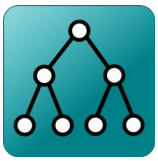
INTOACCESS
THE INTEGRATORS



Net2ADSyncServer

Manual Version 2.6

INTOACCESS B.V. THE INTEGRATORS
A.Hofmanweg 5A · 2031 BH · Haarlem · The Netherlands
info@intoaccess.com · www.intoaccess.com · +31(0)23 7505 138

Index

Installation and Configuration of the Net2ADSyncServer

**Warning: This application may not be compatible with Paxton version 5.03.4427 **

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

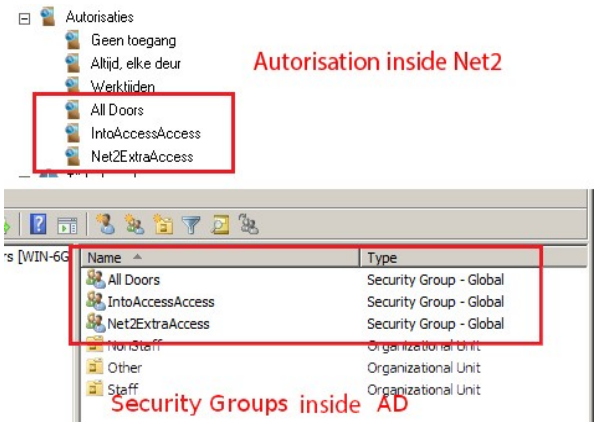
This application is designed from the basic idea that the management of all employees should be done solely on the Active Directory Server itself. At the first run of the SyncServer, all relevant information will be copied to the Net2 database. Any modifications performed afterwards on the AD will result 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 exempt 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

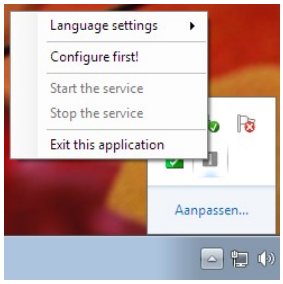
The Configuration of the Net2ADSyncServer application has to be done using the supplied 'Manager application' (Net2ADSyncService Manager). At start of this application, it will give a short notification and place it self in the system tray at the lower right corner of the taskbar. See image 2.

[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.

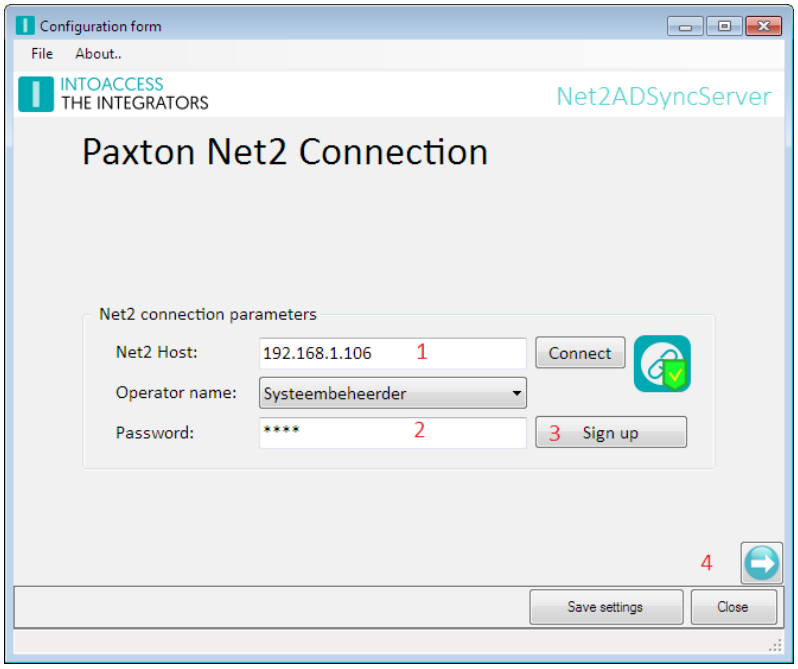


[Image 3]

The Net2 connection page

Purpose

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



[Image 4.]

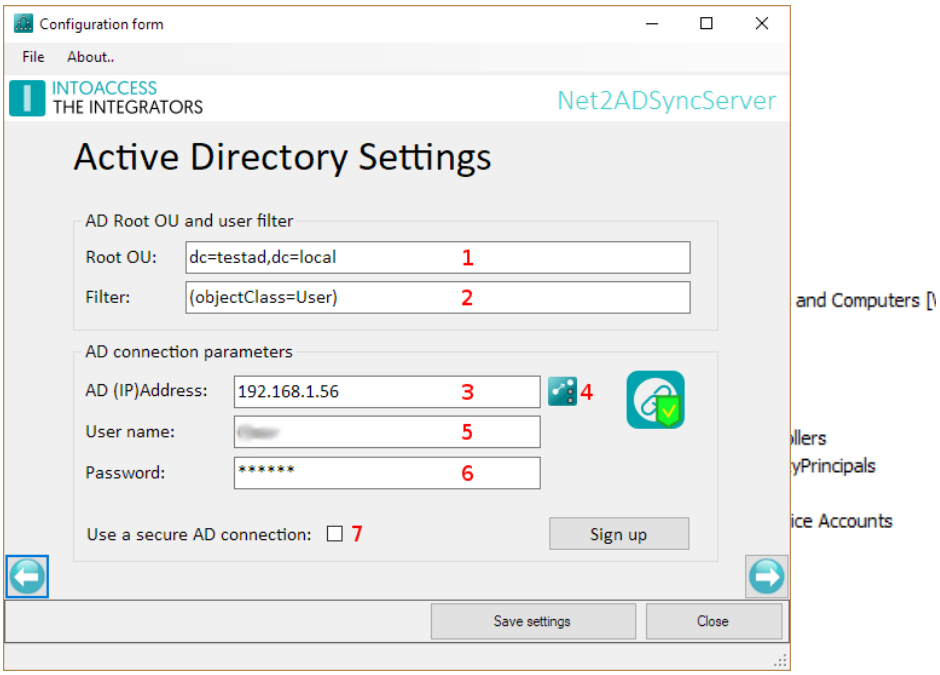
Input fields

- 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 suppling 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.

