MANUAL
XM3 Manage 4

Table of contents

1   Introduction

Thank you for purchasing XM3 Manage. Using XM3 readers, you can build networks of readers while managing them as one *Access Control System*. XM3 Manage enables you to manage an Access Control System by setting different types of parameters on your readers as well as managing ID-tags. Some key features of XM3 Manage are:

- Managing multiple readers over one or more networks (COM ports)

- Adding, removing and editing card users over multiple readers using wizards

- Transfer users and parameters to one or more readers

- Advanced searching capabilities for events and users

- Faster communication at higher baud rates (9600, 19200 and 38400 bps)

In this user guide the functionality and use of XM3 Manage is explained.

Please check the contents of your delivery before proceeding with the installation of XM3 Manage.

The package should contain:

- CD containing the software

- User Guide

1.1   Versions

XM3 Manage behaves differently depending on the type of XM3 that is connected;

- **XM3 Manage**. When connecting Stand-alone readers to a computer running XM3 Manage, you will have all functionality without time schemes and user validation. This version is free of charge and available on CD or can be downloaded from www.crosspoint.nl.

- **XM3 Manage Pro**. This version contains all functionality of XM3 Manage but with time schemes and user validation. For this version, you need a dongle that can be purchased from your dealer. It is not necessary to re-install XM3 Manage when upgrading to the Pro version. Just insert the dongle into the PC and the extra functionality is available.

NOTE   Do not remove the dongle when XM3 Manage Pro is running. The application will close immediately!

- **XM3 Manage Single Door**. If you purchased an XM3 Single Door and you start up XM3 Manage, it will detect this device and will behave differently. Because the XM3 Single Door has limited functionality, XM3 Manage will also have limited functionality. This version has no network functionality and event related features are not available.

This manual describes all three versions. Even when an option or function is not available in a certain version, it will be described.

1.2   Related documents

Document/Manual	Function
Installation Manual XM3	Describes the connection of the readers and to set the Installer and end-user Parameters.
Quick Guide Connection unit	Describes the functionality of this unit as well as how to connect the readers to it.

The Quick Guides are supplied together with the respective products.

2 Getting started

2.1 Install XM3 Manage

To install XM3 Manage, take the XM3 Manage CD and insert it into your computer. Follow the instructions on the screen to install the application. The first screen that will appear is the Installation Wizard. Read the text in the screen carefully, since it contains important information. Click the button **Next** to continue with the procedure. The dialog *Destination Folder* will be displayed (see Figure 1).
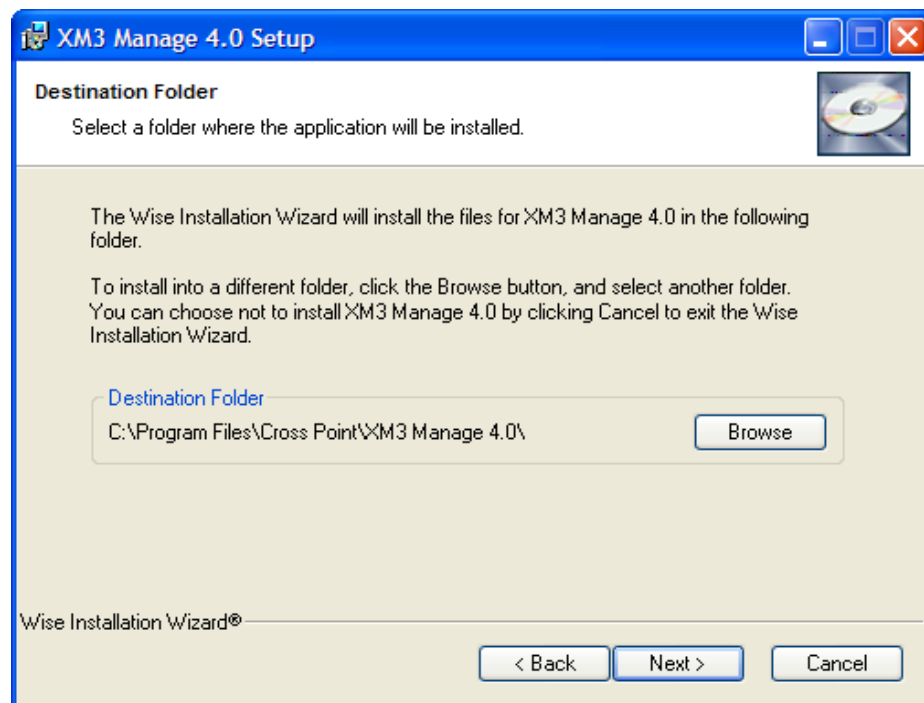
Figure 1: Installation Wizard - Destination Folder

1. Read the information in this dialog before selecting a destination folder. If you click **Next** the *Wise Installation Wizard* will install the files for XM3 Manage in the folder shown in the dialog.

2. To install the files into a different destination folder, click **Browse** to go to the required folder. Click **Next** to continue.

3. The *Ready to Install the Application* dialog appears. Click **Next** to continue.

4. The system will be updated. This is shown in the dialog *Updating system*.

5. Click **Finish** to exit the Installation Wizard.

Now you can start the application.

NOTE   The very first time that you start XM3 Manage, you are prompted to create an account for logging on to the application (see paragraph 2.2.1).

2.2   The configuration wizard

When you start the application the first time after the installation of XM3 Manage, the *Configuration wizard* will appear to help you configure the system. If you use XM3 Manage Pro you can choose whether to use *time schemes and user validation* or not when you configure your system. Since using time schemes will make using XM3 Manage more flexible, normally this option will be selected. If you use XM3 Manage Standard or XM3 Manage Single Door, you will not have this choice.

2.2.1   Initial log on

Since this is the first time XM3 Manage is started, there are no accounts present in the application. The first, primary account has to be created with the help of the Configuration wizard. This primary account is the *Administrator account*, with which all other accounts can be created in the application.

Take the following steps to start the application and to create the primary account for logging on to XM3 Manage:

1. Select the application in the Start menu that is located on:

   All Programs\Cross Point\XM3 Manage.

   The Configuration wizard is displayed. Read the information in this dialog before creating the account.

2. Click the button **Next**. The *Account screen* will be displayed (see Figure 2).
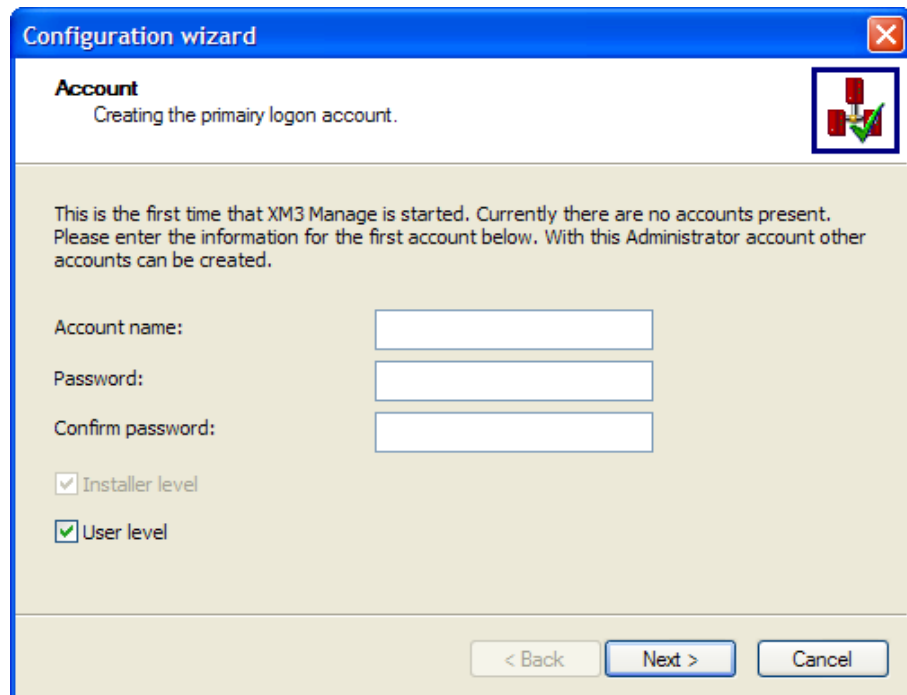
Figure 2: Configuration Wizard - First Account

3. Enter the **name** of the account.

4. Enter a **password**.

5. Confirm the password.

6. Click the button **Next** to continue with the configuration of your system.

2.2.2   Selecting networks

Clicking the button **Next** after confirming your password will make the *Select networks* dialog appear (see Figure 3).
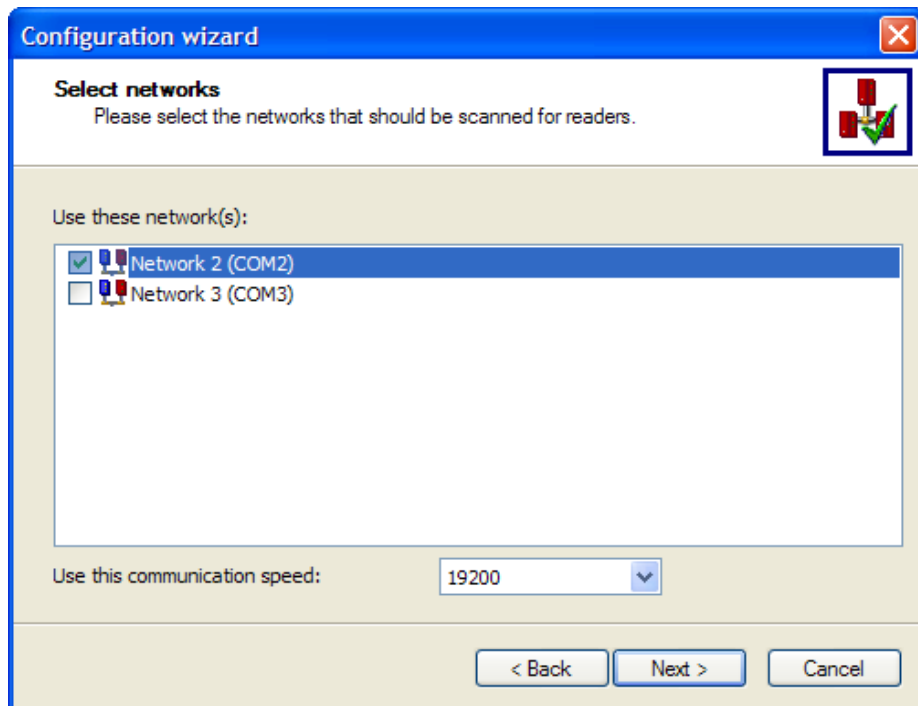
Figure 3: Configuration Wizard - Select Networks

1. Select the network(s) that have to be scanned for readers. If you have virtual COM-ports (like a Bluetooth port or an InfraRed port), do not select these since these can slow down the scanning progress considerably. Cross Point's Connection Unit with the USB converter will also create a virtual COM-port. This port can be selected.

2. In the box **Use this communication speed**, select the speed at which the network has to communicate with the button ⌄.

3. Click the button **Next**. The *Locating readers* dialog will appear (Figure 4), and the Configuration wizard will start to scan the readers in the network and update their communication speed. A progress bar will indicate the status of the process. If not all readers are found or powered, you can use the **Rescan** button to rescan the selected network again.
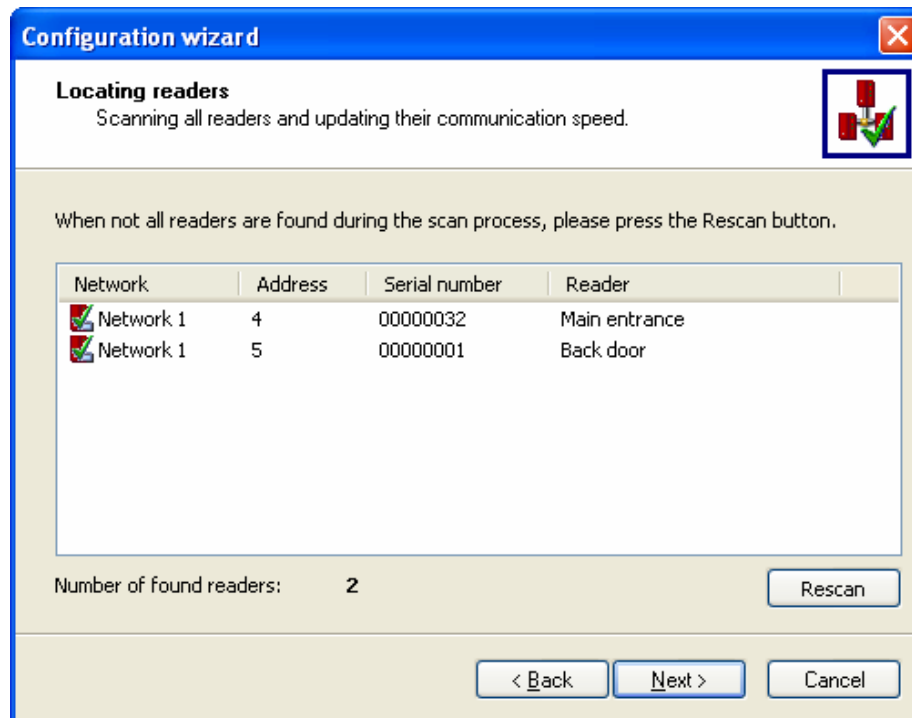
Figure 4: Configuration Wizard - Locating readers

2.2.3 Using time schemes and user validation

When clicking the **Next button**, the *time scheme* dialog will appear (see Figure 5) depending of your XM3 Manage version. Here you can configure whether you want to use *time schemes* or use *user levels*. Time schemes are more advanced but can only be used with XM3 Manage Pro.

NOTE If you do not run XM3 Manage Pro, this dialog is skipped.
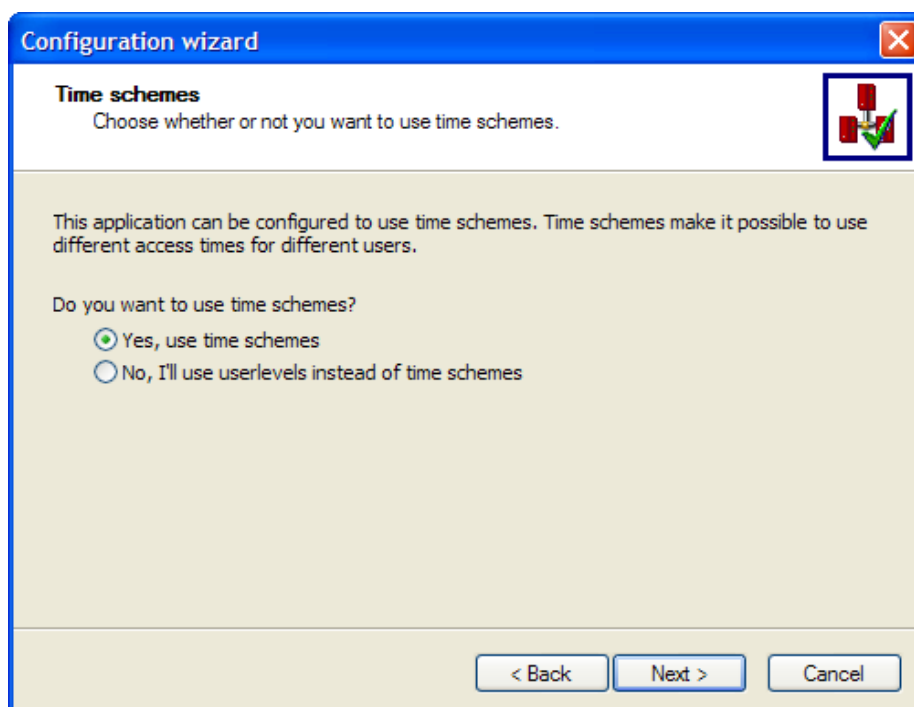
Figure 5: Configuration Wizard - Choosing time schemes

1. Select whether you want to use time schemes and User validation or not.

2. Click the button **Next**.

2.2.4 Uploading new firmware

Depending on the firmware versions in the readers and the selection in paragraph 2.2.3 the *Firmware selection* dialog will appear (see Figure 6).
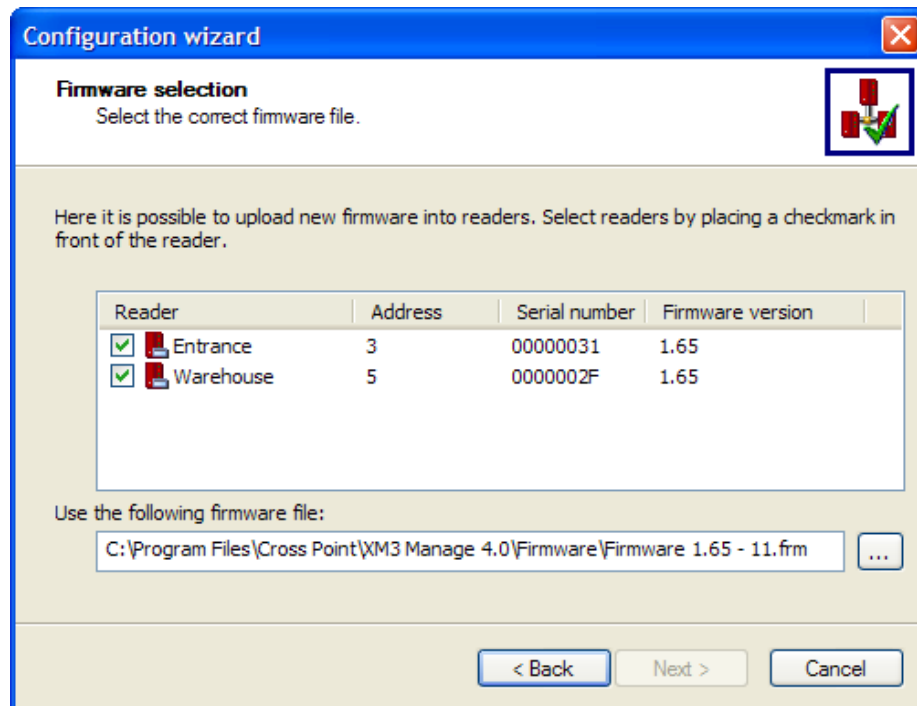
Figure 6: Configuration Wizard - Firmware Selection

In this dialog the readers of the network are displayed. The firmware file is already in the box **Use the following firmware file**.

1. If necessary, select the reader(s) into which new firmware has to be loaded by placing a checkmark in front of the reader(s).

   NOTE   If you must upload, the checkboxes are not displayed and the upload is not an option but is always performed!

2. Select [...] to browse to the location you stored the files you received from Cross Point, if you have to update your firmware.

3. Click the button **Next**.

If the readers do not require a firmware update a notice will be given in the *Progress* dialog. Otherwise, the system will start loading the firmware to the selected readers.

2.2.5   File Systems

A file system is needed to store data in the reader in a predefined format. Depending on the file system, you can store ID cards with names, PIN codes and events. If you know the number of events and users you will store, you can select the appropriate file system.

After you click the button **Next** in the previous dialog, the *Select file system* dialog will appear (see Figure 7). Depending on the selection in paragraph 2.2.3, the dialog that you are seeing is different. When using time schemes, you have two options. When you are not using time schemes the dialog contains eleven options.
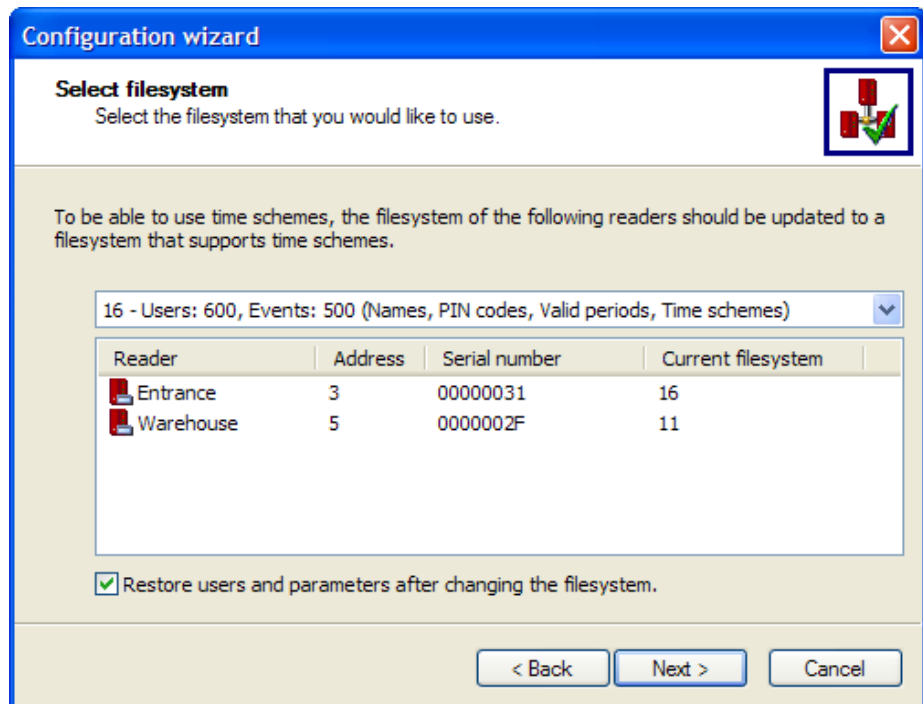
Figure 7: Configuration Wizard - Select file system

In case you use time schemes, this dialog asks you to choose file system 16 (default) or file system 17. Both file system support time schemes and user validation. If you are a not using the Pro version or do not use time schemes, the default file system will be file system 11 with 500 users and 1000 events.

1. Select the file system you want to use.

2. If you want the users and parameters to be restored after changing the file system, select the option **Restore users and parameters after changing the file system**.

3. Click the button **Next**. In the dialog *File systems* a notice will be given whether the readers already have the correct file system, or whether the system is ready to change the file system of the readers.

4. Click the button **Next** to confirm the configuration of the file system. If the file systems have to be updated, the status of the process will be indicated in the dialog *File systems* by a progress bar. The comments will show what part of the process is being executed.

