



Net2AzureSyncServer

Manual 2.3

(October 26, 2026)

Index

Installation and Configuration of the Net2AzureSyncServer.....	3
Installation.....	3
Main principle.....	3
Synchronization rules.....	3
Configuration.....	5
The Net2 Connection page.....	6
The Azure Connections page.....	7
Input fields.....	7
API permissions in Azure.....	9
Card and user properties.....	10
Card / licence plate and PIN settings.....	12
Department source.....	14
Assignment of user attributes.....	15
Sync Timing Settings page.....	16
Synchronization using a fixed interval.....	16
Synchronization at fixed times.....	17
Special Settings page.....	18
Input fields.....	18
Photo Synchronization Settings page.....	21
Third Party Settings page.....	22
Network credentials.....	23
Sync timing.....	23
The Mail settings page.....	24
Standard SMTP.....	24
Azure/Entra.....	25
The Licence page.....	26
The Ultimate licence.....	27
The benefit of the Ultimate licence.....	27
Access level type deployment.....	28
The Service Control page.....	29
The Log Settings page.....	30



Installation and Configuration of the Net2AzureSyncServer

Installation

The Net2AzureSyncServer 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 the actual service. It can also be used to start and stop the service.

Since V2.0, the application is compatible with the **Net2 API interface** and no longer with the SDK interface that was dropped in Net2 v7. In order to activate the Net2 API, you can use the following manual, which also explains how to obtain a trial or regular product licence:

[Manual for setting up API compatible products](#)

Main principle

This application is designed from the basic idea that the management of all employees should be done solely within Azure. At the first run of the SyncServer, all relevant information will be copied to the Net2 database. Any modifications performed in Azure afterwards will result in an update action on the Net2 database.

Synchronization rules

The Net2AzureSyncServer application uses the following synchronization approach:

The application searches in Azure for all 'Groups' whose name match the name of an access level in Net2. (See Figure 1). Only those users who are member of one of those 'Groups' will be synchronized to Net2. They will be assigned the access level with the same name as their group^(*).

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



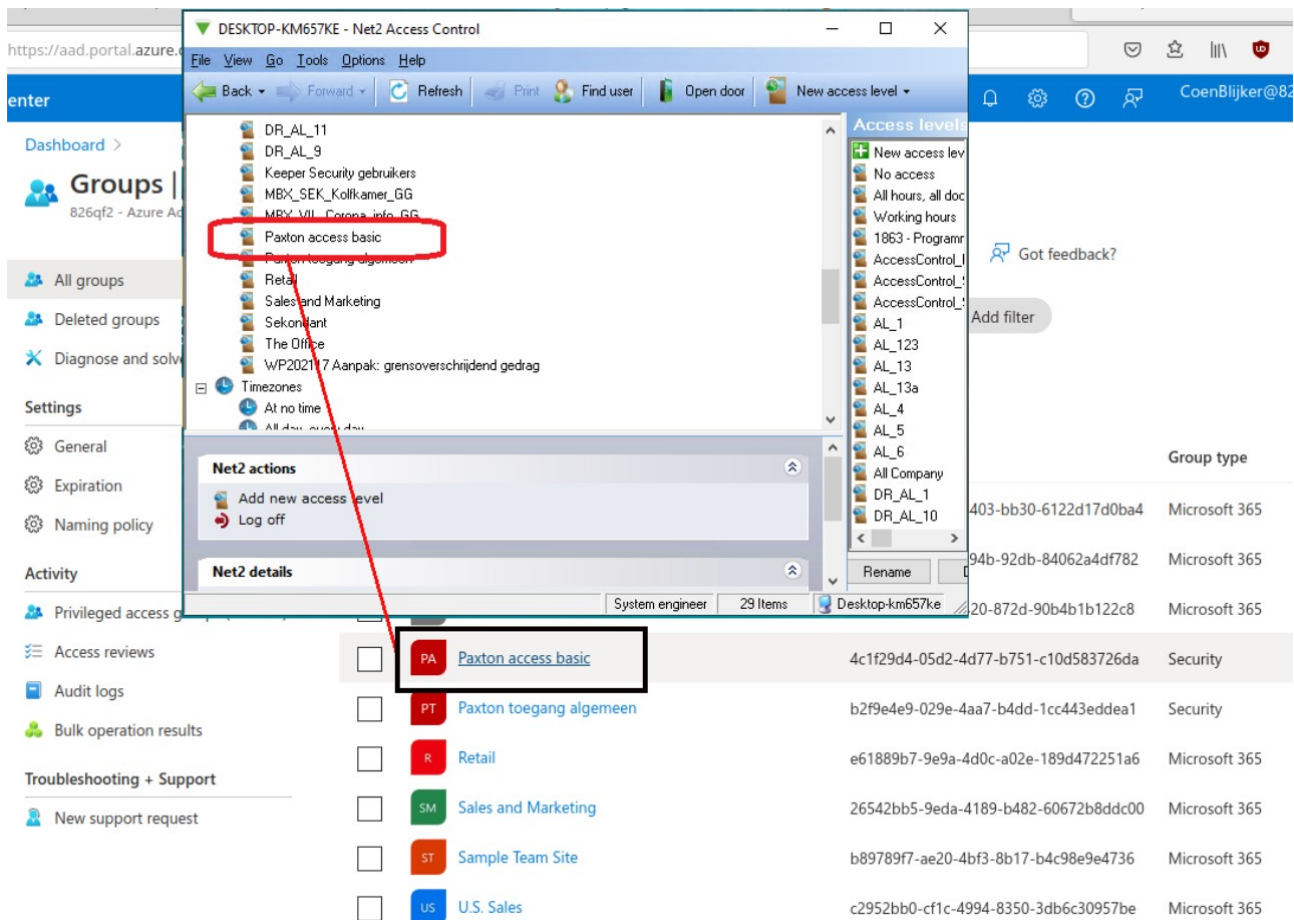


Figure 1

Furthermore, the following rules apply to the synchronization process:

- Azure users who are not member of at least one of the matching 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 when an evaluation is started because these users will end up twice in Net2 if they are present in Azure as well. 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 Azure to Net2. See the: “Card and user properties” page.



Configuration

The configuration of the Net2AzureSyncServer application has to be done using the supplied 'Manager application' (Net2AzureSyncService Manager). At the start of this application, it will give a short notification and place itself in the system tray at the lower right corner of the taskbar. (See Figure2)



Figure2

A right mouse click on the icon opens the main menu. (See Figure 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.

