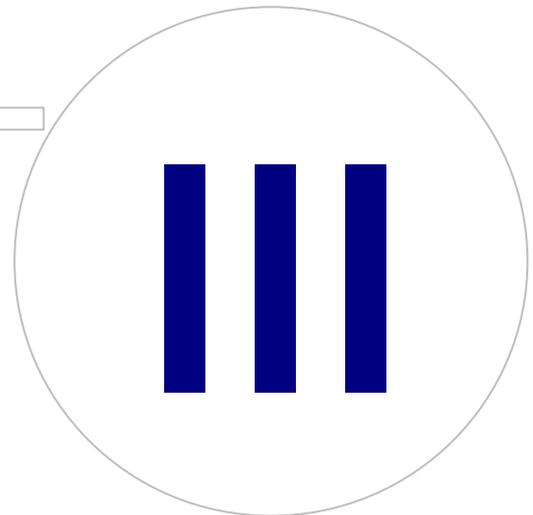


Figure 4: Online settings configuration management.

## Settings Management



## 3 Settings Management

Administration Tool Settings Management allows to make configurations in Persons and Studies features and user interface. The topics in this chapter explain the purpose of each configuration option. First, the available actions for managing settings are explained.

### Manage local application

Persons and Studies reads setting values from "Medikro.ini" file. When settings are taken into use in one Persons and Studies client, it is useful to handle this settings file locally. It is advisable to keep back up of the settings file.

**Save settings to local application:** Updates settings file on computer in question.

**Enable autosaving to local application:** When selected, settings file on computer in question is automatically updated when Administration Tool is closed.

**Load settings from current application:** Loads values from the settings file in current computer into Administration Tool.

### Manage Online Configurations

When multiple Persons and Studies clients are in use, it might be useful to manage settings centralised. In this case settings are handled via database server, and authorisation to the settings database is needed.

**Distribute settings:** Saving settings to database and distributing settings for the Persons and Studies clients that are connected to the database. In the Settings configuration distribution window, correct database connection and authentication information has to be entered. Configuration note can be added to ease identification of the configuration if needed later. This note is also shown in Persons and Studies message box when started the next time if "Inform users about settings change" is selected. Note that "*Update settings when Persons and Studies starts*" setting has to be configured on in the Persons and Studies settings to retrieve distributed settings (see topic [Application Settings](#)<sup>[19]</sup>).

**Manage settings configuration:** Selecting and deleting configurations from settings database. Correct database connection and authentication information has to be entered by selecting "*Show connection options*" button. After connection to settings database has been established, the drop down list shows configurations that are available. "*Load configuration*" loads values of the selected configuration from the settings database into Administration Tool. "*Delete configuration*" deletes the selected configuration from the settings database.

**See changes made in settings:** Shows the difference between handled settings configurations.

### Transfer Settings

**Import settings:** Loads settings from selected configuration file into Administration Tool.

**Export settings:** Writes Administration Tool settings to selected configuration file.

**Import DBConnection.ini:** Loads [database connection settings](#)<sup>[18]</sup> from selected file.

**Export DBConnection.ini:** Writes [database connection settings](#)<sup>[18]</sup> to selected file.

## 3.1 Access Control Settings

For information about access control management see chapter [Access Control Management](#)<sup>[24]</sup>.

**Access control method:**

- **None:** No access control is used and there is no sign in required. User has privileges to all functions in the application. In this case it should be noted that the user cannot be individualised in the Audit Trail.
- **None, simple identification is required:** No access control is used, but the user has to enter a minimum of two characters into the Persons and Studies sign in dialog.
- **Windows group based:** Authentication is done using user's Windows group membership. No additional sign in required.
- **Windows user based:** Authentication is done using user's Windows login. No additional sign in required.
- **Internal users:** Authentication is done using dedicated Medikro Spirometry Software credentials. User has to sign in to Persons and Studies.

**Local access control system:** If selected, user is authenticated against offline access database in local computer. This option should be selected in single workstation setups.

**Path to local access control database:** Path of the offline access database file.

**Offline cache:** Settings are only valid when using online access control.

**Offline cache enabled:** User credentials are stored in temporary offline database. Enables local authentication in case connection to online database is lost.

**Warn user of expiration:** Warning dialogue shows the remaining expiration when user is signing in to Persons and Studies when connection to online database is lost.

