

Net2ADSyncServer

Manual 3.24

(November 17, 2026)

Hexapole IntoAccess BV- The Integrators
Robijnstraat 11· 1812 RB · Alkmaar · The Netherlands
intoaccess@hexapole.com · www.intoaccess.com · +31(0)72 303 4056

Index

Installation and Configuration of the Net2ADSyncServer 3
Installation 3
Main principle 3
Synchronization rules 3
Configuration 4
The Net2 connection page 5
Input fields 5
Interim saving of settings 6
The Active Directory settings page 7
Input fields 7
The AD-Net2 Sync Settings page 9
Input fields 9
The AD cards page 10
Input fields 10
Mifare cards 11
Card numbers 11
PIN numbers 11
Vehicle number plates 11
Synchronizing Card/PIN information to the AD 12
Synchronizing Mifare card numbers to the AD 12
The AD-Net2 Field Relation page 13
Input fields 13
Sync timing page 14
Synchronization with a fixed interval 14
Synchronization at fixed times 15
The Mail settings page 16
Input fields 16
Error and/or activity reports 18
The Licence page 19
Input fields 19
The Ultimate licence 20
The benefit of the Ultimate licence 20
Access level type deployment 21
Special Settings Page 22
Input fields 22
Nested security groups usage 26
The Evaluation page 27
The evaluation process 27
Information shown 27
Linking AD users to already existing Net2 users 29
The Service Control page 32
The log settings page 33
Overview of the derived authorizations 34
Reactivate inactive users 35



Installation and Configuration of the Net2ADSyncServer

Installation

The Net2ADSyncServer application is installed using a single Windows Installer file (*.msi). The complete installation consists of a Windows Service and a 'manager' application which is mainly intended for the configuration of this service. It can also be used to start and stop the service.

Main principle

This application is designed from the basic idea that the management of all employees should be done solely on the Active Directory Server itself. At the first run of the SyncServer, all relevant information will be copied to the Net2 database. Any modifications performed afterwards on the AD will result in an update action on the Net2 database. Since **Version 2.x**, it is also possible to copy user fields and card/PIN numbers **to the AD.**

Synchronization rules

The Net2ADSyncServer application uses the following synchronization approach:

The application searches in the AD for all 'Security Groups' whose name match the name of an access levels in Net2, see Image 1. Only those AD users who are member of one of those 'Security Groups' will be synchronized to Net2. They will be assigned the access level with the same name as their security group(*1).

(1*) This restriction does not apply for the 'Ultimate' version. More details you can be found under the heading 'Licence'. .



Image 1

Furthermore, the following rules apply to the synchronization process: AD users who aren't member of one of the special 'Security Groups' are excluded from the synchronization process.

Any already existing user in Net2 will be ignored. The Manager application will give a warning about this on the 'evaluation page' because these users will end up twice in Net2 if they are included in the synchronization process . This can be a serious problem if these users have an assigned card/badge also. Attempts to create a badge/card for these users will fail because card numbers can only be uniquely assigned to one single user.

Additional user properties can be copied from AD to Net2, and/or vice versa, also. See the: “The AD-Net2 Field Relation page”.

Configuration

The Configuration of the Net2ADSyncServer application has to be done using the supplied 'Manager application' (Net2ADSyncService Manager). At start of this application, it will give a short notification and place it self in the system tray at the lower right corner of the taskbar. See Image 2.

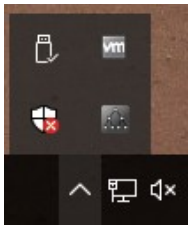

Image 2

A right mouse click on the icon opens the main menu. See Image 3.

It may be that the application will display a menu in Dutch initially. This can be adjusted by selecting 'English' in the menu option 'Taalinstellingen' (Language settings).

The menu options for Starting- and Stopping- the service are grayed out until the configuration process is successfully completed. Please select the menu option: ' Configure first!' in order to open the first configuration window.

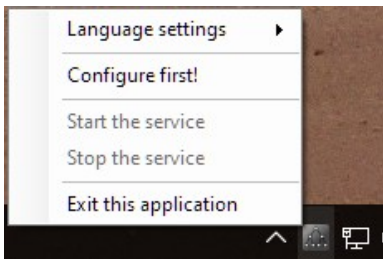

Image 3

The Net2 connection page

The application will start with the page on which the Net2 connection parameters can be entered. See Image 4.

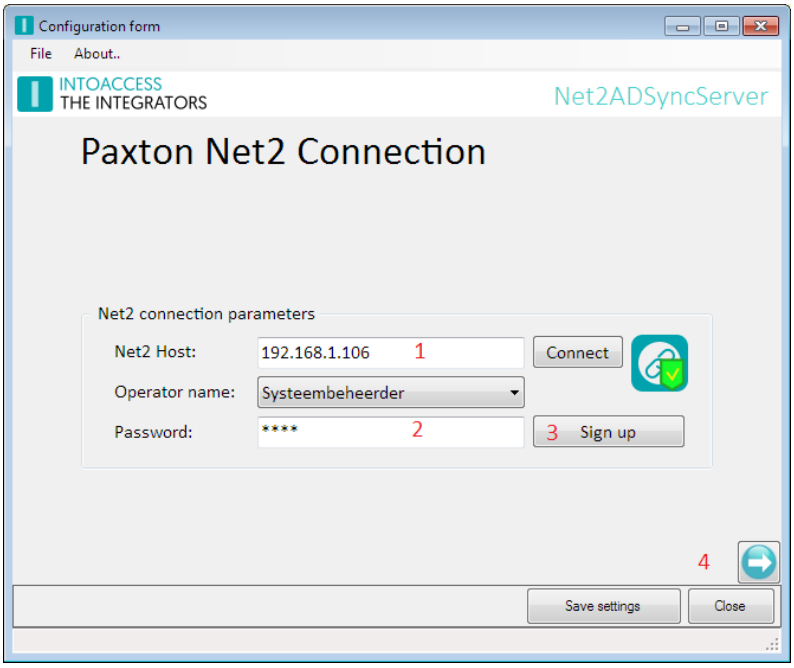

Image 4

Input fields

- First, the (IP) address of the Paxton Server is requested at (1). This can either be an IP address or a network name. 'Localhost' will do if the application is installed on he same machine as the Paxton server application. Please, don't supply an IP address in this case. The application needs to do some version checking based on the machine on which it is installed, the value 'Localhost' has a special meaning in this case.
- Click 'Connect' next, the application will now try to establish a connection to the Net2 server. If this action is successful the options to select the operator name and supplying the corresponding password is enabled (2). Please select a user with 'administrator' rights, preferably the default 'System Administrator'.
- After a click on the 'Sign up' button (3) the application will attempt to sign up to the Net2 server. If this succeeds, a confirmation message will be given and the 'Next Page button' (4) will become enabled. If it doesn't succeed an error message will be given with information about the (possible) cause.

Interim saving of settings

The configuration application is made up of a number of individual pages. The data on all these pages have a great deal of interdependence. For example, changing the address of the Net2 server on the first page will result in data on (almost) all other pages no longer being valid. It is therefore important to *always* go through all pages. Only then can the data be saved in a consistent manner.

Saving in between can be done but will in many cases lead to a warning as shown in Image 5

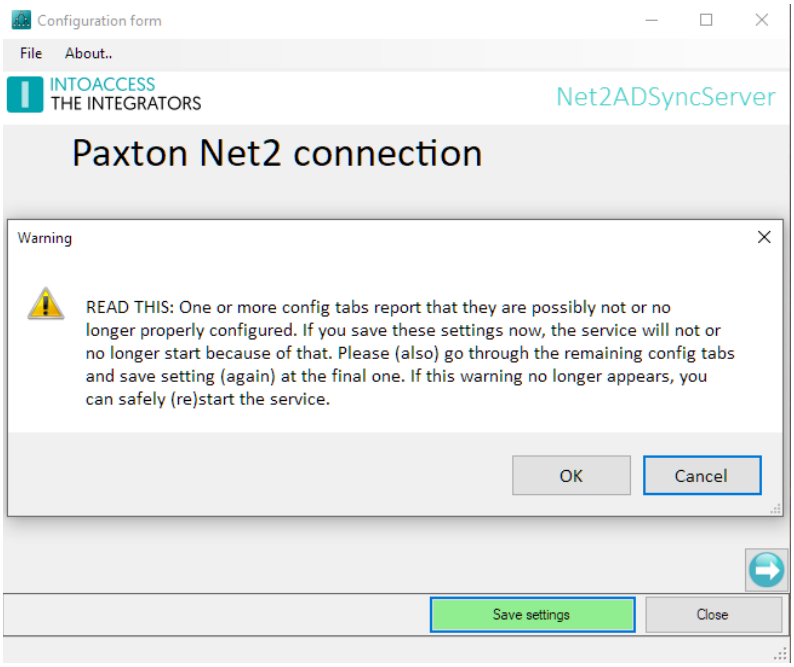

Image 5

The Active Directory settings page

On this page, see Image 6, the parameters for setting up a connection to the AD can be entered.

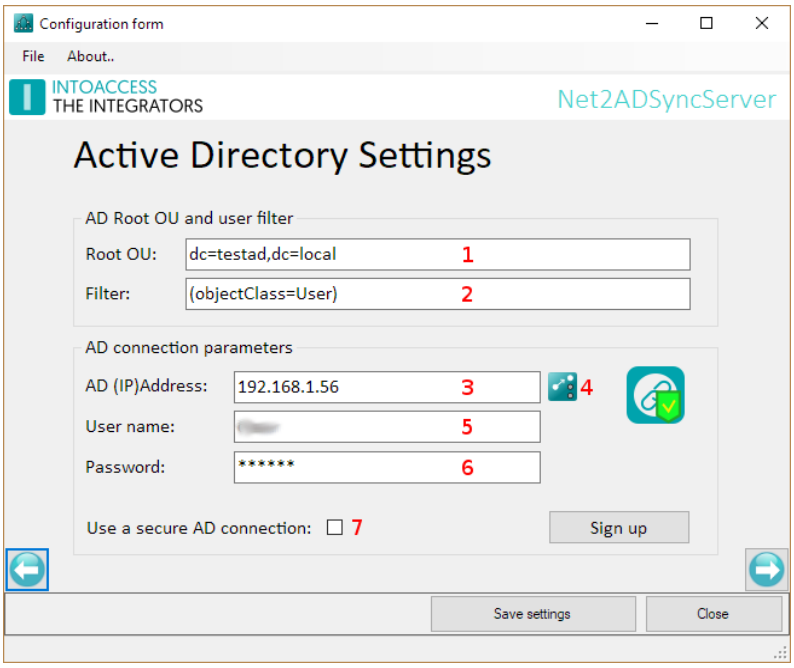

Image 6

Input fields

- First you will be asked for the 'Root OU' (1). This field should contain at least the full Domain Component (DC) of the AD from which the data is to be retrieved. The syntax as shown on image 6 complies with the AD settings as shown on Image 7.