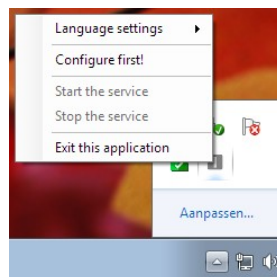
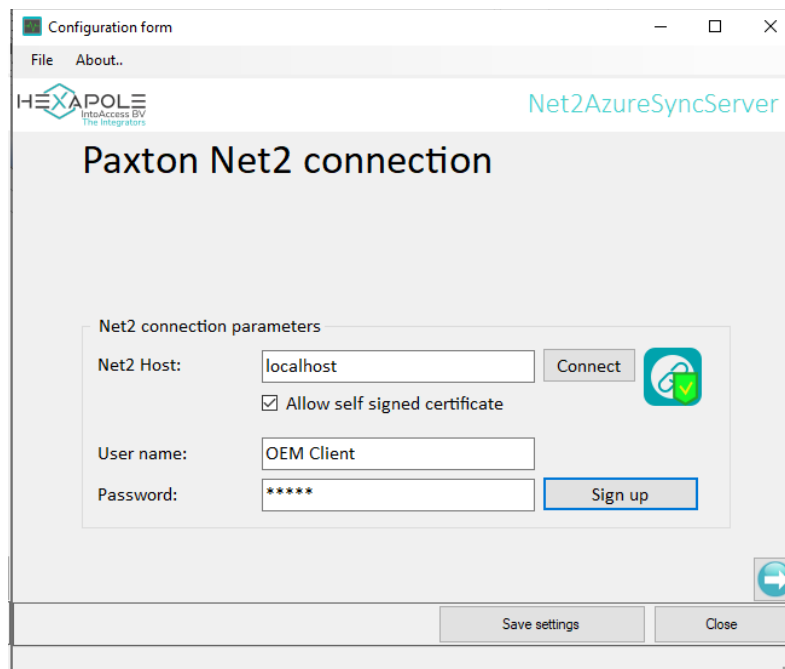


Figure 3

The Net2 Connection page

The first configuration page is for configuring the Net2 connection. When you start the configuration for the first time, this will require a few steps, but after the settings are saved, the next time it will connect automatically.



The screenshot shows a window titled "Configuration form" with a menu bar containing "File" and "About..". The main area has the HEXAPOLE logo and "Net2AzureSyncServer" text. Below this is the heading "Paxton Net2 connection". A section titled "Net2 connection parameters" contains the following fields and buttons:

- Net2 Host:** A text box containing "localhost" and a "Connect" button next to it.
- Allow self signed certificate:** A checked checkbox.
- User name:** A text box containing "OEM Client".
- Password:** A text box containing "*****" and a "Sign up" button next to it.

At the bottom right of the form is a blue arrow button pointing right. At the bottom of the window are "Save settings" and "Close" buttons.

Figure 4

- Enter the (IP)address of the Net2 server. If you have installed the attendance tool on the Net2 server, you can use the default 'localhost' value. Do not use an external adapter ip address in this case!!;
- Allow the use of a self signed certificate, when during the activation of the Net2 API not explicitly an official certificate (issued by a certificate authority) was used;
- Click the Connect button; if the connection succeeds you can enter the username and password;
- Enter an operator name with which you want the application to log on. This needs to be an operator with the "System engineer" role (you will find these accounts under "Net2 operators" in the Net2 application). We advise the use the '**OEM Client**', since it is not subject to MFA. If you have not enabled MFA, you can also use another user. 'The 'OEM Client' user is present by default on every Net2 system, but you will need to assign a known password to it.
- Enter the proper password;
- Click the Sign up button.

If all goes well, a message will appear that the connection was successful and the right hand arrow will change from gray to colored. After closing the success message, you can proceed to the next configuration window, by clicking on the right hand arrow.



The Azure Connections page

On this page, the authorization parameters for one, or more, tenants can be entered. (See Figure 5)

Figure 5

Input fields

- First you will be asked for the 'Domain name' (1) of your tenant.
- In the second field (2) you're asked for the 'Application client ID'. (See also Figure 6, showing where to find it in Azure)
- In the last (3) field you're asked for the 'Client secret'. (See also Figure 7, showing where to find it in Azure)
- Once this information is supplied this tenant information can be added to the tenant overview. (5) by pressing button (4)

The application will then try to make a connection with the supplied parameters. It will give a error message if this fails or some other problem occurs.

- If needed, connection information for more than one tenant can be added. The application will dynamically build separate configuration pages for each tenant supplied.

The 'Next Page button' will be enabled once the application is able to successfully sign up to Azure, using the supplied connection parameters.

Azure Active Directory admin center

Dashboard > 826qf2

826qf2 | App registrations

Azure Active Directory

Overview
Preview features
Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations**
- Identity Governance
- Application proxy
- Custom security attributes (Preview)
- Licenses

+ New registration | Endpoints | Troubleshooting | Refresh | Download

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications | **Owned applications** | Deleted applications

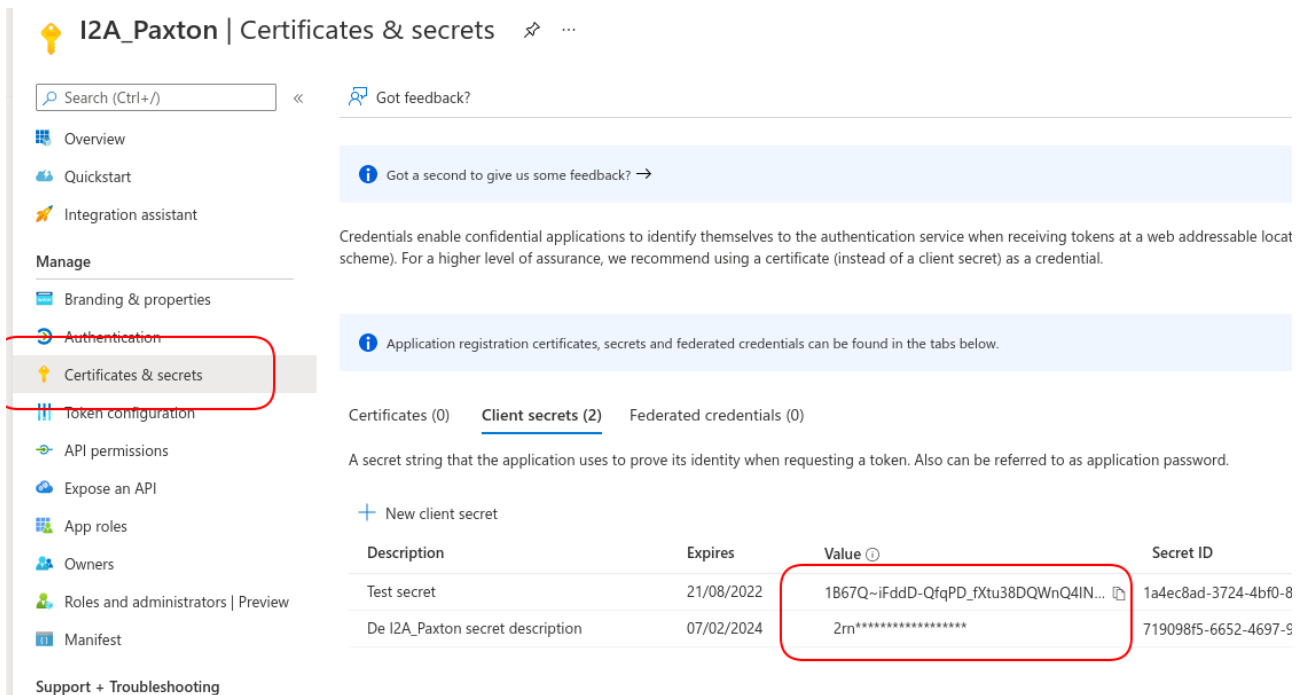
Start typing a display name to ... | Application (client) ID starts with | Add filters