**Expiration time:** User credentials are removed from temporary offline database when expiration time has passed. The expiration time is reset every time the user signs in while online. For example, if expiration time is 5 days, the user can use the same workstation offline for 5 days after his/her latest online sign in.

## 3.2 Audit Trail Settings

For information about audit trail viewing see chapter [Audit Trail Viewer](#)<sup>[30]</sup>.

**Offline audit trail enabled:** Audit Trail is written to offline location if configured not to be written to online database.

**Audit trail offline database location:** Path to a folder where the offline audit trail database is created.

**Online audit trail:** Audit trail is written to the configured action database if not specifically turned off with this setting. Reading or writing this setting requires a connection to be established to the action database.

### 3.3 General Storage Settings

**Offline database location:** Path to a folder where offline databases will be created if connection to online databases cannot be established or if system is configured to exclusively use offline databases.

**Use offline database exclusively:** Local file based databases are used to store person and study data. Audit trail will be written to offline location if offline audit trail is enabled.

**Synchronisation:** For more information about synchronisation see *Medikro Spirometry Software User's Manual* chapter *Database Connection and Synchronisation*. Study and person data from offline databases will be synchronised to online databases when system is connected to them and not configured to exclusively use offline databases.

**Identification criteria:** Selected criteria will be used to determine if person already exists in the database when synchronising.

### 3.4 Database Connection Settings

Database connection settings should be set for online systems. Database settings can be empty for offline systems. Settings are automatically set if "DBConnection.ini" file is used during installation of Persons and Studies or Administration Tool.

**Database:** Select the database you wish to modify settings for. (Databases are described in the *Medikro Spirometry Software Installation Guide* chapter *System Description*)

**SQL type:** Type of the database, MsSQL or MySQL.

**Username:** Username for the database.

**Password:** Password for the database.

**Connection Settings:** Database connection string. Usually contains ODBC driver name and TCP/IP parameters to the database.

Example of SQL Server 2000 connection string connecting person database:

- "Driver={SQL Server};Server=192.168.1.1;Database=persondb;"

Example of MySQL connection string connecting person database:

- "Driver={MySQL ODBC 5.2 UNICODE Driver};Server=192.168.1.1;Database=persondb;"

Note that connection string attributes vary depending on database server and settings. You may need to set attributes like *Network*, *Address* or *Port*.

**Connection parameters:** Database specific connection parameters. Refer to your system's ODBC provider for more information about the values. Values can be set for the following ODBC parameters:

- SQL\_ATTR\_ACCESS\_MODE
- SQL\_ATTR\_LOGIN\_TIMEOUT
- SQL\_ATTR\_CONNECTION\_TIMEOUT
- SQL\_ATTR\_CURRENT\_CATALOG
- SQL\_ATTR\_METADATA\_ID

- SQL\_ATTR\_PACKET\_SIZE
- SQL\_ATTR\_TRACEFILE
- SQL\_ATTR\_TRACE
- SQL\_ATTR\_CONNECTION\_POOLING
- SQL\_ATTR\_ODBC\_VERSION

Connection settings and connection parameters can be given as a single semicolon separated string or by adding values to empty fields.

### 3.5 Application Settings

**Update settings when Persons and Studies starts:** Persons and Studies settings are updated from settings database at start-up.

**Language:** Language for Persons and Studies.

**Date format:** Date format used in Persons and Studies. Medikro Measurements and Results uses Windows' date and time format.

**Default application size:** The size Persons and Studies application window is opened in.

- Saved: Size is the same as when Persons and Studies was closed the last time.
- Standard: Default size that is optimised to use Persons and Studies and Measurements and Results parallel on the screen.
- Full: Full screen.

**Enable notification messages:** Notifications are shown in bottom right corner, for example, when saving data.

**Pre-fill study information:** Study information is pre-filled from person's previous study. For spirometry study, *height*, *weight*, *reference set*, *smoking status*, *smoking info*, *profession*, *illness* and *medication* are prefilled.

**Personal ID systems:** Only selected systems are available to choose from when entering person information in Persons and Studies.

**Default personal ID system:** Default personal ID system when creating new persons.

**Shown ethnic groups:** Only selected ethnic groups are available to choose from when entering person information in Persons and Studies.

**Default ethnic group:** Default ethnic group when creating new persons.

### 3.6 Import/Export Settings

**Import mode:** Defines how to save imported persons and studies if they already exist in the database.

- Insert: Data is taken from the database in case of existing persons and studies. New persons and studies are added to database.
- Update: The information is updated by imported data.