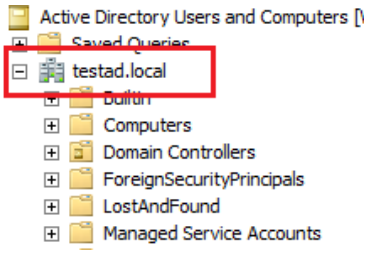

Image 7

  If all employees are contained in a specific OU, it can be stated here also. The more detailed this information, the more efficient the synchronization process will be. It is advisable to start the setup process with the DC parts only, and refine this setting only after the application is working as expected.
- The filter as set by default in (2) will do in most cases, but feel free to refine it if desired.
- At (3), you are prompted for the address of the AD server. As with the Net2 server address, this can either be a 'real' IP address, or a network name.

By clicking on the icon (4), you can optionally add one or more fail over servers. See Image 8. Note that this is an experimental feature.

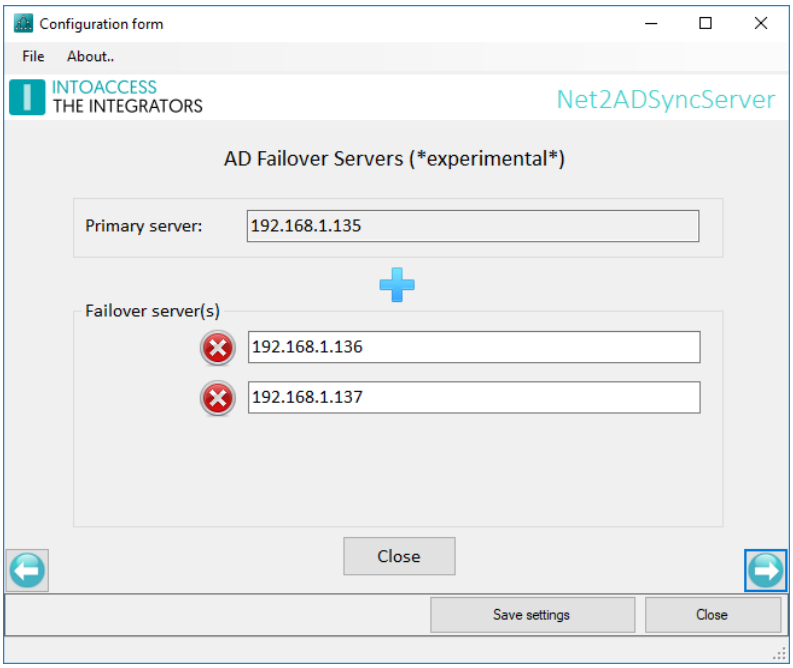

Image 8

- The user name and password prompted for at (4) and (5) will be used, both by the service itself, as well as by this manager application. The manager application uses this user account to retrieve all AD attributes. Please note that only the AD attributes that actually contain a value are retrieved.

  Please note also that this user need to have write access to the AD, but **only** if you plan to sync information **to the AD**.
- If you require a secure connection (LDAPS, port 636), you can check the option at the bottom (7). Note that this feature is (also) experimental and requires a valid ssl certificate on the AD server.

The 'Next Page button' will be enabled once the application is able to successfully sign up to the AD Server.

The AD-Net2 Sync Settings page

On this page, see Image 9, you're asked to provide some basic synchronization parameters.

The application will use the AD attribute 'sAMAccountName' as a key to uniquely identify a user. This value must therefore be stored at all times in one of the Net2 user fields.

In addition, the service uses a 'marker field' to indicate that a particular user is managed by the application. Users where this field is empty, or contains something unrecognized, will be ignored by the application.

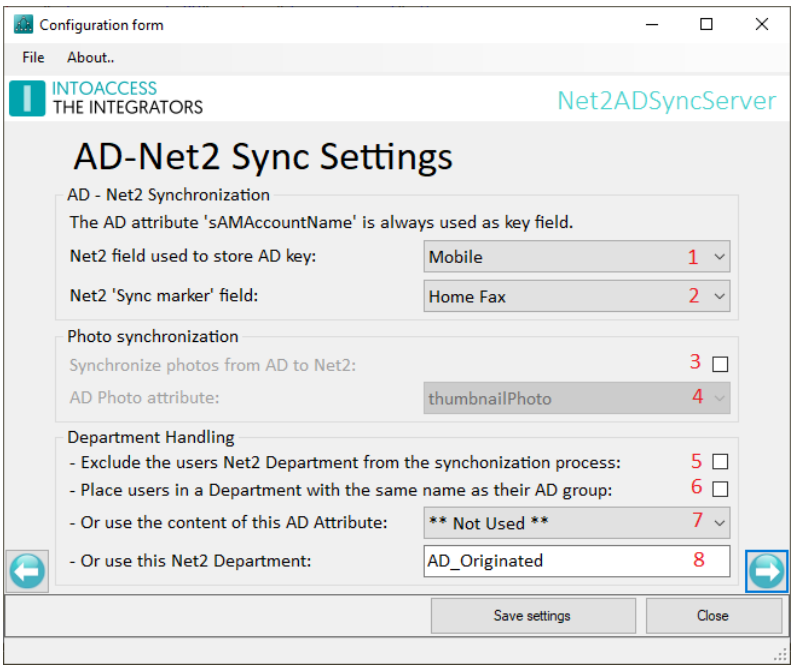

Image 9

Input fields

- At (1) you are prompted for the Net2 user field that will be used to store the 'sAMAccountName'.
- At (2) you are prompted for the Net2 user field that will be used to store the 'marker' value. This field will hold the text "AD_SYNCED" for all users under control by the synchronization process.
- At (3) you are offered the option to synchronize the AD users photos also. If activated, you can select the AD attribute that holds the photo at (4).
- At (5) you can indicate whether the department in which a user will be placed will be included in the synchronization process. If not, you're free to place a user in a different department manually at all times, except when the option to 'bar' and place removed users in a separate department is selected. (See page Special settings)
- At (6/7/8) you can state the name of the 'department' in which all synchronized users will be placed. You can either choose to store users in a department with the same name as their security group at (6), or you can you can designate an AD property as the department source (7), or you can specify a special department (8).

Departments will be created if they don't already exist.

The AD cards page

On this page, see Image 10, you can state whether you want to include card/PIN/license plate information in the synchronization process. Card/PIN and/or license plate information can also be copied to the AD as well.

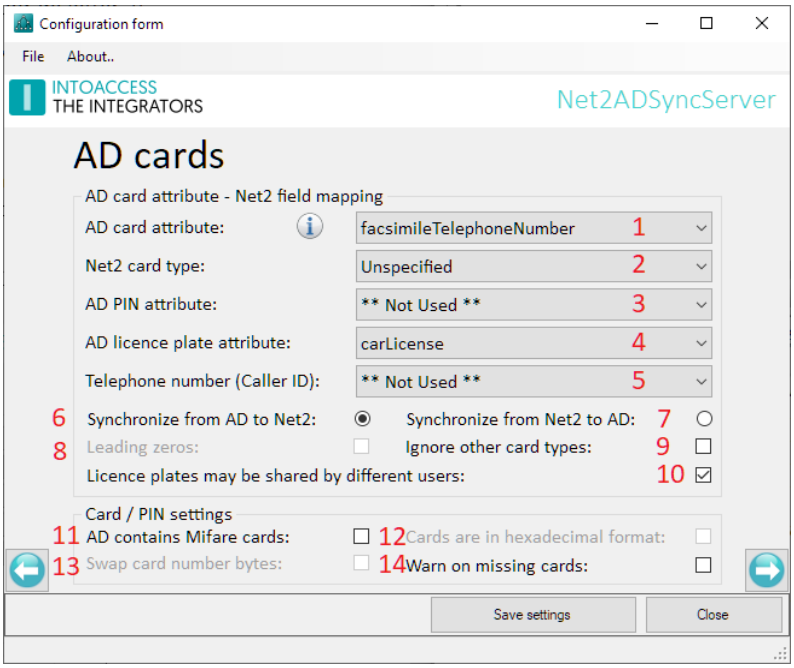

Image 10

Input fields

- Choose at (1) the option '**Not Used**' , see Image 11, if the AD doesn't hold card/PIN/license plate numbers and you have no plans to copy them to the AD either. In this case you may continue directly to the next page.

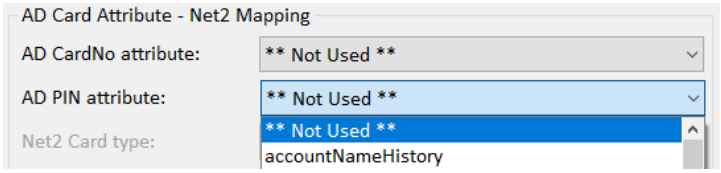

Image 11

- Otherwise select at (1) the AD attribute that is used to store the card/pin/license plate info.
- If a separate attribute is assigned for holding the PIN number, you can select that attribute at (2).
- A separate attribute assigned for holding the license plates can be selected at (3).
- Choose at (4) the card type in use, choose 'Unspecified' if the card type is unknown. If the card attribute is set to anything else than '**Not Used**', the sync app will remove all manually added tokens unless checkbox (9) is checked to leave other type of tokens untouched.

Mifare cards

The application is able to convert, both 4 bytes 'Classic' Mifare cards, as well as the 7 bytes 'DESFIRE' cards, to the format used by Paxton. The actual length of the Mifare card number is recognized by the application automatically.

- Mifare card numbers are mostly stored in hexadecimal format. Set a check-mark at (12) if this is the case.
- Under rare circumstances the Mifare card number bytes may be 'swapped' internally. This is due to the 'Endianness' format being used when the card numbers were read and saved. Set a check-mark at (13) if this is the case.

At (14) the option is offered to let the application send (mail) an error messages in case no card and/or Pin information could be found for a user.