1 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
I2A Paxton	eebcc7d3-bb90-418d-9306-...	07/02/2022	Current

Figure 6





I2A_Paxton | Certificates & secrets

Search (Ctrl+/) Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (2)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Test secret	21/08/2022	1B67Q~iFddD-QfqPD_fXtu38DQWnQ4IN...	1a4ec8ad-3724-4bf0-8
De I2A_Paxton secret description	07/02/2024	2m*****	719098f5-6652-4697-9

Figure 7

API permissions in Azure

Please note that the application needs the following Azure 'Application' type permissions:

Mandatory

- GroupMember.Read.All
- User.Read.All

Optional (set when you want to use application attribute extensions):

- Application.Read.All

Optional (set when you want to use custom security attributes)

- CustomSecAttributeDefinition.Read.All
- CustomSecAttributeAssignment.Read.All

Make sure that all permissions have been granted (have the green check mark).

Note that if you enable the Application.Read.All and you have a lot of applications, this can significantly increase the time it takes to read all available attribute options (when using the manager application).

Card and user properties

Once the setup of all tenants is ready, a new configuration page will become available for each tenant. (See Figure 8).

Figure 8

- A short evaluation of the current settings will be done after pressing button (1). (See Figure 9)
This evaluation is mandatory since version 1.19.0, it will reveal potential problems early on.

Group/Access level name	Number of members
All Company	2
ContainerGroup	2 / 9
Mark 8 Project Team	16
Paxton access basic	2
Paxton_Access_1	3
Sales and Marketing	12
U.S. Sales	10

Figure 9



- On the left side of this panel the name of the Azure group/Net2 access level combination is shown (1). The number of users found in that group is presented on the right side (2). When such a group contains other groups, the number of users found in these groups are also shown. (3)
- The users who are member of more than one group/access level combination are shown at (4). This number can only be more than '0' if opted for an Ultimate licence. Press the [i] (5) to see which users are involved. (see Figure 10)

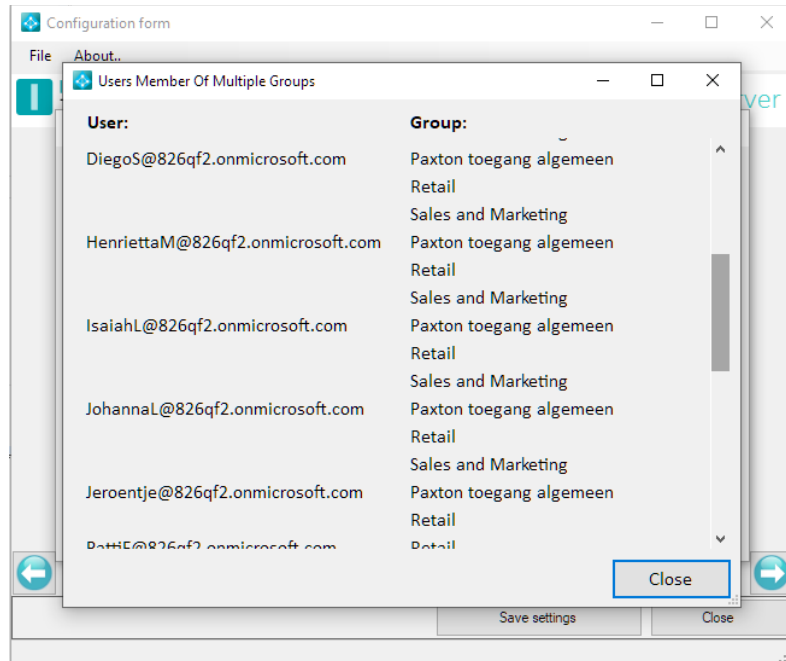


Figure 10

- An overview of all Azure groups found, will be displayed by pressing button (6). Please note that this list can be rather long. (See Figure 11)

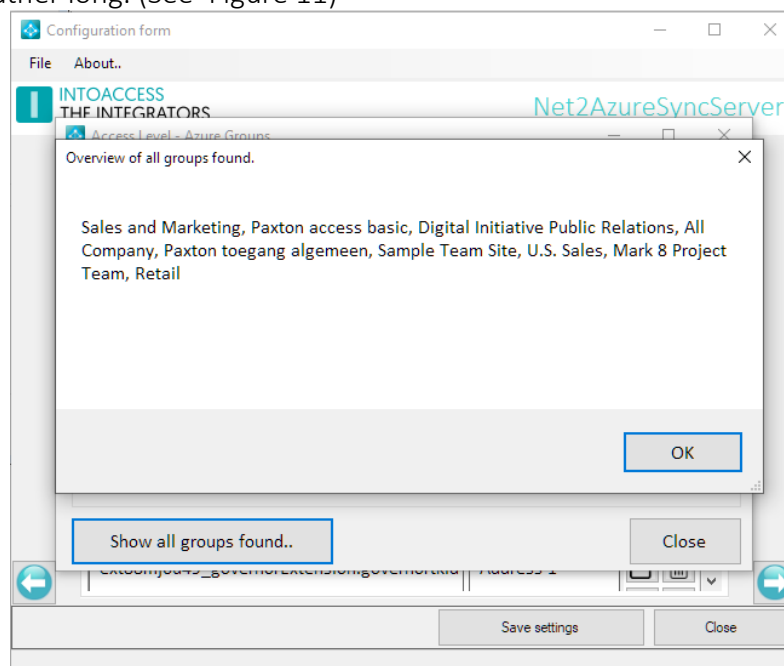


Figure 11



Card / licence plate and PIN settings

- At (2) the card information can be added. (See Figure 8)
After pressing the 'edit' button a new window will be opened. (See Figure 12)
(Leave all entries at '[not used]' if Azure doesn't hold any means of identification.)

Figure 12

At the top left of this window (1) the (default)card type (2) the application may expect to encounter in Azure can be configured.