The Active Directory settings page

Purpose

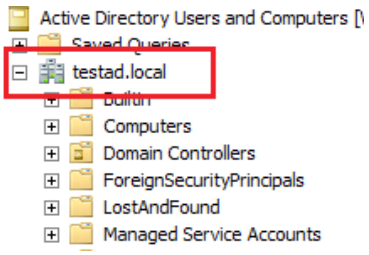
On this page, see image 5, the parameters for setting up a connection to the AD can be entered.



[Image 5]

Input fields

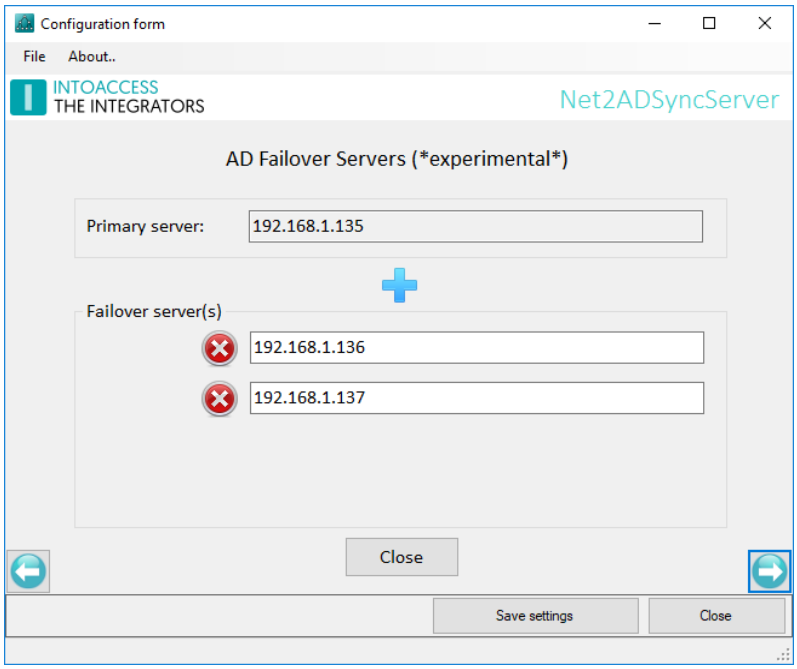
- First you will be asked for the 'Root OU' (1). This field should contain at least the full Domain Component (DC) of the AD from which the data is to be retrieved. The syntax as shown on image 5 complies with the AD settings as shown on image 6.



[Image 6]

  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 7. Note that this is an experimental feature.



[Image 7 (optional fail over)]

- 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.

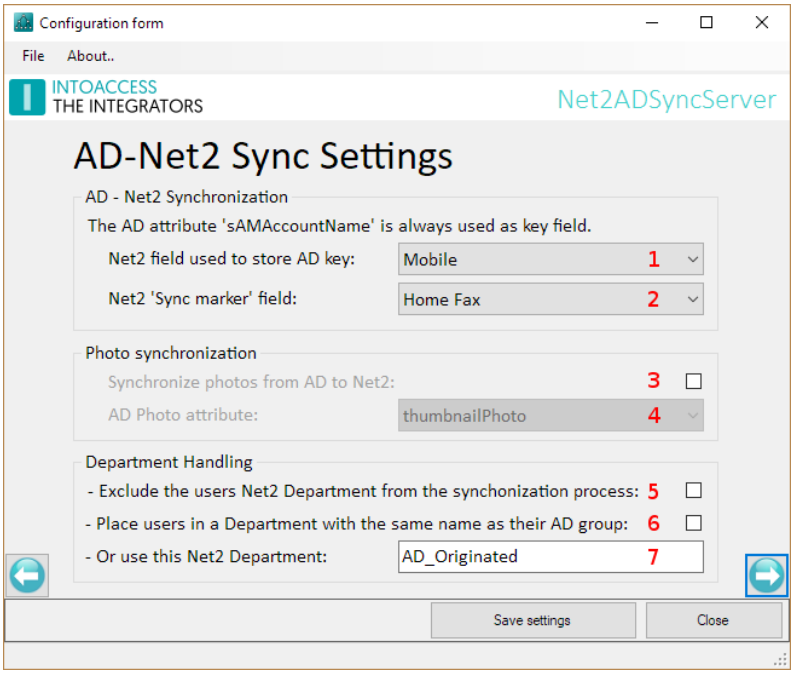
The AD-Net2 Sync Settings page

Purpose

On this page, see image 8, you're asked to provide some basic synchronization parameters.