**Table 3: Import Modes**

	Update	Insert
Add persons that are not in the database	X	X
Add studies that are not in the database	X	X
Update information of person existing in the database	X	
Update information of study existing in the database	X	

**Show dialogue if single matching person found:** Select if you want to see a person identification dialogue when only one matching person is found from the database. The dialogue is always shown in case of multiple matches. NOTE: This selection only applies to manual import.

**Identification criteria:** Select fields that are used to find a matching person from the database.

**Default locations:** Directories that are suggested for the user when executing manual import and manual export operations. User can select other locations.

**Default file format:** File format that is suggested for the user when executing manual import and manual export operations. User can select other format.

- SpiroXML2 format: Set default to SpiroXML2 -format defined in SpiroXML2 HIS Interface Document.
- GDT format: Set default to GDT 2.0/3.0 -format. Only one person per file can be exported.

## Automatic Import/Export

Measurements for persons from external systems can be automatically started with Automatic Import/Export functionality. Automatic import is started in home view of Persons And Studies if a specified input file exists. The person is brought to the system and a new study is created.

When measurement is done and the user goes back to home view, Persons and Studies exports the person with studies to a specified location.

**HIS system file format:** File format that is used for automatic import and export files. Select None to disable Automatic Import/Export.

**Input and output files:** Input and output file name and location.

**Export options:** Selection of whether automatic export occurs manually, automatically or not at all.

- Autoexport: Exports the output file automatically without any dialogues.
- No Autoexport: Dialogue where user has to select whether to export is shown.
- No Export: Export will not happen. No dialogues will be shown.

**Export study data:** Selection whether automatically exported output file has the data for the current study only or for all studies of the current person.

- Current Study: Exports the current study data of the current person.
- All Studies: Exports all studies data of the current person.

**Proceed into measurement automatically:** Select if automatic import proceeds automatically to a point where measurement can be started. Otherwise application will stay at the study view. Automatic import will stop and relevant view will be shown if mandatory information is missing.

### 3.7 Person Information Settings

**Standard fields:** Select which fields are shown and mandatory in Persons and Studies Person view. Fields that are required by a plugin are always visible, despite of the selection. For example *Birthdate* and *Gender* are mandatory for spirometry study.

- **Mandatory:** Field is shown and mandatory.
- **Visible:** Field is shown but not mandatory.
- **Not visible:** Field is not shown.

**Custom fields:** Custom fields can be used to introduce new information fields to person data. They are shown in person view below the standard fields in the configured order. Name, visibility and line expanse can be configured as well. Name of the field cannot include reserved special characters: “,” “:” “=” . Removing the custom field does not remove any data from the database.

**Order of the full name:** Full name is shown in the given order.

**Summary fields:** Summary of the person information is shown in top area of the Persons and Studies application.

### 3.8 Person Search Settings

**Search results in single row:** Person information cells are laid out in single row instead of two rows.

**Person search result:** Four cells are available to present person information at person search result list. Cell content can be configured to contain any person field information. The leftmost cells are displayed with bold font.

**Minimum search characters:** Person search is started when given amount of characters is entered to search.

**Search parameters:** Persons are searched for by matching the search term to information in all of the fields selected here.

### 3.9 Study Settings

**Study information settings for:** Study type selection. Spirometry is the only option, unless other study type plugins are installed.

**Hidden spirometry prediction models:** Prediction models can be hidden from users by selecting them from the list.

**Default spirometry prediction model:** Prediction model that is selected when new study is created.

**Study list fields:** Four cells are available to show selected study information when studies are listed. The first field is shown with bold font.

---

**Hidden study field editors:** Selected fields are not shown when viewing study. Data cannot be manually entered to hidden fields but may be updated by the measuring application.

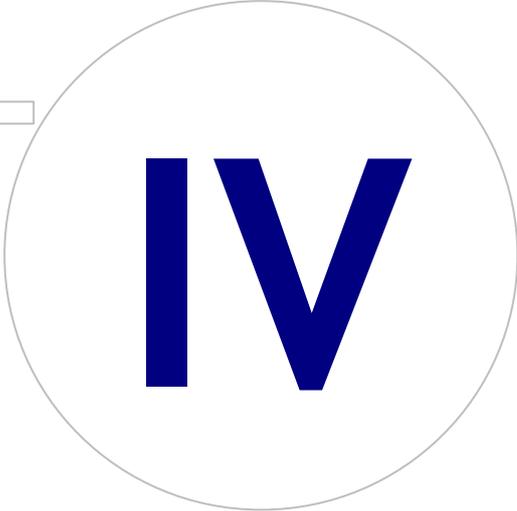
## 3.10 Other Settings

### Interpretation sentences

The interpretation of the session results is written in free text format on the Study view of Persons and Studies application. With Sentence editor it is possible to save interpretation texts for later use. For Sentence editor usage, see Medikro Spirometer User Manual.