Since version 1.22.0 it is allowed to also specify a card type in this field. This can be done using the following syntax: <n>#<card number>. For example: 3# 345689033 can be used to specify a keyfob with number '345689033'. It is permitted to specify a licenceplate in this field also!

If needed it is possible to enter multiple cards in this field. Separate the different numbers with a semicolon in this case. F.i. 1#87776676;7#87 XXP 32;8777672

Will create:

- a 'Proximity card' with number: 87776676
- a 'LicensePlate' with number: '87XXP32'



- a card with number: 8777672. This card will be assigned the default card type as stated at '2' in the image above.

The following cardtypes are supported:

- 0-> Unspecified
- 1-> ProximityCard
- 2-> ProximityISOCard
- 3-> Keyfob
- 4-> HandsfreeToken
- 5-> WatchProx
- 6-> ProximityISONoMagCard
- 7-> LicensePlate
- 8-> HandsfreeKeyCard
- 9-> FingerprintCard
- 10-> TelephoneNumber

You can ignore specific card types (3). Ignored card types cannot be used as default, the default card type cannot be ignored; Ignored card types can be set manually in Net2 and will be excluded from the sync process.

Shown on the right hand side, are all possible sources that can contain the actual card/(licence/pin information and are of the 'string' type:

- 'Extension attr. by application' will only be enabled when one or more 'applications' that expose their attributes are detected in Azure for which the permission must be set.
- 'User attribute' (6) will offer the standard Azure user attributes.
- 'Schema extension' (7) will offer attributes that come with a schema extension and will show at (8)
- 'Security Attribute Sets (9) group one or more attributes that will show at (10). As with the Application extensions, using Security attributes is optional and these will only show if the proper permissions are assigned.

Note that attributes that are already assigned, will no longer be available to assign again.

Press the appropriate 'set' (11) button to make the final selection. The choice made will be presented in one of the boxes on the lower left hand side. (12)

The origin of an optional licence plate and/or PIN code can be defined in a similar fashion.



Department source

- At (5) the way the users department name is determined can be set. (See Figure 8)
After pressing the edit button the a new window is presented in which the method for determining the department can be set. (See Figure 13)

Figure 13

The application offers three different options to determine the department name.

- A depart name can be used which has the same name as the users access level (1). This department name will be created by the application if it doesn't already exists. This method isn't advised when deploying an Ultimate licence as users may be member of multiple Azure groups in this case.
- The users can be placed in a fixed department (2). This is presumably an appropriate option when multiple tenants are to be synchronized to Net2. The desired department must be created in advance in this case though. A selection can be made from the list of existing departments shown at (6)
- The department name may be retrieved from an Azure attribute (3). Select the attribute holding the department name from one of the possible provided sources at the right side. In the example above the 'department' attribute is selected. Press the 'set' button to confirm this choice. The selected attribute will then be placed in the panel at the lower left (7).

Assignment of user attributes

- At (6) a selection can be made of Azure user attributes that must be synchronized to Net2.
(See Figure 14)

Figure 14

The Paxton user field can be selected on the left hand panel (1),
The connected source attribute can be selected from any of the three sources at the right hand panel. Both the Net2 field, as well as the Azure attribute, will be added to the overview (see Figure 8) when the 'Add' button (3) is pressed.

Press the 'Close' button when done.

Sync Timing Settings page

This page offers the possibility to let the application perform the synchronization either at a fixed interval or at fixed times. (See Figure 15 and Figure 16)

Synchronization using a fixed interval

When using a fixed interval (1), two fields can be configured. The actual interval time can be set at (3). The minimum interval time is 10 seconds. However, such a small interval time is only necessary in very exceptional cases. An interval time of around 300 seconds (5 minutes), or even more, will be sufficient in most cases.

The synchronization will only take place 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 selection list (4).

Figure 15

Synchronization at fixed times

When using fixed times (1), the option to add one or more time of day 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).

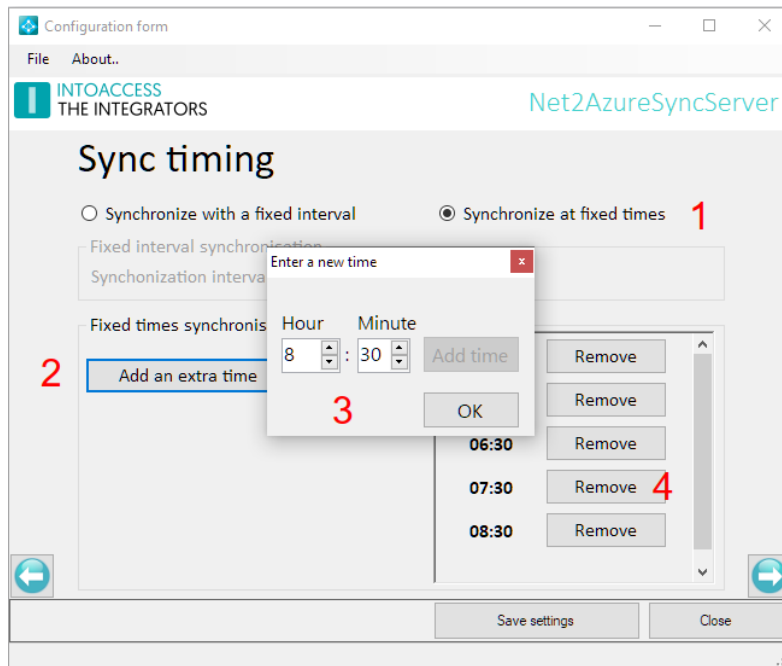


Figure 16

Special Settings page

This page offers the possibility to change the default behavior of the application (See Figure 17).

Configuration form

File About..

HEXAPOLE IntoAccess BV The Integrators

Net2AzureSyncServer

Special settings

Handling of Azure users with a 'disabled' account

Remove from Net2: **1a** ☒

Bar this user and move him/her to a separate department: **1b** ☐

Ignore this state: **1c** ☐

Handling of users who are no longer present in Azure:

Remove from Net2: **2a** ☒

Bar this user and move him/her to a separate department: **2b** ☐

Access level handling

Exclude the user's Access Level from the sync process: **3** ☐

Department handling

Exclude the user's department from the sync process: **4** ☐

Temporary Access Levels handling

Allow the employment of 'Temporary Access Levels': **5** ☐

Utilization of nested AD groups

Activate the utilization of nested groups: **6** ☐

Default values for unmapped boolean fields

Alarm user: **7a** True ☐ False ☒ Sync. initially only: ☐

Anti-passback user: **7b** True ☐ False ☒ Sync. enkel initieel: ☐

Save settings Close

Figure 17

Input fields

- At (1[x]) can be stated how the application should deal with users whose account are disabled in the Azure.
 - By default (1a) these users will be removed from the Net2 database.
 - The second option (1b) will bar (block) the user and move him/her to a separate department. When this option is selected the application will ask for the target department. (See Figure 18)



The screenshot shows a configuration window with two main sections. The first section, titled 'Handling of Azure users with a 'disabled' account', has three radio button options: 'Remove from Net2:', 'Bar this user and move him/her to a separate department:', and 'Ignore this state:'. The second section, titled 'Select the department for the barred users', contains a dropdown menu for 'Barred user department:' set to 'I2A' and a checkbox for 'Remove cards:' labeled '8a' which is checked. The third section, titled 'Handling of users who are no longer present in Azure:', has two radio button options: 'Remove from Net2:' and 'Bar this user and move him/her to a separate department:'. The fourth section, also titled 'Select the department for the barred users', contains a dropdown menu for 'Barred user department:' set to 'I2A' and a checkbox for 'Remove cards:' labeled '8b' which is checked.