The application will use the value of the AD attribute 'sAMAccountName' as 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 8]

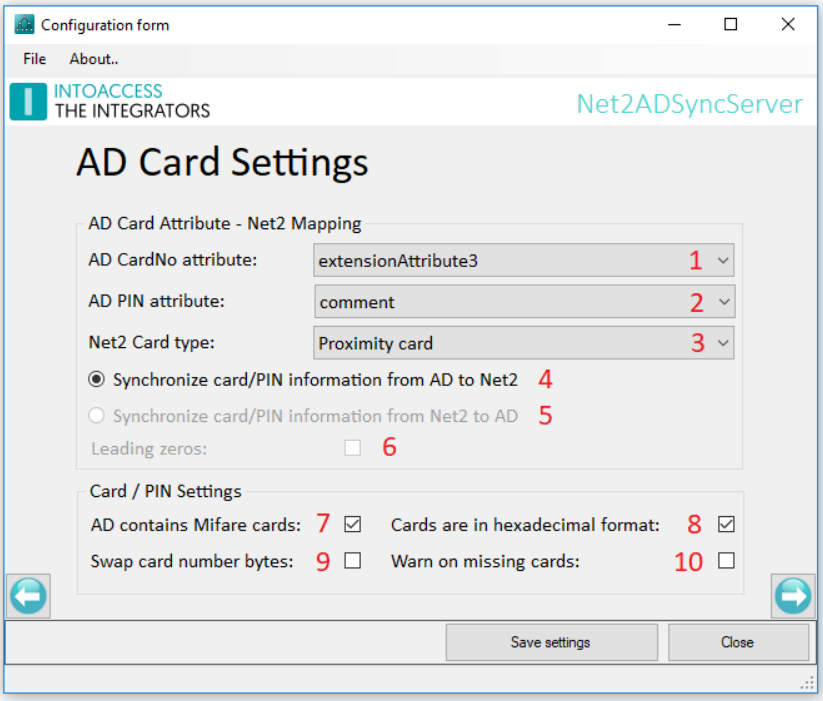
Input fields

- 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 holding the image 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.
- At (6/7) 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 specify a special department (7). This department will be created if it doesn't already exist.
  Synchronized users must always be placed in a department, it is not permitted to leave this field empty.

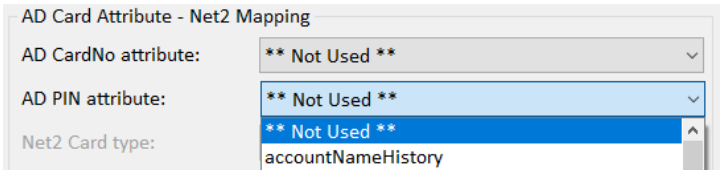
The AD card settings page

Purpose

On this page, see image 9, you can state whether you want to include Card/PIN information in the synchronization process. Since version 2.x, Card/PIN information can also be copied **to the AD** as well.



[Image 9]



[Image 10]

Input fields

- Choose at (1) the option '**Not Used**' , see image 10, if the AD doesn't hold card/PIN numbers and you have no plans to copy them to the AD either. In this case you may continue directly to the next page.
- Otherwise select at (1) the AD attribute that is used to store the card and/or PIN number.
- If a separate attribute is assigned for holding the PIN number, you can select that attribute at (2).
- Choose at (3) the card type in use, choose 'Unspecified' if the card type is unknown.

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 (8) 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 (9) if this is the case.

At (10) 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.

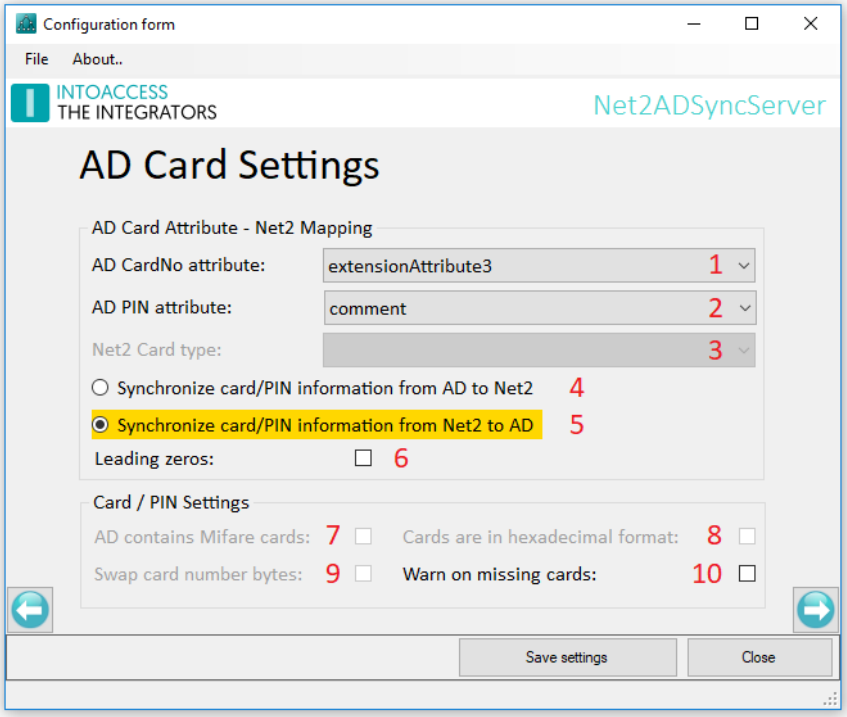
PIN numbers

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'. In case multiple cards/badges are used they need to be separated by either a comma, semicolon, space or 'TAB' character.