The sentences created with Sentence editor are saved in local Medikro.ini. Interpretation sentences are saved to settings database and distributed to the clients the same way as Administration Tool settings even though the sentence management is not part of the Administration Tool.

Access Management



IV

## 4 Access Management

Medikro Spirometry Software utilises a discretionary access control implemented by a role based security. This means that privileges to perform operations are mapped to roles and users (or user groups) are then assigned those roles. Roles can have privileges from none to all. User can be assigned a single role or many roles.

A user can be the owner of a Windows user account or an internal user created in its entirety in the Access Control Management. Instead of individual users, the access control can be directed to Windows groups by assigning roles to the groups. The three methods are described in Figure 5.

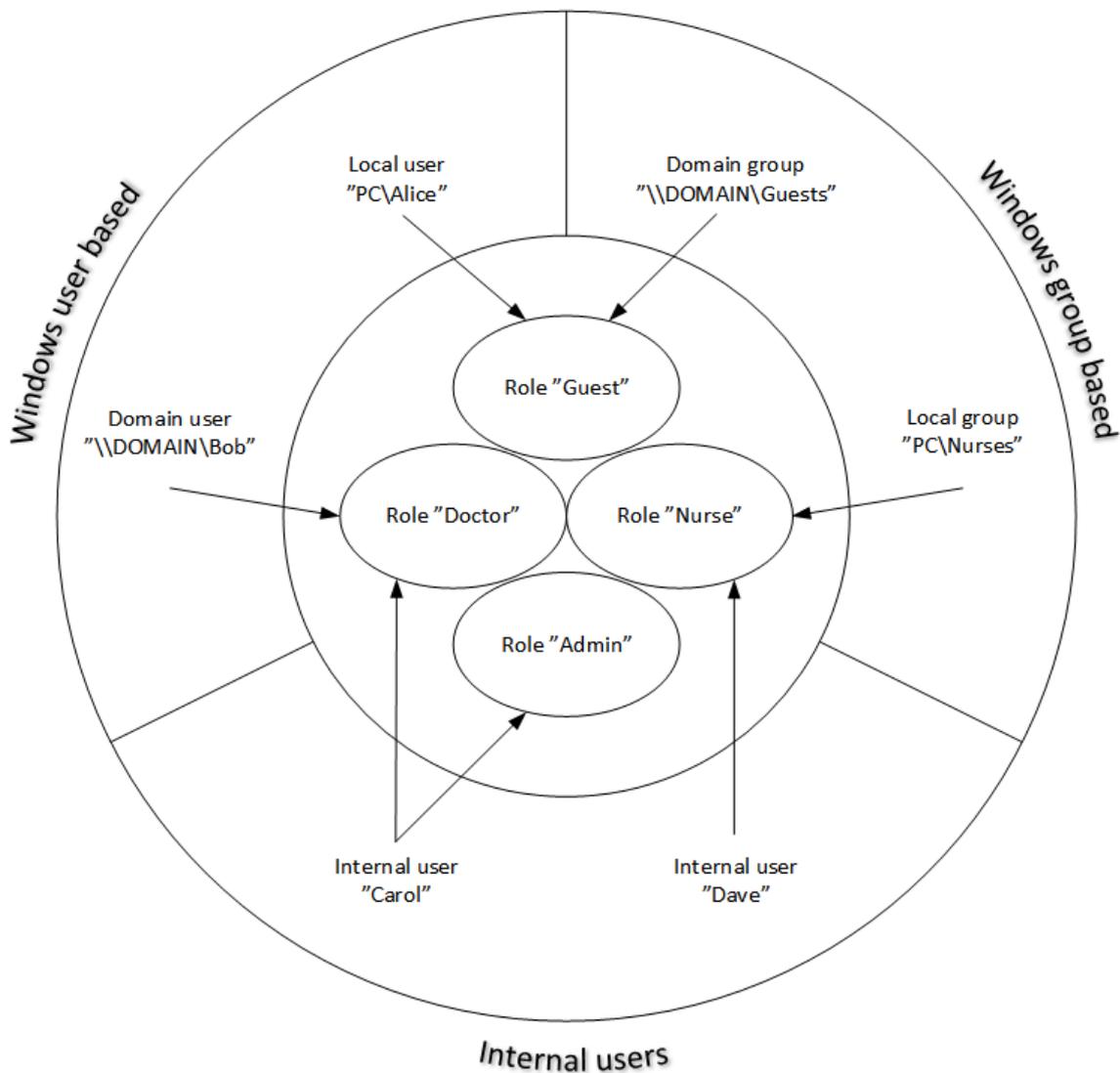


Figure 5. Access control methods.