Figure 18

- The third option (1c) will cause the application to completely ignore this state. In this case disabled users will retain their access rights in Net2.
- At (2[x]) can be specified how the application should deal with users who are 'no longer present' in Azure.
 - By default (2a) these users will be removed from the Paxton database.
 - The second option (2b) will bar (block) the user and move him/her to a separate department. When this option is selected you'll be asked to select the target department. This works the same as with 'disabled' users.
- At (3) the option is given to exempt access levels from the synchronization process. In this case a user will be given an access level only initially. The access level may then later be changed manually if needed.
- At (4) the option is given to exempt a users department from the synchronization process. This option will affect the 'barring' of a user. When this option is selected a barred user will NOT be placed in the barred user department but will be left untouched instead.
- At (5) it is possible to have the application respect manually assigned 'temporary access levels'. Normally the original access level is restored on the next synchronization cycle. However, the application will ignore temporary access levels if this option is set.
- At (6) Users who are member of a 'nested' group can be synchronized also. 'Nested groups' are groups that are it self member, direct or indirect, of one of the Net2 access level related groups.
- At (7) the default values can be set regarding the 'Alarm-' and 'Anti-passback user'. This is relevant if no Azure attributes have been designated that contain these values. These values can also be exempted from the synchronization process, allowing manual modifications. Note that when exempted (but mapped to an Azure attribute), the initial value assigned to a newly created user will be selected default and not the Azure value.
- At (8[x]) the option is given to remove cards for barred users. To ensures that no conflicts arise when reusing these cards.



When the remove cards option(s) are enabled, already barred users will not have their cards automatically removed. This only applies to users who are barred when this option(s) are enabled.

- Option (8a) to remove cards for barred users for disabled accounts
- Option (8b) to remove cards for barred users who are no longer present in azure.

To remove the cards of already barred users:

1. Stop the service.
2. In Net2, rename the current barred users department(s) so the department set in the Manager Settings no longer exists.
Example: rename it to "Old barred users".
3. Start the service.
4. The service will create a new barred users department and bar the required users again. The "Old barred users" department will be empty after the sync.
5. Delete the "Old barred users" department when it is empty.



Photo Synchronization Settings page

At this page, you can enable the photo synchronization from Azure to Net2. This is a function separate from the main/regular user synchronization. Since synchronizing photos can be time consuming, you can choose to configure it not to run as often as the regular user synchronization.

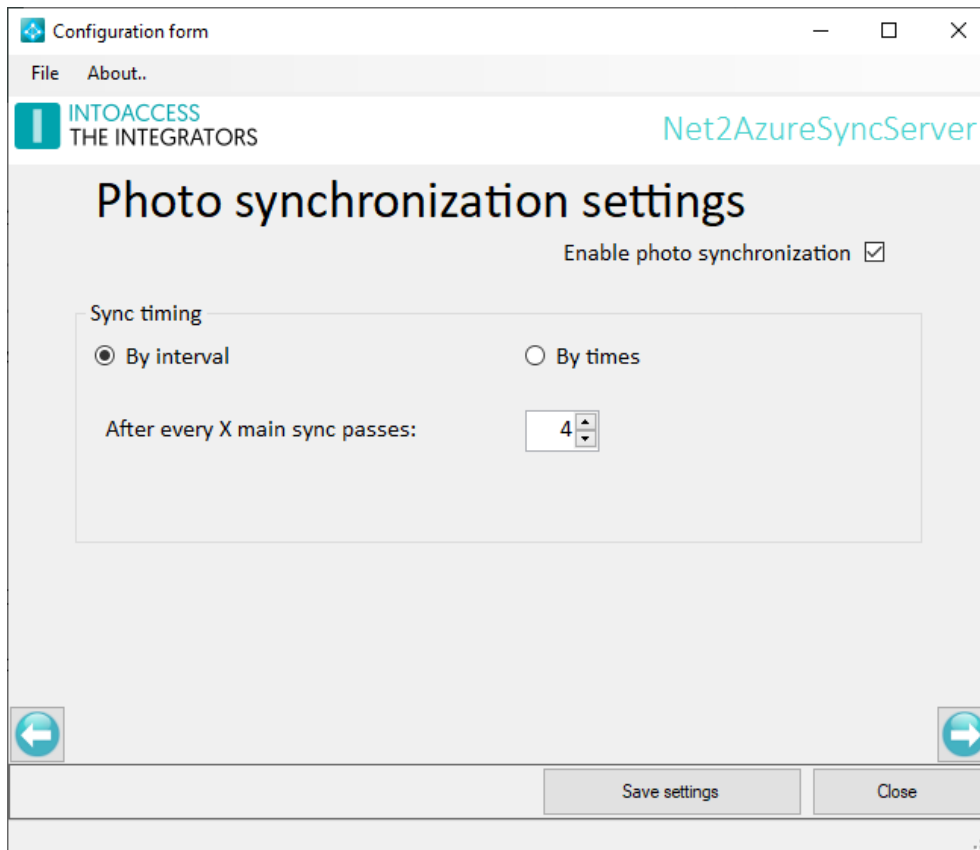


Figure 19

Options:

- By interval: If set to 1, the photo sync will be performed after every regular pass, if set to 2 it will skip every other pass and if set to 20, the photo sync will only be performed once in every 20 regular passes. Note that the counter that tracks this is non persistent (*) and the service will (upon startup) always start with an execution before starting to skip.
- By times: You can define one or more times in a day, after which the photo sync gets performed. Note that this will only set a (non persistent *) flag that a photo sync is required and does not do any scheduling itself. So, for example, if you have set your regular sync pass to run every 30 minutes, the actual photo sync may occur 30 minutes later than the time you configured.

(*) Non persistent: the current state of skip interval and the flag set for timed photo synchronization are kept in memory only, so if you restart the service it will not know of the state it had before the restart.

Third Party Settings page

This page offers the possibility to add execution of a third party application, after a regular sync pass has taken place (See Figure 20).