Synchronizing Card/PIN information to the AD

It is also possible to synchronize card and/or PIN information to the AD. See image 11. Select option (5) 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 (6). For example: card number 123 will appear as 00000123 in Active Directory.



[Image 11]

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:

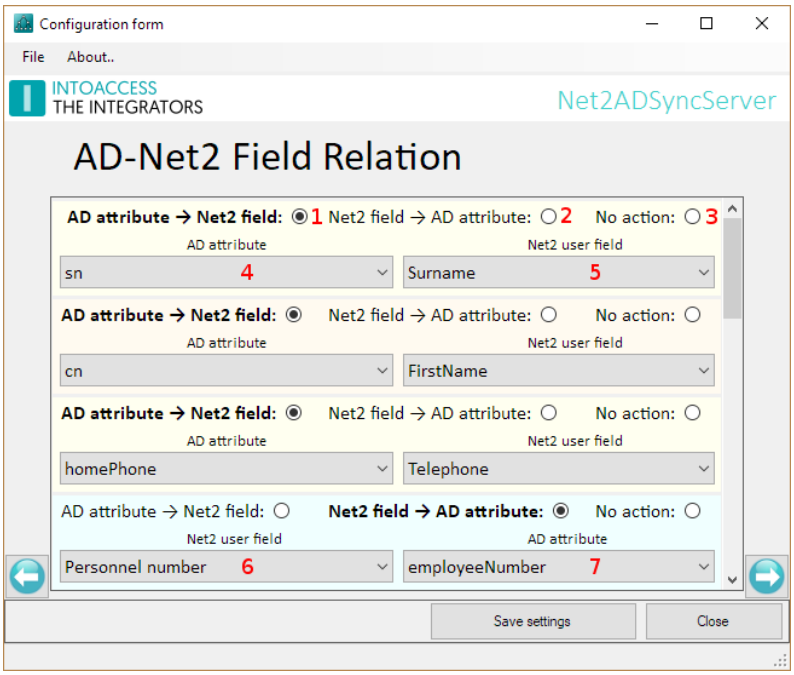
- *The Mifare card number is stored in (f.i.) the Net2 user field: 'Personnel number';*
- *The 'Personnel number' field is synchronized with AD attribute: 'extensionAttribute1';*
- *The same 'extensionAttribute1' is selected as 'AD cardNo attribute' on the 'AD Card Settings page';*
- *At the 'Card/PIN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

Purpose

This page, see image 12, offers the possibility to add multiple AD attributes to the synchronization process.



[Image 12]

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 in the 'AD-Net2 Sync Settings' page.

Input fields

- First select the 'source' or 'target' of the synchronization at (1) or (2).

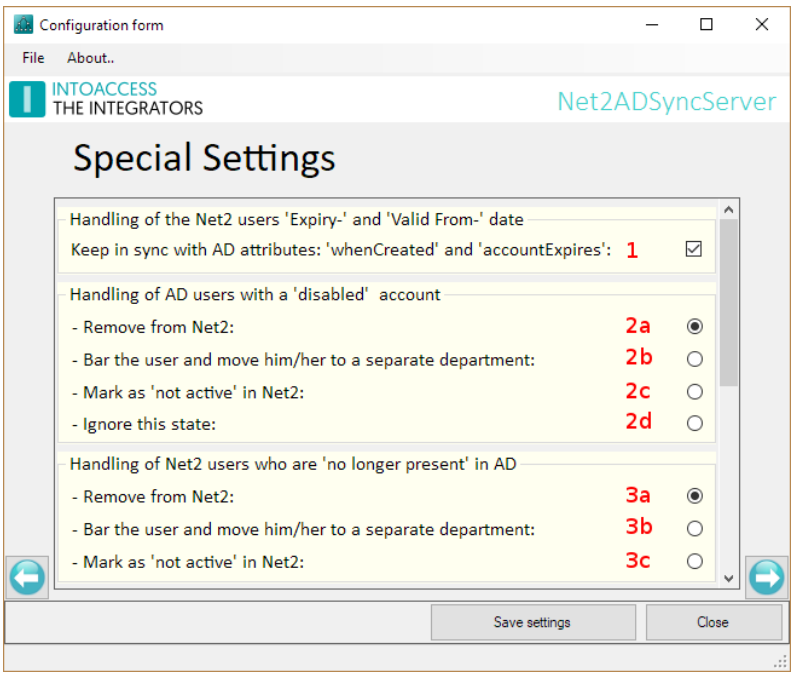
  The option (1) offers the possibility to synchronize an AD attribute with a Net2 user field **where the AD attribute is leading**.

  - 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.

Special Settings Page

Purpose

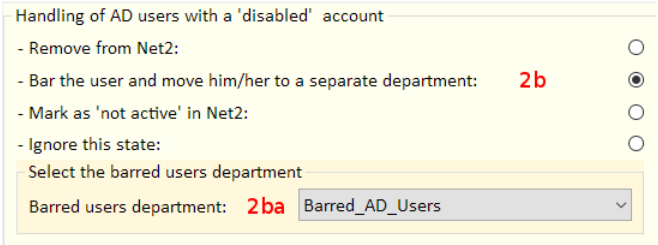
This page, see images 13..17, offers the possibility to apply a different value for some of the basic parameters. In most cases, except for the 'Utilize nested groups' option, the already set values will suffice, only in exceptional cases it might be desirable to set a different value here.