Card numbers

Multiple cards need to be separated by either a comma, semicolon, space or 'TAB' character. The card attribute can also used to store PIN numbers and vehicle number plates. For example, if a user has a card with number 12345678, and a PIN with number 1234, and a license plate which is 11-ABC-9, the card attribute should have the following value:

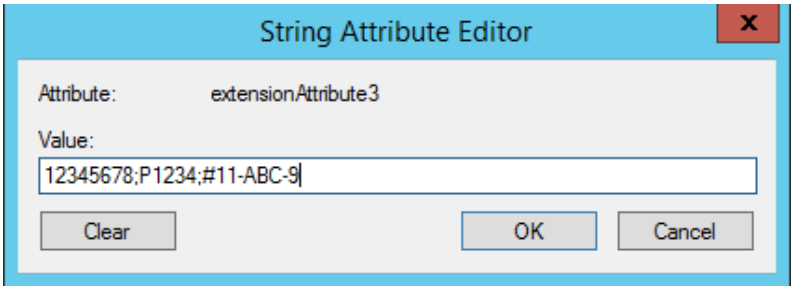

Image 12

PIN numbers

A PIN can be stored in AD in the same attribute value as used for the card number, or in a separate attribute. In the former case the PIN code must be preceded with the letter 'P'. If a PIN has its own attribute, the PIN should NOT be preceded by the letter 'P'.

Vehicle number plates

A vehicle number plate can be stored in AD in the same attribute value as used for the card number, or in a separate attribute. In the former case the license plate must be preceded with a hashtag '#'. If a license plate has its own attribute, the license plate should NOT be preceded by a hashtag. In case multiple cards/number plates are used they need to be separated by either a comma, semicolon, space or 'TAB' character.

In Net2, a license plate may only be assigned to one user. Normally the application will give an error message if an attempt is made to assign a single license plate to multiple users. In that case, the license plate will also be removed from both users. This removal can be prevented by allowing (option 10) a licence plate to be shared by multiple users. In that case, the license plate will be physically assigned to the first user only, and the application will ignore further attempts to assign this same license plate to other users.

Synchronizing Card/PIN information to the AD

It is also possible to synchronize card and/or PIN information to the AD. See Image 13.

Select option (6) if you want to do so. This option is clearly marked, especially to prevent it from being accidentally selected.

If you want the card numbers to appear in Active Directory with leading zeros, check the check-box at (8). For example: card number 123 will appear as 00000123 in Active Directory.

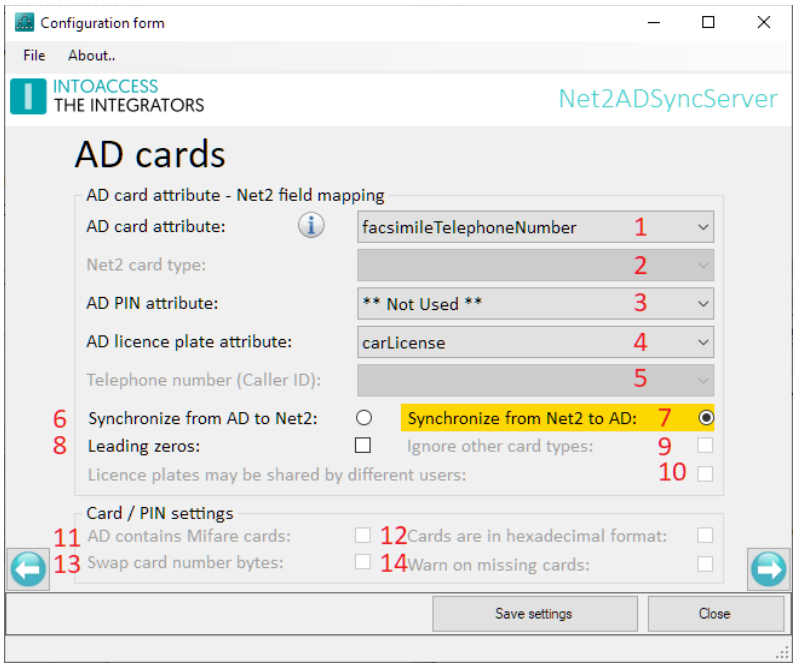

Image 13

Synchronizing Mifare card numbers to the AD

The option to synchronize card/PIN numbers to the AD has, when using Mifare cards, the limitation that only the Paxton card number is synchronized, and not the Mifare card number itself.
This can be overcome by saving the Mifare card number in one of the Net2 user fields. This user field can then be synchronized with a designated AD attribute. (See also the section: 'AD-Net2 Field relation page').
It is also possible to use this same AD attribute as 'source' for the card number in Paxton.
In concrete terms, this could be setup as follows:

- *The Mifare card number is stored in (f.i.) the Net2 user field: 'Personnel number';*
- *The 'Personnel number' field is synchronized with AD attribute: 'extensionAttribute1';*
- *The same 'extensionAttribute1' is selected as 'AD cardNo attribute' on the 'AD Card Settings page';*
- *At the 'Card/PIN Settings' section the card type is marked as a Mifare card.*

As soon as a new, or modified, Mifare card number is detected for a user, it will be synchronized to the AD. At the next synchronization cycle this Mifare card is recognized as being changed and hence synchronized as a Paxton card number, back to Net2.

The AD-Net2 Field Relation page

This page, see Image 14, offers the possibility to add multiple AD attributes to the synchronization process.

It is mandatory that the Net2 field 'Surname' is given a value at all times. So, as an absolute minimum, it would suffices if the AD attribute: 'sAMAccountName' is assigned to this field on page: 9 (The AD-Net2 Sync Settings' page.)

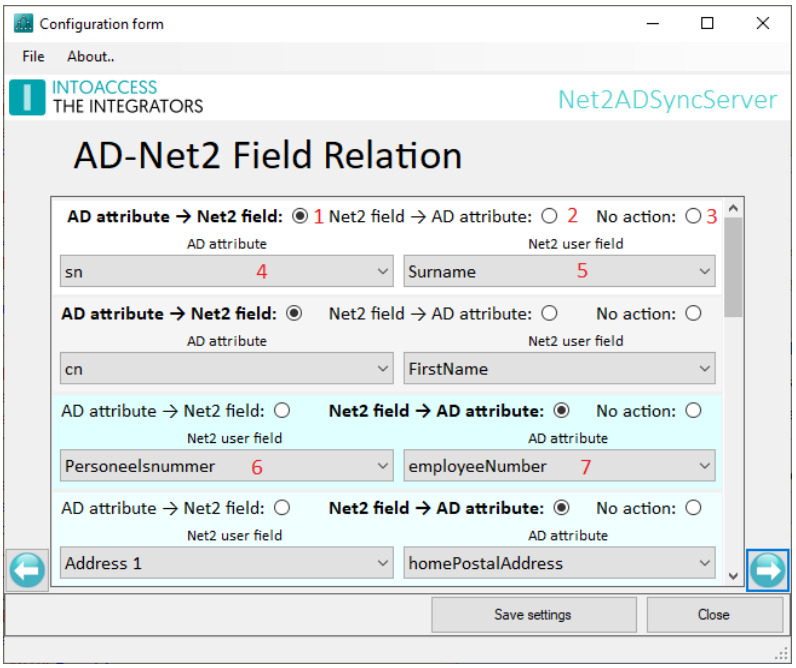

Image 14

Input fields

- First select the 'source' and 'target' of the synchronization at (1) or (2).
- The option (1) offers the possibility to synchronize an AD attribute with a Net2 user field **where the AD attribute is leading**.
  - In this case select the desired AD attribute at (4) and the desired Net2 user field at (5).
- The option at (2) offers the possibility to synchronize a Net2 user field with an AD attribute **where the Net2 field is leading**.
  - In this case, select the desired Net2 field at (6) and the desired AD attribute at (7).
- Select 'No action (3) to withdraw a field from the synchronization process.

Sync timing page

This page, see Image 15 and Image 16, offers the possibility to let the application perform the synchronization either at a fixed interval or at fixed times.

Synchronization with a fixed interval

When using a fixed interval (1), two fields can be configured. The actual interval time can be set at (2). The minimum interval time is 10 seconds. However, such a small interval time is only necessary in very exceptional cases. An interval time of 300 seconds (5 minutes), or even more, will be sufficient in most cases.

The synchronization will only be done during the selected (Net2) timezone. This means that the interval will not trigger a synchronization cycle when the current time is not within the selected timezone. The default timezone is the timezone that is active all day and every day. If a timezone doesn't have any time slots, it will not appear in the list (3).

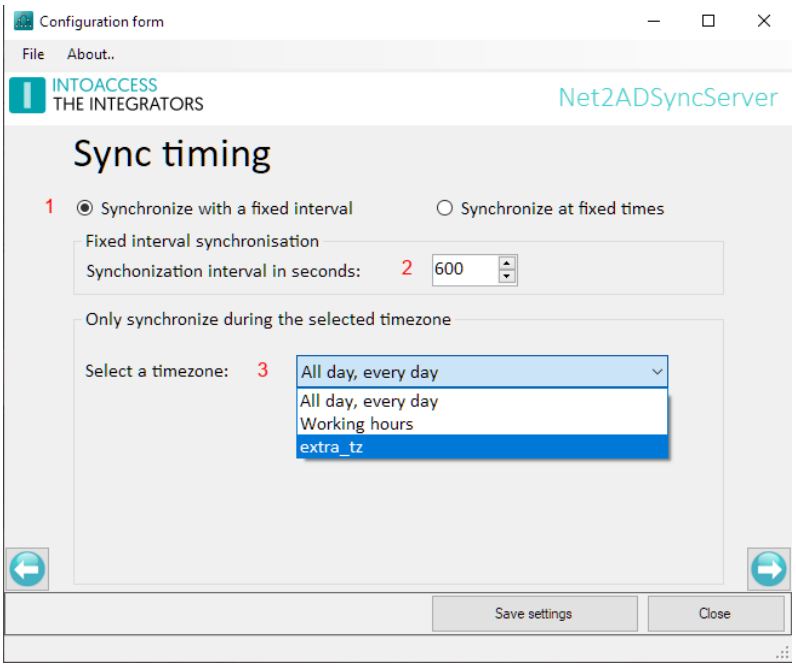

Image 15

Synchronization at fixed times

When using fixed times (1), the option to add one or more times is enabled (2). After clicking this button a new 'Enter a new time' window (3) will be opened. You can enter multiple times with this window open by pressing the 'Add time' button. Times already entered can be removed by pressing the corresponding 'Remove' button (4).