Configuration form

File About..

INTOACCESS THE INTEGRATORS Net2AzureSyncServer

Third party settings

Enable third party application execution ☒

Application

Executable: C:\Program Files (x86)\IntoAccess\Net2ImageSyn...

Parameters: -x "C:\Program Files (x86)\IntoAccess\Net2AzureSyncServer\Net2AzureSyncServer.exe.config" -p "\172.28.240.30\public\Images" -v

Network credentials (optional)

User: user

Password: *****

Domain:

Sync timing

☐ By interval ☒ By times

Add time

00:00	Remove
12:00	Remove

Save settings Close

Figure 20

You can select a third party executable (.exe, .bat, .cmd) by entering the full path manually or by clicking on the folder icon and browse for it. If the executable required parameters, you can add

those in the designated field. Note that you should double quotes to delimit any parameters that contain whitespace.

Network credentials

If the third party app requires credentials to access a network share or something else that needs authentication, you can optionally add a user, password and domain. Even if user and password are entered, you may leave the domain blank if it is not applicable. To use this (and other) settings in the third party application, you can either offer the XML config file path as a parameter (like in the example) or, if you only need the credentials, use the following place holders in the Parameters field:

- **#3rd_user#**: Third party user
- **#3rd_password#**: Third party user
- **#3rd_domain#**: Third party domain

Note that using credentials on a command line, is typically considered unsafe if non privileged parties have access to your server. Also note that credentials may not be needed at all, if the AD/Azure computer account is given access to the share. In that case, leave the credential fields blank.

Sync timing

The third party application will be executed **after** a regular sync pass. Since some third party applications require a lot of time (during which the regular sync is on hold), you may not want to execute it after every sync pass. You have two options to influence the third party execution frequency:

- By interval: If set to 1, the third party application will execute every pass, if set to 2 it will skip every other pass and if set to 20, the third party application will only execute once in every 20 sync passes. Note that the counter that tracks this is non persistent (*) and the service will (upon startup) always start with an execution before starting to skip.
- By times: You can define one or more times in a day, after which the third party application gets executed. Note that this will only set a (non persistent *) flag that execution is required and does not do any scheduling itself. So, for example, if you have set your regular sync pass to run every 30 minutes, the actual execution of the third party application may be 30 minutes later than the time you configured.

(*) Non persistent: the current state of skip interval and the flag set for timed execution are kept in memory only, so if you restart the service it will not know of the state it had before the restart.

Please note that any third party application should not do anything that confuses the functioning of the Net2AzureSyncServer. In the example of Figure 20 the Net2ImageSync application is called, which imports images from a directory/share into Net2, using a name for the image that matches a given Net2 user attribute value (that is synced from Azure). This should never be activated at the same time as synchronization from Azure images by the sync service (once that feature is offered), since these two would conflict.



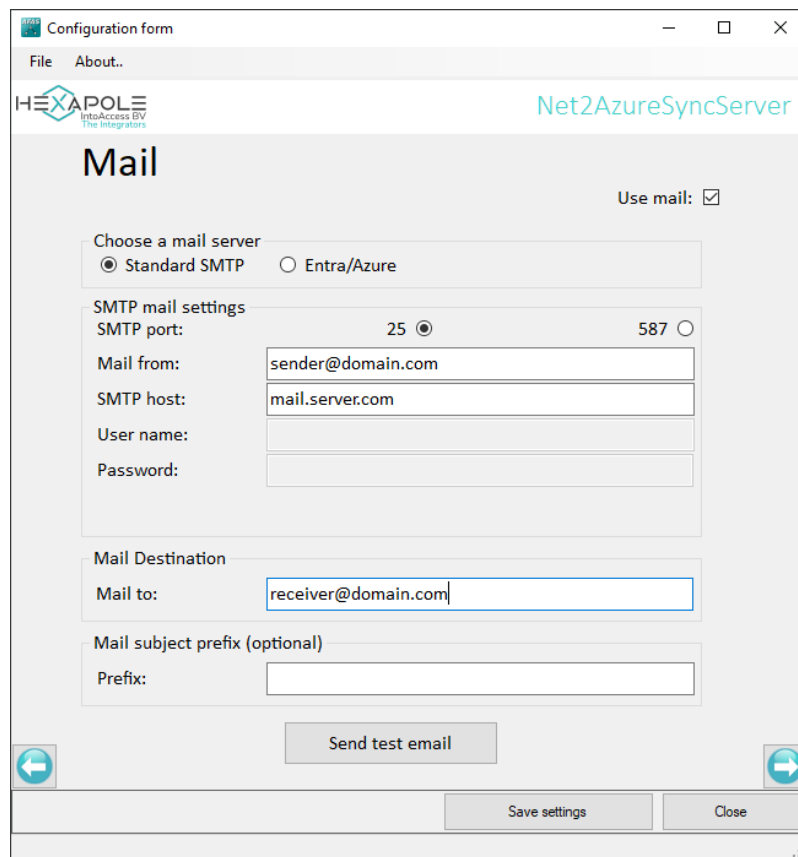
The Mail settings page

The email configuration is optional and offers the possibility to send application messages to anyone that needs to take action if the system malfunctions.

Standard SMTP

The SMTP settings allow you to configure which SMTP server and port to use. If you select port 587, authenticated SMTP is also possible by supplying credentials. You may consider using a (free) web mail provider like Hotmail, but note that such providers make it increasingly harder (or even impossible) to use SMTP via their servers.

SMTPS (port 465) is not supported.



The screenshot shows a web-based configuration form titled "Configuration form" for "Net2AzureSyncServer". The form is for "Mail" settings. It includes a "Use mail:" checkbox which is checked. Under "Choose a mail server", "Standard SMTP" is selected. The "SMTP mail settings" section includes "SMTP port:" with radio buttons for 25 (selected) and 587. Below this are input fields for "Mail from:" (sender@domain.com), "SMTP host:" (mail.server.com), "User name:", and "Password:". The "Mail Destination" section has a "Mail to:" field (receiver@domain.com) and a "Mail subject prefix (optional)" section with a "Prefix:" field. A "Send test email" button is located below the subject prefix field. At the bottom of the form are "Save settings" and "Close" buttons. The form also features a left arrow button and a right arrow button.