5. Click the button **Next**. If you choose file system 16 or 17, XM3 Manage Pro will update all readers with the correct time schemes (see Figure 8). A progress bar is shown during this process.
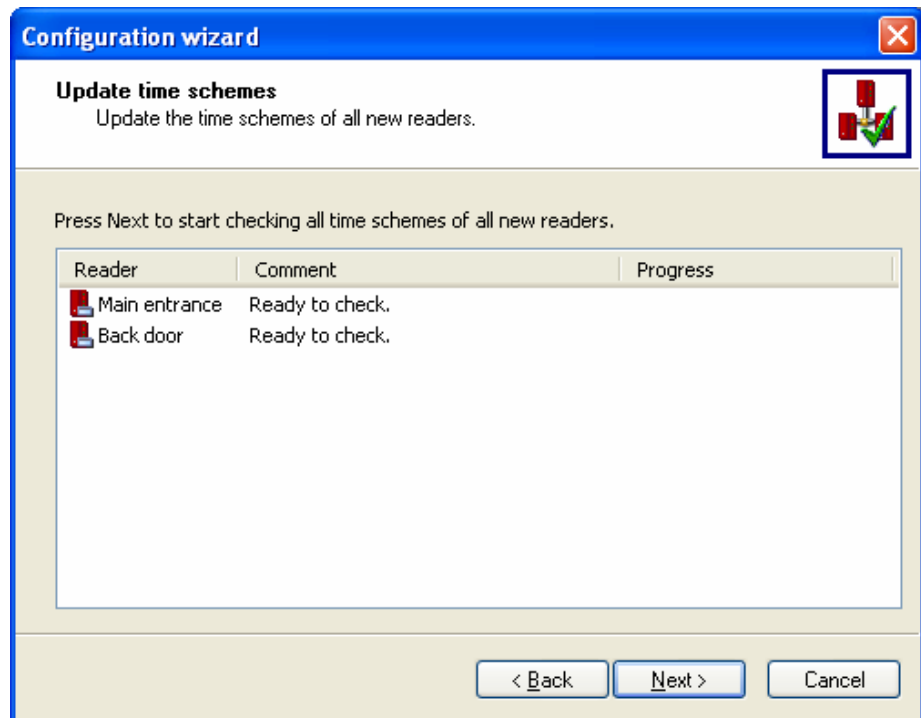
Figure 8: Configuration Wizard - Updating time schemes

6. Click the button **Finish** to close the *Configuration wizard*.

The *Logon* dialog will appear. For logging on see section 4.

The Configuration wizard can also be addressed after the application has started. Select **File -> Configuration wizard**. The procedure for configuring or modifying the system then is the same as described above, with one exemption.

For installers, it is convenient to set the option **Always start-up the Configuration wizard** in the options dialog and clear the option **Display a warning when not all readers were found** (see paragraph 13.1).

NOTE When the dongle was inserted the previous time XM3 Manage was started and is not found the next time, the user will be asked to insert it now. If it is not inserted, XM3 Manage Pro will behave like XM3 Manage!

2.3 Setting other reader parameters

Now you have completed the Configuration wizard, all readers are up to date and an installer account is created. The reader still operates on *Installer level* and this should be set to *User level* if configuration by the installer is finished. When you are ready as an installer, you should switch to *User level* as described in paragraph 11.13.

The parameters that have to be set on Installer authorization level are listed below. In chapter 8 is described how the parameters can be set. Between brackets, the reference to the chapter for more information about the parameter is mentioned as well.

- Open time (see paragraph 9.1)

- Close time (see paragraph 9.1)

- Lock type (see paragraph 9.2)

- Egress (see paragraph 9.2)

NOTE   If you have more than one reader in your network, you can repeat the previously mentioned steps again or you can transfer the settings to the other readers (see chapter 10).

3 The User Interface

3.1 Global Screen layout

In this User Guide terminology like right pane, menu bar, title bar et cetera of the global screen layout is used. The global screen layout is depicted here to explain the fields of the screen (see Figure 9).
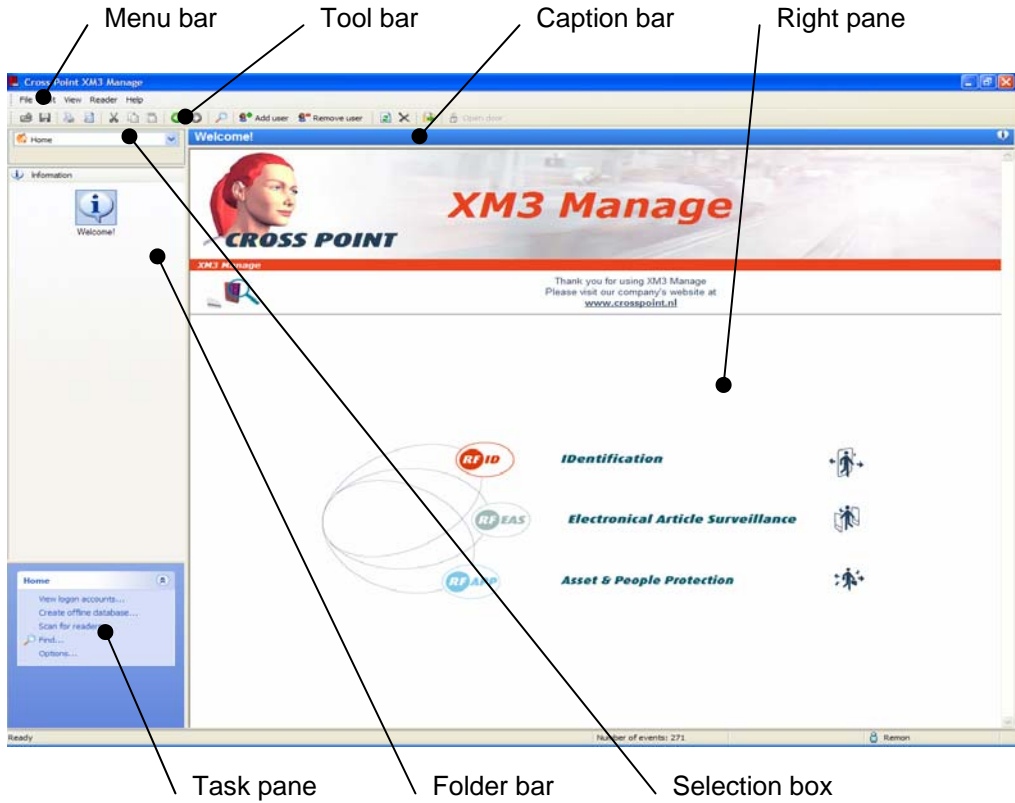
Figure 9: Global screen layout

3.1.1 Views in XM3 Manage

XM3 Manage is able to organize your readers in two different views. From the menu **View** you can select either the **Folder Bar** or **Tree** (see Figure 10).

Figure 10: Folder bar view and Tree view

4   Logon Accounts

4.1   Creating logon accounts

To create logon accounts, an account with administrator rights has to logon to XM3 Manage. One such an account was created during installation of XM3 Manage. Take the following steps to create a new logon account:

1. Select form the Menu bar, **File -> Logon accounts**…. The *Logon accounts* dialog is displayed (see Figure 11). Here an overview of all accounts currently available is displayed.
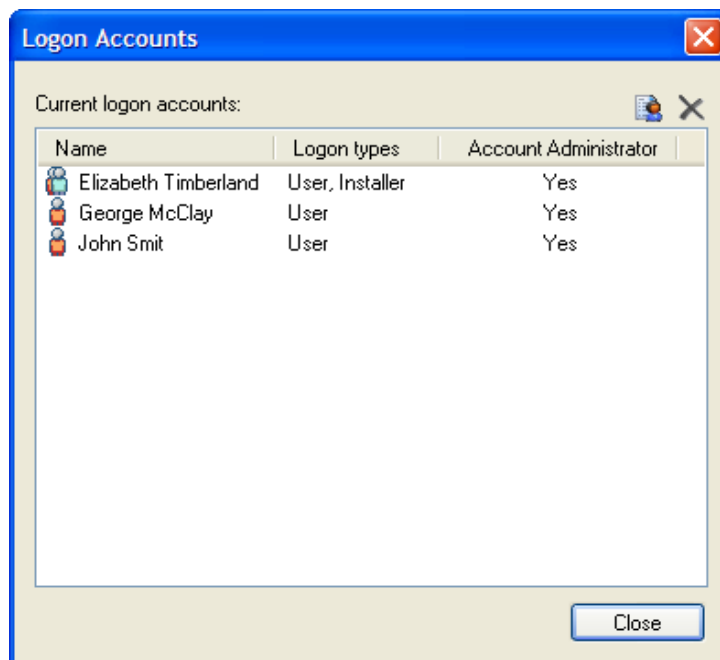
Figure 11: Logon Accounts dialog

2. Click the button ![icon] to add an account. The *Account properties* dialog is displayed (see Figure 12).
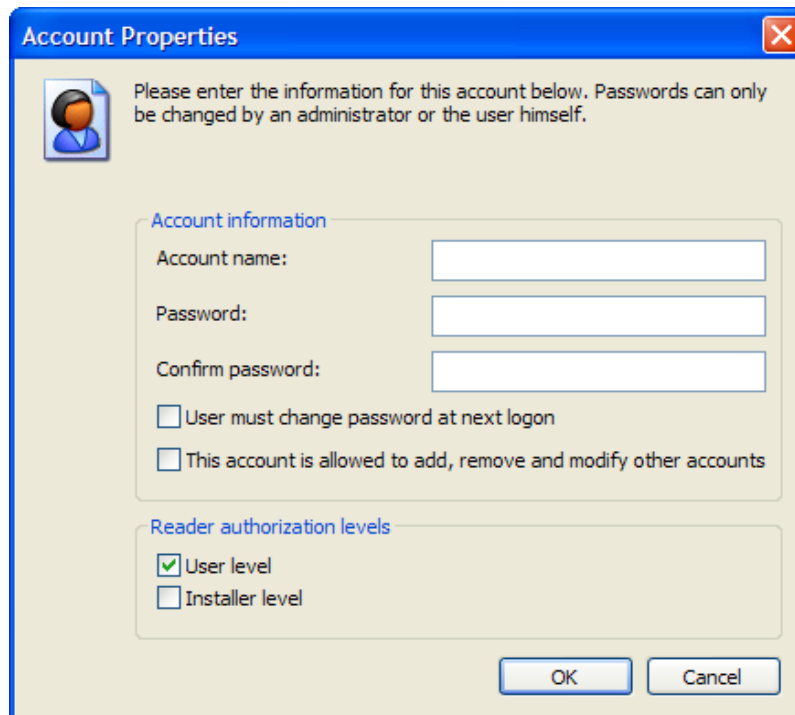
Figure 12: Account Properties dialog

3. Enter an **Account name**.

4. Enter a **Password**.

5. Confirm the **Password** entered in the previous step.

6. If you want the user to change the password at the next logon, select the check box **User must change password….**

7. If you want the account to be able to create other accounts, select the check box **This account is allowed to add, …**

8. Select the required authorization level.

   The following reader authorization levels are available:

   - **Installer authorization level** (marked by a blue icon). This level is used to set certain settings on the readers before switching to the user authorization level. This level has full access to the XM3 Manage application.

   - **User authorization level** (marked by a red icon). During normal operation, your access control system is set to this authorization level. This level has limited access to the XM3 Manage application.

9. Click the button **OK** to save the account and to return to the **Logon**.

10. To close this window, click the button **Close**.

4.2 Modifying an XM3 Account

XM3 Manage offers the possibility to modify an account. This can be necessary if for instance a user should be an installer. Take the following steps to modify an account.

1. Select from the Menu bar, **File -> Logon accounts…** to display the *Logon accounts* dialog.

2. In this dialog, double click an Account. The *Account Properties* dialog is displayed (see Figure 13).

3. When modifying an XM3 Account the option **This account is allowed to add, …** cannot be selected.
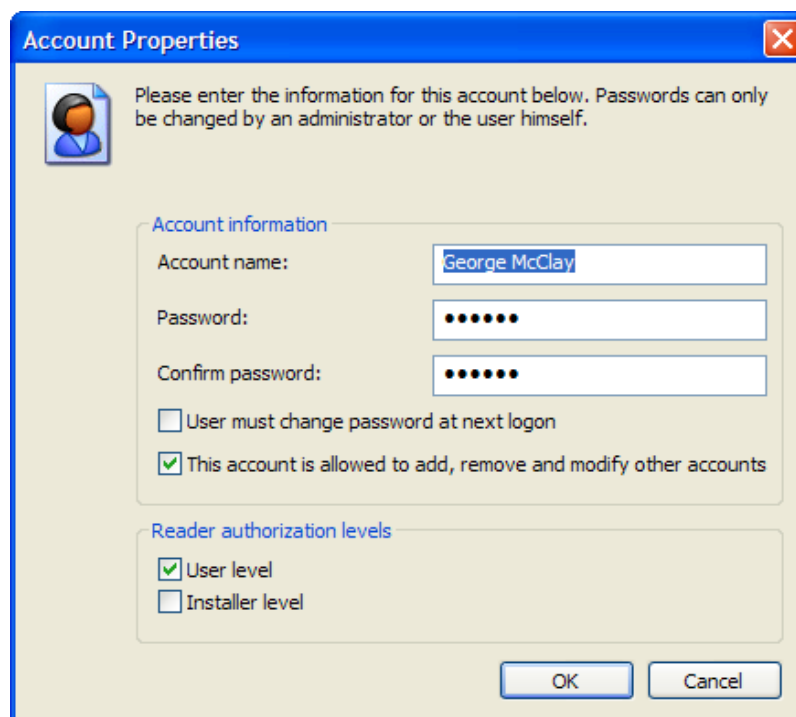
Figure 13: Account Properties Dialog

4. Change any setting you want.

5. Click the button **OK** to confirm the changes and to return to the application.

6. To close this window, click the button **Close**.

4.3 Removing an account

If it is not necessary for some one to logon to XM3 Manage, the account of this person can be removed. Take the following steps to remove an account.

1. Select from the Menu bar, **File -> Logon accounts…** to display the *Logon accounts* dialog.

2. Select an account

3. Click the button ✕. If you have set the option **Show warnings when**…, a warning is displayed asking you whether you are sure to delete this account. For setting this option, see chapter 13.

4. Confirm this question and the account is deleted.

5. Click the button **Close** to close the *Logon accounts* dialog.

5   Logging on to XM3 Manage

An account logging on to XM3 Manage has to take the following steps to do this.

1. Select the application in the Start menu that is located on: **All Programs\Cross Point\XM3 Manage.** The *XM3 Manage Logon* dialog is displayed (see Figure 14).
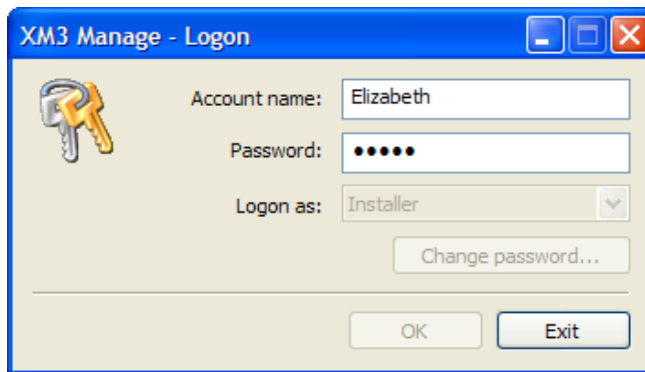
Figure 14: Logon dialog

2. Enter your **account name.**

3. Enter the password that has been entered at the creation of the logon account (case sensitive).

   NOTE   The drop-down menu **Logon as**: becomes active if this account has the reader authorization level for both the Installer and User.

4. If applicable, select the reader authorization level on which you want to logon to XM3 Manage.

5. Click the button **OK**.

It is always possible that you change the password.

6. Click the button **Change password**. The *Change Password* dialog is displayed (see Figure 15).
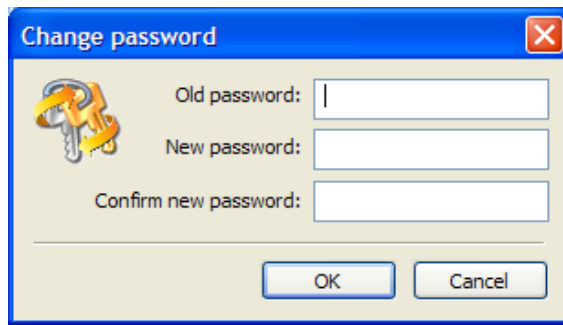
Figure 15: Change Password dialog

7. Enter the fields in this dialog, and click the button **OK**.

8. The application starts scanning for readers. In the screen all readers that are found will appear. If one or more readers in the network are not found by the application, the following notice will appear in the screen.
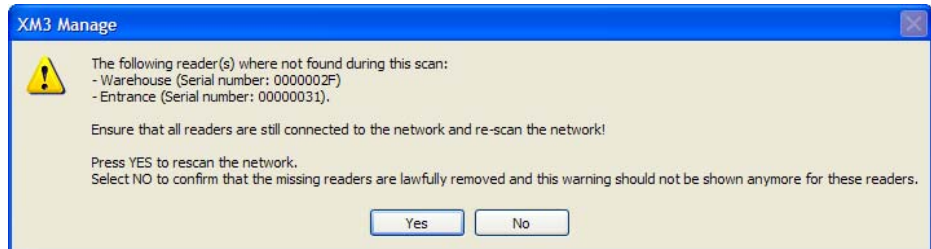
Figure 16: Connection error notice for the readers

NOTE Read the text in the notice and rescan the network(s) if you are certain the readers are properly connected. You can turn off this message in the *Options* dialog.

9. Click the button **Finish** to start the application.

6 Time schemes

NOTE   This functionality is only available in XM3 Manage Pro. Please contact your dealer for more information.

Time Schemes in XM3 Manage Pro make it possible to use different access times for different users. Default XM3 Manage Pro contains three time schemes: **Daytime users**, **Nighttime users** and **24 hour users**. You can easily and quickly set or adjust the access zones of (groups of) users, and you can easily create multiple, new time schemes, adapted to your situation. To assign a time scheme to a user also see 7.2.1.

Time schemes are defined system wide which means that when adding or removing time schemes, all readers are updated. Also, when a new reader is connected, the Configuration Wizard will notice this and add the time schemes to this new reader.

6.1   Create a new time scheme

To create a new time scheme you have to take the following steps.

1. From the Menu bar, select **File -> Create a new time scheme**. The *time schemes* pane will appear (see Figure 17). The current time schemes are displayed in the Folder bar. You can also use the *Task pane* when the time schemes pane is currently selected.

2. In *General*, enter a name for the new time scheme.

3. Select whether this time scheme has to overrule the **public holidays**. This will give a user using this time scheme the ability to get access during holidays. Normally, users do not have access during holidays.

4. Select whether this time scheme is the **default time scheme**. The default time scheme is used when a user is added with an *Add Master* or a *Program master*. This user will then use the default time scheme. Also, when using the *Add User Wizard*, the default is selected in the dialog.

5. Go to the pane *Scheme* and select a day and a time by pointing the cursor to that day and time, and clicking the left button of the mouse. You can also create new blocks by clicking the mouse on a yellow part of the day and drag the mouse to the right. Point and click a green block to move a zone. To modify a block, you can point and click the edges of a green block.

6. Drag the cursor to the end time on that day. The part of the time bar you have selected will turn green to indicate the access time. While you drag the cursor the time will be displayed in yellow at the bottom of the time table.
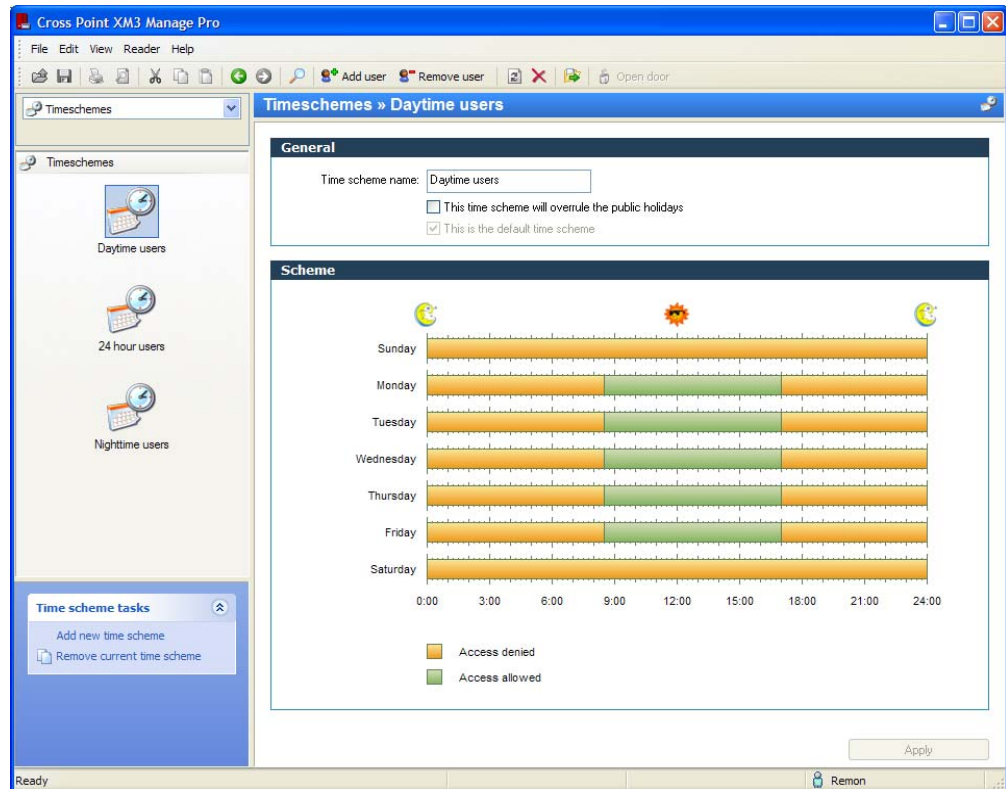
Figure 17: time schemes view

7. Set the other days. If they have to have the same start and end access time as the day you have just set you can copy the setting by pointing the cursor at the day you have set and clicking the right button of your mouse. This will give you the following options: **Remove**, **All days like this one** or **All working days like this one**.

8. Click the button **Apply**.

The new time scheme will be uploaded to all readers and will be added to the Folder bar.

6.2 Removing a time scheme

If you want to remove a time scheme from the system you have to take the following steps.

1. Select **time schemes** from the selection box in the upper left corner of the screen.

2. Select the icon of the time scheme you want to remove. The *time schemes – <selected scheme>* pane will appear with the selected time scheme already filled in.

3. Select the option **Remove current time scheme** in the Task pane on the left or select **File -> Remove Time Scheme** from the menu.

4. XM3 Manage Pro shows the following dialog:
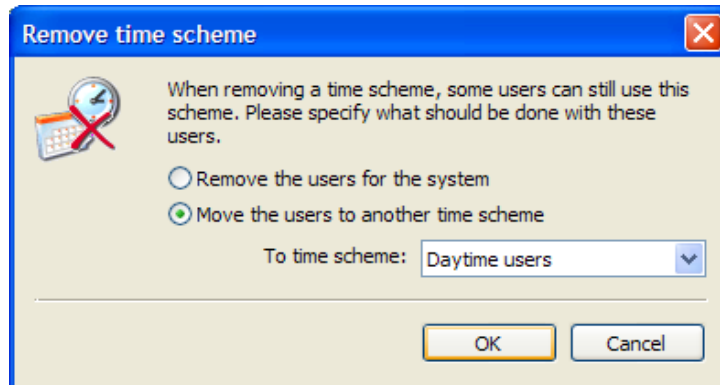
Select the right option and click **OK**. If you do not want to remove the time scheme click **Cancel**.

The deleted time scheme will be removed from the Folder bar directly.

NOTE   You cannot remove the default time scheme from the system!

7 Users

After you have configured the readers, you can add users. Users are the ID-tag holders of your access control system. In paragraph 7.2, is explained how you can add users. Most functionality described in the next paragraphs can also be accessed using a context menu that pops up when you press the right mouse button in the user pane.

7.1 Viewing users

Users can be displayed per reader or from all readers. Take the following steps to view the users.