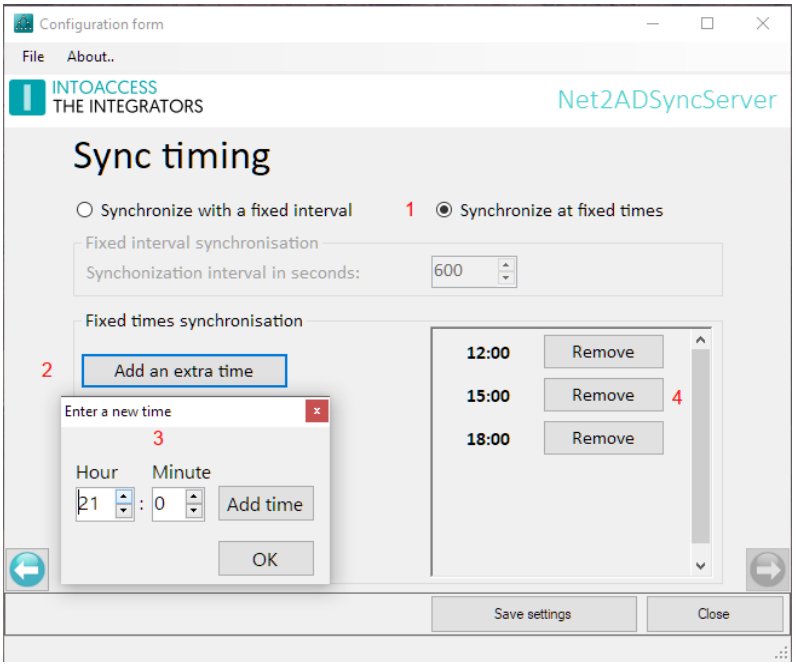

Image 16

The Mail settings page

This page, see Image 17, offers the possibility to configure the application such that possible problems can be reported by mail. It is strongly advised to activate this option because the application is running as a 'Windows service' and hence not capable of showing error messages on screen. If this mail option is activated, the application can also create a daily usage report with all changes made in the past 24 hours.

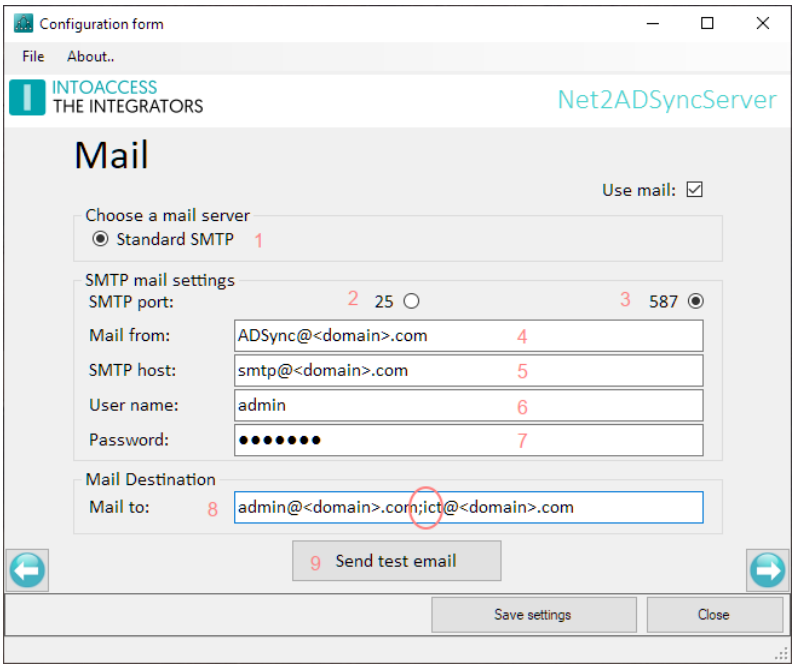

Image 17

The application can utilize a company SMTP server (1), or a web mail account (like Gmail) for sending mail. In case of a web mail provider, it is recommended to create a separate account with minimal safety rules applied, otherwise the web mail provider won't accept messages sent by the application (if they do at all).

Some notes:

- There is no real difference in the settings between using web-mail and a SMTP server using the STARTTLS protocol over port 587.
- Mail providers using the SMTPS (port 465) are not supported.

Input fields

- Select the desired port number, and hence the applied security, at (2) or (3);
- Enter the senders address at (4);
- Enter the address of the mail provider at (5);
- The fields for entering the user name (6) and password (7) are only relevant if a secure connection over port 587 is selected;

- Enter the recipient address(es) at (8). Multiple addresses can be entered here separated by a semicolon.

Error and/or activity reports

If on the previous page the option to be able to send email is activated, on this page, see Image 18 can be specified what kind of messages are desired.

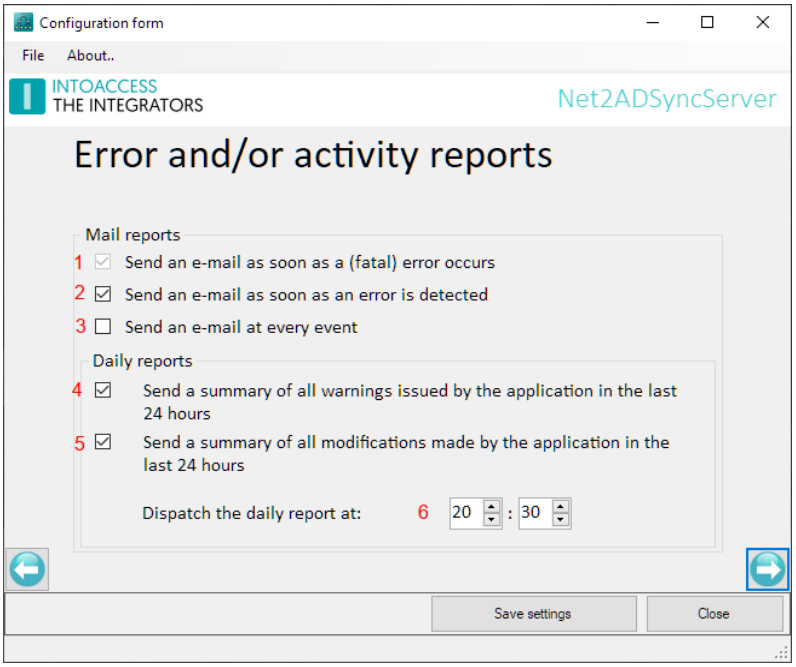

Image 18

- In all cases (1) an email will be sent the moment a fatal error occurs from which the application cannot recover by itself.
- If desired (2) problems can also be reported that will (normally) not impact the functioning of the application.
- Optionally (3) an email can also be sent at every modification made by the application, or every problem detected, by the application.

In addition, the application can also email daily reports.

- At (4) the option can be activated to send a daily overview at a fixed time of all warnings/errors the application has collected in the past 24 hours.
- The option at (5) causes the application to send a daily report containing all changes made in the past 24 hours.
- At (6) the time at which the report should be sent can be specified.

The Licence page

This page, see Image 19, offers the possibility to select-, enter-, and validate-, a licence.

A licence can be obtained directly from IntoAcces BV.

Please send an email to info@intoaccess.com for more information about the procurement process.

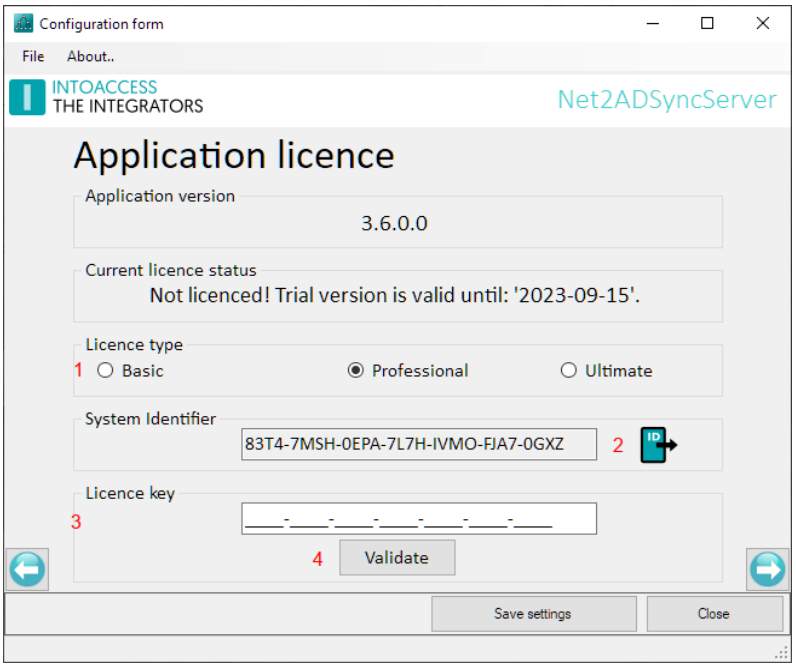

Image 19

Input fields

- The desired licence can be selected at (1);
  - The 'Basic' licence is suited for small companies where the number of synchronized users is less than 100 and the number of controlled doors is less than 25.
  - A 'Professional' licence is functionally similar to the 'Basic' version but without the restrictions that apply to the Basic version.
  - The Ultimate licence adds the ability to utilize multiple 'AD Security Group – Net2 Access Level' combinations. See below for a more elaborated explanation.
- You'll be asked for the 'System Identifier' export file as shown at (2); click on the icon to create this readable text file if you want to order a licence for this application. Please note that a licence is **not restricted in time**, and **all future updates will be provided for free**. Check our website for information about the availability of new versions.
- Once you have received a licence code you can enter it at (3). Please do not forget to validate the supplied licence. It can be validated by pressing the Validate button (4).

The Ultimate licence

The benefit of the Ultimate licence

As mentioned above the Ultimate version can utilize the deployment of multiple 'Security Groups'.

An example of such a deployment is elaborated below.

Consider the following situation:

The following access levels are defined in Net2:

- 'Basic Access', this access level contains the access rights which applies to all personnel. As an example it might regulate the access rights at the Main entrance, the Central lobby, the Bicycle storage, and the doors of department 'A' and 'B', but only allow access during 'Working hours'.
- 'Department A', this access level allows access to the doors of department 'A' from 6:00 AM to 22:30 PM only.
- 'Department B' , this access level allows 24x7 access to the doors of department 'B' only.
- The AD contains Security Groups with the (exact) same name.

All AD users may now be assigned to the Security Group: 'Basic Access'. By doing so they will gain all the access rights as defined by the Net2 Access level 'Basic Access'.

Anyone who needs extra access rights, for instance the rights as defined in the Net2 access level 'Department A', can now be made member of this AD Group also. In this case the application will create a new access level in which the access rights of both the access levels 'Basic Access' and 'Department A' are merged. This new access level will give access to the Central lobby, the Bicycle storage and Department 'B' as defined by the 'Basic Access' access level, and the additional rights as defined by the access level 'Department A'. The application will use the least restrictive timezones in case of overlapping doors. It will create a new time zone if applicable.

This behavior is an extension of the Paxton 'Advanced Permissions' concept. In contrast to the advanced permissions, which prohibits the combinations of access levels containing overlapping doors. This situation is solved by this application by creating a new Timezone for each of these overlapping doors if necessary.

The only limiting factor that applies to this solution is the total number of access levels which may not exceed 255. This number is imposed by Paxton.