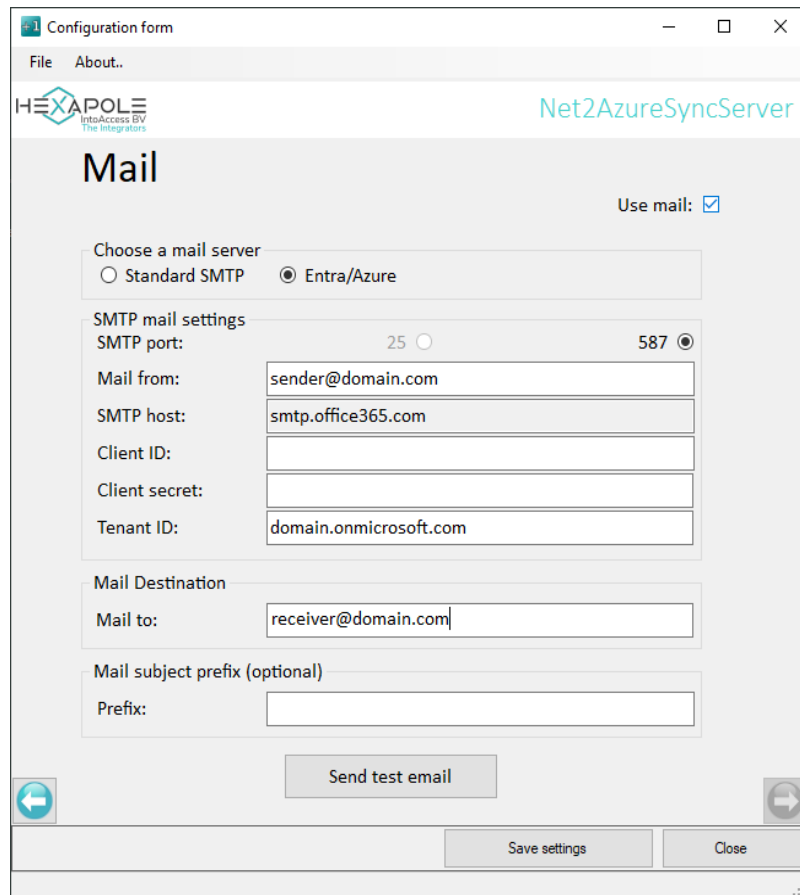
Image 21

To address multiple persons, additional email addresses can be added separated by a semi-colon (;).



Azure/Entra

It is possible to use SMTP with OAuth2 on Azure/Entra. For that to work properly, you need to create an App Registration and follow this manual: [Entra Manual](#).



The screenshot shows the 'Configuration form' window for 'Net2AzureSyncServer'. The 'Mail' section is active, with the 'Use mail' checkbox checked. Under 'Choose a mail server', 'Entra/Azure' is selected. The 'SMTP mail settings' section includes a port selector set to 587, and fields for 'Mail from' (sender@domain.com), 'SMTP host' (smtp.office365.com), 'Client ID', 'Client secret', and 'Tenant ID' (domain.onmicrosoft.com). The 'Mail Destination' section has a 'Mail to' field (receiver@domain.com) and an optional 'Mail subject prefix' field. A 'Send test email' button is located below these fields. At the bottom are 'Save settings' and 'Close' buttons.

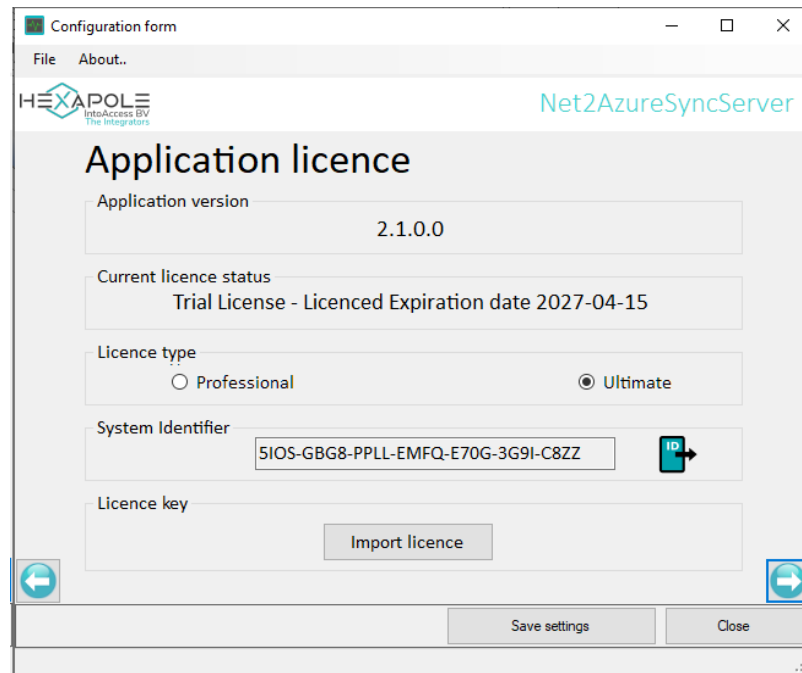
Image 22

The Azure Tenant ID may be provided in either domain format or as a GUID.

The Licence page

The software as it can be downloaded from the IntoAccess website, is fully functional but will not work without the API or (trial) product licence. In this manual, the procedure to follow is explained in more detail:

[Manual for setting up API compatible products](#)



The screenshot shows a window titled "Configuration form" with a menu bar containing "File" and "About..". The window displays the "Application licence" section for "Net2AzureSyncServer". The section includes the following fields and controls:

- Application version:** 2.1.0.0
- Current licence status:** Trial License - Licenced Expiration date 2027-04-15
- Licence type:** Radio buttons for "Professional" and "Ultimate" (selected).
- System Identifier:** 5IOS-GBG8-PPLL-EMFQ-E70G-3G9I-C8ZZ, with an "ID" icon to its right.
- Licence key:** A text input field with an "Import licence" button below it.

Navigation arrows are visible on the left and right sides of the form. At the bottom right, there are "Save settings" and "Close" buttons.

Figure 23



The Ultimate licence

The benefit of the Ultimate licence

As mentioned above the Ultimate version allows the use of multiple 'Azure Groups', to assign access rights in Net2.

An example of such a configuration is described 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.

Azure contains Groups with the (exact) same name.

All Azure users may now be assigned to the 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 additional access rights, for instance the rights as defined in the Net2 Access level 'Department A', can now be made member of that Group also. In this case the application will create a new Net2 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 time zone definition in case of overlapping doors. It will create a new time zone if needed.

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) and the total number of time zones (which may not exceed 64). These limits are imposed by Paxton.



Access level type deployment

New is the option to deploy 'individual' authorizations instead of the normal 'global' access levels.