1. Select a reader or *All readers*

2. Select the *Users* folder in the folder bar or tree (dependent on the selected view).

The users are displayed in the right pane and are listed in columns (see Figure 18).
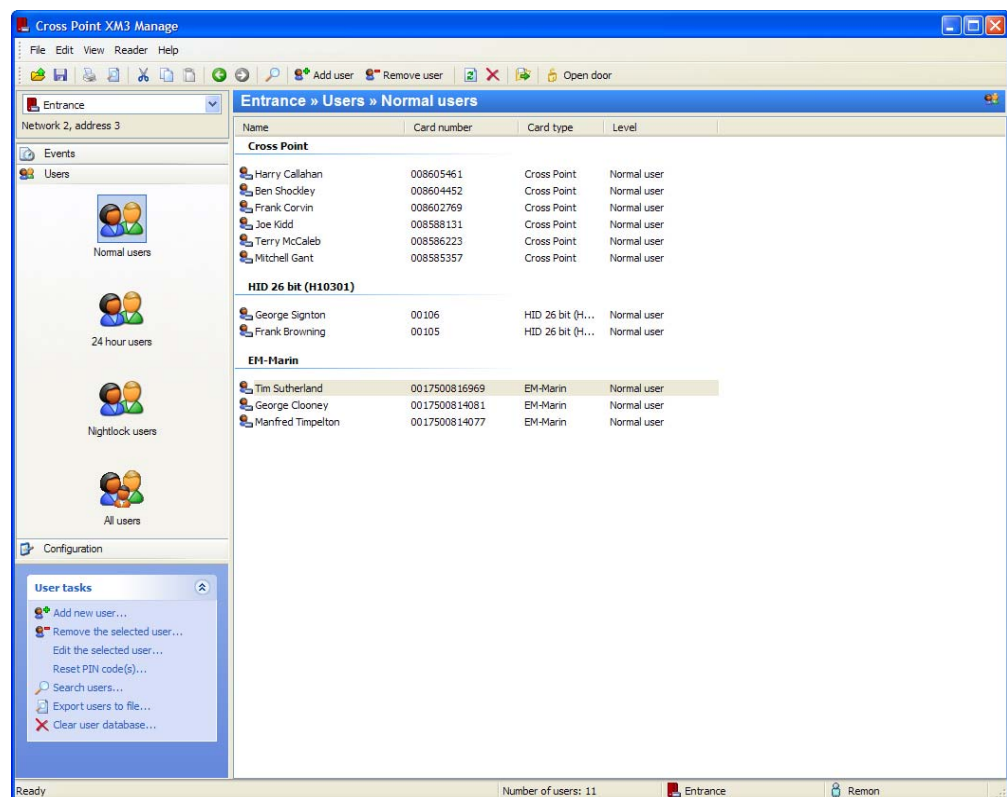
Figure 18: Users view

7.2 Creating users

XM3 Manage is provided with a Wizard that enables you to add Users (cards and/or tags), Master cards and programming pads. Furthermore with this wizard you can select also the readers you want to add the users to.

7.2.1 Add a Normal User

Take the following steps to add a Normal User (day time) via the Wizard:

1. From the Menu bar, select **File -> Add new user to reader(s)…** to display the *Add User Wizard*.

2. In this Wizard, select the button **Next**.

3. The dialog *User Properties* is displayed (see Figure 19).
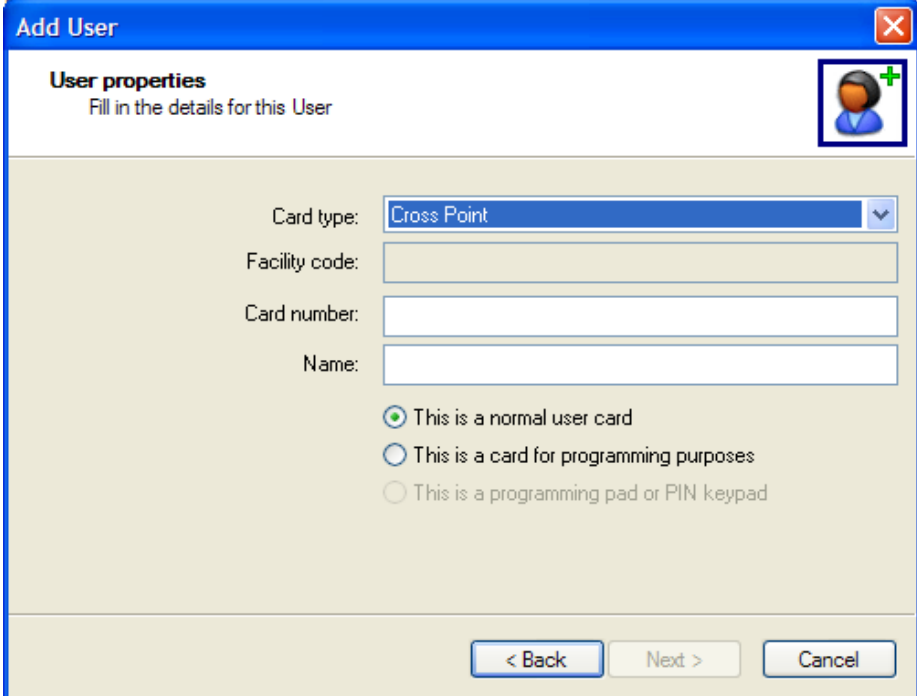
Figure 19: Add User Wizard – User Properties

4. In this dialog, select ⌄ to choose the correct **Card type** from the displayed drop-down menu.

5. In case of a HID Card type, enter the **Facility code**. This code is provided by the supplier of your HID Cards.

6. Enter the **Card number**.

7. Enter the **Name** of the person who will use the Card.

8. Select the option **This is a normal user card**.

9. Click the button **Next**.

Depending on whether you use XM3 Manage Pro and time schemes, The time scheme dialog is displayed (see Figure 20). If you do not use time schemes, you need to select the level of the user (see Figure 21).
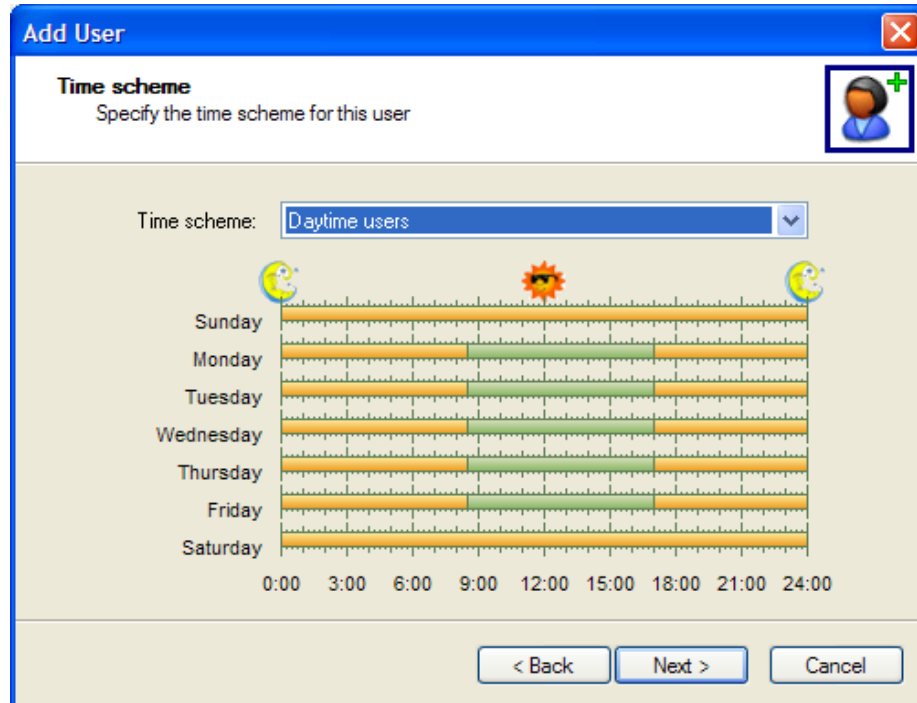
Figure 20: Add User Wizard - Time Scheme
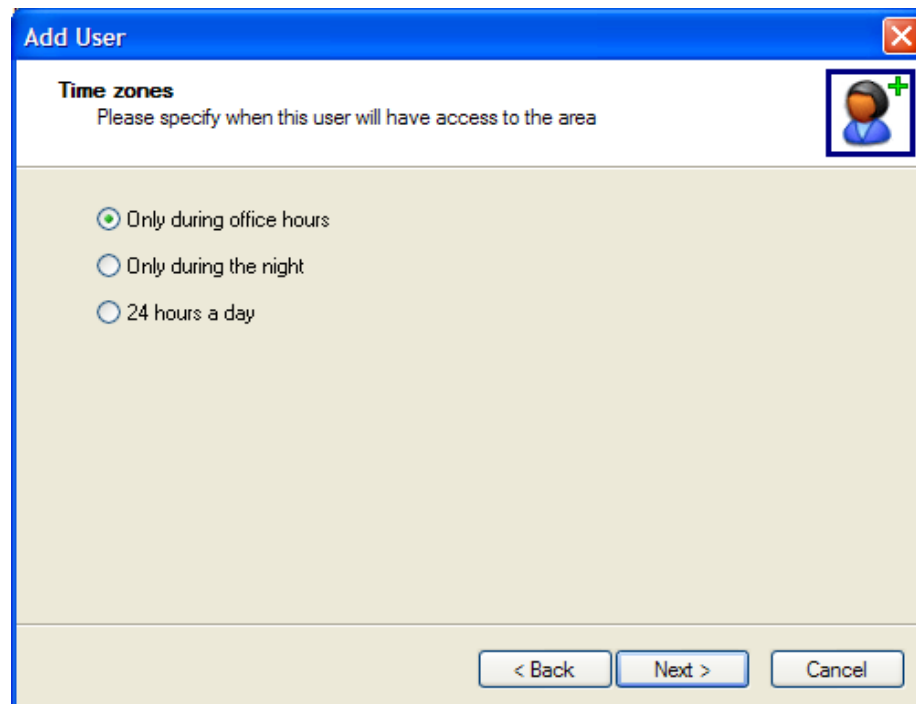
Figure 21: Add User Wizard - Choosing a user level

10. In the *time scheme* dialog you can select one of the time schemes. The corresponding time scheme will be displayed. If you wish to make another time scheme, you can select **File -> Create new time scheme** (see paragraph 6.1).

11. Click the button **Next**.

12. The User validation period dialog is displayed (see Figure 22).
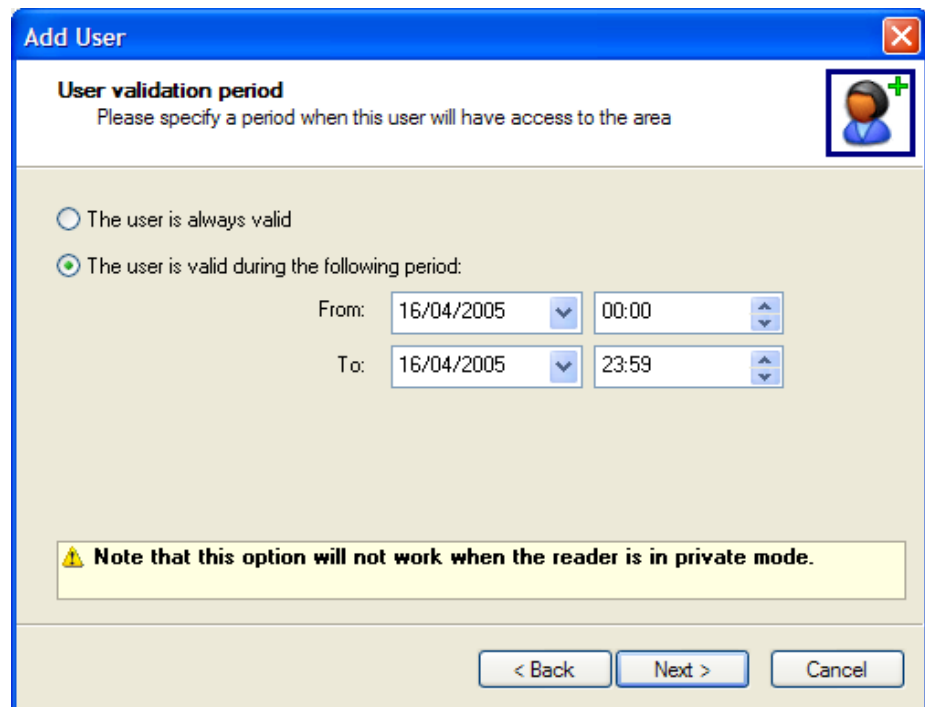
Figure 22: Add User Wizard - User validation period

13. In this dialog select whether the user always has access to the area or whether access is only allowed during a specified period of time.

14. In case the user is limited to a specified period of time, select ⌄ in the boxes **From** and **To**, in order to specify the beginning and the end of the period. Also specify the start time and end time at the date concerned.

15. Click the button **Next**. The *Select proximity readers* dialog is displayed (see Figure 23).
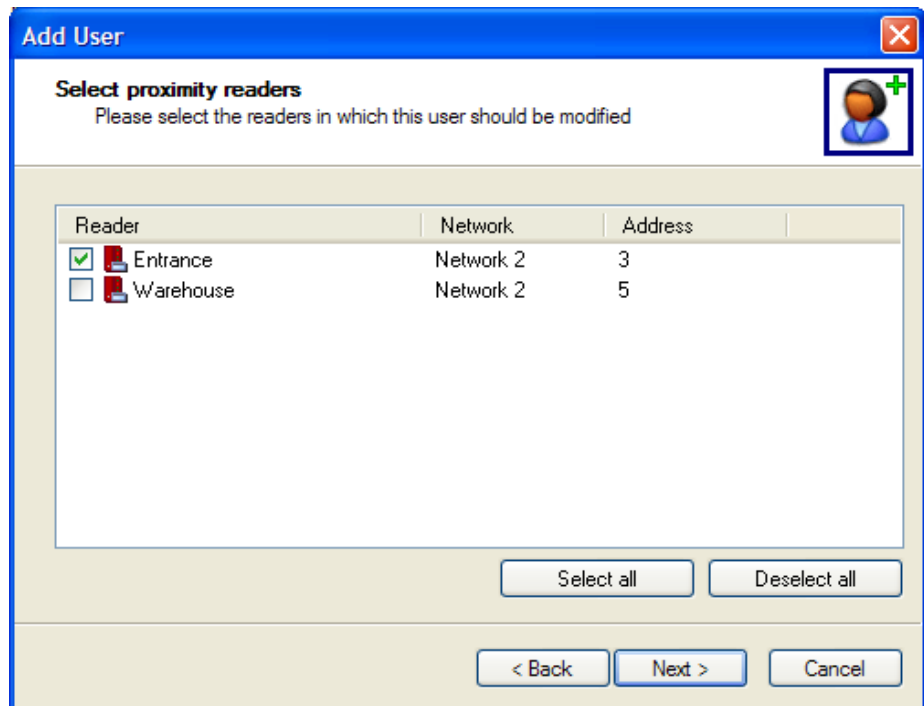
Figure 23: Add User Wizard - Select readers

16. Click the button **Select all** for all readers or select the checkbox(es) for the readers you want to add the user to.

17. Click the button **Next** and the *Progress* dialog is displayed.

18. Click the button **Next** and the dialog to complete the wizard is displayed. This dialog also gives information about the add process.

19. Select the check box **Check this box to add…** if more users have to be added. If you do so, clicking the button **Finish** will take you back to the beginning of this wizard, instead of completing and closing it.

or

20. Click the button **Finish** to complete and close the Wizard.

7.2.2   Add a card for Programming purposes

Apart from the normal cards, there are other types of cards that offer the possibility of adding, removing et cetera of normal cards. These types of cards are so-called *Master cards*. To add these cards to your access control system via the wizard, take the following steps:

1. Take the steps 1 up and including 7 from chapter 7.2.1.

2. Select the option **This is a card for programming purposes**.

3. Click the button **Next**. The dialog *Programmer pads and cards* is displayed (see Figure 24).
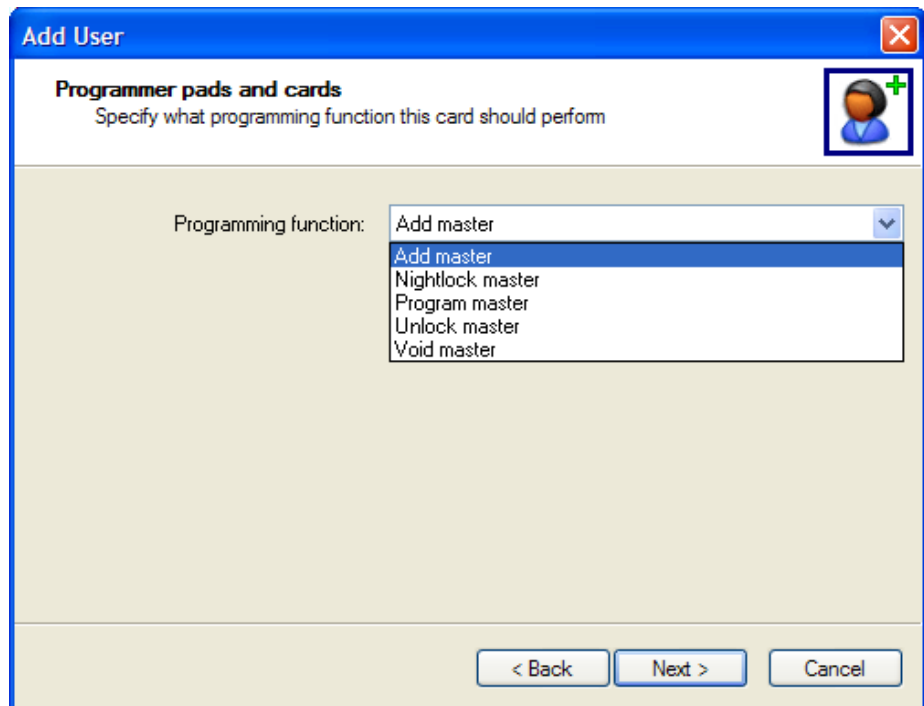
Figure 24: Add User Wizard - Programmer pads and cards

4. In this dialog, select ⌄ to choose the correct Programming function from the displayed drop-down menu. You can make a selection from:

    - **Add master**, a special card that can be used to add other cards to the reader.

    - **Night time master**, a special card that can be used to bring a reader into Night time mode.

    - **Program master**, a special card that can be used to add Add master, Night time master, Unlock master and Void master cards to a reader.

    - **Unlock master**, a special card used to unlock the door,

    - **Void master**, a special card that can be used to remove other cards from the reader.

5. Click the button **Next**, and proceed with steps 12 up and including 18 as mentioned in paragraph 7.2.1 to finish and close the Wizard.

7.2.3 Add a Programming pad

A programming pad is a device that can be used, as in the XM3 Manage application, to change reader parameters and to add/remove users to/from an XM3. A programming pad is always a Cross Point card type. For a higher level of security, an additional PIN keypad can be used for entering a PIN code in combination with the ID-tag to gain access. To add these programming pads via the wizard, take the following steps:

1. Take the steps 1 up and including 7 from chapter 7.2.1.

NOTE The unique number of any programming pad always begins with 8 and ends with 15. When you have entered this number, the option **This is a programming pad or PIN keypad** becomes active and the other options are grayed.

2. Click the button **Next**. The dialog *Programmer pads and cards* is displayed (see Figure 25).
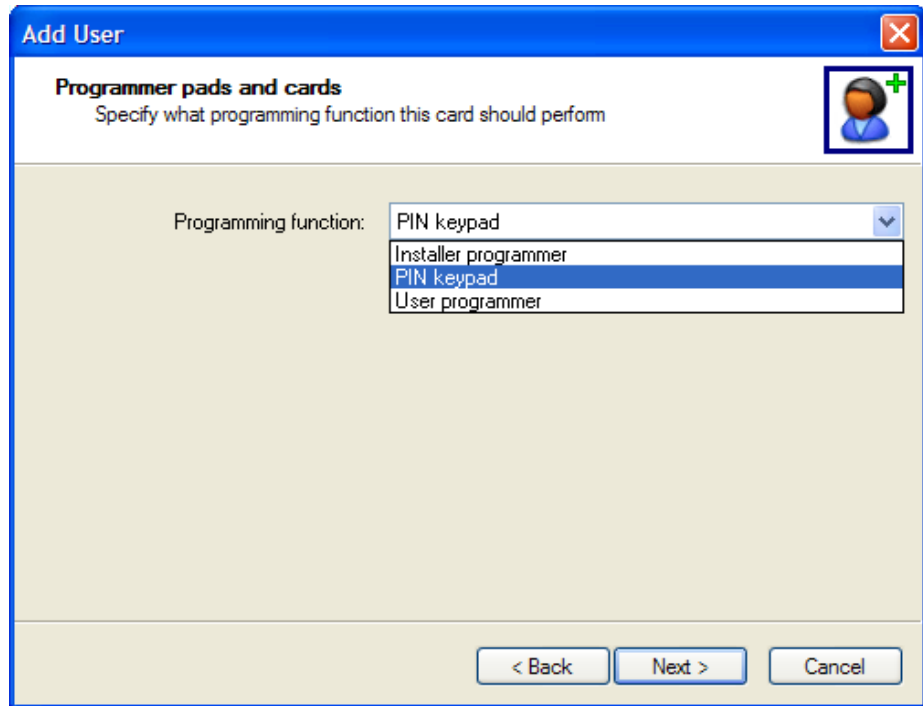
Figure 25: Add User Wizard - Programmer pads and cards

3. In this dialog, select ⌄ to choose the correct **Programming function** from the displayed drop-down menu.

4. You can make a selection from:

- **Installer programmer**, a keypad that is used by installers to configure the system.

- **PIN keypad**, a numeric keypad next to a reader to enter a PIN code.

- **User programmer**, a keypad that is used by end users to configure the system.

NOTE When logged on as an Installer, you can make a selection of all the different programming pads to choose from. Logged on as a user, only a *User programmer* pad can be chosen.

5. Click the button **Next**, and proceed with steps 16 up and including 18 as mentioned in the paragraph 7.2.1 to finish and close the Wizard.

7.3 Modifying users and programming pads

XM3 Manage offers the possibility to modify users, programming pads and master cards. This can be necessary if for some reason the access settings of a user or the authorization level of a programming pad must be changed. In the following chapters is explained how to do this.