Access level type deployment

New in version 3 is the option to use 'individual' authorizations instead of the normal 'global' access levels. See Image 20

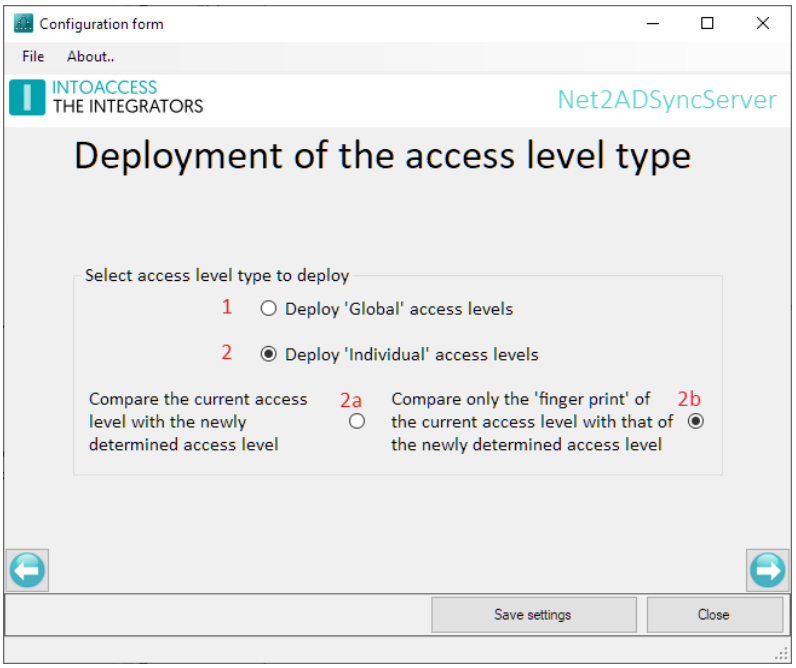

Image 20

Please note that this option is exclusively available (and only useful) for users using the 'Ultimate' licence.

The use of 'global' authorizations is the most insightful. A possible disadvantage of this method is that the number of authorizations can reach the limit of 255 (global) authorizations. This issue can occur in situations with many access points where fine-grained access policies are important..

This limit can now be circumvented by using 'individual' authorizations. This authorization form has no limit on the number of authorizations that can be used.

Please note: in both cases there is an absolute limit on the number of different time zones (64) that can be created.

When using 'individual' authorizations you can choose to compare, per user, the determined authorization with the already assigned authorization. This method is the safest but also the most labor intensive. (2a)

Alternatively, one may choose to compare a "fingerprint" of the calculated authorization to the stored "fingerprint". This method is significantly faster but is only safe when it can be guaranteed that a user's authorization will never be changed manually.

Special Settings Page

This page, see Image 21 up to Image 25, offers the possibility to apply a different value for some of the basic parameters. In most cases, except for the 'Utilize nested groups' option, the already set values will suffice, only in exceptional cases it might be desirable to set a different value here.

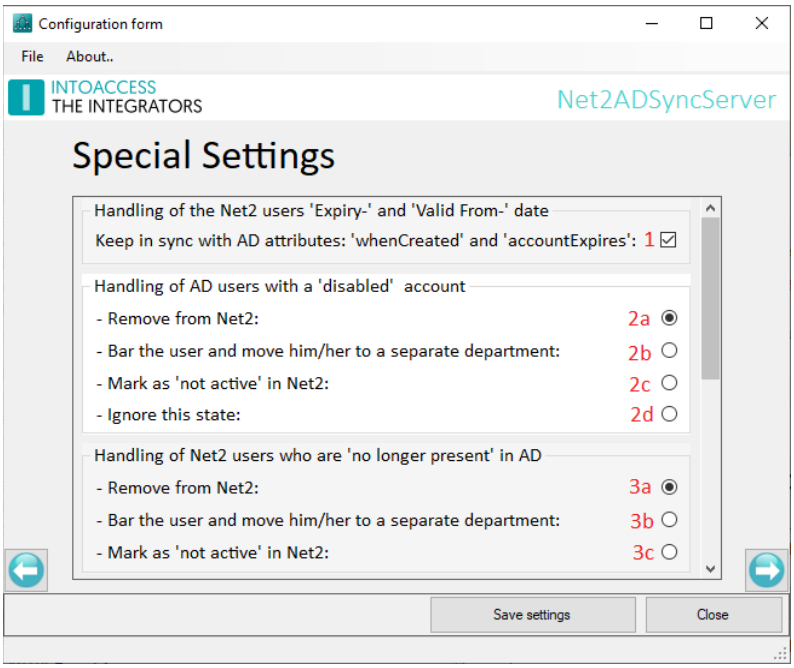

Image 21

Input fields

- If the check-box (1) is checked, the 'Expire-' and 'Valid From-' dates of a Net2 user will be kept synchronized with the 'whenCreated' and 'accountExpires' AD attributes. At removing the check mark, these fields can be set at will in Net2. Newly inserted users will always have the 'whenCreated' and 'accountExpires' values assigned initially though.
- At (2a..2d) can be stated how the application should deal with users whose account are disabled in the AD.
  - By default (2a) these users will be removed from the Net2 database.
  - The option (2b) will bar (block) and move the user to a separate department. When this option is selected the application will ask for the target department. See Image 22.

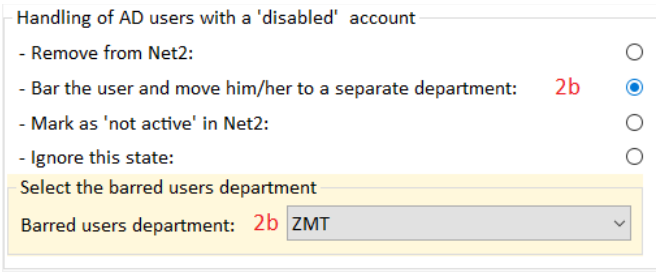

Image 22

- If the department is exempt from the synchronization process (see page: The AD-Net2 Sync Settings) that setting will have precedence over this target department.
- The third option (2c) will mark the user as 'Not active'. Users with this state are hidden in Net2 but their history will be retained. When this option is chosen you'll be asked what should happen when the user is 'enabled' again in the AD. See Image 23

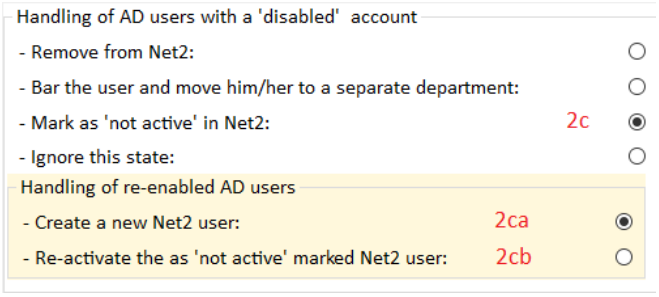

Image 23

- Option (2ca) will cause the creation of a new user in Net2.
- Option (2cb) will reactive the previously inactivated user in Net2.
- The fourth option (2d) will cause the application to completely ignore this state. In this case disabled users will be fully functional in Net2.

- At (3a .. 3c) can be specified how the application should deal with users who are 'no longer present' in the AD.
  - By default (3a) these users will be deleted from the Paxton database.
  - The disadvantage of completely deleting a user is that the complete history of this user is deleted also.
  - The second option (3b) will bar (block) the user and move it to a separate department.

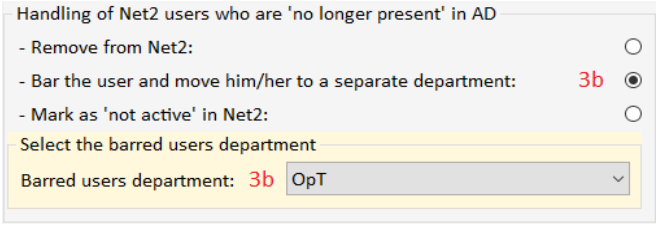

Image 24

  - When this option is selected you'll be asked to select the target department. See Image 24
  - This target destination will have precedence over the 'Exclude the department from the synchronization process' setting as stated on page: The AD-Net2 Sync Settings.
  - Alternatively (3c) the user can be marked as 'inactive' in Net2 thereby saving the users history.
- At (4) See Image 25. The utilization of 'nested security groups' can be activated. (See page 26 for more information about this feature).

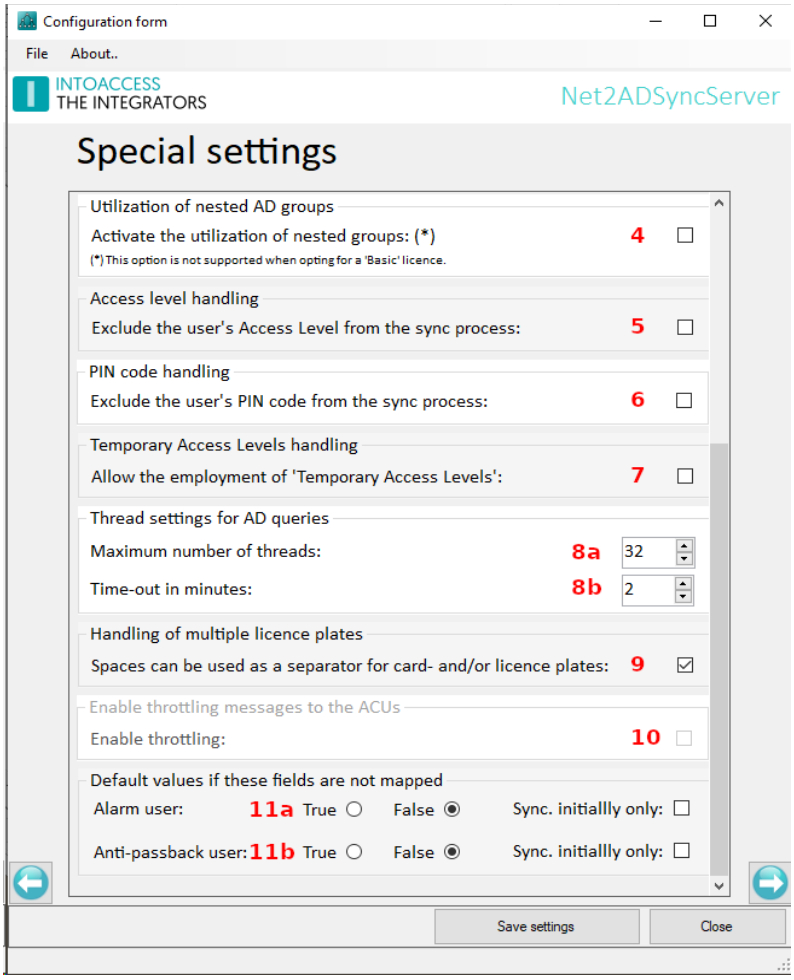

Image 25

- Access levels can be exempt from the synchronization process as well (5). With this option selected, access levels are only synced when a user is created in Net2. Once created, the users access level can be freely modified. This setting will be ignored though for users with a disabled account and for users who no longer appear in the AD and are to be placed in a separate department. (See 2b and 3b)
  *Access level handling can only be set when Temporary authorization (7) is not set.
- Pin codes can also be exempt from the synchronization process (6). With this option selected, pin codes are only synced when a user is created in Net2. Once created, the users pin code can be freely modified in Net2. Note that you need to check this option if you chose to sync card numbers from AD, but want to use manual pin codes. Since a card attribute also allows a pin to be included (like P1234), you need to explicitly configure to exclude pin codes from being synced, to prevent the application from removing it when none is present in the card attribute.
- In Paxton a "temporary authorization" can be granted to a employees. Normally, at the next round of synchronization, the application will reset any modified access levels back to the original value. If the check mark at (7) is set, the application will respect any manually assigned "temporary authorizations". This offers the possibility to grant employees, temporarily, a different authorization than they should have according to the settings in the AD.
  *Temporary authorization can only be set when Access level handling (5) is not set.