[Image 13]

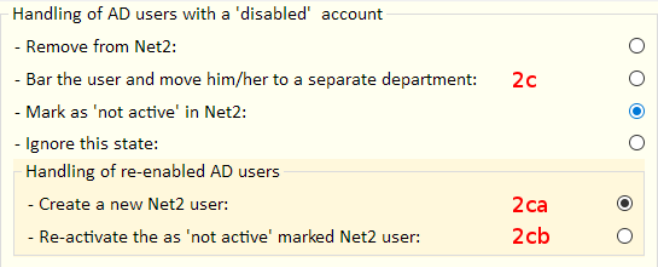
Input fields

- 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 (2x) 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) the Net2 user and move him/her to a separate department. When this option is selected the application will ask for the target department. See image 14.



[Image 14]

- 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 15

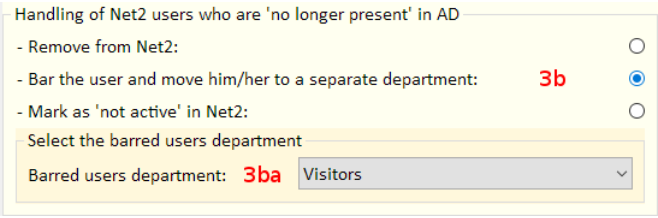


[Image 15]

  - 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 (3x) 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.

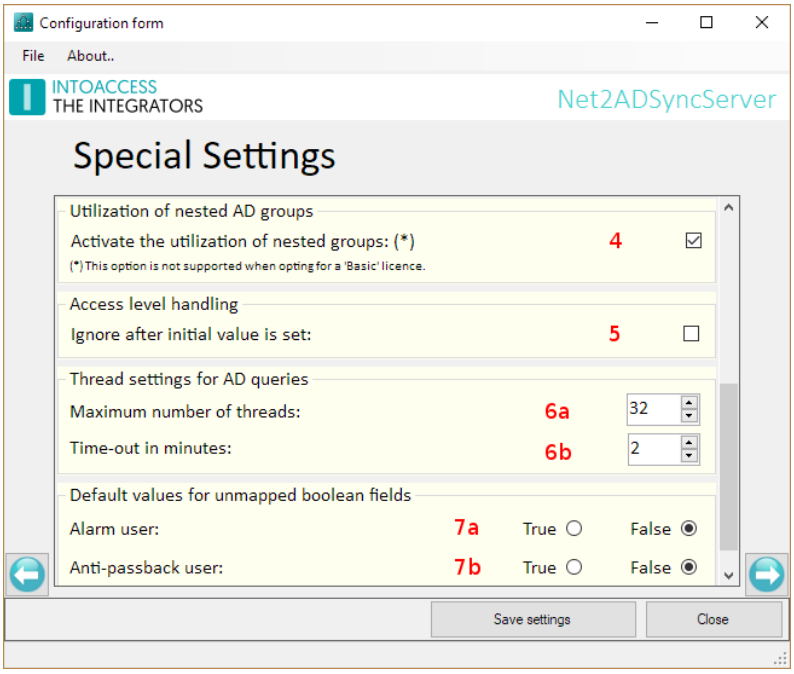
    The disadvantage of completely deleting a user is that the complete history of this user is deleted also.
  - The second option (3b) will bar (block) the user and move it to a separate department.
    - When this option is selected you'll be asked to select the target department. See image. 16



[Image 16]

  - Alternatively (3c) the user can be marked as 'inactive' in Net2 thereby saving the users history.
- At (4) See image 17. The utilization of 'nested security groups' can be activated. See page 16 for more information about this feature.
- Access levels can by 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.
- 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, for old machines for example, this can lead to certain problems. That's why you can tweak the settings at (6a) and (6b), to achieve an effective and solid performance for the application.

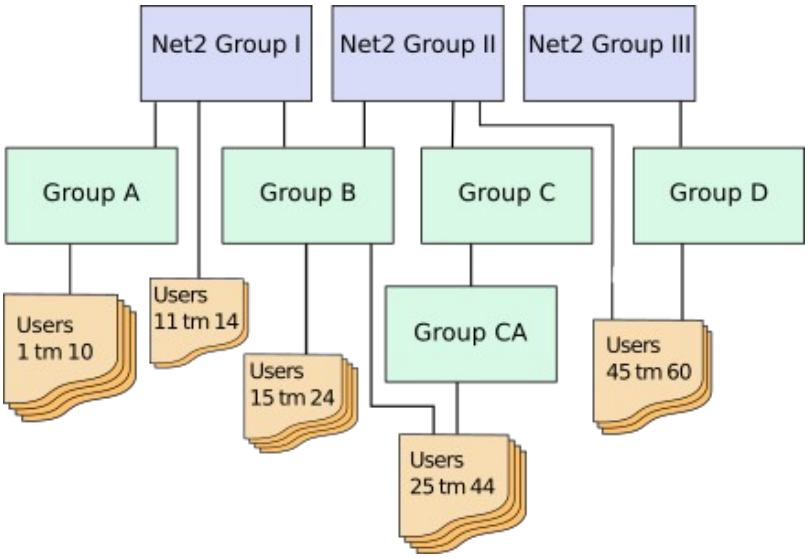
- If every user in Net2 should be able to arm/disarm the alarm system, or must obey anti-pass back rules, you can set the default value at (7a) and/or (7b). These settings will only work if no AD-fields are connected to these Net2 fields on the page 'AD-Net2 Field Relation'.



- [Image 17]

Nested security groups usage

See image 18.