7.3.1 Modifying users

Take the following steps to modify a user:

1. Select the *User folder* in the Folder bar from the reader you are logged on to. The users are displayed (see Figure 26).
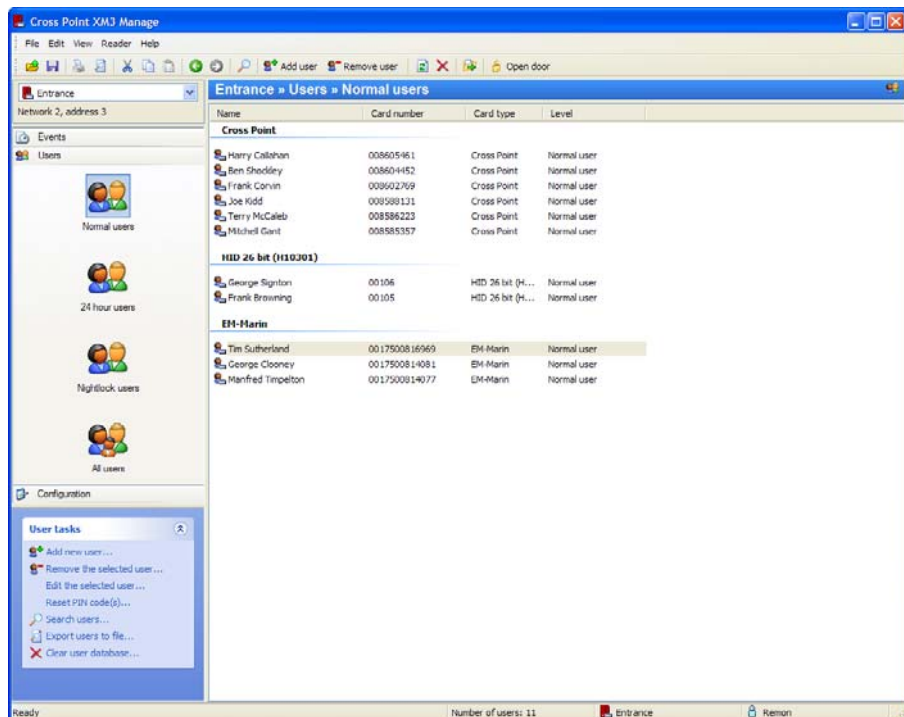
Figure 26: User view

2. Double click the target user from the list to display the *Edit User* dialog (see Figure 27). You can also use the context menu when clicking the right button on the mouse when pointing to a user or you can use the *Task pane* after selecting a user from the list.
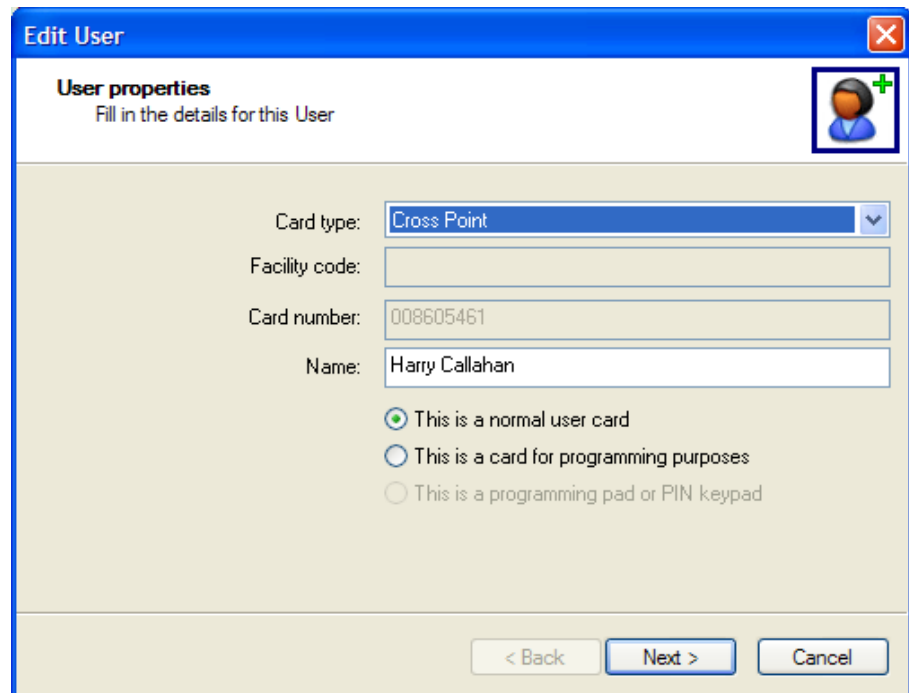
Figure 27: Edit User Wizard

3. Select the option **This is a normal user card**.

4. The rest of the procedure for editing a user is the same as the procedure for adding a user (also see 7.2.1).

If the PIN Access Code has been forgotten by the ID-tag user, the user can ask the XM3 Manage user to reset it. The user can define a new PIN Access Code, by presenting the ID-tag to the reader and enter on the PIN keypad a new Access Code. This code consists of maximum 4 characters and is for example defined as: 9467*. The user has to verify the Access code, by entering 9467* again.

5. Select the user or users of whom you want to reset the codes.

6. Select the option **Reset Pin code(s)** in the *User tasks* on the right or using the context menu.

> **NOTE** Reset of the PIN access code is only possible if a PIN keypad is available and the Installer has configured it, a PIN code change code is defined (see 8.1.7), and the PIN Keypad option Enable PIN code is selected (see 9.2.6).

7. Confirm whether you want to reset the selected Pin codes.

8. Click the button **OK** to make the changes effective.

7.3.2 Modifying a programming pad

The following steps are only accessible if a programming pad is already present. Take the following steps to change the authorization level of a programming pad.

1. Select the *User* folder in the Folder bar from the reader you are logged on to, to display the users view again.

2. From the list, select the target programming pad to display the *Edit User Wizard* (see Figure 28). Note the change in the lay-out of the dialog compared with the lay-out as displayed in paragraph 7.3.1.
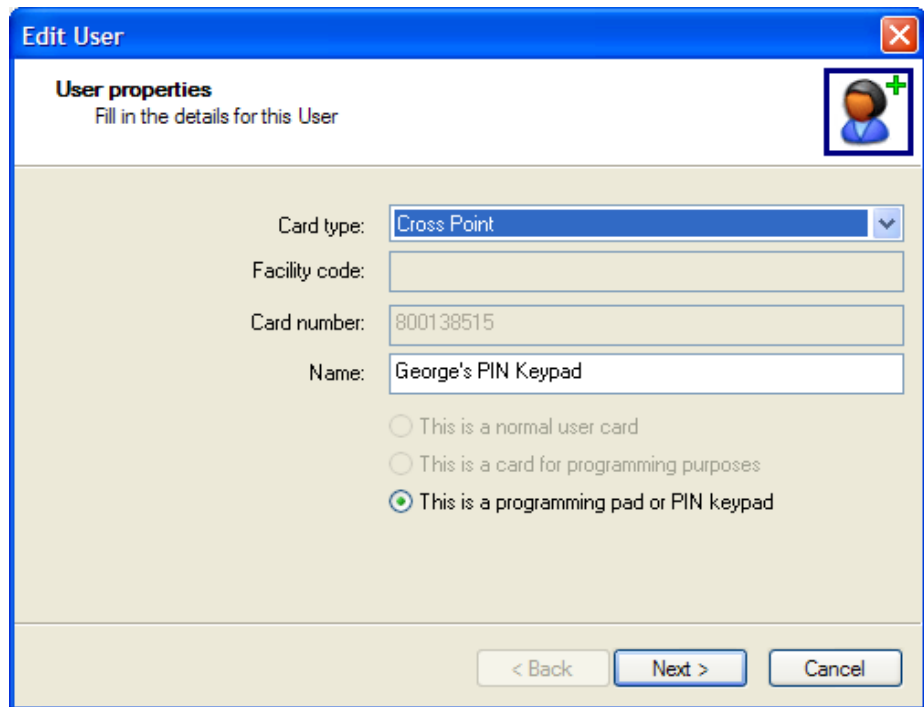
Figure 28: Edit User Wizard - Programming pad

3. Select from the drop down menu *Programming Pad* the required one.

   NOTE   When logged on as an Installer, you can make a selection of all the different programming pads to modify. Logged on as a user, only a User programmer pad can be selected to modify.

4. Select the check box **Change user settings in…** if you want the changes to apply to all the readers.

5. Click the button **OK** to make the changes effective.

7.3.3 Modifying a master card

The following steps are only accessible if a master card is already present. Take the following steps to modify a master card.

1. Select the *User* folder in the Folder bar from the reader you are logged on to, to display the users view.

2. From the list, select the target master card to display the *Edit User Wizard* (see Figure 29). Since you have selected the target master card from the list the details are already filled in.
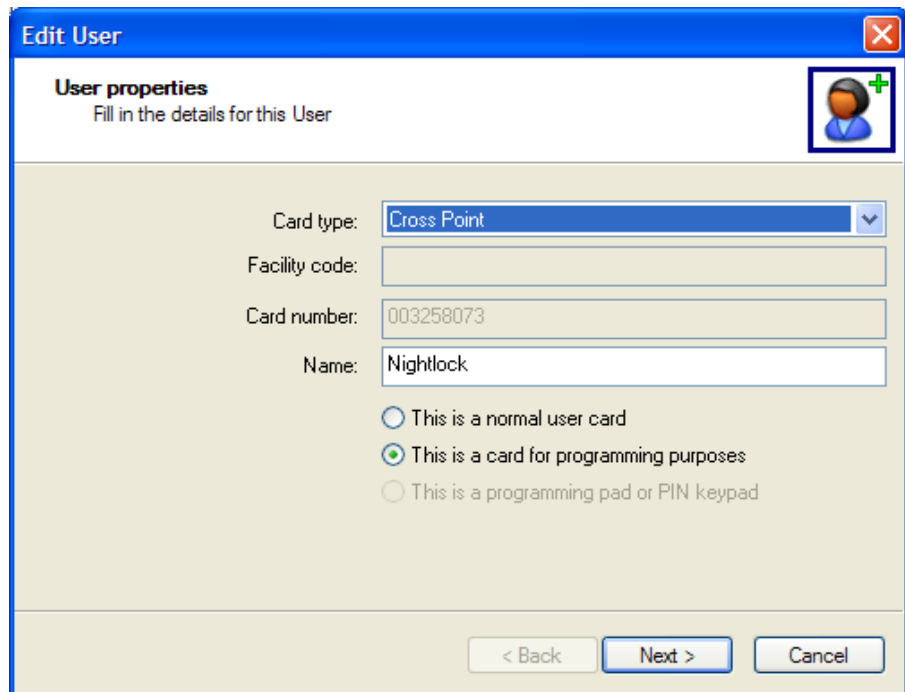
Figure 29: Edit User Wizard - Programming Cards

3. Click the button **Next**. The Programming pads en card dialog will appear.

4. Select from the drop-down menu **Programming Card**, the required one.

5. You can make a selection from:

   • Add master

   • Night time master

   • Program Master

   • Unlock master

   • Void master

6. Select the check box **Change user settings in…** if you want the changes to apply to all the readers.

7. Click the button **OK** to make the changes effective.

7.3.4 Modifying the level or time scheme

Sometimes it is convenient to change the user level of multiple users in one step. When you are not using user levels but time schemes, assigning multiple users to another time scheme can be hard when doing this for each

user separately. Therefore XM3 Manage has an option to quickly move users to another time scheme or level.

1. Select the *User* folder in the Folder bar from the reader you are logged on to, to display the users view.

2. Select the users that should be moved and click the right mouse button. The following menu appears:
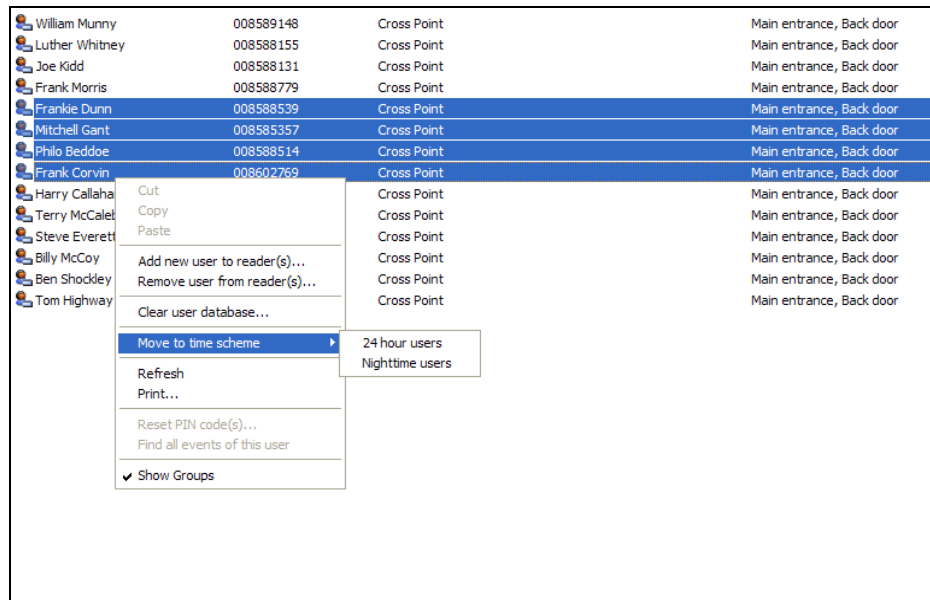
3. In this menu, select **Move to user level** when using levels or **Move to time scheme** when using time schemes. Another popup menu appears with the levels or time schemes.

4. Select the level or time scheme where you want to move these users to. The users are moved to the selected user level or time scheme.

7.4 Removing users

When, for instance, access control for a certain reader in combination with a card user is no longer valid or a user is considered not to be part of your access control system any longer, the user can be removed from your system.

XM3 Manage knows different ways to remove users. In paragraph 7.4.1 and 7.4.2 is explained how.

7.4.1 Remove User Wizard

Take the following steps to use the Remove wizard:

1. From the *Menu* bar, select **File -> Remove user from reader(s)…** to display the *Remove User Wizard*.

2. In this Wizard, select the button **Next**. The *User properties* dialog is displayed (see Figure 30).
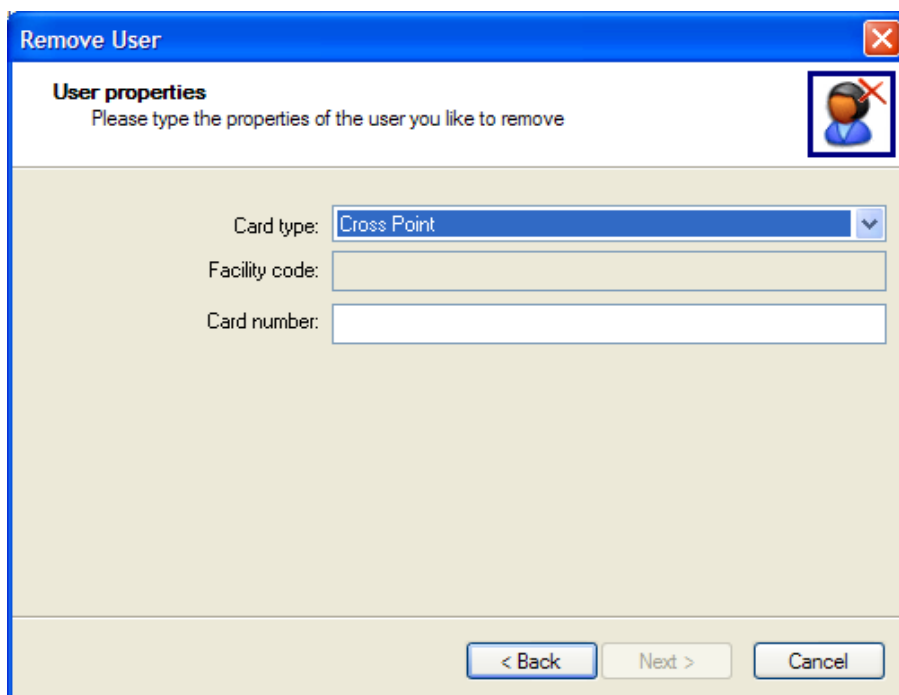
Figure 30: Remove User Wizard

3. In this dialog select ⌄ to choose the correct *Card type* from the displayed drop-down menu.

4. In case of an HID card, enter the **Facility code**.

5. Enter the **Card number**.

6. Click the button **Next**. The *Select Proximity readers* dialog is displayed (see Figure 31).
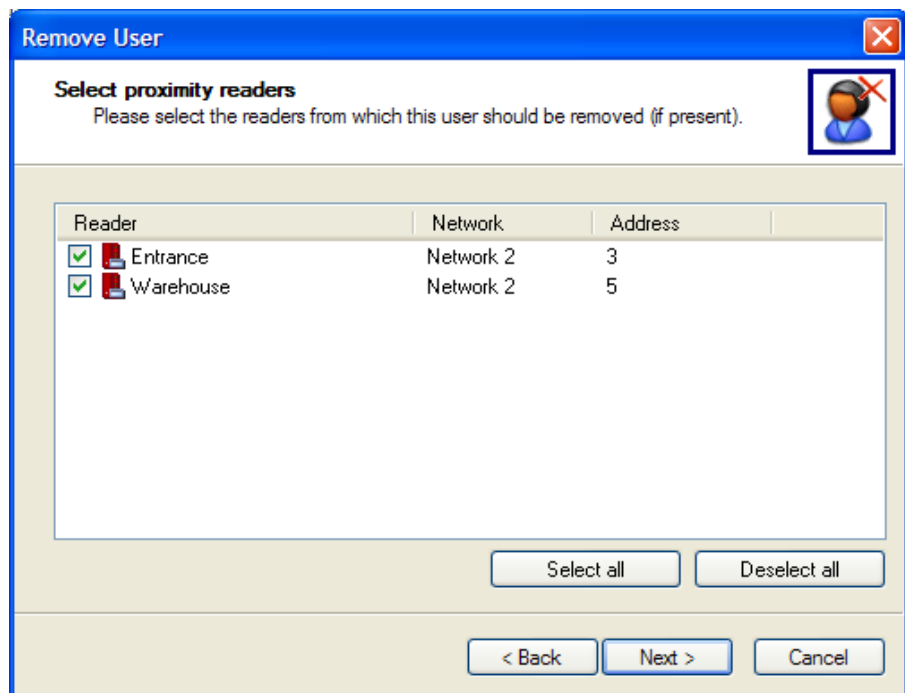
Figure 31: Select readers dialog

7. Click the button **Select all** for all readers or select the checkbox(es) for the readers you want to remove the Card or Pad from.

8. Click the button **Next** and the *Progress* dialog is displayed.

9. Click the button **Next** and the dialog to complete the wizard is displayed. This dialog also gives information about the remove process.

10. Select the checkbox **Check this box to remove…** if more card users have to be removed. Now, clicking the button **Finish** will take you back to the beginning of this wizard, instead of completing and closing it.

Or

11. Click the button **Finish** to complete and close the Wizard.

7.4.2   Remove Users via the right pane

Another way of removing users is via selecting users in the right pane.

1. Select the reader from which you want to remove the users.

2. Select the Users icon to display the users.

3. Select the users you want to remove.

4. Click the button [icon] in the tool bar or in the *User Tasks* pane to start the *Remove User wizard*, and you can remove the users. The tag number is automatically filled in.

NOTE   You can also use the context menu in the *User pane* to remove users.

7.5   Saving Users

It may be convenient to make back-up files of the users of your access control system.

XM3 Manage offers the possibility to create back-up files in .xml or .csv format and to save them on your PC.

It is necessary that you have selected the correct subject you want to make a back-up from. For example: If you want to make a back-up of the Users of a certain reader, it is necessary that these Users are being displayed in the right pane.

NOTE   To prevent back-up files to be overwritten, it is recommended to identify them uniquely. Per reader, you can make a separate user back-up file.

Take the following steps for making a back-up of the Users.

1. Select from the Folder bar or tree (dependent on the view setting) the *Users* folder. The Users are listed in the right pane.

2. From the Menu bar, select **File -> Save**. The *Save As* dialog is displayed.

3. Enter a name for the file and select a location where to store it.

4. Click the button **Save** to save the back-up file.

Back-up files of the users can be used as a basis for the off-line user database. They can also be used, for instance, to load the users to another reader.

NOTE   If you want to upload the users to another reader, that reader should have the same file system set as the one from which the file originates.

Take the following steps to do this.

1. Select the reader in which you want to store the contents of the back-up file.

2. Select the **Users** folder of this reader in the Folder bar or tree.

3. From the Menu bar, select **File -> Open**. The *Open* dialog is displayed.

4. Select the required file.

5. Click the button **Open**. The *Transfer settings* dialog is displayed (see Figure 32).
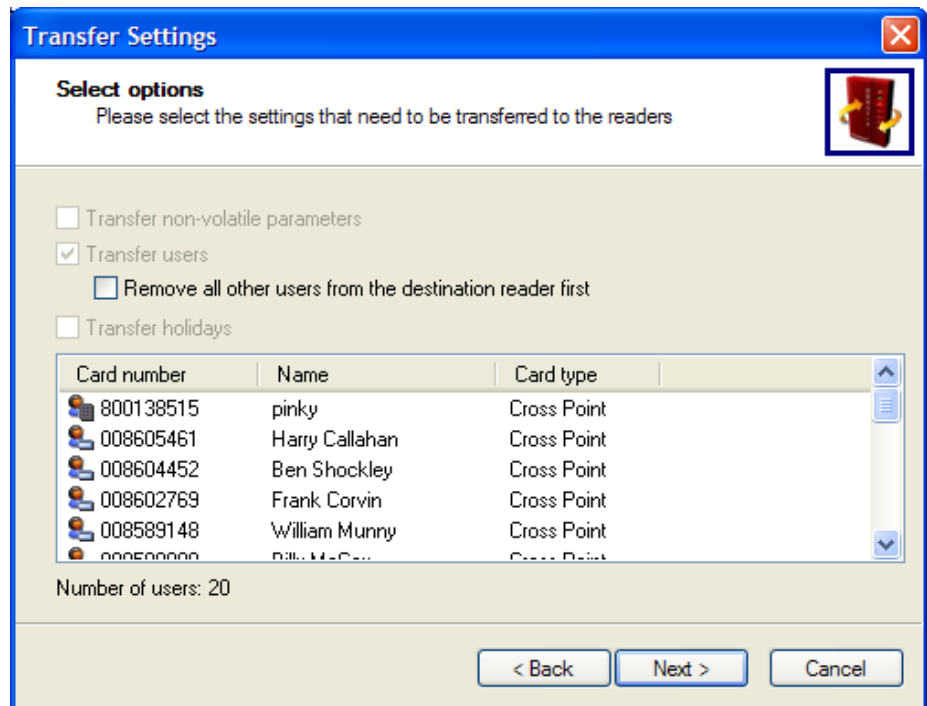
Figure 32: Transfer Settings Wizard to upload users

6. Select the check box **Remove all other…** if you want to remove all users from the destination reader.

> **NOTE**   If there are users present in the reader that are not yet in the database file, these users will be lost if you select this option.

7. Click the button **Next**.

7.6   Create an off-line user database

Another possibility to back-up users is to create an off-line user database. This database can be used for back-up purposes, but also for quickly transferring user data to and from readers. The off-line user database gives you the possibility to maintain your user file without the need to directly communicate with the readers in the system. After updating the database off-line you can upload all readers with the latest version of your database (also see 7.5).

NOTE   Since users can be added through the readers as well as in the off-line user database, we strongly recommend synchronizing the data on a regular basis.