- The application tries to be as effective as possible when reading data from Active Directory. A lot of processes will run simultaneously to accomplish this. In some cases, on old machines for example, this can lead to certain problems. That's why you can tweak the settings at (8a) and (8b), to achieve an effective and solid performance for the application.
- In version 2.13.9, the option (9) was added to enable the use of spaces as separators between license plates. This option has been added especially for the English market. In contrast to the Netherlands, a space seems to be a legitimate character in a license plate in England.
- New in version 3.0 was the option (10) to limit ('throttle') the number of messages that will be queued for sending to the individual ACUs. This option can be important when the first initial synchronization cycle is started and the number of ACUs involved is greater than ~30. On the "old" V5 version of Paxton, flooding the ACUs with a lot of messages can even cause one or more ACUs to crash. This option is only relevant when opted to deploy 'individual access levels'.
- If every user in Net2 should be able to arm/disarm the alarm system, or must obey anti-pass back rules, you can set the default value at (11a) and/or (11b). These settings will only work if no AD-fields are connected to these Net2 fields on the page 'AD-Net2 Field Relation'. The option to set this value only initially offers the possibility to adjust this value manually later.



Nested security groups usage

See Image 26.

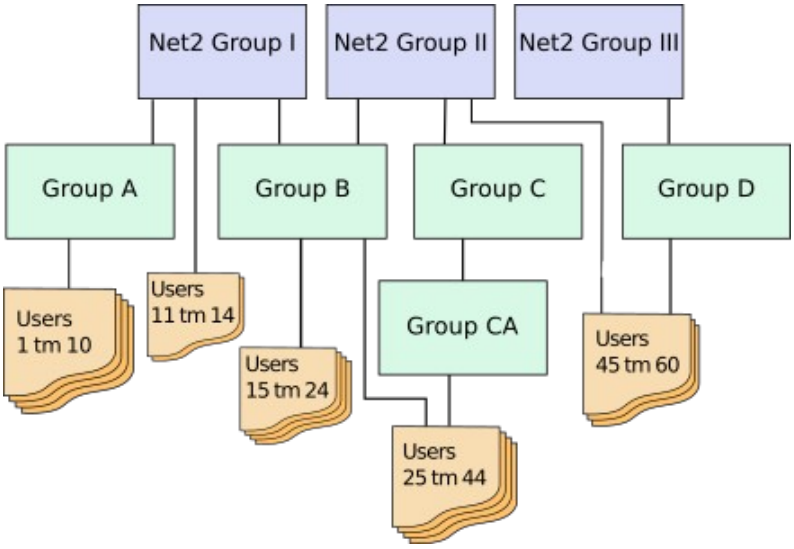

Image 26

In this example, the AD security groups: 'Net2 Group I to Net2 Group III' all have a counterpart in Net2 in the form of an access level with the (exact) same name.

- The AD groups: 'Group A' to 'Group CA' are just 'normal' security groups, so these groups have no counterpart in Net2.
- The users: 'Users 1 to 10' are member of 'Net2 Group I' via 'Group A'. These users will now be synchronized to Net2 due to their 'Group A' relation. These users would be ignored if the 'use nested group' option was deselected.
- The users: 'Users 11 to 14' are direct member of 'Net2 Group I'. These users will be synchronized regardless of the 'use nested groups' selection.
- The users: 'Users 15 to 24 are member of both the groups 'Net2 Group I' and 'Net2 Group II' via 'Group B'. These users will get the combined access rights as defined by the access levels 'Net2 Group I' and 'Net2 Group II'.(*)
- The users: 'Users 25 to 44 are member of 'Net2 Group II', both via the groups 'Group CA' → 'Group C', as well as via 'Group B' .
- The users: 'Users 45 to 60' are direct members of 'Net2 Group II' and, via 'Group D', also members of Net2 Group III'.

Please note, that users may be member of a Net2 related authorization group by various routes.

(*) Please note that this example would require an Ultimate licence.

The Evaluation page

This page, see Image 27, offers the possibility (mandatory) option to evaluate the settings as stated in the previous pages, thereby forestalling problems as early as possible.

This evaluation will not make any alterations in Net2, (nor in the AD), so it is possible to experiment freely without the risk of corrupting your Net2 database.

The evaluation process

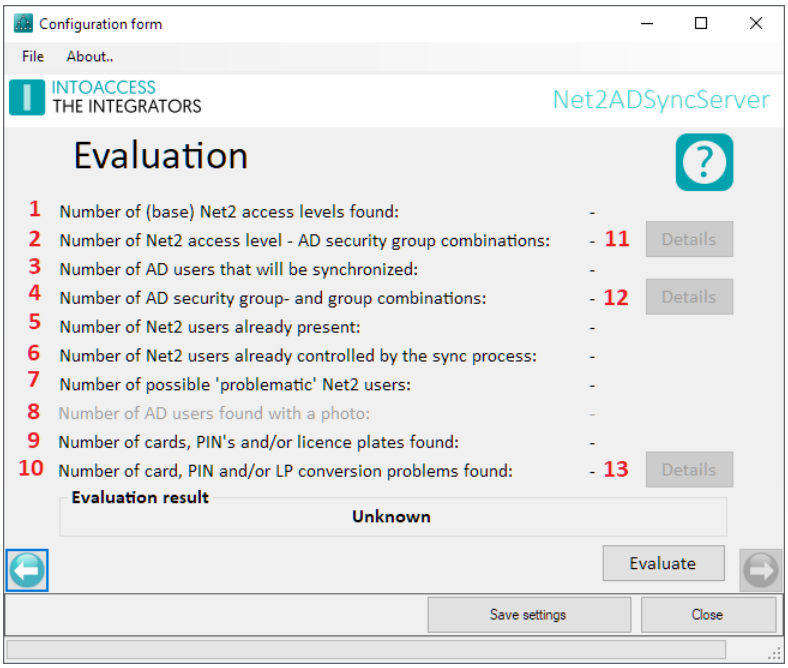

Image 27

After clicking the 'Evaluate' button, the application will collect data both from AD and Net2 based on the settings supplied thus far. It will do so based on the same rules as deployed by the actual synchronization process.

Information shown

- The total number of access levels found in Net2 will be shown at (1).
- In case an 'Ultimate' licence is deployed, and the application has run before, it might be that the Net2 database contains 'merged' access levels already. The number of merged access levels will be exempt from this number.
- At (2) the number of corresponding 'AD Security Group – Net2 authorization' pairs found are shown. This value is important because only members of these AD group(s) will be synchronized.
- At (3) the total number of AD users that will be synchronized is shown.
- At (4) the number of the 'AD Security Group- Net2 access levels' combinations is shown. This number may only deviate from the number found at (2) if the 'Ultimate' licence is selected.
- Buttons (11) and (12) offers the possibility to show the underlying combinations in more detail.
- At (5) the total number of employees already present in Net2 is displayed. Please note that if employees are already present in Net2 and do not fall under the management of the

synchronization process but do appear in the AD, this, at best, will lead to duplicates in Net. Even worse, the application won't be able to create card/badges for these users, because Paxton demands every assigned card number to be unique. The application will just fail in this situation, creating a lot of error messages.

- At (6) the number of employees controlled by the synchronization process is presented. Initially this number should always be zero.
- At (7) the number of users is presented that are already having a 'value' in the field assigned for the storage of the 'sAMAccountName' name while not being managed by the synchronization process. This normally signals a configuration problem.
- Whether or not a user is managed by the synchronization process is solely determined by the presence of the Net2 Sync 'marker' value. See also image 8.
- At (8) the number of photos found in AD are presented. (If applicable).
- At (9), the number of cards, PINs and license plates found in AD is displayed.
- At (10), the number of errors that occurred while processing cards, PINs and license plates is shown. The selection of an incorrect card type (Mifare/Paxton) is a common cause of these types of errors. (See page 10, AD card data.) Another possible cause is the selection of the wrong AD attribute. The errors found are shown after pressing button (13).
- The lines/buttons at (9), (10) and (13) are 'greyed out' if the possibility to synchronize maps is not used.

Linking AD users to already existing Net2 users

Since version 2.15.0, it is possible to include already existing Net2 users in the synchronization process.

If during the evaluation process more than a certain percentage of users are found, who exist in Paxton but are not included in the synchronization process, the application will ask if it is desirable to link them. See Image 28.