Access control information can be saved to a server to provide access control across network to several workstations. If only one workstation is used, the access control information can also be saved locally to the workstation. The preferred usage and connection options for the clients can be configured in the Settings Management, see [Settings Management - Access Control Settings](#)<sup>[17]</sup> section in this manual.

Access control is managed in the Administration Tool in a section called Access Control Management. Connection to a support database in a server or to a local access control database file must be established when entering. A dialogue opens automatically when entering the Access Control Management without established connection. Connection to a database in a server can be established by selecting “*Online*” from the combo box on top of the dialogue, entering connection information and pressing “*Connect*” at the bottom. Connection to a local database file can be established by selecting “*Offline*” from the combo box on top, setting location of the file and pressing “*Connect*” at the bottom. New local database file, “*offline.access*”, can be created by choosing “*Create new database*” after selecting “*Offline*” from the combo box in the dialog. The location of the local access control database has to be entered in [Access Control Settings](#)<sup>[17]</sup> “*Path to local access control database*” configuration to take it into use.

Access Control Management has a view for managing users (See [Manage Users](#)<sup>[27]</sup>), a view for managing roles (See [Manage Access Roles](#)<sup>[25]</sup>) and views to manage organisation (See [Manage Organisation](#)<sup>[27]</sup>) and department (See [Manage Department](#)<sup>[28]</sup>) information. See corresponding manual sections for more detailed information. The views can be switched from a combo box on the left. Another access control information base can be selected by pressing “*Connection options*” at the bottom, setting the new source database connection and pressing “*Reconnect*” in the dialogue which is opened.

## 4.1 Manage Access Roles

The access rights of users are controlled by assigning role(s) for the user. Each role has permissions that define what the users are allowed to do. Definitions of permissions can be found from Table 4. Some of the permissions require other permissions and are selected and deselected automatically. For example in order to modify person information, the permission to read person information is needed.

By default there are three roles in the database. You can use/modify/delete them if you wish and/or create new ones.

“Nurse”: Nurse can create, modify and read person and study information. Importing and exporting is also allowed. Controlling settings is forbidden in Administration Tool.

“Doctor”: Doctor is only allowed to see person information and to modify (and read) study information.

“Admin”: Has the rights to do anything.

### Managing Roles

Adding new role: Click “*Add new role*” button, enter name for the role and save.

Edit role name: Click the role title on the role table, enter a new name and save.

Delete role: Click the role title on the role table, select “*Delete Role*”

Modifying role permissions: Tick the appropriate checkboxes on the role table, and save.

Table 4. Permissions

Permission	Description
Distribute settings	Allows user to distribute and save settings to database.
Download settings	Allows user to get saved settings to Administration Tool from database.
Write local DB settings	Allows user to modify connection settings for online databases in Administration Tool.
Access control management	Allows user to manage access control rights and settings.
Audit trail management	Allows user to open Audit Trail Viewer and manage audit trail settings.
Read person	Allows user to search persons and to see person information.
Modify person	Allows user to modify and save person information.
Create person	Allows user to create new person.
Delete person	Allows user to delete person.
Read study	Allows user to see study information in Persons And Studies. To open the study in Measurements and Results -application the 'Modify study' permission is also needed.
Modify study	Allows user to modify and save study information.
Create study	Allows user to create new study.
Delete study	Allows user to delete study.
Import	Allows user to execute manual or automatic import operation

Permission	Description
Export	Allows user to execute manual or automatic export operation.

## 4.2 Manage Users

Select wanted user type from the drop-down menu on top-right of the table. The type that Persons and Studies is using for access control is defined in "Access control method" configuration in [Access Control Settings](#)<sup>[17]</sup>.

**Adding a new user:** Press "Add new internal user" / "Add new Windows Group" / "Add new Windows user", a new dialogue opens.

