

Net2MultiSyncServer

Manual 2.1

(October 26, 2026)

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

Table of contents

Principle....3
Blacklisting....3
Installation....5
Configuration....6
Net2 Connection....7
Net2 Child Connections....8
Sync Timing Settings page....10
Synchronization using a fixed interval....10
Synchronization at fixed times....11
Sync Settings....12
Mail Settings....14
SMTP....14
Azure/Entra....15
Application Licence....16
Service API settings....17
Service Control....18
Log Settings....19



Principle

The Net2MultiSyncServer allows you to synchronize users from one Net2 server (the master/main server) to one or more other Net2 servers (child servers). With this functionality, you can manage your users in one instance of Net2, instead of separately on all Net2 servers.

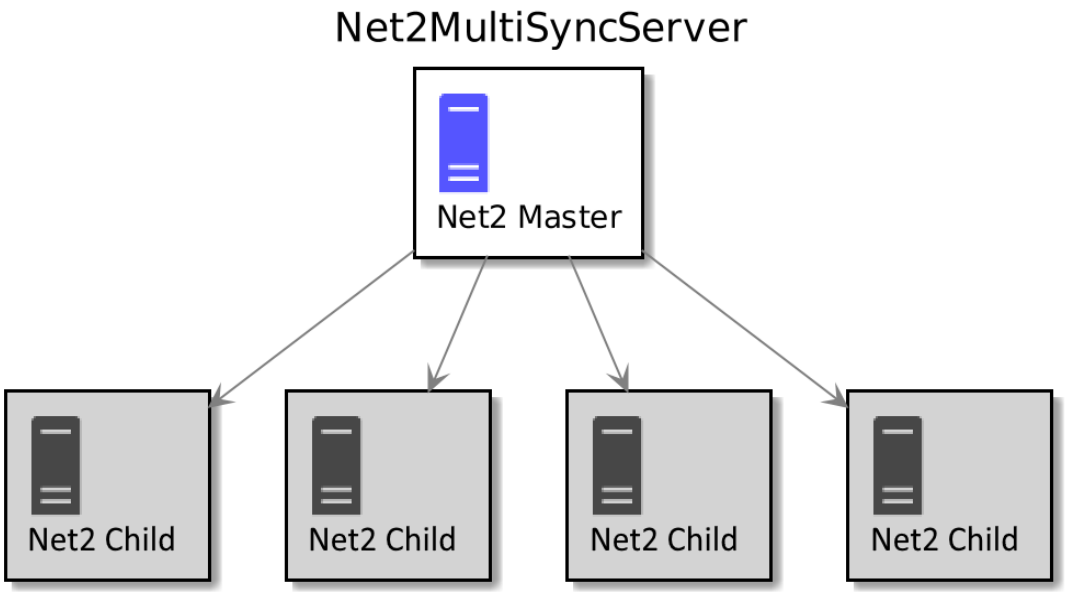


Image 1

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

If you have multiple buildings that use Net2 Access Control, and users need access to multiple buildings, maintaining your users in a single place will save time and will be less error prone. You just add a user to the main server and let the synchronization add the user to the child servers. Changes to a user in the main server will be synchronized towards the child servers. Changes made to a synchronized user in a child server, will be overridden by the main server. This allows control from one single location, with the flexibility of refining access control locally.

Blacklisting

Every time the service is trying to synchronize the master server with the child servers, the Net2 settings will be checked for equality. Not only settings are source of errors, but also other problems can make synchronization impossible for a server. If any errors are encountered, the child server will be put on a 'blacklist'. This server will be taken out of the synchronization process, so that other servers can still be synchronized. Once you have fixed the errors, and you have restarted the service

(an automatic reset of the blacklist is also possible), the blacklist will be reset. An error can be caused by the following:

- The Net2 settings on the master server are different then those on the child server. Settings that are of importance, are:
  - Language settings (needed for comparing access levels);
  - Enabled or disabled advanced permissions;
  - PIN length;
  - Duplicate PINs are (dis)allowed;
  - 50.000 user mode is enabled/disabled;
  - Security lockdown integration settings (optional).
- Access levels are present on the master server, but not on the child server;
- Advanced permissions cause a conflict on the child server.

The log files will show if any errors have occurred during the synchronization. We recommend that you make use of the e-mail functionality, which you can configure with the Manager application. When an error occurs, you will get an e-mail with details about the error. This way, you will know when an error occurs and what you have to do to solve it. If you don't use the e-mail functionality, you will have to check the log settings page on the Manager application.

As as a safety measure, for a rare incident where querying the master for users or access levels returns no results, the application will refuse to synchronize. This implies that **you should have at least 1 user record defined on the master, for the synchronization to work**. Note that this will automatically be the case for access levels.



Installation

The application can be installed, using a single setup file: **Net2MultiSyncServer.msi**

It is not mandatory to install the software on the Net2 server, but we advise you to do so in order to have the most robust configuration.