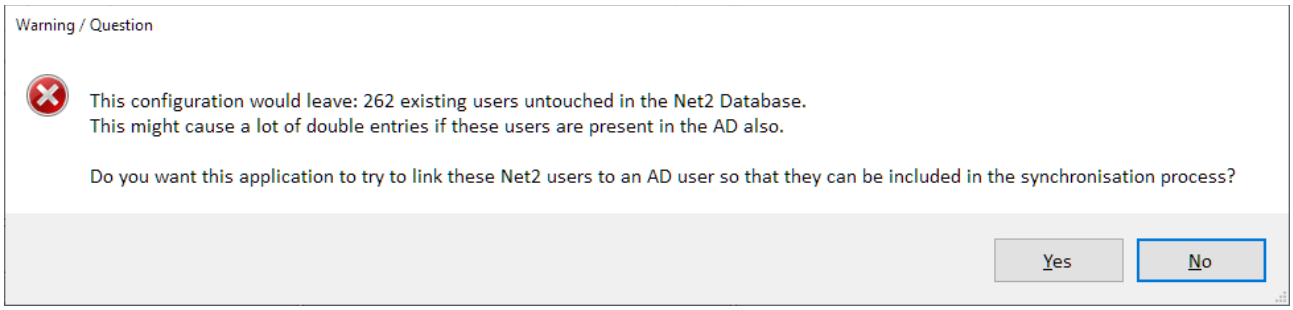

Image 28

If this is indeed desired, an additional button is enabled with which the link process can be started. See Image 29

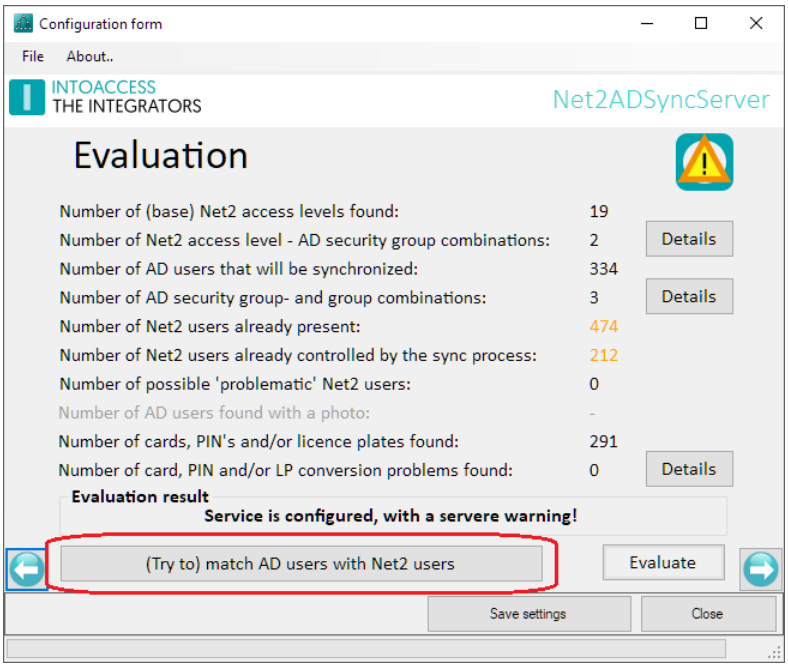

Image 29

After pressing the '*(Try to) match AD users with Net2 users*' button, a new window will be opened. See Image 30. (Although without the search result.)

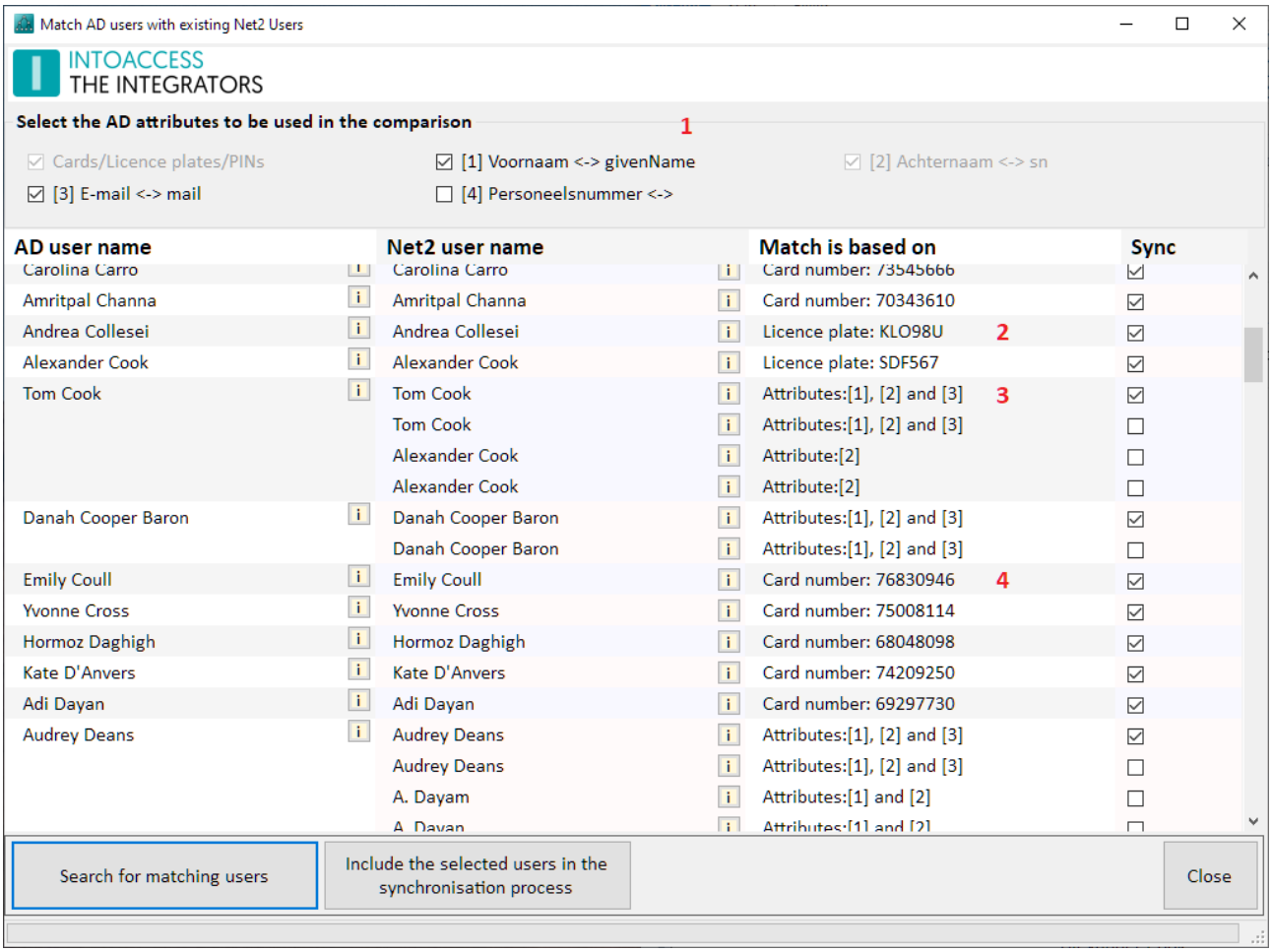

Image 30

- First at (1), select the fields/attributes to be included in the search process.
- The last name will always be included in this process, and therefore cannot be deselected. This also applies to cards, PIN codes and license plates, if they are included in the synchronization process (*). All other fields are optional. If these fields contain corresponding data, the matching process will be more accurate.
- (*) Cards, PIN codes and license plates are only used if they are to be synchronized from the AD to Net2.
- After pressing the '*Search for matching users*' button, the users found will be displayed. (If any)
- Only one Net2 user can be selected per AD user. The application will check for this before the user can be linked in the database.
- The application will first attempt to link users based on corresponding license plates, card and/or PIN numbers. If a matching value is found, no further attention is paid to the name of the user nor to the value of the other fields.

- If no matching values can be found, or if card/PIN/license synchronization is not used, the application will try to link users based on similar last names. The remaining fields of the found series will then be compared. The range with the highest number of matches will then be selected by default.
- If the 'First name' field is part of the comparison process, the application will also try to include any initials in the comparison. So for example, 'J. Johnson' will match 'John Johnsen'.
- The rightmost column shows on what bases the person found was selected.
- Using the 'beige' i-buttons, detailed information can be requested about the person in question. See Image 31

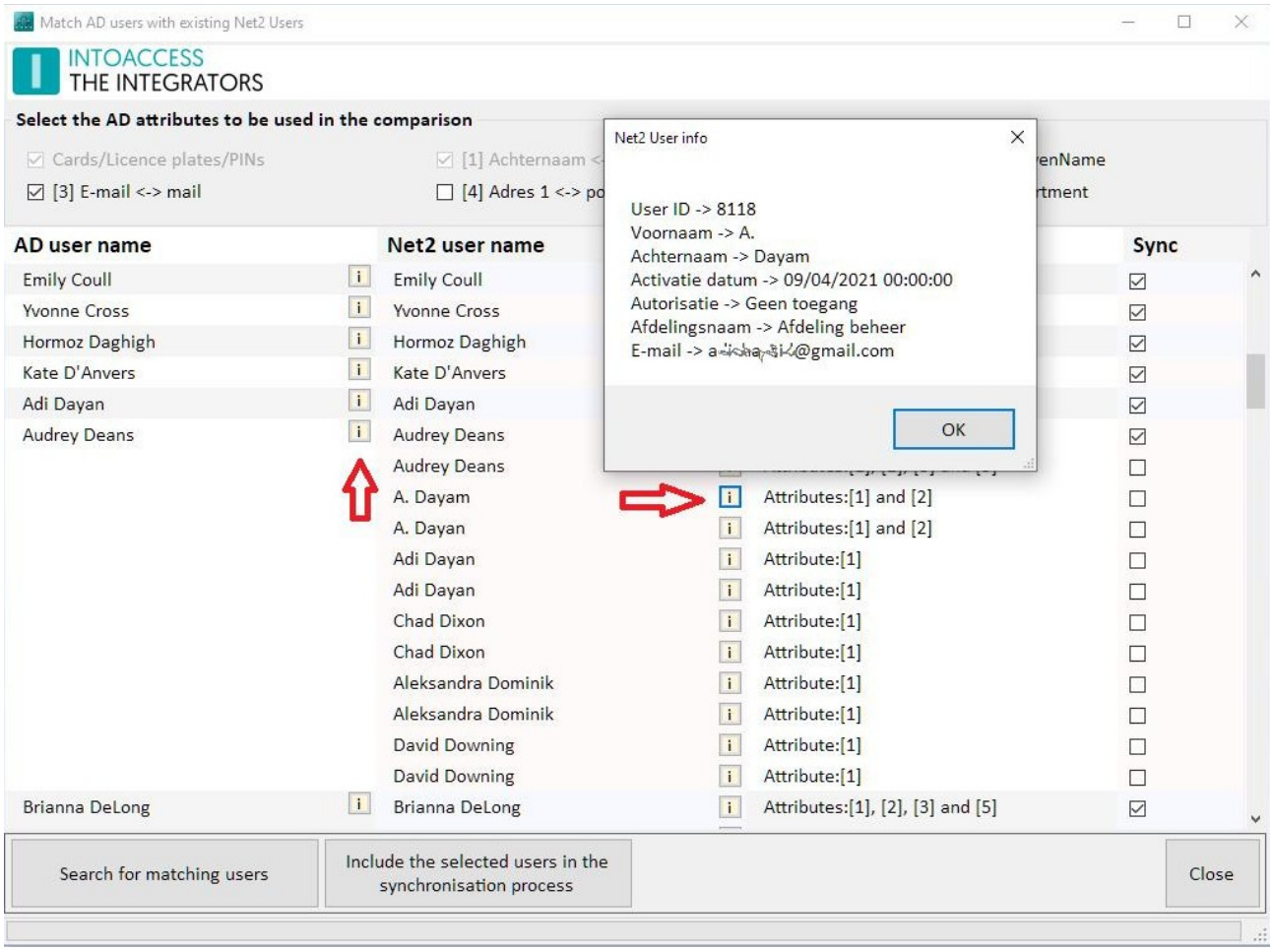

Image 31

After pressing the '*Include the ... process*' button the selected users will be included in the synchronization process. To this end, both fields as appointed at (1) and (2) in chapter: 'The AD-Net2 Synchronization Settings' on page 8, will be filled with the 'sAMAccountName' and the correct 'marker value'.