- When adding an internal user, enter user information and press "Save". Unique username has to be entered for each internal user. For department/organisation fields department/organisation information must be added beforehand in the department-/organisation view. The password can only be changed via this window by editing the user.
- When adding a Windows group, you can change the used domain from the drop-down menu on top of the window. Select a group from the list and press "Save".
- When adding a Windows user, you can change the used domain from the drop-down menu on top of the window. Select user from the list and press "Save". After user selection, a dialogue opens, where it is possible to enter user information if desired. For department/organisation fields department/organisation information must be added beforehand in the department-/organisation view.

Please note that domain users and groups are only visible in the Administration Tool if the application is opened with a Windows user account belonging to the domain and allowed to access the Windows domain controller.

**Edit user information:** Click the username on the user table, and modify fields and press "Save".

**Delete user:** Click the username on the user table and press "Remove user" / "Remove group".

**Assigning roles:** Select appropriate checkboxes on the user table and save. To modify or add roles go to [role-view](#)<sup>[25]</sup>.

## 4.3 Manage Organization

Organisation is one of the input fields when adding/editing user information. Any number of users can belong to the same organisation, the organisation information is given separately in this view and is linked to the users in the [user-view](#)<sup>[27]</sup>. When an organisation is added, it can be selected from the drop-down menu in the user information dialogue. If the organisation's name is changed later, the information is updated automatically in the user information.

**Add new organisation:** Select "Add new organisation", enter organisation name to the table below and press "Save".

**Delete organisation:** Press "Delete" next to the organisation name.

---

## 4.4 Manage Department

Department is one of the input fields when adding/editing user information. As many users can belong to same department, the department information is given separately in this view and is linked to the users in the [user-view](#)<sup>[27]</sup>. When a department is added, it can be selected from the drop-down menu in the user information dialogue. If the Department name or address is changed later, the information is updated automatically in the user information.

**Add new department:** Select “*Add new department*”, enter department name and address to the table below and press “*Save*”.

**Delete department:** Press “*Delete*” next to the department name.

Audit Trail Viewer



## 5 Audit Trail Viewer

In Medikro Spirometry Software, it is possible to log actions that user performs. The feature can be activated/deactivated from the [Settings Management](#)<sup>[16]</sup>. Purpose of the action logging is to have a chronological record of actions performed by an operator.

Audit trail viewer is a tool that helps to detect illegal or harmful use of the software.

### How Audit Trail Works

Action logging is storing actions to an action database called *actiondb*. Actions can be stored either to online or offline database system.

Medikro Administration Tool is always storing to an encrypted offline database located in “ProgramData\Medikro\AdminActions\actionlog.db”. The content can be seen only by using Audit Trail Viewer of Medikro Administration Tool.

Persons and Studies stores actions either to offline or online database depending on how it is [configured](#)<sup>[17]</sup>. It is recommended to use online action logging in systems with multiple workstations. If action logging is configured to work online, it can be switched to offline only by the administrator user created by the database creator -installer.

### Access to Audit Trail Database

By default the database connection used by Medikro Persons and Studies only has the rights to insert actions to the action table of Action database. The administrator user created by the installer has the rights to login to audit trail viewer and see the content of the online database.

### Security of Audit Trail

Action database contains the information on what the user has done when using Medikro Spirometry Software. For that reason, access to the action database should be restricted only to those persons that need this information. Deleting and modifying entries should be forbidden for all users.

### Connection of Audit Trail Viewer

To configure connection options, select “Connection options” from the drop-down menu at the bottom. From the options, first select whether to connect to online or offline database.

Online settings are taken automatically from the [database settings](#)<sup>[18]</sup> the first time the “*Connection options*” -dialog is opened. Saved modifications are also available next time the Audit Trail Viewer is open. The given username and password are not stored.

For offline database settings, location of the database file must be specified and saved. Saved modifications are also available next time the Audit Trail Viewer is opened.

To connect to a database click “*Connect to database*”. The viewer will connect to online/offline database depending which one is active in the connection options.

To disconnect, select “*Disconnect*” from the drop-down menu at the bottom.

## 5.1 Using Audit Trail Viewer

The Audit Trail viewer shows all actions performed in the applications. Different actions are listed in Logged Actions- Table. You can filter the actions from the “*Filter by:*” section (see Figure 6) by using multiple different criteria. The results are shown in the table below the filter criteria (see Figure 7). When no criterion is selected all the recorded actions are shown.