1. From the Menu bar, select **File -> Create off-line user database** to display the dialog *Create off-line user database.*
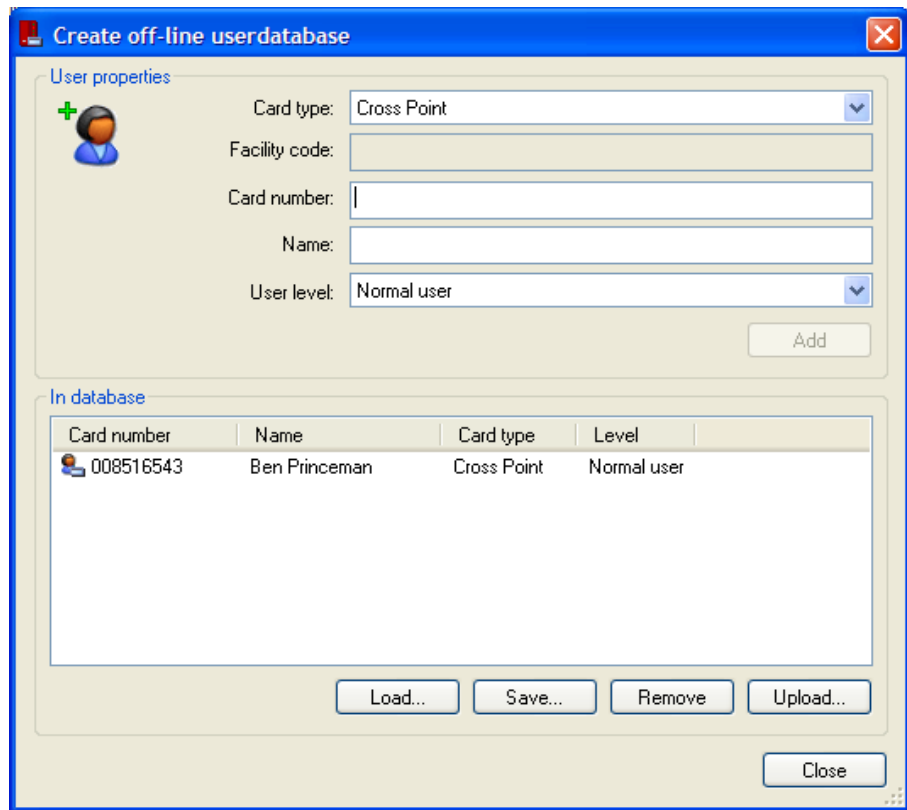
Figure 33: Create off-line user database

2. Enter the card number of the user you want to add to the database.

3. Enter the name of the user.

4. Select the user level.

5. Click the button **Add**.

The user is added to the bottom pane of the dialog. Repeat step 1 up to 5 if you want to add more users.

7.6.1   Loading/Saving off-line user database files

If you have already saved a database file you can load this file by taking the following steps.

1. Click the button **Load**. The *Open* dialog is displayed.

2. Select the required file.

3. Click the button **Open**.

The contents of the file appear in the bottom pane of the dialog, and can be modified. After modification of a file (or after creating one) it can be saved by taking the following steps.

1. Click the button **Save**.

2. The *Save as* dialog is displayed.

3. Enter a name for the file and select a location where to store it.

4. Click the button **Save** to save the file.

7.6.2   Uploading data to readers

After creating or modifying an off-line user database file you can upload the users to one or more readers. The database file functions as a back-up for the readers. To upload user data to the readers, take the following steps.

1. Click the button **Upload** in the *Create user database* dialog. The *Transfer Setting Wizard* is displayed (see Figure 34).
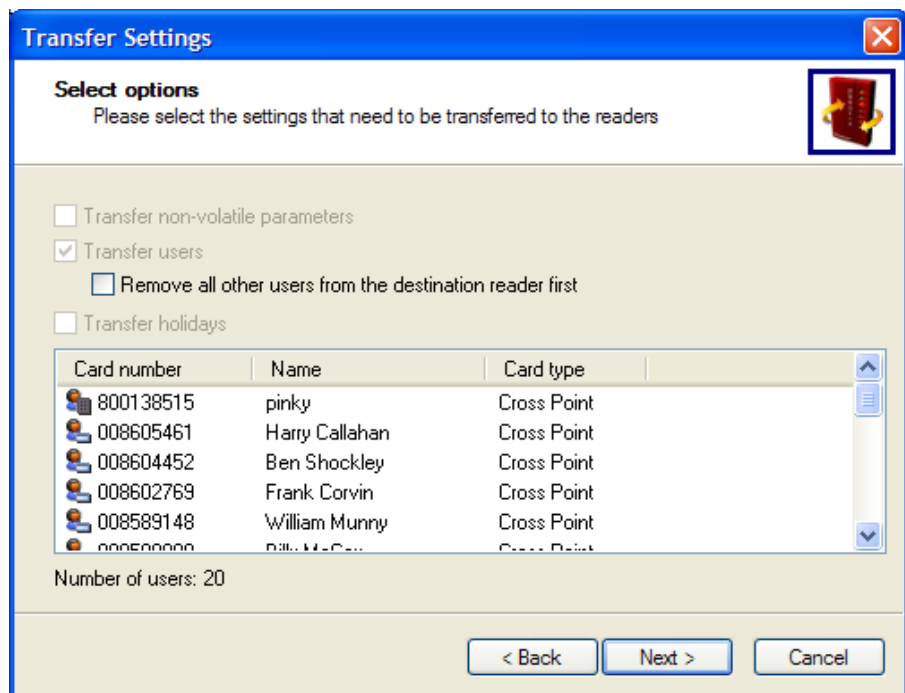
Figure 34: Transfer Setting Wizard

2. Select the check box **Remove all other…** if you want to remove all users from the destination reader.

NOTE   If there are users present in the reader that are not yet in the database file, these users will be lost if you select this option.

4. Click the button **Next** and the *Selecting Proximity Readers* dialog is displayed.

5. Select the readers to which the settings should be transferred.

6. Click the button **Next** and the *Progress* dialog is displayed.

7. When all readers have been uploaded, click the button **Finish** to return to the application.

8 Events

After selecting a reader, you can view the events for this reader. You can clear this event log or print its contents. This functionality can be accessed using a context menu that pops up when you press the right mouse button in the events pane or using the reader menu.

8.1 View events

XM3 Manage logs the events that occur while using the readers. Per reader you can view these events. Take the following steps to view the events.

1. Select a reader

2. Select the *Events* folder in the folder bar or tree (dependent on the selected view).

The events are displayed in the right pane (see Figure 35). The events are listed in two columns indicating the date and time of occurrence and a description of the event.
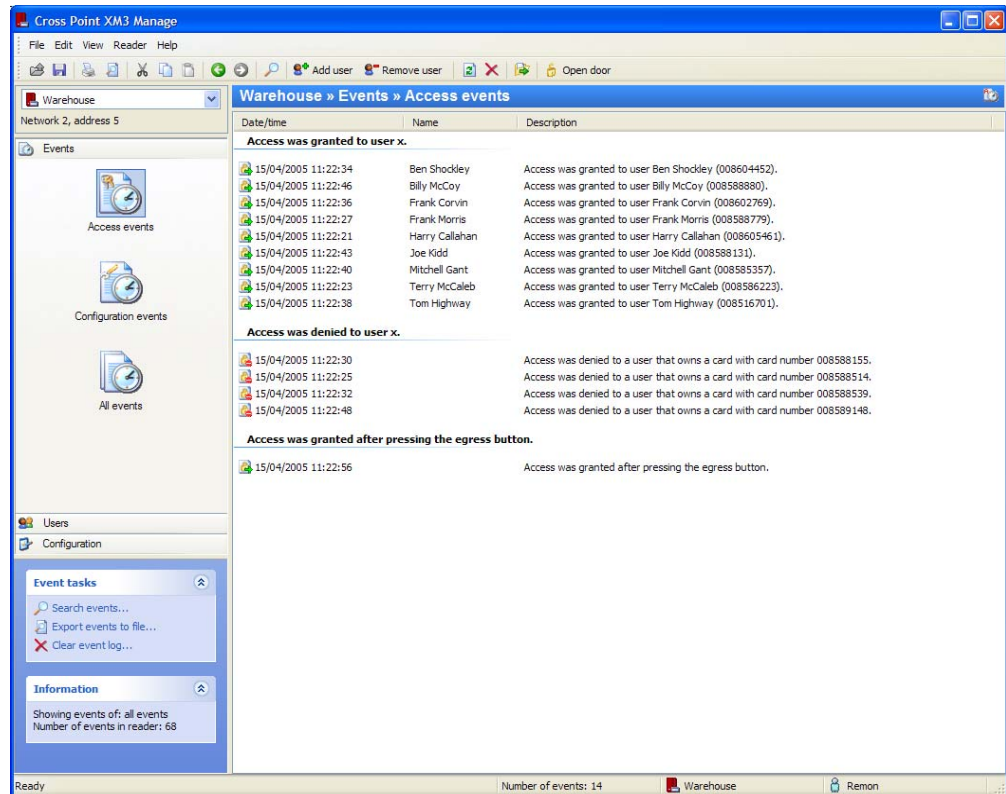
Figure 35: Events View

8.2   Add users via an event

Another way of adding users is via an event. Presenting unknown ID-tags, programming pads et cetera to a reader will result in **Access was denied …** events. Via these events, you can add the ID-tags et cetera. Take the following steps to do this:

1. Select a reader

2. Select the *Events* folder in the folder bar or tree (dependent on the selected view).

3. Select the icon *Access Events.* The events are displayed in the right pane (see Figure 35). The events *Access was denied…* indicate the unknown tags that have been presented to the reader.

4. Double click an **Access was denied** event. The *Add User wizard* is opened, and you can add the users.

   NOTE   The Card type, Card number and in case of an HID tag also the facility code are filled in automatically.

8.3   Saving events

You may want to know how your system is used, or whether unauthorized access attempts have been made. For this purpose, you can store the events that occurred in a back-up file. Take the following steps for making a back-up of the events.

1. Select a **reader** from the Folder bar or tree (dependent on the view setting).

2. From this reader, select the **Events** folder. The Events are listed in the right pane.

3. From the Menu bar, select **File -> Save**. The *Save As* dialog is displayed.

4. Enter a name for the file and select a location where to store it.

5. Click the button **Save** to save the back-up file of the events.

9 Setting reader parameters

A number of parameters can be set to customize the readers in your Access Control system. Take the following steps to display the Parameters:

1. Select the reader for which you want to set parameters

2. Select the folder **Configuration**

3. Select the **Parameters** icon in the Folder bar

The Parameters in the right pane are divided in two columns: a name and a value column (see Figure 36).

Clicking in a value field will display an arrow down ⌄ or a scroll ⬍ button. Selecting the arrow down button will open a drop-down menu from which a selection can be made. Using the scroll button will increase or decrease the value of a parameter. When all the parameters have been set, click the button **Apply** to make them effective. Select **Restore defaults** in the Task pane if you want the factory default values to be restored again. You can also use the context menu to refresh or print the parameters in this pane.

NOTE   Parameters marked with ⚠ will cause the reader to reset.
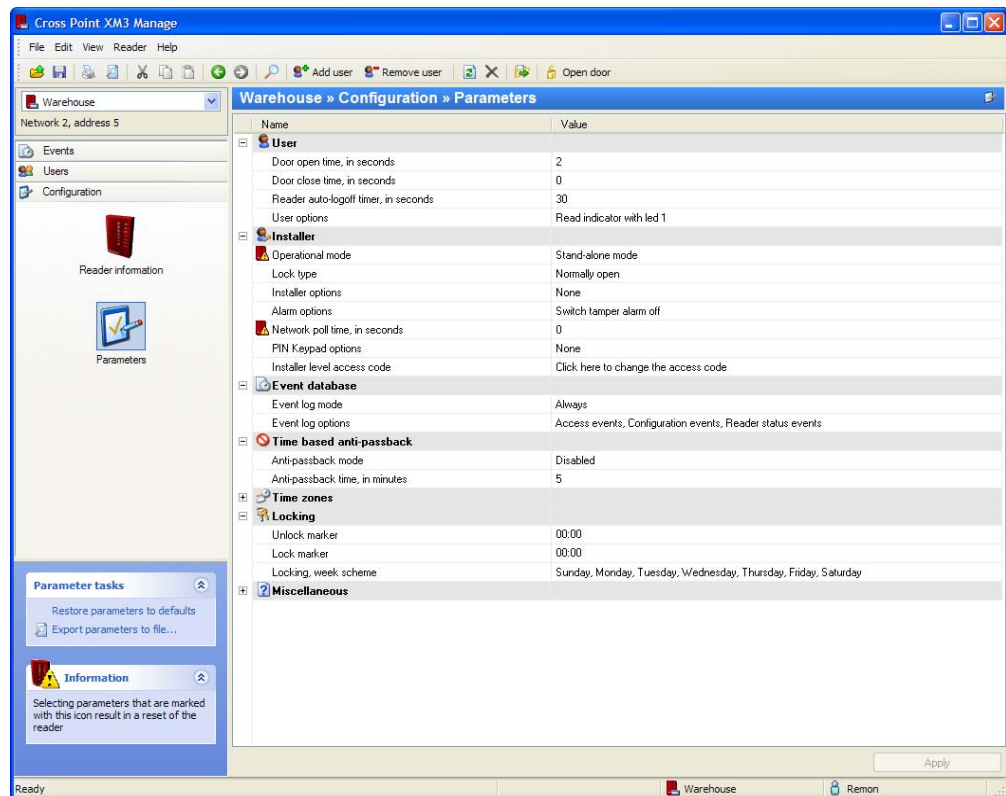
Figure 36: Parameter View

In the following chapters, the parameters that can be set will be described.

9.1 User Parameters

Open time

Whenever access is granted for a user, the relay of the reader will be activated during a certain number of seconds before closing an entrance again. This period of time is called the Open time. The default value is 2 seconds, but can be set from 1 to 255 seconds.

Close time

The reader can check whether the gate or door has been closed after a certain period of time. This period of time is called the *Close time*. When the door contact is not closed within the specified time an alarm is generated and it is logged in the event log of the reader. The default value is 0 seconds (inactive), but can be set from 0 to 255 seconds. Any value other than 0 will activate the Close time option (active). I/O1 must be connected to ground via a door contact when the Close time option is used.

NOTE   The Close time must be equal or larger than the Open time.

Reader auto-logoff timer

The reader can also be programmed by Programming pads and Master cards. The timer of the reader can count the number of seconds that passed since the latest key press on a Programming pad or when the last card has been presented while in program mode. If a preset period of time is exceeded, the reader exits the program mode and resumes normal operation. This period of inactivity can be adjusted from 5 up to 255 seconds. The default value is 30 seconds.

User options

On User level, the following options can be set:

- **Protect option**. If this option is selected, an Installer Programmer pad cannot set the reader in program mode. In this way it is prevented that an Installer can access the system after installation.

- **Read indicator with LED 1**. If this option is selected, LED 1 will go on when a tag or programmer is detected by a reader.

By default the **Protect** option is off and the **Read indicator** option on.

PIN keypad alarm code

An alarm code can be programmed that enables a user to activate a silent alarm. This code is maximally 4 characters and identical for all users. Upon presenting the card to the reader and then entering this code, the silent alarm is activated. The alarm code is the same for all users, meaning that all users knowing this code can activate the silent alarm. An external alarm panel can be activated through I/O 3.

NOTE For security reasons, the code is not displayed. Click on the text to change the code. To use the PIN keypad alarm code, at Installer level the PIN Keypad option **Enable PIN code** must be checked. This option is only visible when the reader is in user level.

PIN access code

A PIN access code can be programmed to grant users access using this code in stead of their card. When they want to enter all they have to do is enter this code on the PIN keypad. This code is maximally 4 characters but cannot be 0000, since 0000 is used to deactivate this code. The access code is the same for all users, meaning that all users knowing this code can have access using this code.

NOTE For security reasons, the code not displayed. Click on the text to change the code. To use the PIN Access code, at Installer level the PIN Keypad option **Enable PIN code** must be checked. This option is only visible when the reader is in user level.

PIN code change code

On the PIN keypad, a card user may want to change the PIN code he identified for his card. To be able to do this, a PIN code change code must be

defined. When presented to the reader, this change code must be entered before the user can change the PIN code for his card. This code is maximally 4 characters but cannot be 0000, since 0000 is used to deactivate the change code. In addition, the Change code may not be the same as the Alarm code.

NOTE   For security reasons, the code not displayed. To use the PIN code change code, at Installer level the PIN Keypad option **Enable PIN code** must be checked. This option is only visible when the reader is in user level.

If a card user wants to change his PIN code, he has to take the following steps:

1. The user must present his card to a reader near a PIN keypad.

2. On the PIN keypad, the **PIN code change code** must be entered, for instance *5555.

3. Now the user can enter his old PIN code, for instance 3333*.

4. A new PIN code can be entered, for instance 1234*.

5. To confirm this PIN code, the user must again enter 1234*

User Access code

By default all the readers have the same User access code, which is: 123456789. The User Access parameter is only visible if you are logged on as user. This default code should be changed. However, you can change the default code to a unique one per reader or one for all the readers.

NOTE   For security reasons, the code is not displayed.

9.2   Installer Parameters

NOTE   These parameters are not visible if the reader is in User level.

Operational Mode

The reader can be set to different operational modes. The modes can be separated in modes where controlling of the system is done by the reader or in modes where external controllers take over the reader. In the following tables an overview of the possibilities is given.

Modes where the reader is the controller as well:

Sleep mode   If you have chosen this mode, the reader in fact is not active.

Stand-alone mode   This is the normal Stand-alone mode.

Night time mode   A special mode in which normal users are denied access. Night time and 24 hour users have access.

Unlock   The mode when access is granted without the use of a card.

Modes where an external controller takes over the reader:

RS-485 interface   The mode when the readers are connected to a controller via RS-485.

Wiegand interface   The mode when the readers are connected to a controller supporting the Wiegand protocol

Magstripe interface   The mode when the readers are connected to a controller supporting the Magstripe protocol.

Lock Type

The relay output of the reader can be used to switch an electrical door lock. From the following lock types a selection can be made:

Lock Type	Description
Normally open	The settings *normally open* and *normally closed* are used when a lock is directly connected to the reader.
Normally closed	
Coded signal	Coded signal is used to trigger an external relay on Cross Point's Connection Units. The external relay offers a higher level of security.

The default value for the lock type is: Normally open.

Installer Options

When the reader is in the Stand-alone mode, at Installer level, three different access options can be set.

- **Private option**

   Selecting this option will switch the reader into a special operation mode in which it will grant access to only one user tag at a time after which the reader will go into "Lock" status. Until the "Lock" status is switched off by the same tag, no other tags are accepted. The "Lock" status can also be switched off by pressing (if mounted) the egress button. I/O4 can also be used in this option to switch an external device via the external relay circuit.

   For safety reasons, and in case of emergency, access can be obtained by either:

   - presenting a Night time Master
   - switch the power off and on again and present any user card
   - programming pads

- **Public option**

   This option disables the check for the presence of a presented card in the memory of the reader in Access mode. Any tag type accepted by your Access Control system is allowed access, whether or not it is in

the reader's memory. This option cannot be used in the Night time mode.

- **Egress option**

  This option is used together with a push button mounted for instance near an exit inside a building. When this option is set, and somebody wants to leave the building, pushing the button will unlock the door lock and the person can leave the building. When set, this option will disable the external Night time control that uses the same I/O2 input (access is granted when I/O2 is connected to ground potential for a short while). This method of access is controlled in a similar way as normal access using the Open Time and Close Time, starting form the moment that the button was pushed.

The Installer options can be used in combination. By default the Installer options are disabled.

Alarm Options

At Installer level, the following alarm parameters can be set.

- **Change alarm tone**

  The default alarm tone is a continuous one. Selecting the alarm tone option, changes the default continuous alarm tone into a pulsing tone.

- **Redirect tamper alarm output**

  By default the tamper alarm and the forced entry alarm are connected to I/O3. This option separates the tamper alarm from the forced entry output and redirects it to I/O4.

- **Switch tamper alarm off**

  When you want to use the tamper alarm, deselecting this option makes it possible to use this alarm.

Any combination of the options is possible. By default, the *Switch tamper alarm off* is selected.

PIN Keypad options

The PIN keypad is an additional device that can be used for instance to get access to a building by using a PIN code. It can also be used to do settings on the reader, provided that the PIN keypad is mounted next to the reader and present in the memory of the reader. XM3 Manage offers the following functionality that can be set for using a PIN keypad.

- **Alarm notification mode**

  The PIN keypad must be mounted within range of the reader. With this mode set and an alarming device connected to I/O3, the Alarm notification mode will raise an alarm if for some reason the PIN keypad is longer than 15 seconds out of range of the reader. If this occurs, the reader will sound an alarm as well.

- **Enable PIN code**

The reader offers the possibility for users to get access by using a predefined PIN code in combination with their cards. Selecting this **Enable PIN code** option enables the use of the PIN keypad alarm code, PIN access code and the PIN code change code (see paragraph 9.1).

- **Use PIN keypad as user programmer**

  The PIN keypad can be used also to perform remote user programmer settings on the reader. Selecting this option enables this function. In addition a Program Master must be presented to the reader to activate the User programming pad.

- **PIN at night only**

  As an extra security, selecting this option grants users access through their PIN code only during the night time zone. When this option is set, the PIN code is only active in the Night time mode. By default this option is not selected, meaning that the PIN code is active in access mode.

Installer level PIN code

By default all the readers have the same Installer access code, which is: 123456789. This default code should be changed. However, you can change the default code to a unique one per reader or one for all the readers.

NOTE   For security reasons, *the Installer access code* is not displayed.

9.3   Event database

NOTE   Those options are not available when using XM3 Manage Single Door.

The reader supports logging of events that occur while using the Access Control system.

Event log mode

You can choose from two different types of logging of events:

- **Enabled**. Events are logged at all times
- **Disabled**. Events are not logged

By default events are always logged.

Event log options

You can make a selection of the events you want to log. You can choose from:

- **Security**. Security related events are for instance: Tamper alarm activated/deactivated, Access was granted/denied et cetera.

- **Configuration**. Configuration related events. For instance: A system parameter has been changed; a user changed the PIN code of his card et cetera.

- **Status**. Status related events, being specific system statuses; errors et cetera that were detected by the firmware of the reader. For instance: System startup.

- **Destructive Read**. When you select destructive read for events to log, the events are erased from the reader memory after reading.

Any combination is possible. By default, Security, Configuration and Status are selected.

9.4 Time based anti–pass back

The time based anti-pass back feature provides extra safety for readers in stand-alone mode. When a user has obtained access, the reader will temporarily disable the user's card for a specified period of time. This prevents that another person can use the same card to get access also. Anti-pass back is only applicable for "normal users", "special users", and "Night time only". The anti-pass back time is the same for all applicable cards and becomes effective the moment the card is presented. The anti-pass back time can only be set in the stand-alone mode. In the following paragraphs the setting of this function is explained.

Anti-pass back mode

You can enable or disable the anti-pass back mode. By default the mode is disabled.

Anti-pass back time

The anti-pass back time can be set from 1 up to 255 minutes. The default setting is 5 minutes.

9.5 Time zones

Time zones can be used to set a day-night scheme for switching between time zones.

NOTES For security reasons it is not possible to switch from Nighttime to Unlock mode. This prevents that while being in the Nighttime mode an Unlock Master card user can obtain access.