[Image 18]

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.

Sync Timing Settings Page

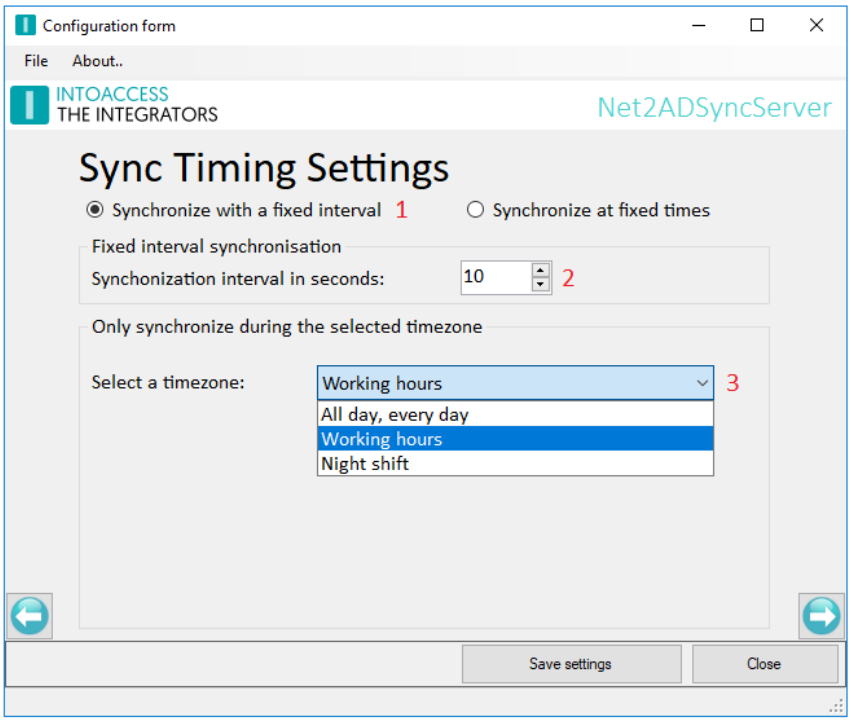
Purpose

This page, see images 19 and 20, 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.

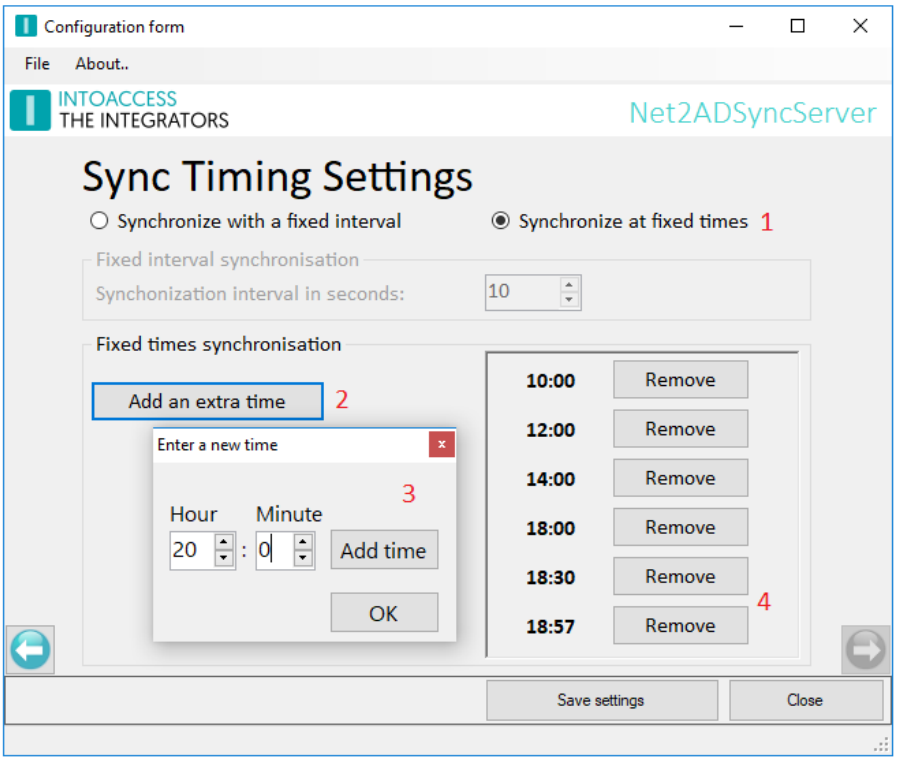
The synchronization will only be done during the selected timezone. This means that the interval will not trigger a synchronization cycle when the current time is not within the time of the selected timezone. The default timezone is the timezone that is active all day and every day. If a timezone doesn't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



[Image 19]

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).