The Service Control page

This page, see Image 32, offers the possibility to start- and stop- the actual service.

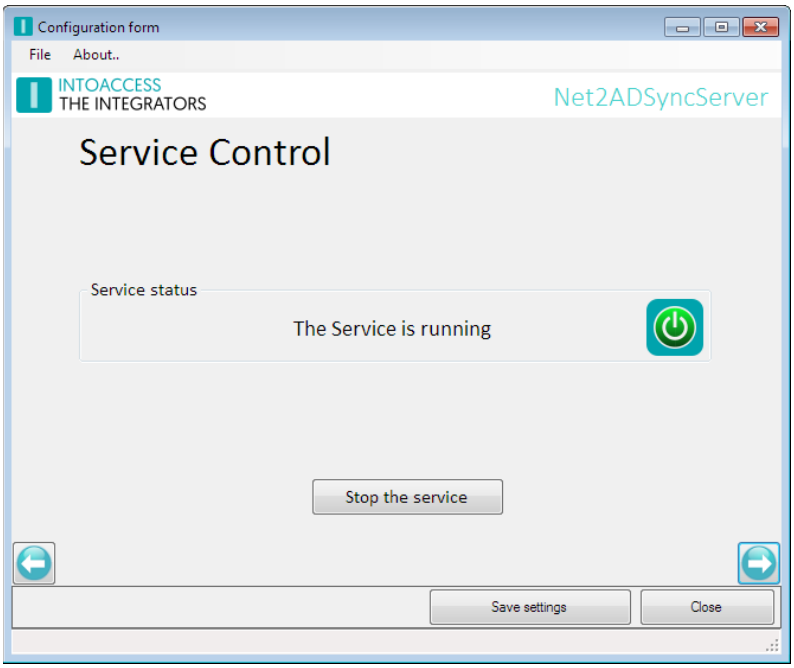

Image 32

The starting- and stopping- of the service may take a few seconds, so please be patient.

In rare cases the Service may refuse to start. If this happens to you please have a look at the end of the log-file to find out what might caused it. In case the reason is not obvious, please send all log files to info@intoaccess.com with a short description of what went wrong. The development team will investigate your problem with the highest priority.

These log-files can be found in the folder: C:\IntoAccess\Logging\Net2ADSyncServer\

The log settings page

This page, see Image ,33 offers the possibility to review the last (max. 500) lines of the log file. The application will log it's activity with a high level of detail. Especially when the application encounters an unexpected problem this log file might contain invaluable information, even for you as an end user.

Please have a look at the last lines of this file if the application refuses to start or otherwise behaves unexpectedly.

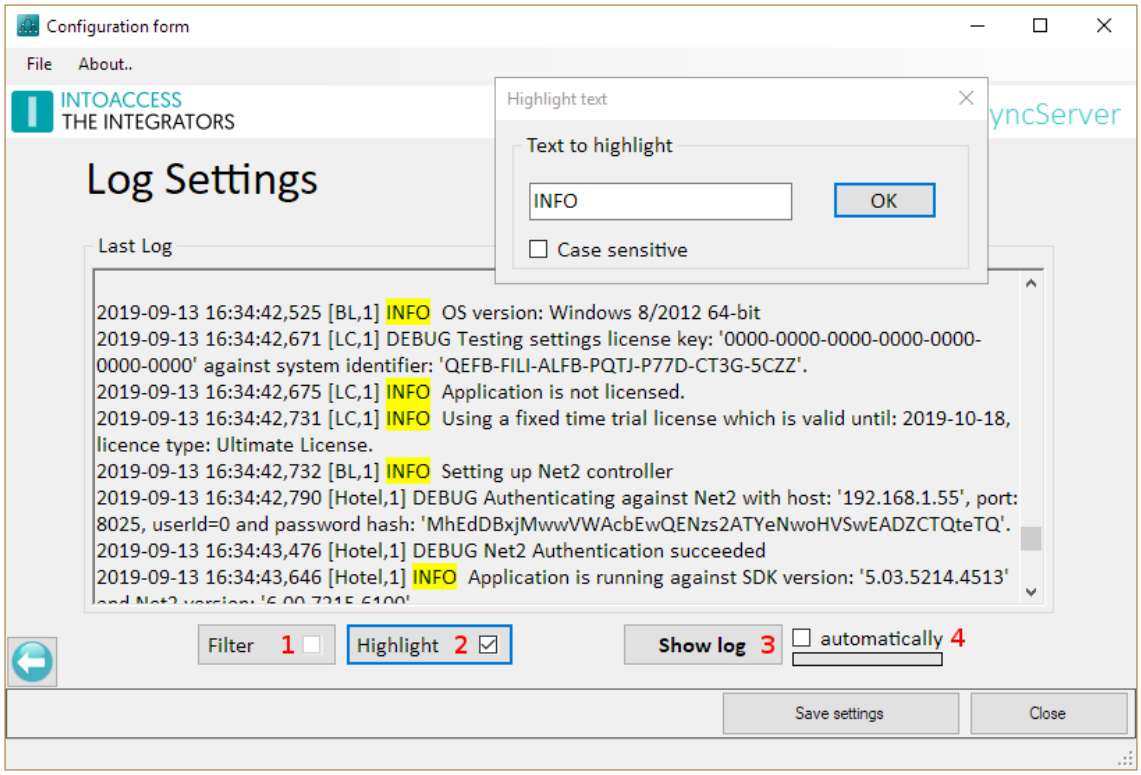

Image ,33

You can resize the window in order to get a better overview of the content.

This page also offers the possibility to filter the log file on certain terms (1) and/or to mark certain terms (2). An obvious 'filter term' could be the word 'ERROR' or 'WARN'. If the application works properly, both terms should not appear in the log file.

Option (4) offers the possibility to automatically reload the log file at a fixed interval.

The log file itself can be found in the folder: c:\IntoAccess\Logging\Net2ADSyncServer\

Overview of the derived authorizations

This page can show an overview of the structure of the authorizations generated by the application (the DR_AL_<n> authorizations). From each of these derived authorizations you can see from which "basic" authorizations it is constructed.

This page is only displayed if:

- An 'Ultimate' license is being used;
- The use of 'Global' authorizations is selected;
- The application has previously created at least one derived authorization;

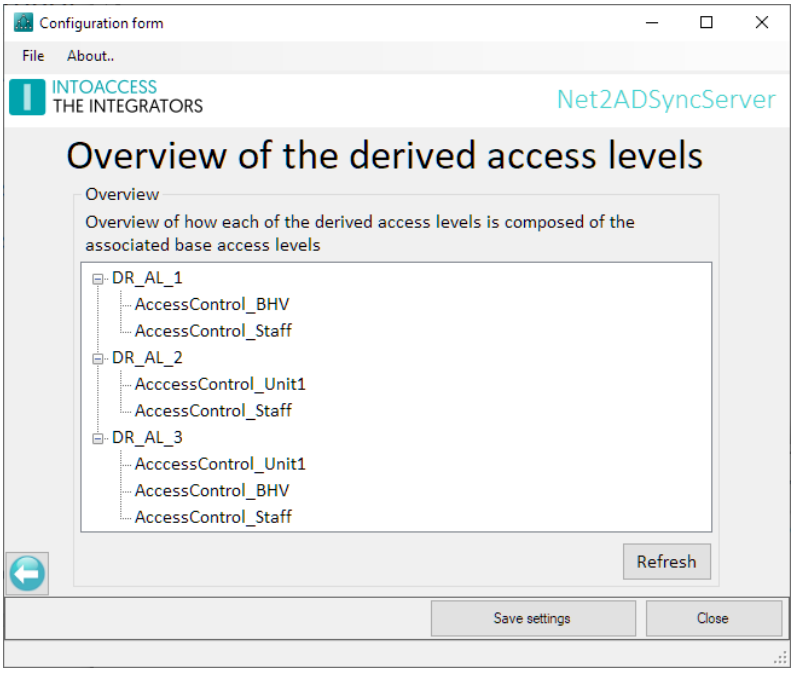

Image 34

Reactivate inactive users

On this page (See image 35) you can reactivate users who have become inactive. You check the checkbox behind the name of the user you want to reactivate. You then have the choice to link the user to a specific department or you leave the department on *Keep current department* to only reactivate the user. Then you click on the Reactivate button to reactivate the users.

This page is only shown when there are inactive users.

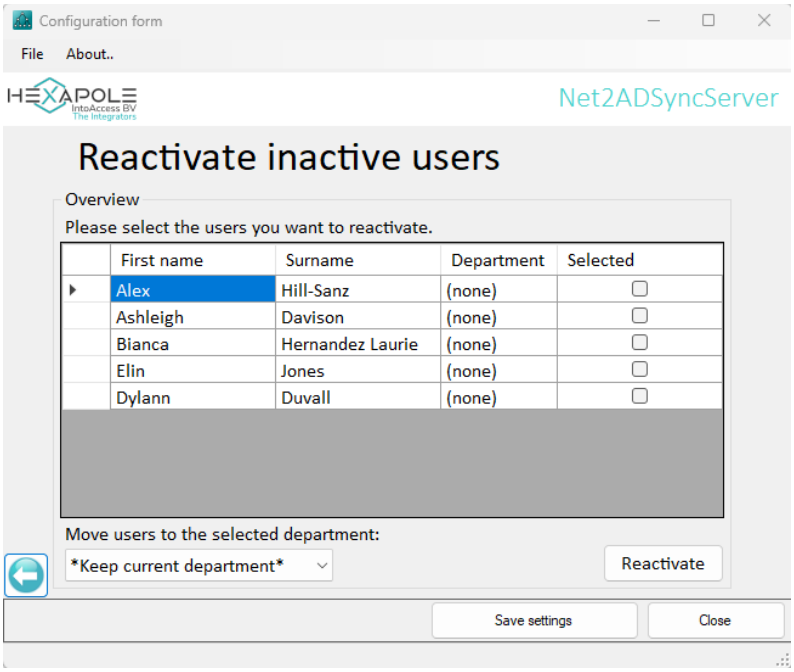

Image 35

HEXAPOLE
IntoAccess BV
The Integrators

Manual Net2ADSyncServer

Version 3.24