Those options are NOT available when using XM3 Manage Pro, because then we have the more advanced time schemes functionality to do this.

Time zones markers (only XM3 Manage)

The time markers indicate the first minute during which access in the respective time zone is possible.

Setting the **night-to-day marker** to **08:30** and the **day-to-night marker** to **17:00** means that access is granted from 08:30 AM to 16.59 PM. From 17:00 to 8.29h access is only possible for Night time users and 24 hours a day users.

NOTE Please check if you have synchronized the date and time of your readers with the time of the host PC.

Time zones week scheme

You can select the weekdays for which you want the time zones markers to be active. By default the time zone markers are enabled for every weekday.

9.6   Locking

The Lock/Unlock option makes it possible to give access during a defined time without the need of presenting an RFID tag. This can be very useful during working hours. After working hours, the reader switches to access mode, and users that want to enter have to identify them with a valid RFID tag. While in Unlock mode, the green access LED will be lit continuously. Dependent on the lock type, the door lock will be activated or not. The Unlock option is always overruled by the Night time option. In the following paragraphs you find information how to set this option.

NOTE For security reasons it is not possible to switch from Night-Lock to Unlock mode. This prevents that while being in the Night-Lock mode an Unlock Master card user can obtain access.

Unlock marker

The time marker indicates the first minute during which access in the respective time zone is possible.

Setting the **unlock marker** to **08:00** means that Unlock (access is granted without the use of a card) is active from 08:00 AM.

NOTE Please check if you have synchronized the date and time of your readers with the time of the host PC.

Lock marker

The time marker indicates the first minute from which access in the respective zone is denied. Setting the **lock marker** to 17:00 means that Lock is active from 17:00 PM.

NOTE Please check if you have synchronized the date and time of your readers with the time of the host PC.

Unlock, week scheme

You can select the weekdays for which you want the Unlock markers to be active. By default the Lock/Unlock scheme is enabled for every weekday.

9.7　Miscellaneous

Reader name

You can enter a name to identify a reader, for instance the location where it is mounted. Up to 23 characters including spaces can be used for a name.

Magstripe output format

If you have chosen for the Magstripe interface, you need to select an output format that corresponds with the number of digits of the cards you use in the Access control system. You can choose from:

- 9 digits
- 13 digits
- 14 digits

The default value is 9 digits.

Support for Bioscrypt V-PASS fingerprint reader

When setting this option, the Wiegand output interface is reversed to Wiegand input so that the Bioscrypt fingerprint reader can be attached to the XM3 for more secure access control.

Magstripe number of start bits

This function enables the controlling of the number of start bits (leading zeroes) that precede the Magstripe frame. This value can be set from 1- 255. The default value is 8 bits.

Magstripe number of stop bits

This function enables the controlling of the number of stop bits (trailing zeroes) that follow the Magstripe frame. This value can be set from 1-255. The default value is 8 bits.

Wiegand output format

If you have chosen for the Wiegand interface, you need to select an output format that corresponds with the format of the cards you use in the Access control system. You can choose from:

- HID standard 26 bits
- HID standard 34 bits
- HID standard 37 bits
- HID corporate 1000
- CP - 42 bits
- CP - 46 bits

The default value is HID standard 26 bits.

Selected HID 37 bits card type

You may use the HID standard 37 bits ID-tag, with or without facility code. Select from the drop-down menu the correct value.

9.8 Saving Parameters

It may be convenient to make back-up files of the parameters that you have set. You can use this file for instance to upload the settings to other readers.

NOTE To prevent back-up files to be overwritten, it is recommended to identify them uniquely. Per reader, you can make a separate back-up file.

Take the following steps for making a back-up of the parameters.

1. Select the reader from which you want to make a back-up file.

2. Select from the Folder bar or tree (dependent on the view setting) the **Configuration** folder and select the **Parameters** icon. The Parameters are listed in the right pane.

3. From the Menu bar, select **File -> Save**.

4. The *Save As* dialog is displayed.

5. Enter a name for the file and select a location where to store it.

6. Click the button **Save** to save the back-up file.

9.9 Loading parameters

The Back-up files of parameters can be used to upload for instance the parameters to other readers. Take the following steps to do this.

1. Select the reader in which you want to store the contents of the back-up file.

2. Select the **Configuration** folder and select the **Parameters** icon of this reader.

3. From the Menu bar, select **File -> Open**. The *Open* dialog is displayed.

4. Select the required file.

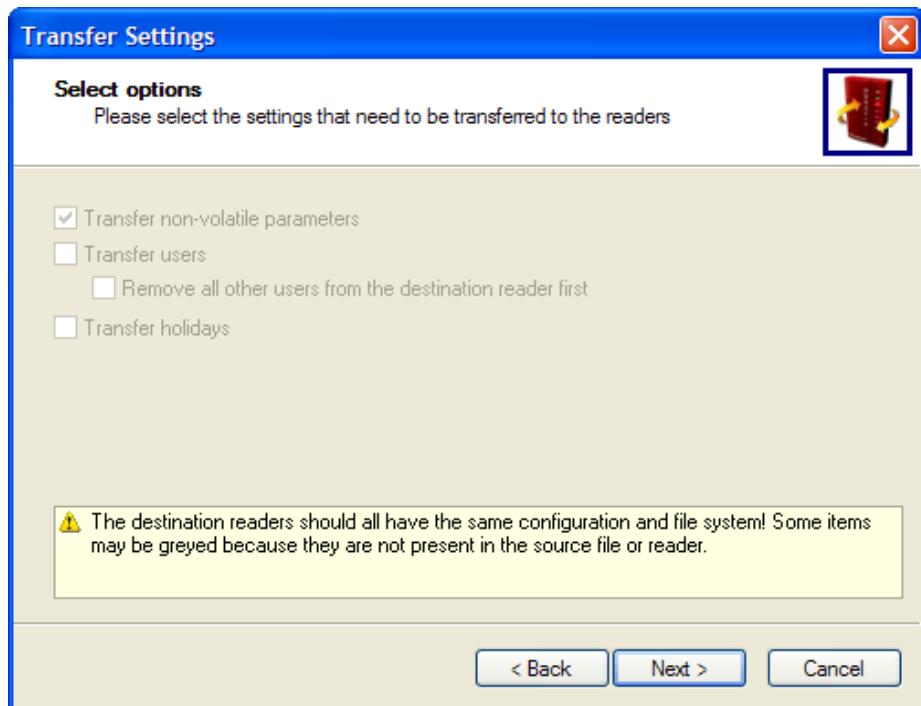5. Click the button **Open**. The *Transfer settings* dialog is displayed (see Figure 37).

Figure 37: Transfer Setting Wizard to upload parameters

6. Click the button **Next**. The dialog to select readers is displayed (see Figure 38).

Figure 38: Select Readers dialog
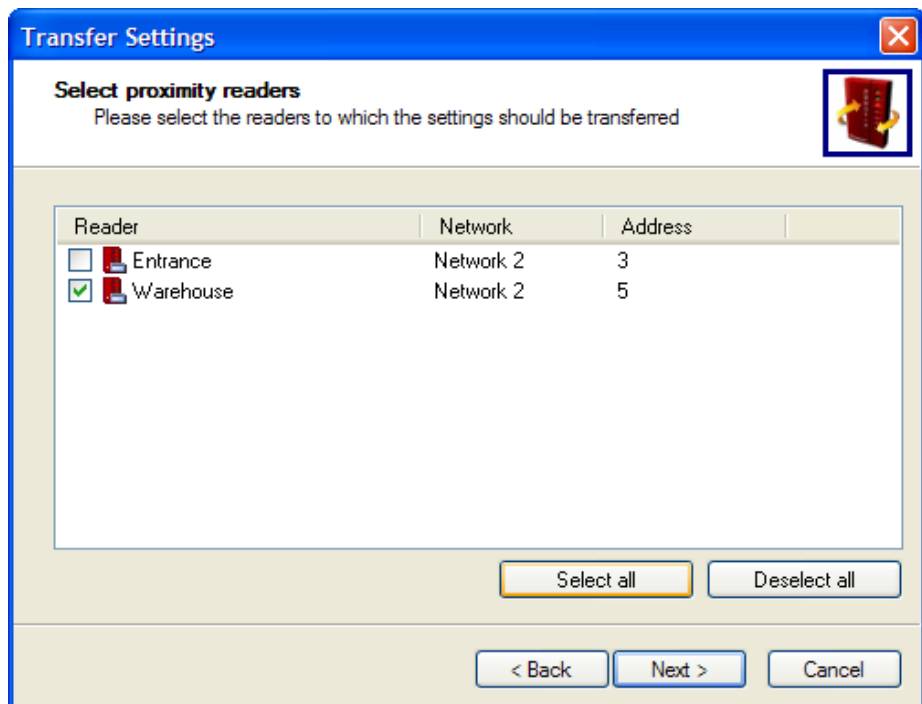
7. Click the button **Select all** for all readers or select the checkbox(es) for the readers you want to upload the parameters to.

8. Click the button **Next** and the *Progress* dialog is displayed.

9. Click the button **Next** and the users are copied to the selected readers.

10. When all parameters have been uploaded, click the button **Finish** to return to the application.

10   Transfer reader parameters and users

If you want to use other readers in your system, XM3 Manage is provided with a wizard that offers the possibility to transfer settings from an existing reader to the other readers. Take the following steps to transfer parameter settings and/or users:

1. From the Menu bar, select **File -> Transfer reader settings…** to display the *Transfer settings Wizard*.

2. In this Wizard, select the button **Next**. The *Select source* dialog is displayed (see Figure 39).
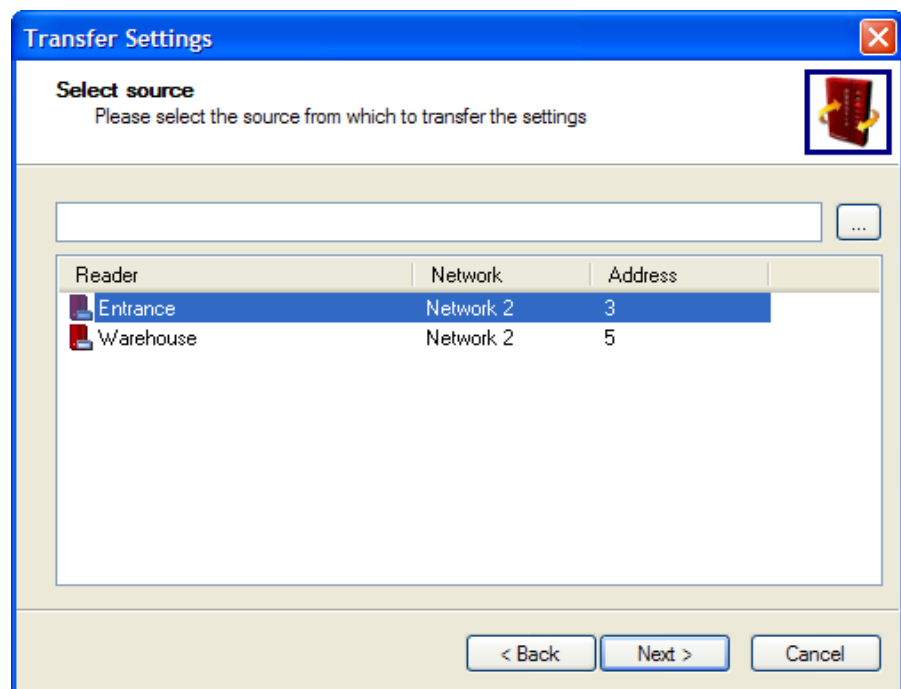

Figure 39: Transfer Settings Wizard - Select Source

3. In this dialog, select the reader from which you want to transfer the settings.

or

4. Click [...] to select a file.

5. Click the button **Next**. The *Select options* dialog is displayed (see Figure 40).
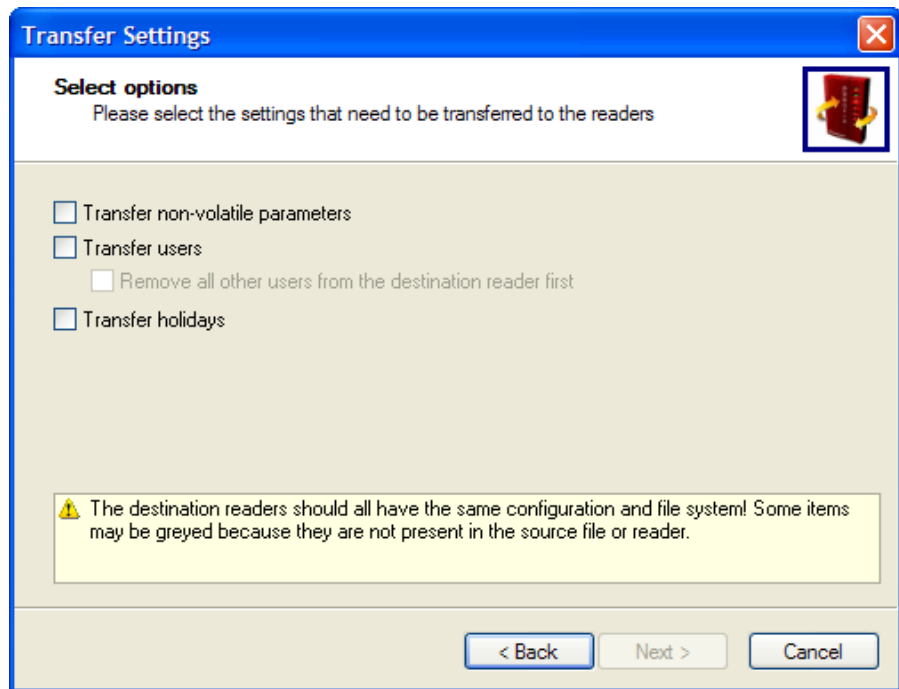
Figure 40: Transfer Settings Wizard - Select Options

6. Select the checkbox(es) for the options you want to transfer.

   NOTE   Selecting the check box **Transfer users** activates the check box **Remove all other users from…** Select this box as well if you want the users in the destination reader to be removed. If you do not select this box, matching existing users in the destination reader are overwritten, and unknown users are added. If you want to transfer users to another reader, that reader should have to same file system set as the one you transfer from.

7. Click the button **Next**. The *Select proximity readers* dialog is displayed (see Figure 41).
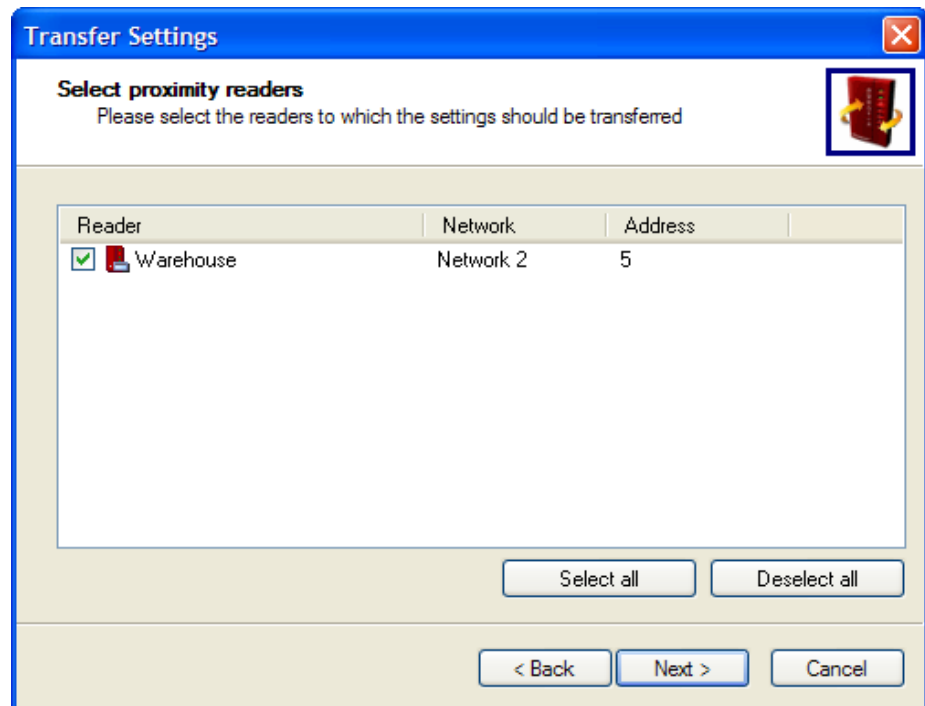
Figure 41: Transfer Settings Wizard - Select destination reader

8. Click the button **Select all** for all readers or select the checkbox(es) for the readers you want to transfer the settings to.

9. Click the button **Next** and the *Progress* dialog is displayed.

10. Click the button **Next** and a progress bar is displayed indicating the process of transferring the settings. After this the dialog to complete the wizard is displayed. This dialog also gives information about the transfer process.

11. In this dialog, click the button **Finish** to complete and exit the Wizard.

11 Reader Management

In the reader(s) a number of settings can be made. In the following paragraphs these setting are described.

11.1 Change name

With this menu-item you can change the name of your reader(s). To do so:

1. From the Menu bar, select **Reader-> Change name**. The *Change name* dialog is displayed (see Figure 42).
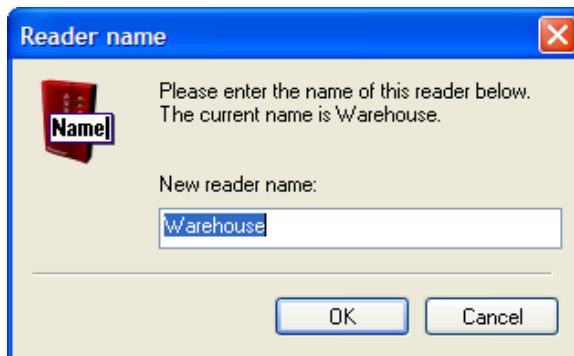
Figure 42: Change Reader Name

2. Enter the new reader name.

3. Click the button **OK** to change the name of the reader.

4. Click the button **Close** to close this window and to return to the application.

11.2 Set date/time

You can synchronize the date and time of your reader(s) with the time of the host PC or choose other date/time settings. Take the following steps to do so:

1. From the Menu bar, select **Reader -> Set date/time**. The *Set reader date/time* dialog is displayed (see Figure 43).
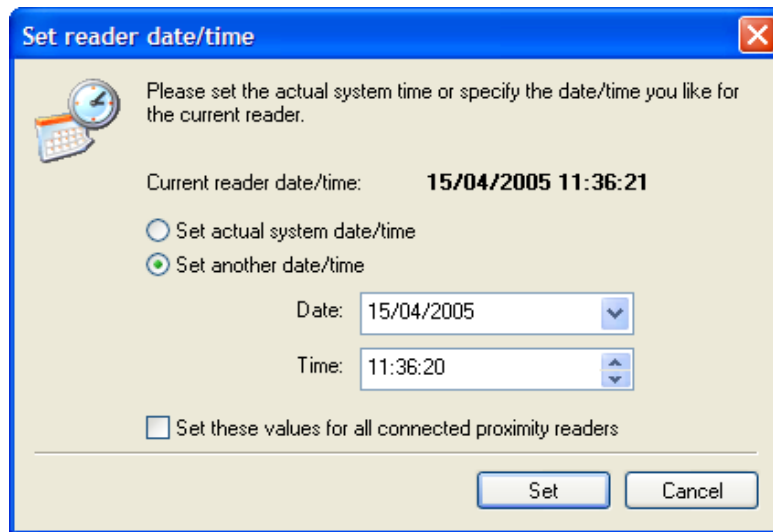
Figure 43: Set reader date/time dialog

2. Select the option **Set actual system date/time**, if you want to synchronize the reader with these values of the host PC,

or

3. Select the option **Set another date/time**. Selecting this button activates the edit boxes **Date and Time**.

4. Next to the edit box of the current date, select ⌄ to display a calendar.

5. From this calendar select the date.

6. Next to the edit box of the current time, select ⌄ to either increase or decrease the value of the time to adjust the current time.

7. Select the checkbox **Set these values for…** if the set date and time should apply to all readers.

8. Click the button **Set** to adjust the date and time.

9. Click the button **Close** to close this window and to return to the application.

11.3   Define holidays

It is possible to define holidays for the reader(s) by entering a start/end date and time for a holiday period. During these holiday periods only a 24- hour user may gain access. If you are using time schemes and the time scheme overrules holidays, you also have access during holidays. To enter or edit holidays:

1. From the Menu bar, select **Reader -> Define holidays**. The *Define holidays* dialog is displayed (see Figure 44). The icon in front of the holiday indicates if a holiday is in the past, the future or if today is a holiday.
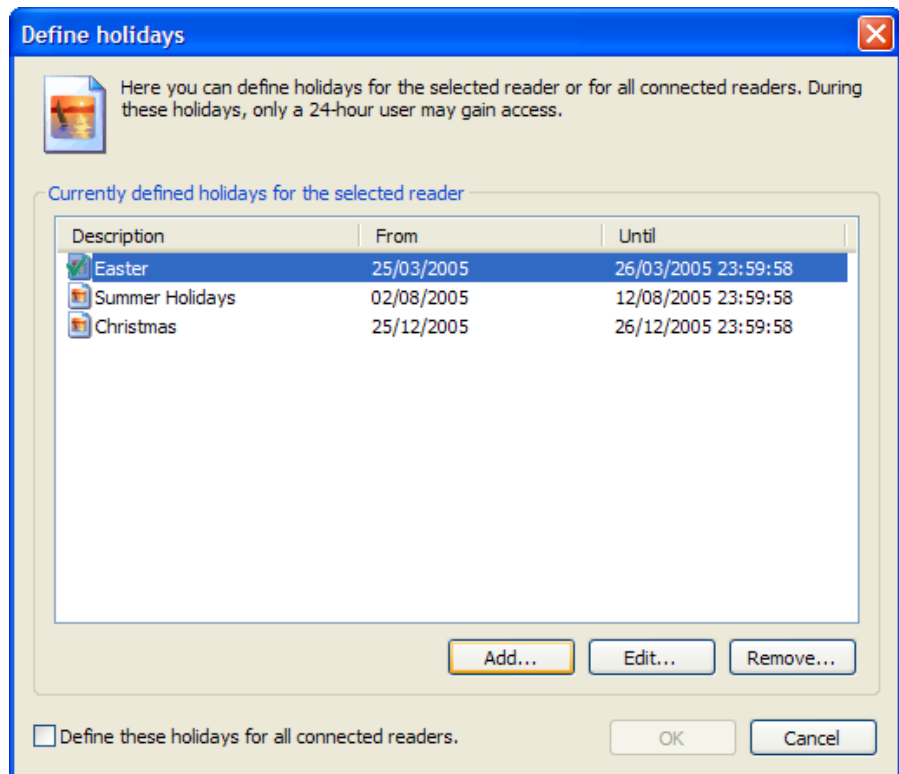
Figure 44: Define Holidays

2. Select the button **Add** if you want to add a new holiday

or

3. Select the button **Edit** if you want to edit a selected holiday. Selecting either of these buttons activates the edit box **Add/Edit holiday**.

4. Enter the description of the holiday, e.g. Christmas.

5. Next to the edit box of the starting date, select ⌄ to display a calendar. From this calendar select the starting date.