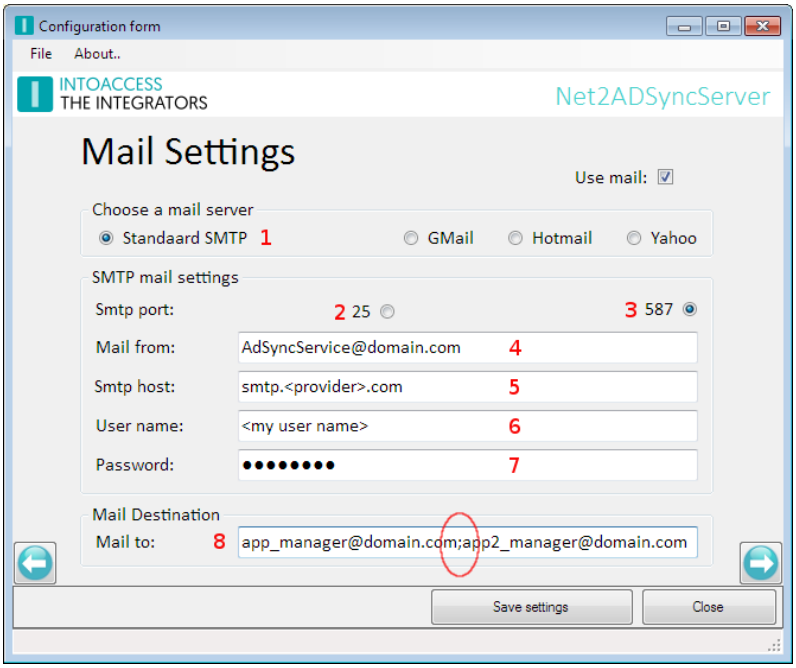


[Image 20]

The Mail settings page

Purpose

This page, see image 21, 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 will create a daily usage report as well containing all the modifications performed the last 24 hours.



[Image 21]

The application can utilize a SMTP server (1), or a Web mail account 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.

Some notes:

- There is no real difference in the settings between using webmail and a SMTP server using the STARTTLS protocol over port 587.
- Mail providers using the the SSL/TLS protocol 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.

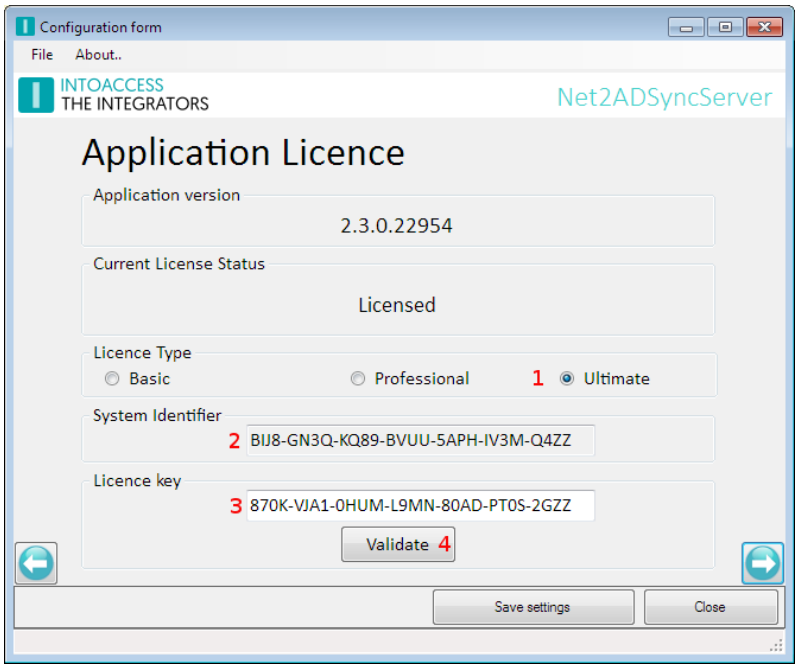
The Licence page

Purpose

This page, see image 22, 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 22]

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' as shown at (2) 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.

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 that apply to all personnel. 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. Paxton prohibits situation where the combination of desired Access levels would contain overlapping doors. This situation is solved by this application by creating a new Timezone for each of these overlapping doors if necessary.

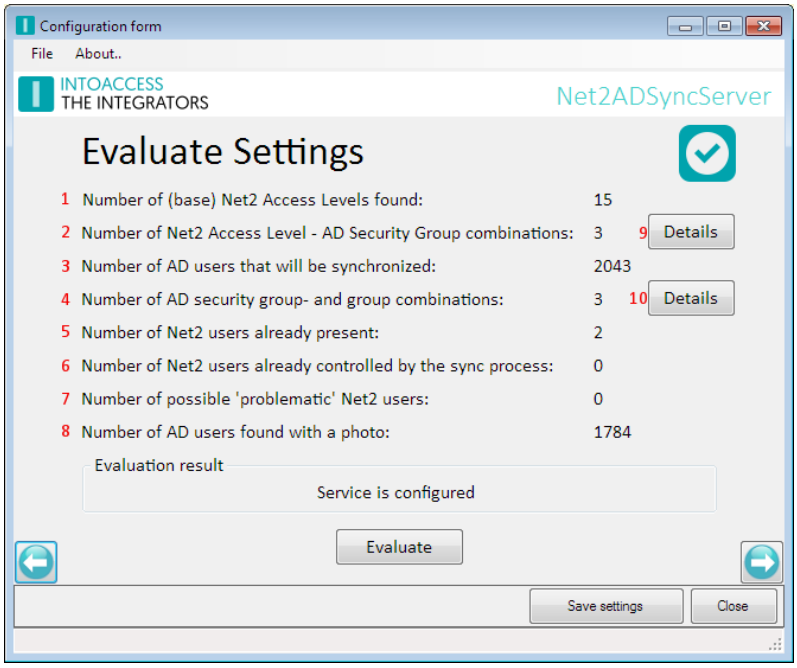
The only limiting factor that applies to this solution is the total number of Access levels which may not exceed 255. This number is imposed by Paxton.

The Evaluation page

Purpose

This page, see image 23, 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.



[Image 23]

The evaluation process

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.

- At (5) the total of users already present in Net2 are shown.