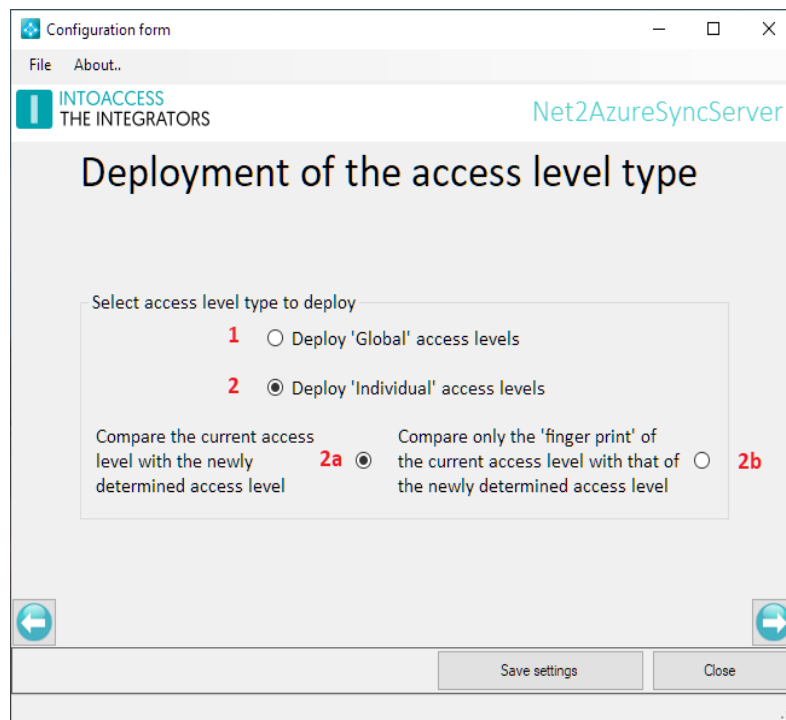


Figure 24

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.



The Service Control page

This page, see Figure 25, offers the possibility to start and stop the background service.

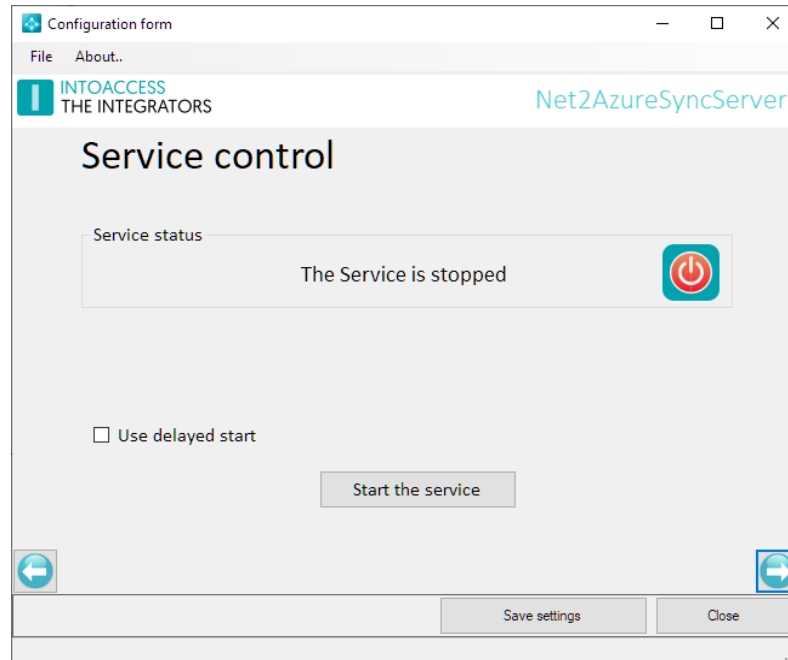


Figure 25

Other ways to start and stop the service are:

- Using the tray icon pop-up menu;
- Using the Windows service manager (look for “Net2AzureSyncServer”);

By default, the Net2AzureSyncServer has a service dependency on Nginx, in order to make sure that it will only start after Net2 is up and running. If this is inconvenient for you, you can select the Use delayed start option, which will remove the Nginx dependency and replace it by a ‘delayed’ service start. Note that you have to reboot the PC in order to have the service show up with a ‘delayed’ startup type in the Windows service manager.

Also note that this setting is only relevant when the service is running on the same PC as Net2.

The Log Settings page

This page, see Figure 26, 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.

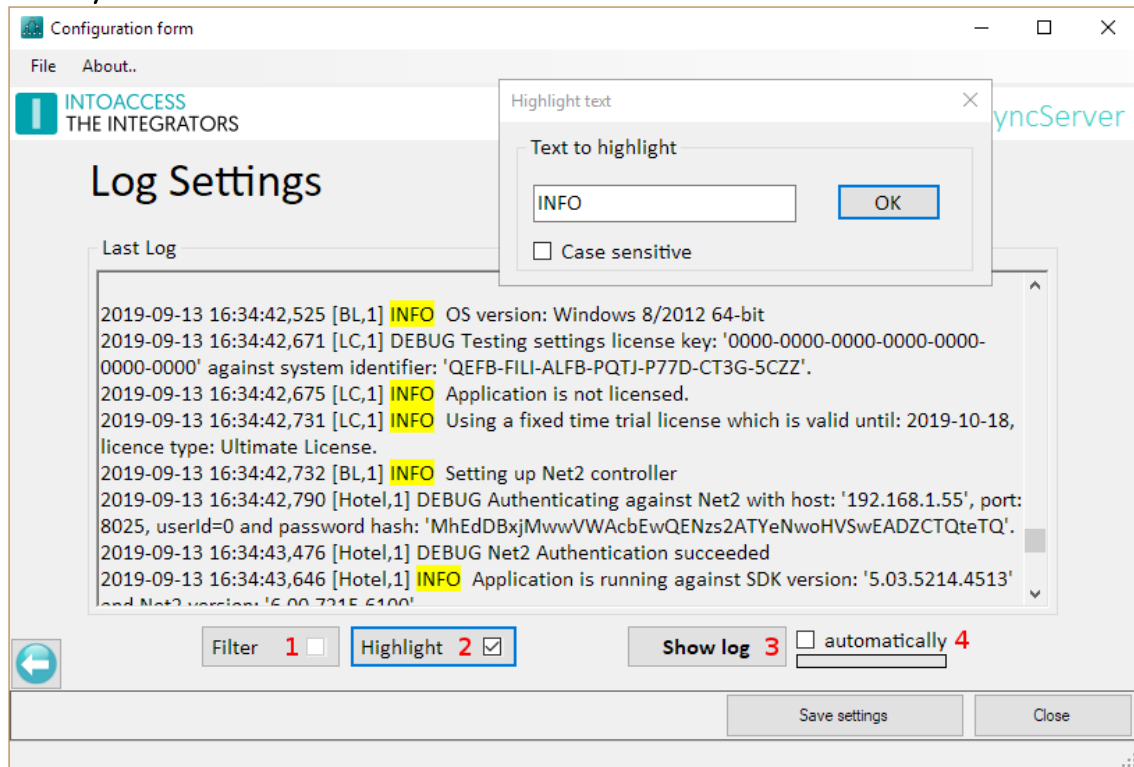


Figure 26

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\Net2AzureSyncServer\



Manual Net2AzureSyncServer

Version 2.3