6. Enter a starting time.

7. Next to the edit box of the end date, select ⌄ to display a calendar. From this calendar select the end date.

8. Enter an end time.

9. Click the button **OK** to confirm.

10. Select the checkbox **Define these holidays for…** if the set holidays should apply to all readers.

11. Click the button **OK** to close this window and to return to the application.

11.4 Locate

With this menu item you have the possibility to physically locate a reader in a building. When this menu item is selected the reader it concerns will start to beep and the LEDs will blink continuously. To do so, select **Reader -> Locate (beep).** The reader will continue to beep until the menu item is selected again.

11.5 Open Door

When selecting this item, the door where this reader is attached to is opened. The door will remain open as specified in the parameter *Door Open time.*

NOTE   When a reader is selected and the **Open door** button from the tool bar is pressed, the door is opened directly. When no reader is selected or if you want to open another door, you can use the drop-down menu on the right of this toolbar button. Select a reader from this menu and the specific door will be opened.

11.6 Reset

Sometimes a reset of the readers is necessary. To reset the readers:

1. From the Menu bar, select **Reader -> Reset**. The *Reset reader* dialog is displayed (see Figure 45). The name of the selected reader is mentioned in the dialog.
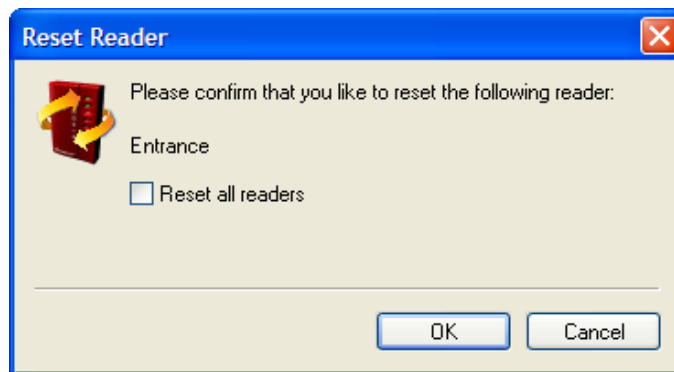
Figure 45: Reset Reader

2. Select the check box **Reset all readers** if you want all readers to be reset.

3. Click the button **OK** to confirm.

4. Click the button **Close** to close this dialog.

NOTE   This option is only available at installer level. The date of the reader is changed to 1-1-2000 and the time to 12:00:00 AM after the reset. Synchronize the date and time again to the actual time or the time of the host PC. This can be done automatically by setting the right option in the *Options* Dialog (Reader page).

11.7 Clear user database

If you want to remove all users from a reader you can use this menu-item to clear the user database:

1. From the Menu bar, select **Reader -> Clear user database**

2. A dialog is displayed asking you whether you are sure to clear the user database. Select the check box **Reset all readers** if you want to clear the user database of all readers.

3. Confirm this question and the users will be removed and you will return to the application.

11.8 Remove all expired users

When using XM3 Manage Pro with time schemes and user validation, this option is available. With this option, you can remove all expired users from a reader:

1. From the Menu bar, select **Reader -> Remove all expired users.**

2. A dialog is displayed asking you whether you are sure to remove the users. Select the check box **Reset all readers** if you want to remove expired users from all readers.

3. Confirm this question and the expired users will be removed and you will return to the application.

11.9 Clear event log

If the event log is full, and a new event occurs that should be registered, the oldest entry is overwritten by the newest. This feature of the reader assures that the events in the event log are up to date, even in case of an event overflow. However, you may decide that you want to clear the event log of the reader. To clear the events:

1. From the Menu bar, select **Reader -> Clear event log**

2. A dialog is displayed asking you whether you are sure to clear the event database. Select the check box **Clear all readers** if you want to clear the event database of all readers.

3. Confirm this question and the events will be removed and you will return to the application.

11.10 Change network address

NOTE You cannot change the address of your XM3 Single Door. It is fixed to 255. This option is only available to installers.

By default readers have a unique network address. In this way, communication with each reader in a network is enabled. You need to

change the address if for any reason you have readers in your system with an identical address. The first thing you have to find is which readers have the same address. Take the following steps to find out the address of the readers:

1. Power no more than 1 reader.

2. Logon to it via XM3 Manage.

3. Select the folder *Configuration* and select the *Reader Information* icon to display the reader information in the right pane (see Figure 46).
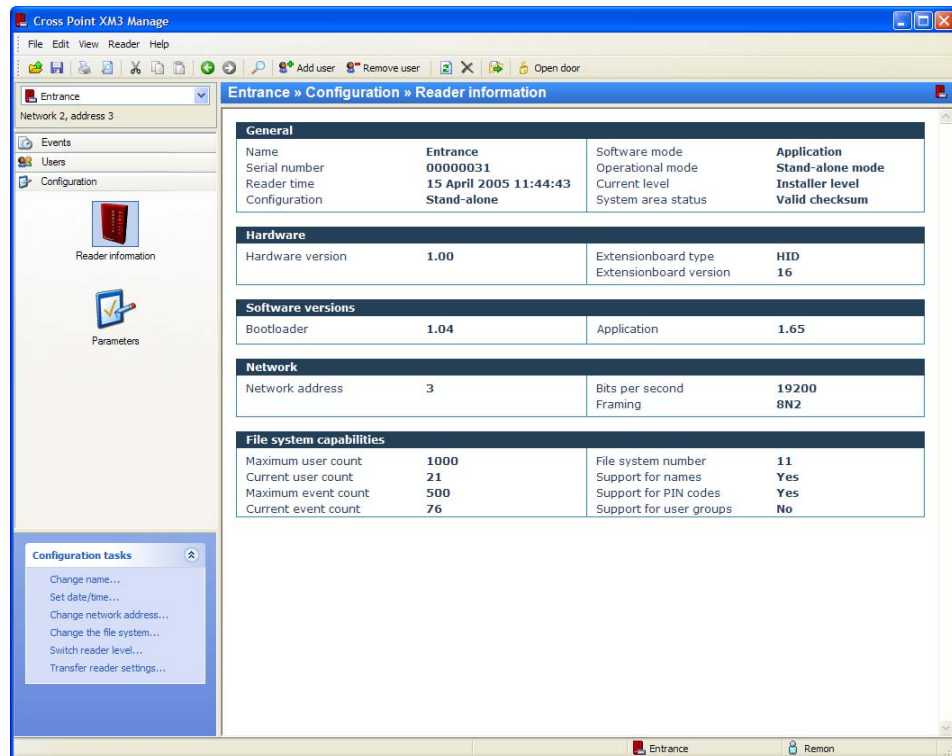

Figure 46: Reader Information View

In the pane, the network address is listed.

Once you have determined which readers have the same network address, you can change these. Proceed with the following steps to change the address.

4. From the Menu bar, **select Reader -> Change network address**.

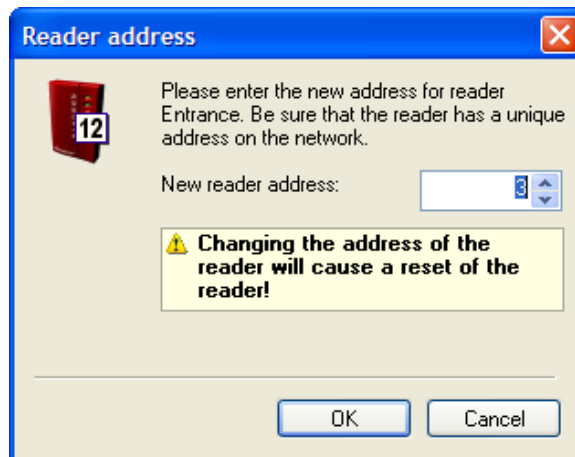5. The *Reader address* dialog is displayed (see Figure 47).

Figure 47: Reader Address dialog

6. Enter a new address, or select ⬍ to choose one.

7. Click the button **OK** to confirm the new address.

8. If the new address is not unique, an error message is displayed to inform you.

9. Click the button **Close** to close this dialog,

11.11   Set file system

XM3 Manage makes use of file systems to store the users of your Access control system as well as their PIN codes and names. Also the number of events that occur while using the systems can be stored. There are a number of predefined file systems that determine how the internal memory of your reader is partitioned.

NOTES   Choosing a different file system will erase all current information in the user and event databases of the reader. Also the Access codes for the Installer and User as well as the parameters are reset. Select the option to copy Users and parameters when there is data stored in the reader. Also, make a backup of the data! This option is only available for installers.

When using XM3 Manage Single Door, the number of file systems is limited.

When using Time Schemes (XM3 Manage Pro), you cannot change the file system other than with the *Configuration Wizard*.

Take the following steps to choose a file system:

1. From the Menu bar, select **Reader -> Set new file system**. The *Change file system* dialog is displayed (see Figure 48).
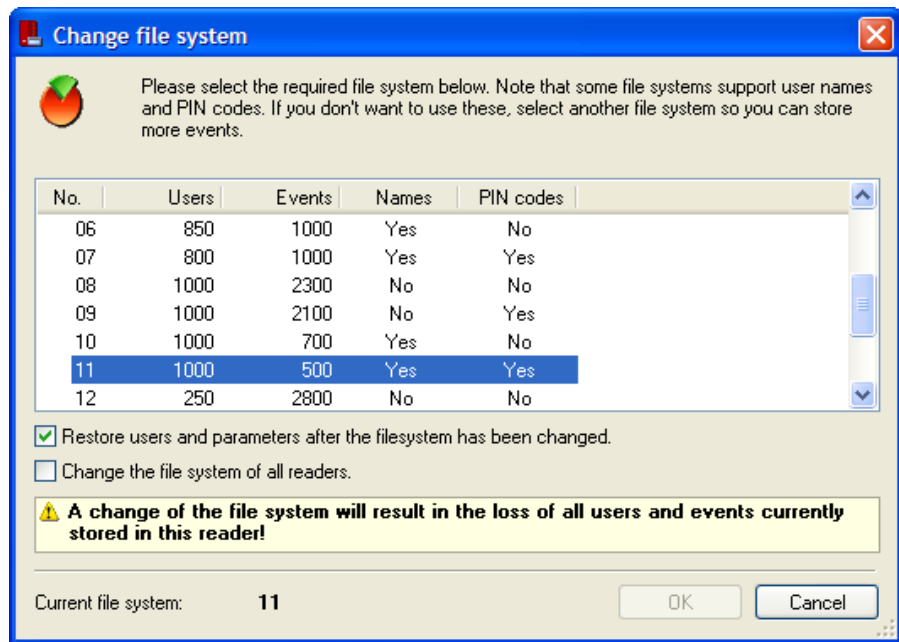
Figure 48: Change File system dialog

2. Select the required file system

3. Click the button **OK**. A dialog is displayed asking for confirmation to change the file system.

4. Confirm the selection of the chosen file system.

   NOTE The reader will reset and return to sleep mode at Installer level. Also the date and time will change to another value.

5. Click the button **Close** and you return to the application.

11.12 Switch to User operational level

Since during normal operation, the reader(s) are at User authorization level, you have to switch to that level after the reader(s) have been configured. Take the following steps to switch the level:

NOTE The cover must be on the reader to switch to *User level*. This option is only available for installers.

1. From the Menu bar, select **Reader -> Switch operational level**

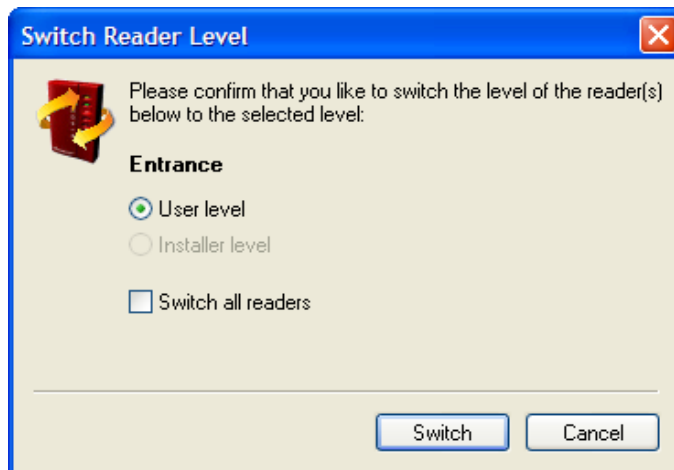   The *Switch Reader Level* dialog is displayed (see Figure 49).

Figure 49: Switch Reader Level dialog

2. Select the box **Switch all readers** to switch all readers in your Access Control system to the User level.

   NOTES When at Installer level and you want to switch to User level, the button **User level** is already selected.

   Switch all readers is not available if you are using XM3 Manage Single Door.

3. Select the button **Switch**. A processor indicates that switching is taking place.

4. Select the button **Close** to return to the application.

   NOTE During normal operation it may be necessary to switch to Installer level to do some changes. Remember that after the changes have been made you have to switch back to the User level.

Now you have completed all the steps required to get a reader started. The end-user now can start creating accounts, managing users et cetera.

11.13   Switch reader configuration

NOTE This option is not available when using XM3 Manage Single Door.

The reader supports a basic and stand-alone configuration. If you have used for instance a basic configuration and want to use more functionality of the reader, a unique and reader specific switch key is necessary. Use for this purpose the form at the end of this manual, and your dealer will provide you with this key. To switch a reader configuration:

1. From the Menu bar, select **Reader -> Switch reader configuration**. The *Switch reader configuration* dialog is displayed (see Figure 50).
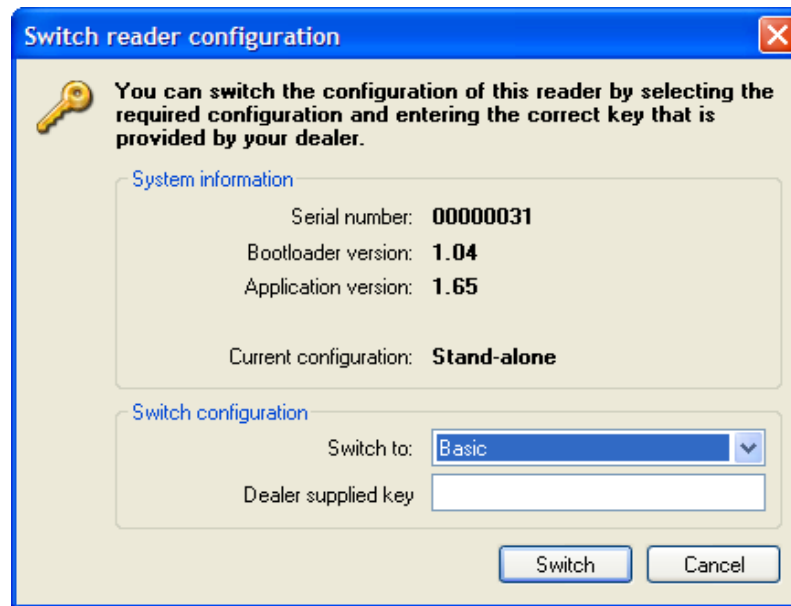
Figure 50: Switch reader configuration dialog

2. From the drop down menu **Switch to**, select the required configuration. You can choose from the following configurations:

   - Basic configuration

   - Stand-alone configuration

3. Enter the key in the edit box **Dealer supplied key**.

4. Select the button **Switch**. A processor indicates that switching is taking place.

5. Select the button **Close** to return to the application.

NOTE Downward switching is not recommended, since this will decrease the functionality of the reader.

11.13.1 Basic configuration

In Basic mode, the reader offers the most elementary functionality. The ID-tags can communicate with the host via:

   - RS-485

   - Wiegand

   - Magstripe

The reader only reads the presented ID-tag and sends the tag ID to an external controller. The external controller does the checking of the tag ID. When the ID is present in the controller's memory access will be granted by the controller.

NOTE XM3 Manage functionality is limited when the readers communicates via RS-485, Wiegand and Magstripe with the host.

11.13.2 Stand-alone configuration

In the stand-alone configuration or in a RS-485 network, the reader is not connected to a controller. This means that checking of presented ID-tags, opening door locks et cetera is managed by the reader. The stand-alone configuration offers the entire functionality of the readers including the support of Master Cards.

12   Finding items in XM3 Manage

XM3 Manage offers the possibility to find events and users in the connected readers. The Find function can be performed on all the connected readers in your access control system. In the following paragraphs is explained how to use the Find functionality.

12.1   Find Events

The tab Events can be used to find events that have been logged while using your access control system. Take the following steps to select the criteria on which you want to base the search and how to get the find result.

1. Select from the Menu bar, **Edit -> Find** to display the *Find* dialog (see Figure 51).
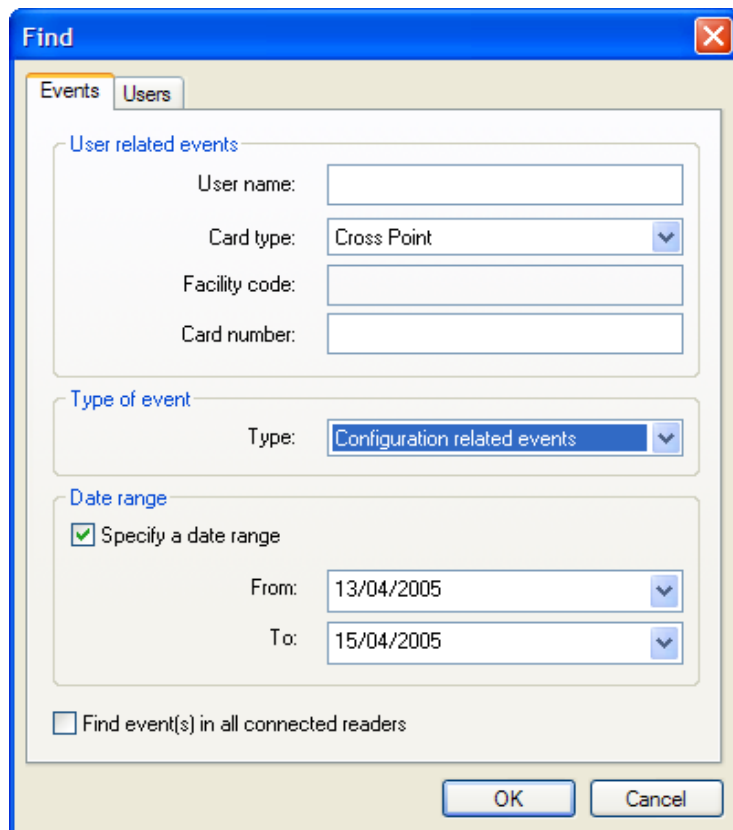

Figure 51: Find dialog - Events

2. Enter or select from the User related events:

- the name of the user in the edit box **User name**.

- • the required card type from the **Card type** drop-down menu.

- • the required value in the edit box **Facility code**.

  NOTE The facility code is only applicable for HID card types and is provided by your card supplier. The facility code has to be used in combination with the Card number to perform a search.

- • the required value in the edit box **Card number**.

3. Select the type of event from the drop-down menu **Type**.

4. Select the checkbox **Specify a date range to activate From and To**. Here you can define a period of time in which you want to search for the events based on your search criteria.

5. Select ⌄ in **From** and **To**, to display a calendar.

6. In these calendars, select the required dates.

7. Select the check box **Find event(s) in all connected readers** if you want to have find results based on your criteria in all the readers.

8. Click the button **OK** to start the find process.

When the process is completed, the results are displayed in the right pane.

12.2 Find Users

The tab Users can be used to find out details about the users of your Access Control system. Think of details such as the readers the users have been added to or the level of users et cetera. Take the following steps to select the criteria on which you want to base the search and how to get the find result.

1. Select form the Menu bar, **Edit -> Find** to display the *Find* dialog.

2. Select the tab *Users* (see Figure 52).
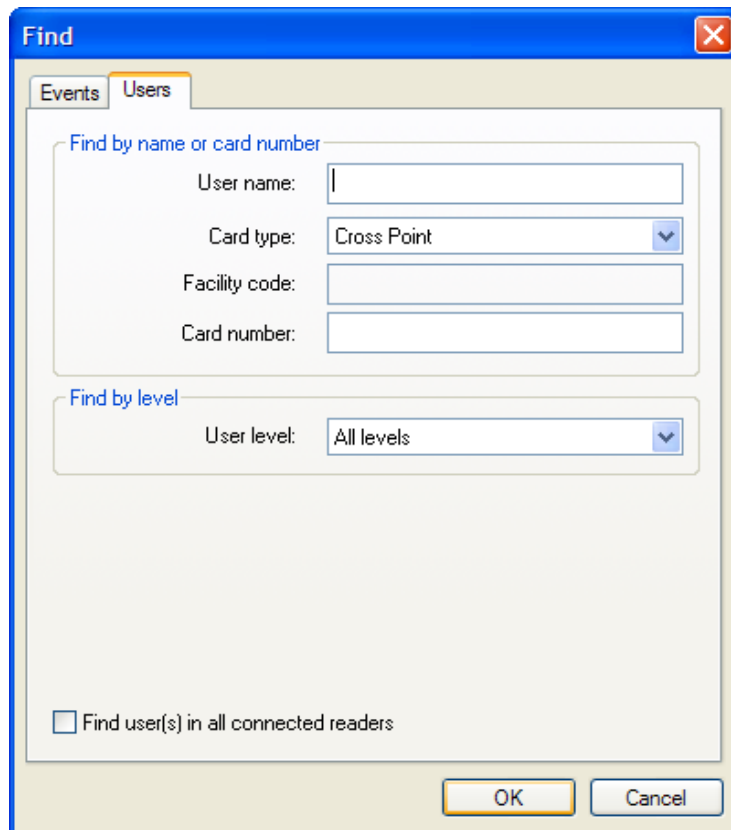
Figure 52: Find dialog - Users

3. Enter or select from **Find by name or card number**:

    - a **User name**

    - the **Card type** drop-down menu the required type.

    - the required value in the edit box **Facility code**. The facility code is only applicable for HID card types and is provided by your card supplier. The facility code has to be used in combination with the **Card number** to perform a search.

    - Enter the required value in the edit box **Card number**.

4. Select from the drop-down menu **User level** the required level.

    NOTE   A Find by name or card number and Find by level cannot be performed at the same time: Find by level becomes grayed when entering a search criteria in Find by name or card number.

5. Select the check box **Find user(s) in all connected readers** if you want to have find results based on your criteria in all the readers.

6. Click the button **OK** to start the find process.

When the process is completed, the results are displayed in the right pane.

13   Options

XM3 Manage offers the possibility to customize the application to your own preference. In the next paragraphs is explained how to customize your XM3 Manage application.

13.1   General options

Select from the Menu bar, **View -> Options**, to display the *Options* dialog (see Figure 53).