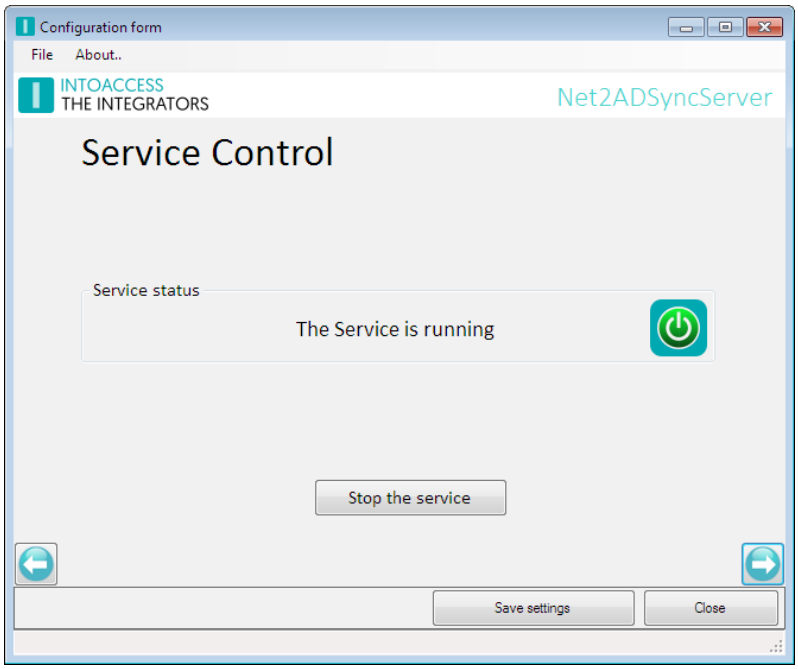
  Please note that already present Net2 users will **not** be handled by the synchronization process. In the situation where these users are present in AD also, you might end up in a situation where these users will appear twice in Net2. Even worse, the application won't be able to create card/badges for 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).
- Buttons (9) and (10) offers the possibility to show the underlying combinations in more detail.

The Service Control page

Purpose

This page, see image 24, offers the possibility to start- and stop- the actual service.



[Image 24]

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

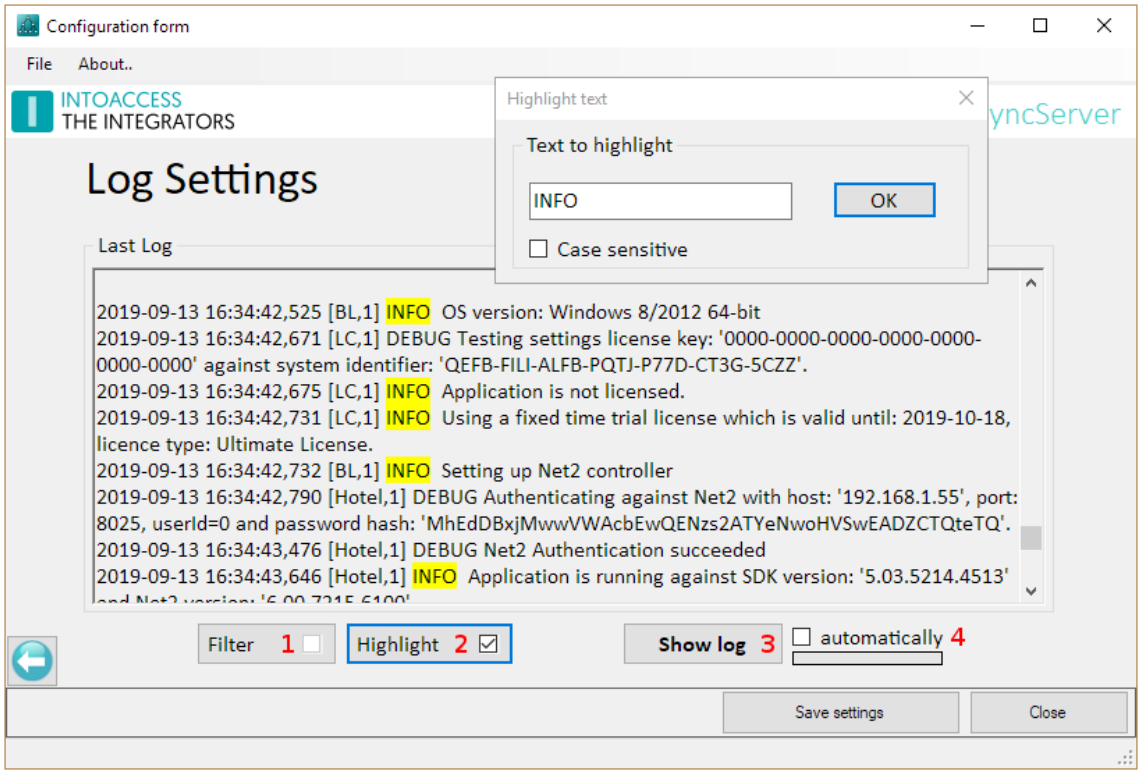
In rare cases the Service may refuse to start. If this happens to you please have a look at the end of the log-file to find out what might caused it. In case the reason is not obvious, please send all log files to info@intoaccess.com with a short description of what went wrong. The development team will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

The log settings page

Purpose

This page, see image 25, 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 25]

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\

INTOACCESS
THE INTEGRATORS

Manual Net2ADSyncServer

Version 2.6