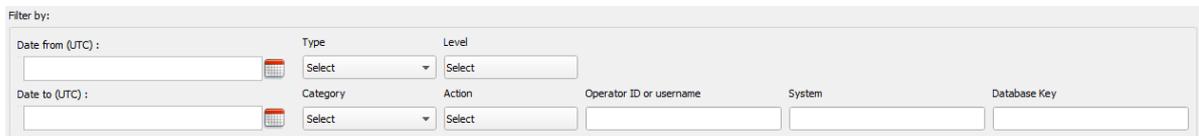


Figure 6: Filter criteria selection.

Time (UTC)	Category	Level	Action	Type	Operator ID	Operator username	System	Database key	Additional Information	Target Database	Target Server
1 18.03.2016 08:4...	System	Low	LoadPlugin	Automatic			Computer	00000000-0000-...	GDT (*.gdt)		Computer
2 18.03.2016 08:4...	System	Low	LoadPlugin	Automatic			Computer	00000000-0000-...	GDT 3.0 (*.gdt)		Computer
3 18.03.2016 08:4...	System	Low	LoadPlugin	Automatic			Computer	00000000-0000-...	Spirometry		Computer
4 18.03.2016 08:4...	System	Low	LoadPlugin	Automatic			Computer	00000000-0000-...	SpiroXML2 (*.x...		Computer
5 18.03.2016 08:4...	System	Low	Started	Automatic			Computer	00000000-0000-...	C:\ProgramDat...	offline.person.db	Computer
6 18.03.2016 08:4...	System	Low	Started	Automatic			Computer	00000000-0000-...	C:\ProgramDat...	offline.study.db	Computer
7 18.03.2016 08:4...	System	Low	Started	Automatic			Computer	00000000-0000-...	C:\ProgramDat...	SupportOffline	Computer
8 18.03.2016 08:4...	System	Low	Started	Automatic			Computer	00000000-0000-...	communicatio...		Computer
9 18.03.2016 08:4...	Access	High	Login	Human	11111111-1111-...	default	Computer	00000000-0000-...	PersonsAndStu...		Computer
10 18.03.2016 08:4...	System	Low	Started	Human	11111111-1111-...	default	Computer	00000000-0000-...	Persons And St...		Computer

Figure 7: Results table.

## Filters

**Date from (UTC)/Date to (UTC):** You can specify the time frame to filter the actions. You can also use only one of them, for example by selecting Date From: 1/1/2015, you get all actions after 1/1/2015 in UTC time.

**Action:** You can select which actions to show. Multiple actions can be selected and selected actions can be deselected by choosing them again.

**Type:** Filter based on Type column. One action type can be chosen and selection can be deselected by choosing deselect.

**Category:** Filter based on category column. One action category can be chosen and selection can be deselected by choosing deselect.

**Level:** Filter based on Level column. Multiple levels can be chosen.

**Operator ID or username:** Filter based on operator ID or Operator username column. You can write multiple operator ID:s or operator usernames separated by a comma (e.g. “00000000-0000-0000-0000-000000000000, 12345678-1234-1234-123456789012”).

**System:** Filter based on system column. You can write multiple system names separated by a comma (e.g. "Workstation 1, Workstation 2").

**Database key:** Filter based on Database key column. You can write multiple keys separated by a comma (e.g. "00000000-0000-0000-0000-000000000000, 12345678-1234-1234-123456789012").

## Result table columns

**Time (UTC):** Timestamp when the action has occurred in UTC time.

**Category:** Category of the action.

- Access: Actions are related to user authentication.
- Database: Actions are related to reading, writing and deleting data on database.
- User: Actions are related to user interaction with the application
- Transfer: Actions are related to importing and exporting data.
- System: Actions are related to application module state changes.
- Error: There has been an error when performing an action.

**Level:** Severity level of the action.

**Action:** Action that has been executed. Description of the actions can be seen in Table 5.

**Type:** Is the action executed directly by human interaction or is it done automatically.

**Operator ID:** Database ID of the operator who has performed the action. Every operator has a unique ID that can be found on the operator table of supportdb database (operator\_id column). In case the user has not yet been signed in, the ID is "00000000-0000-0000-0000-000000000000" and when no access management is used, the ID is "11111111-1111-1111-1111-111111111111".

**Operator username:** Username of the operator who has performed the action.

**System:** The name of the workstation where the operator has used the software during the action.

**Database key:** ID of the target of the action. For example, if a person is stored, it is the ID of the stored person. In case of no information, the ID is "00000000-0000-0000-0000-000000000000".