NOTE   Some options are not available in XM3 Manage Single Door.
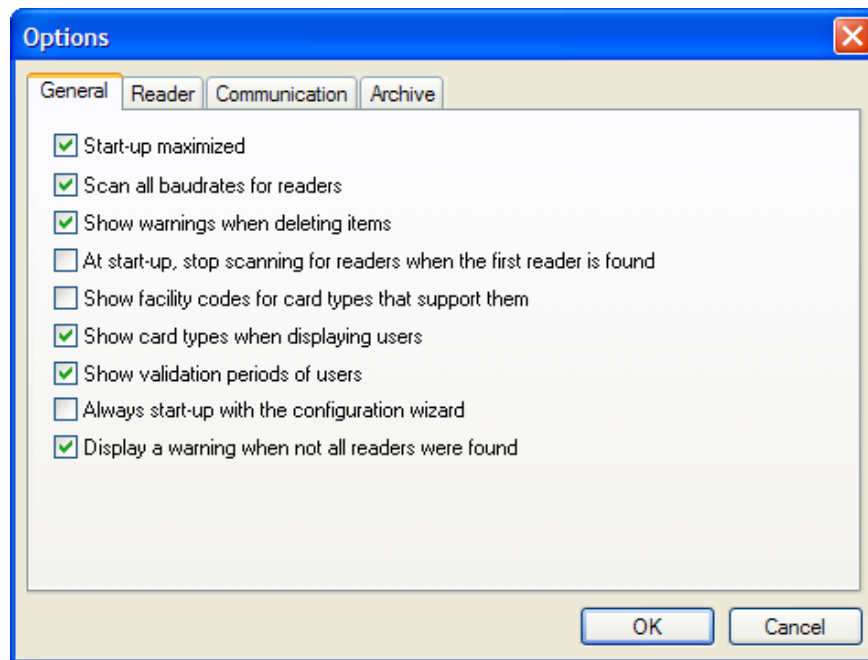
Figure 53: Options dialog - General

In the tab *General*, the following options can be set:

- **Start-up maximized**. Check this box if you want the application to display maximized on the screen at start-up.

- **Scan all baudrates for readers**. When this option is checked, all baud rates are scanned, otherwise only the selected baud rate for each network is scanned.

- **Show warnings when…** Selecting this box will display a window asking your confirmation whether you are sure to delete for instance an ID-tag from the reader.

- **At start-up, stop scanning for…** If you select this box, the application stops scanning the network as soon as a reader has been found.

- **Show facility codes for…** HID ID-tag types have apart from a unique tag number also a facility code. If you select this box, the application will show both.

- **Show card types.** In the user pane, a column *card types* is displayed if this option is selected.

- **Show validation periods.** In the user pane, a column *validation period* is displayed if this option is selected.

- **Always start-up with the configuration wizard.** When selecting this option, XM3 Manage always starts with the configuration wizard, also when the system is already configured. This is a handy option for installers that use the same laptop for each new installation.

- **Display a warning when not all readers were found.** Standard, XM3 manage will check if the readers that are found during the scan are the same as the previous time. If there is a difference, the user will be noticed. When switching this option off, this message is not displayed anymore. This is a handy option for installers that use the same laptop for each new installation.

13.2   Reader options

Select from the Menu bar, **View -> Options**, to display the *Options dialog*, then select the tab *Reader* (see Figure 54).

NOTE   The *Event Database Settings* in Figure 54 are not available in XM3 Manage Single Door.
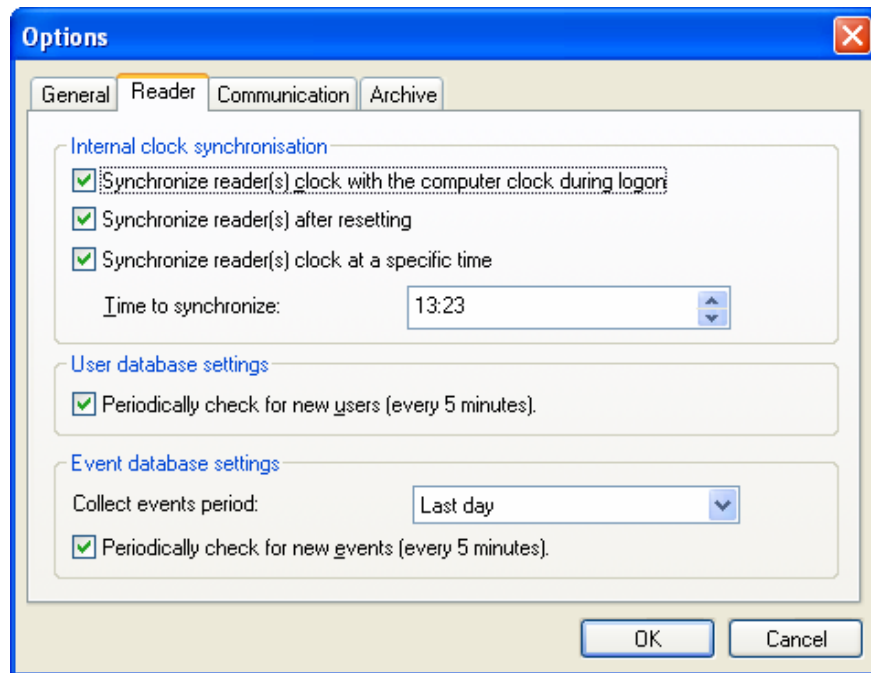
Figure 54: Options dialog - Reader

In the tab Reader, the following options can be set:

- **Synchronize reader(s) clock at specific time**. Selecting this option will synchronize the internal clock of the reader at a specific time. The time at which the reader will be synchronized can be set in the box Time to synchronize. If you use the scroll buttons of the box the time to execute will be in full hours. If you enter a value manually you can enter any value. XM3 Manage will start automatically when it is not running at the specified time.

- **Synchronize reader(s) after resetting**. Selecting this option will synchronize the internal clock of the reader after a reset of the reader.

- **Synchronize reader(s) clock …** Selecting this option will synchronize the internal clock of the reader with the date and time settings of the host PC every time you log on.

- **Periodically check for new users (every 5 minutes)**. If you select this box, the application checks periodically if new users have been added to the reader.

- In the box **Collect events period** you can set the period of which the events have to be collected. The options are: *Current day*, *Last day*, *Last two days*, *Last two weeks*. This option is not available in XM3 Manage Single Door.

- **Periodically check for new events (every 5 minutes).** If you select this box, the application checks periodically if new events have been logged in the reader.

13.3   Communication options

Select from the Menu bar, **View -> Options**, to display the *Options* dialog, then select the tab *Communication* (see Figure 55).
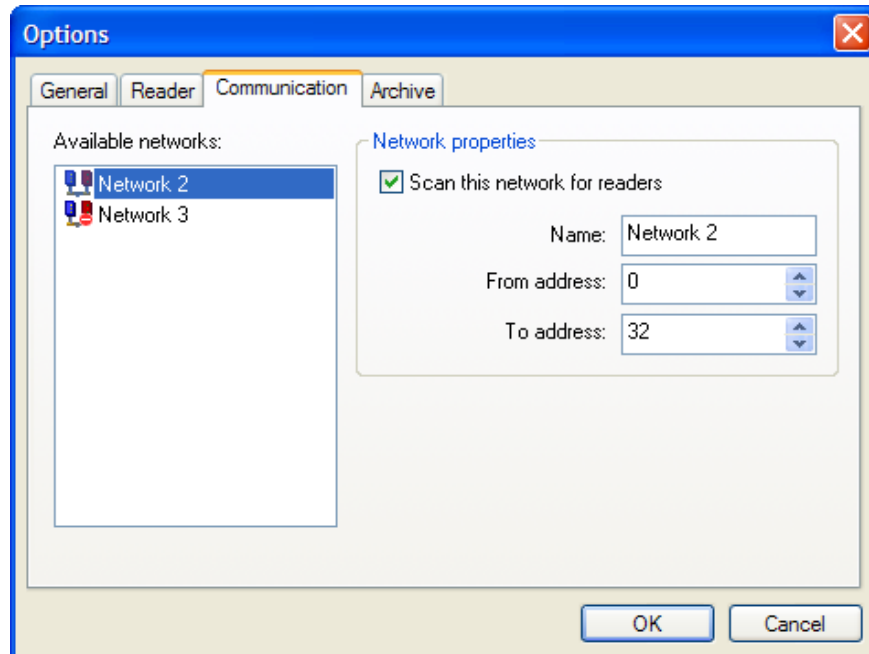
Figure 55: Options dialog - Communication

The tab *Communication* gives an overview of the reader networks connected to your PC as well as the possibility to select the network you want to scan while starting up XM3 Manage.

Per network, you also can select a range of addresses that should be scanned while starting up the application.

NOTE   The From- and To address fields are not available in XM3 Manage Single Door.

13.4   Archive options

NOTE   The tab *Archive* is not available in XM3 Manage Single Door.

Select from the Menu bar, **View -> Options**, to display the *Options* dialog, then select the tab *Archive* (see Figure 56).

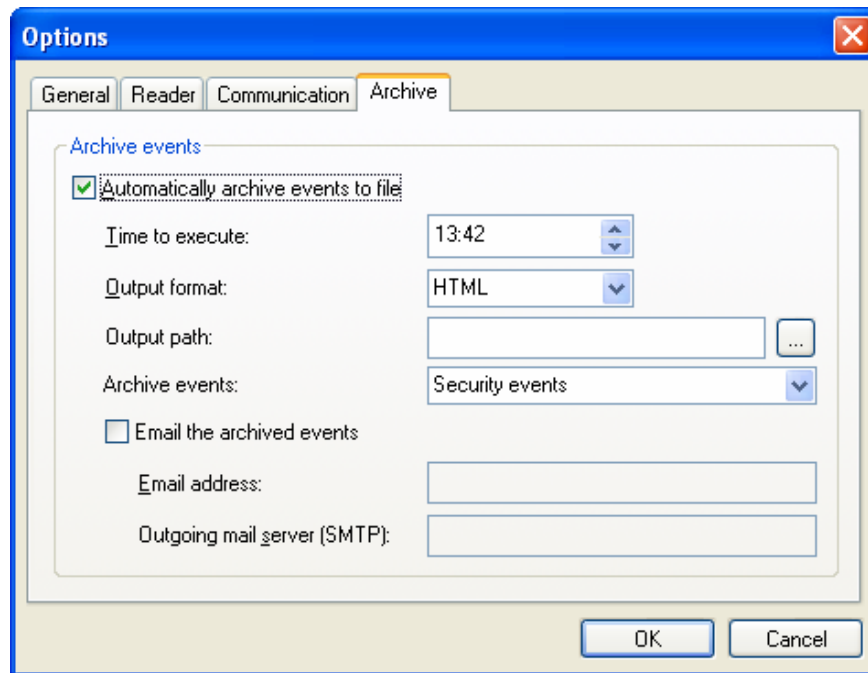**Figure 56: Options dialog - Archive**

With the tab *Archive* it is possible to automatically store events at a specified time of the day. Thus, a back-up file of events will be available on a daily basis. Take the following steps to activate automatic archiving.

1. Select **Automatically archive events to file**. The boxes **Time to execute**, **Output format** and **Output path** will become active.

2. Enter the **Time to execute archiving**. If you use the scroll buttons of the box the time to execute will be in full hours. If you enter a value manually you can enter any value.

3. Enter the **Output format** by using the scroll buttons.

4. If you are using XM3 Manage Pro, you can also select if you want to archive **All events** or only **Access Events**.

5. Enter the **Output path**. You can do this by using the button [...] or manually.

You also have the possibility to email the archived events to a location designated by yourself. To do so take the following steps. This option only becomes active after selecting **Automatically archive events to file**.

6. Select **Email the archived events**. The boxes with the email details will become active.

7. Enter the **Email address** to which the archived events have to be sent.

8. Enter the address of the outgoing mail server (SMTP).

9. Click the button **OK** and the changed settings will be retrieved.

NOTE   XM3 Manage does not have to be running when archiving. It will startup automatically at the specified time. When the path is left empty, the data will be mailed only, not stored on disk.

14 Uploading new firmware

NOTE This option is only available for installers.

The firmware for a reader is subject to change because of improved functionality, bug fixes, et cetera. The firmware files are supplied by Cross Point. When you upload these files to the reader the cover must remain on it. Take the following steps to upload new firmware.

1. From the Menu bar select **File -> Upload new firmware…** to display the *Upload firmware wizard*.

    NOTE The Welcome screen to this wizard contains important information. Read this before you proceed.

2. In this wizard select the button **Next**. The *Upload firmware* dialog is displayed to select the options you want (see Figure 57).
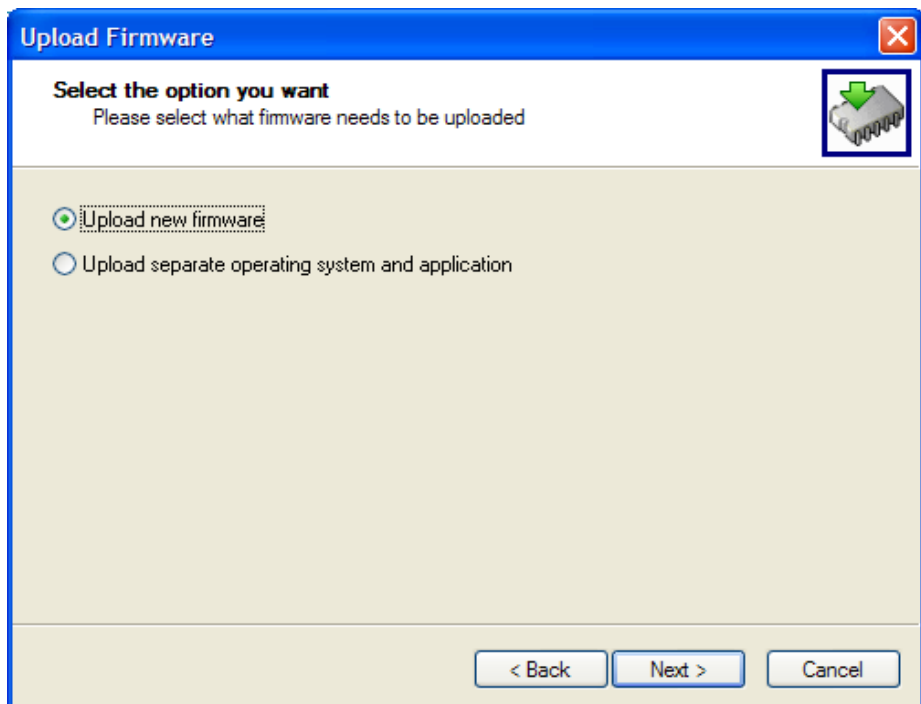
Figure 57: Upload Firmware Wizard - Select option

3. Choose whether you want to upload new firmware or whether you want to upload a separate operating system and application.

    NOTE Which option has to be selected depends on the hardware of your system. For newer hardware versions the option **New firmware** has to be selected, since the operating system and the application are no longer separated. **It is not recommended to upload old firmware to a reader!**

4. Click the button **Next**.

In case of Upload new firmware the following dialog *Gathering files* is displayed (see Figure 58).

Figure 58: Upload firmware dialog

5. Enter the Application file or select [...] to browse to the location you stored the files you received from Cross Point.

or

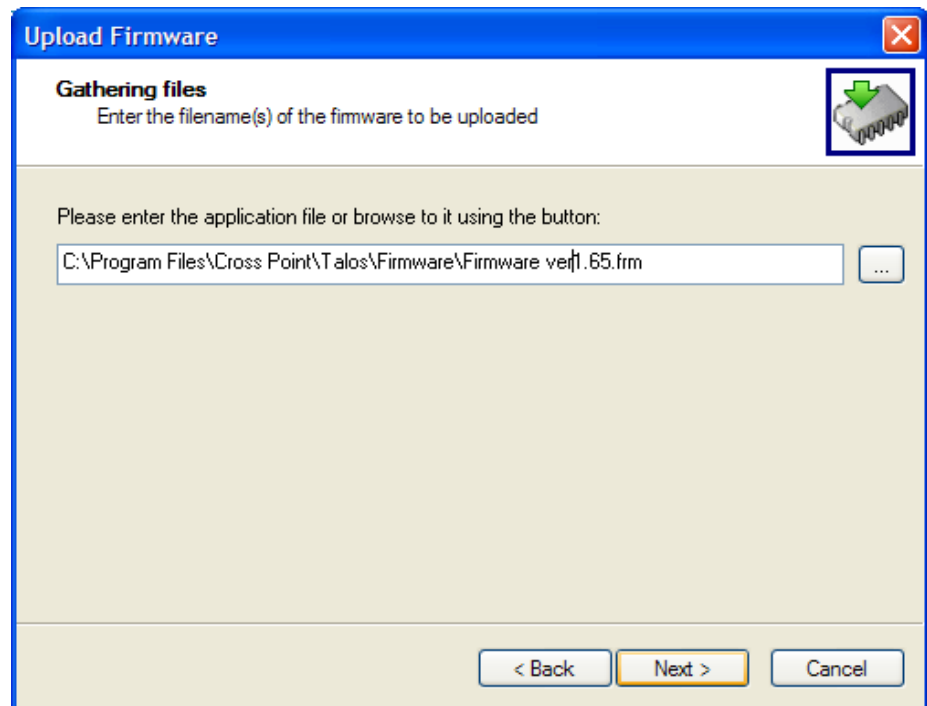In case of Upload a separate operating system and application the following dialog Gathering files is displayed (see Figure 59).
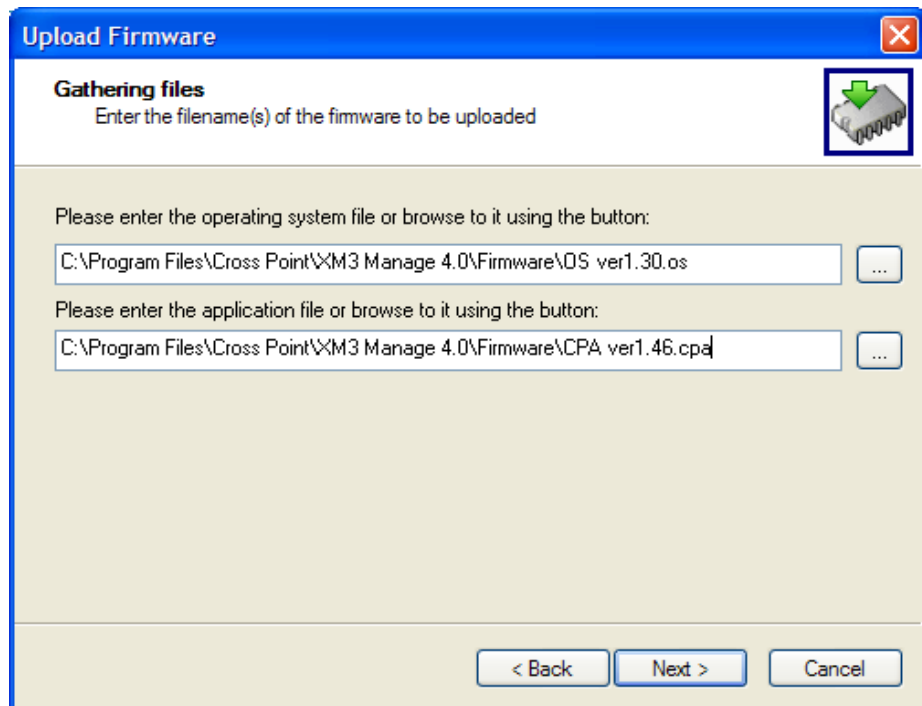
Figure 59: Upload firmware dialog - Gathering files

6. Enter the **Operating System file** and/or **Application file**, or select to browse to the location you stored the files you received from Cross Point.

7. Click the button **Next**. The *Select proximity readers* dialog is displayed.

8. From the list in this dialog, select the checkbox for the reader you want to upload the files to.

9. Click the button **Next** and the *Progress* dialog is displayed.

10. Click the button **Next** and a progress bar is displayed indicating the process of uploading the firmware.

The dialog to complete the wizard is displayed. This dialog also gives information about the upload process.

11. In this dialog, click the button **Finish** to complete and close the Wizard.

15   Help

Via Help on the Menu bar additional information can be obtained about the XM3 Manage application and the Cross Point organization.

- Select from the Menu bar **Help -> Visit Cross Point**, and Cross Point's website is opened on the internet. Here you can find lots of information about Cross Point and its products.

- Select from the Menu bar **Help -> About** to display a window with information about the XM3 Manage application, such as version number and year of release as well as the intellectual property rights.

16   Trouble shooting

Scanning the network

If you scan the network, but no readers are found, check whether:

- the baud rate of the network and the connected readers is the same.
- all readers have a unique network address.
- all readers are powered.
- the RS-485 network is properly connected.
- The RS-232 cable is connected to the correct COM port.

Events are not displayed

If events are not displayed, check if you:

- have chosen a file system that supports logging of events.
- have the Event log mode disabled (Installer parameter).
- have selected the right event type
- have a Single Door XM3 reader.

NOTE   If you have an XM3 Single Door, event logging is not available.

Time markers do not work

If the time markers for the Lock/Unlock options do not work, check whether you have synchronized the date and time of the readers with the date and time of the host PC.

PIN code options do not work

If your PIN code options do not work, check if:

- the PIN keypad is correctly installed.
- You have selected from the parameter PIN Keypad options the Enable PIN code.

Communication problem with HID standard 37 bits card types

In case you have communication problems with you HID standard 37 bits card types, check whether you have selected the correct value from the drop-down menu. Select HID 37 bits card type. Your cards may have an assigned facility code.

Date/time change due to a reset of the reader

Selecting another file system will reset the reader. As a result, the date of the reader is changed to 1-1-2000 AM. This will result in unexpected behavior of the Lock/Unlock and Night-to-day/Day-to-Night time markers. Also events logged after the reset will have a date/time notation based on the changed date and time, thus giving wrong information about the occurrence of the event. Provided that you use the date/time of the PC for your readers, set the date and time of the readers to the actual system date/time of the host PC to solve this, or select another date/time.

The reader does not accept any ID-tags

When performing certain actions, the reader does not accept ID-tags.

These actions are:

- Retrieving users
- Retrieving events
- Retrieving parameters
- Clearing events
- Adding users
- Removing users
- Transferring settings

In this case, the Programming LED of the XM3 is lit.

NOTE   An XM3 Single Door reader only accepts Cross Point card types. All other card types are ignored!

A card has no access

When adding a new user or presenting a card that should have access, please check the following.

If you use User levels for cards:

- The card is a nighttime user and currently it is daytime.
- The card is a daytime user and currently it is nighttime.
- You defined holidays and today is a holiday. Daytime and nighttime users have no access during holidays.

If you use time schemes:

- The card is added with an Add Master card and is placed in the default time scheme. Check if this time scheme has access on this hour of the day.
- The card is added to a time scheme that has currently no access. Check the time scheme of this user and the access hours of the time scheme.

- Currently this is a holiday and the time scheme that is assigned to this user does not overrule holidays.

- The user is expired.

Appendix A: XM3 Configuration Switch Form

For receiving a software configuration switch code, Cross Point requires some information about your current XM3 configuration. This information can be found on the reader info page in XM3 Manage.

Please fill in this form and fax it to Cross Point (+31 591 668867).

XM3 Serial Number	……………………………………………
Extension Board type*	……………………………………………
Extension board version*	……………………………………………
Bootloader version	……………………………………………
Operating system version**	……………………………………………
Application or firmware version	……………………………………………
Current software configuration	……………………………………………
Requested software configuration	……………………………………………
Description of XM3 usage	……………………………………………
	……………………………………………
	……………………………………………
	……………………………………………

* Only if an extension board is present

** Only for separated OS and CPA versions.