**Additional Information:** Free form additional information about the action.

**Target Database:** Name of the database where the action has been performed. Related to Database-category actions. Empty if no database is needed for the action.

**Target Server:** Name of the workstation or database connection where the action has been performed.

Table 5: Logged actions.

Action	Description
*	* Error can be logged from any action.
Login	Sign-in action of the operator.

Action	Description
Logout	Sign-out action of the operator.
FetchPersonCustomFields	Get person's custom fields from database. Person id in info field.
FetchPersonStudies	Get person's studies from database. Study id(s) in info field.
AddPerson	The Operator stored a new person, info field contains new person database key.
UpdatePerson	The Operator updated person information, info field contains person database key and fields that were updated.
SearchPerson	The Operator has performed a search and received/viewed the results, info field contains the database keys for persons viewed.
MatchPerson	Matching persons from the database to a person when synchronising offline database or when importing person(s).
MergePerson	Merge person information to another person in database when synchronising offline database or when importing person(s).
DeletePerson	The Operator deleted a person, info field contains the deleted person database key.
AddStudy	The Operator stored a new study, info field contains new study database key.
UpdateStudy	The Operator updated study information, info field contains study database key and fields that were updated.
SearchStudy	The Operator has performed a search and received/viewed the results, info field contains the database keys for studies viewed.
MatchStudy	Finding same study from database when synchronising offline database or when importing person(s).
MergeStudy	Merge study information to another study in database when synchronising offline database or when importing person(s)
DeleteStudy	The Operator deleted a study, info field contains the deleted study database key.
SetActiveSettings	Setting new active settings configuration to support database. Active configuration id as database key.
LoadSettings	Loading settings from support database. Setting id in info field.
SaveSettings	Storing settings to support database. Setting id in info field.
DeleteSettings	Delete setting from support database. Deleted setting id in info field.
SearchAuditTrail	Operator searches information from Audit trail database. Info field contains the SQL query
GetOperator	Operator information query from support database. Searched Operator id in info field.
AddOperator	Adding new operator to support database. Operator id in info field.

Action	Description
UpdateOperator	Updating operator information. Operator id in info field.
DeleteOperator	Removing operator. Operator id in info field.
LoadRoles	The Operator loads roles. Loaded role ids in info field.
AddRole	The Operator adds a new role. Added role id in info field.
ModifyRole	The operator modifies role. Modified role id in info field.
DeleteRole	The operator deletes a role. Deleted role id in info field.
LoadOperatorRoles	Load operator roles table.
AddOperatorRole	Adds a role to operator. Operator id and role id in info field.
DeleteOperatorRole	Removes a role from operator. Operator id and role id in info field.
AddOperation	Adds an operation to a study. Used only in errors.
SearchOperation	Searches operation from the database. Used only in errors.
AddOrganization	The operator adds a new organisation. Organisation name in info field.
UpdateOrganization	The operator updates an existing organisation. Organisation name in info field.
LoadOrganization	Load organisation information from database. Used in errors.
AddDepartment	The operator adds a new department. Department name in info field.
UpdateDepartment	The operator updates an existing department. Department name in info field.
LoadDepartment	Load department information from database. Used in errors.
Transaction	Starting/committing a SQL transaction. Used in errors.
ModifyPerson	Modifying person information. Used only in errors.
ViewPerson	Operator views person information. Viewed person id as database key.
ModifyStudy	Modifying study information. Used only in errors.
ViewStudy	Operator views study information. Viewed study id as database key.
ViewSettingsDiff	Operator views differences of two settings. Used in errors.
AutomaticImport	Automatic import process.
AutomaticExport	Automatic export process.
Import	Importing person/study/settings
Export	Exporting persons/studies/settings
Started	Module/Database connection/Plugin is started.
Stopping	Module/Database connection/Plugin is stopped.

Action	Description
Initialise	Used only in errors when initialising fails.
Deinitialise	Used only in errors when deinitialising fails.
LoadPlugin	Used only in errors when loading plugin fails.
PluginAction	Action from plugin application. Used in Errors.
Synchronisation	Used only in errors when synchronisation fails.
ActionLogSynchronizati on	Action log synchronisation action.
SynchronizationStarted	This action is logged when synchronisation is started.
SynchronizationStopped	This action is logged when synchronisation is stopped
ConnectionChange	Database connection status has been changed