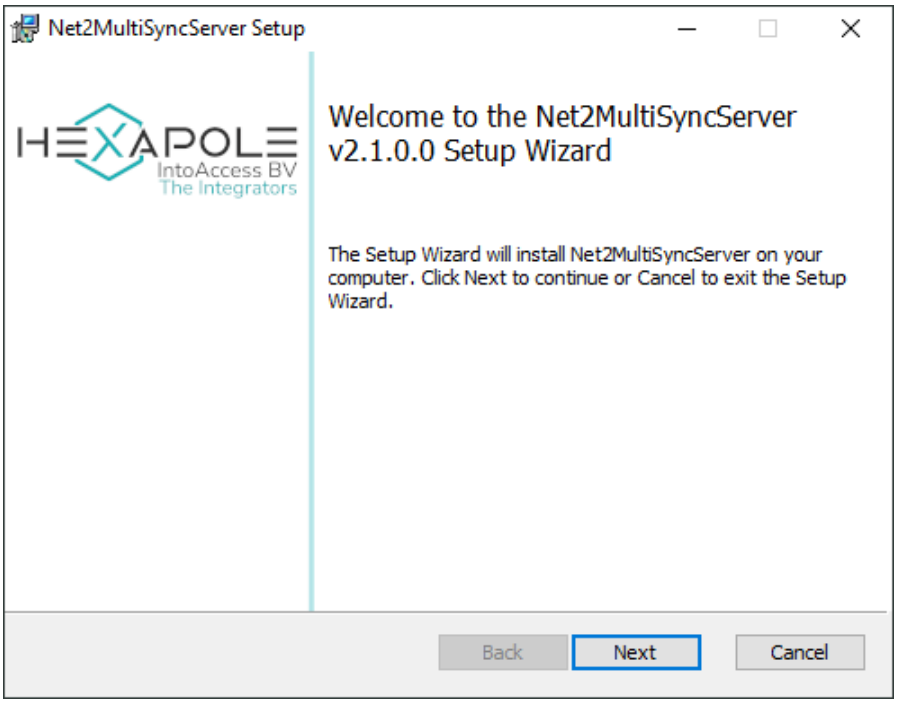


Image 2

Updates

Although a newer version should automatically replace any older version that may be present, you can choose to uninstall the existing version first. The configuration settings are not removed during this process, so after installing the new version, you do not have to configure everything all over again.

Configuration

To help with the configuration, the *Net2MultiSyncServer manager* application is available and allows you to configure:

- how the application should connect to Net2;
- how the service should be configured;
- if you require emails of application starts/stops/errors;

When the manager application is started, a splash screen is displayed for a short period. After that, the application will minimize to a 'tray icon' in the bottom right corner of the screen.

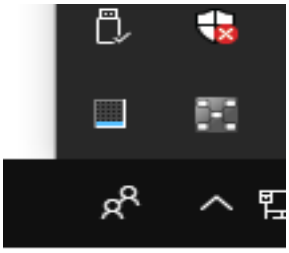


Image 3

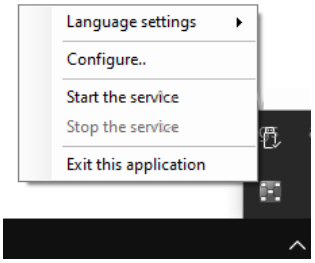


Image 4

By right clicking on the tray icon, the following pop-up menu will appear :

- Language settings: Pick your language;
- Configure (first): Start application configuration;
- Start the service: Start the service (allowed after configuration);
- Stop the service: Stop the service (allowed after configuration);
- Exit this application: Exit the manager application.

The color of the tray icon is indicative of the service state. When the service is not running, its color is gray. The icon gets colored when the service is running.

Net2 Connection

The first configuration page is for configuring the Net2 connection. This is the Net2 connection for the main server, which holds the data that will be synchronized towards the child servers. 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.

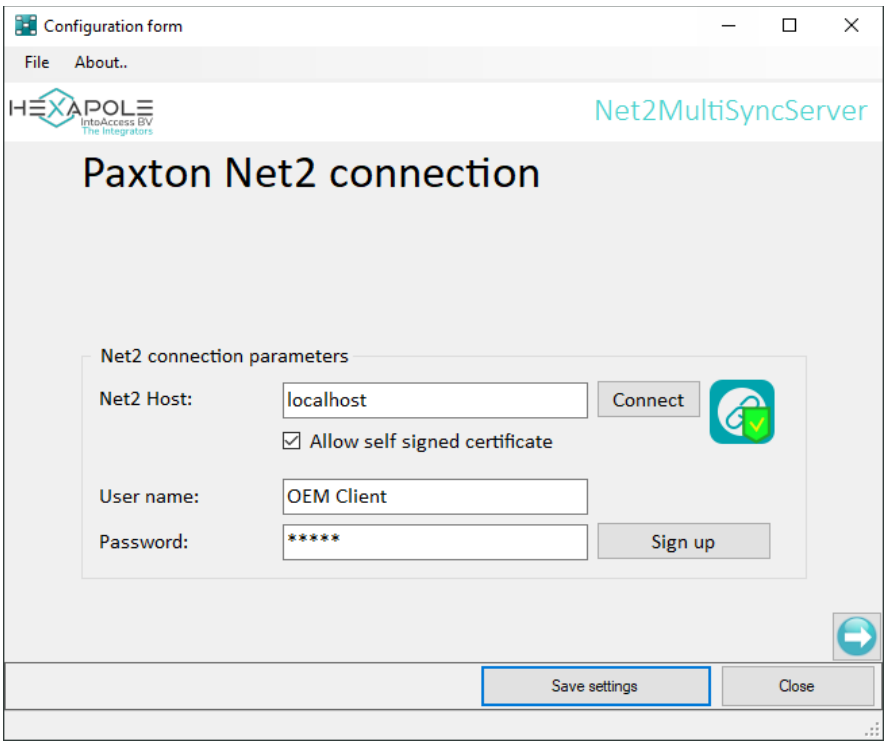


Image 5

- 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.

Net2 Child Connections

On this page, you can manage the Net2 child servers. The main server will synchronize its data to the servers that are configured here.

Use the 'New' button to configure a new server. After adding a server, it will appear in the list. You can use the 'Notes' field to store additional information about the server. Behind the notes field are three icons. The first icon allows you to edit the server configuration. The second icon is used to enable or disable the server. You can disable a server if it is causing issues while you still want to synchronize with the other servers. The last icon is used to remove a server from the list.

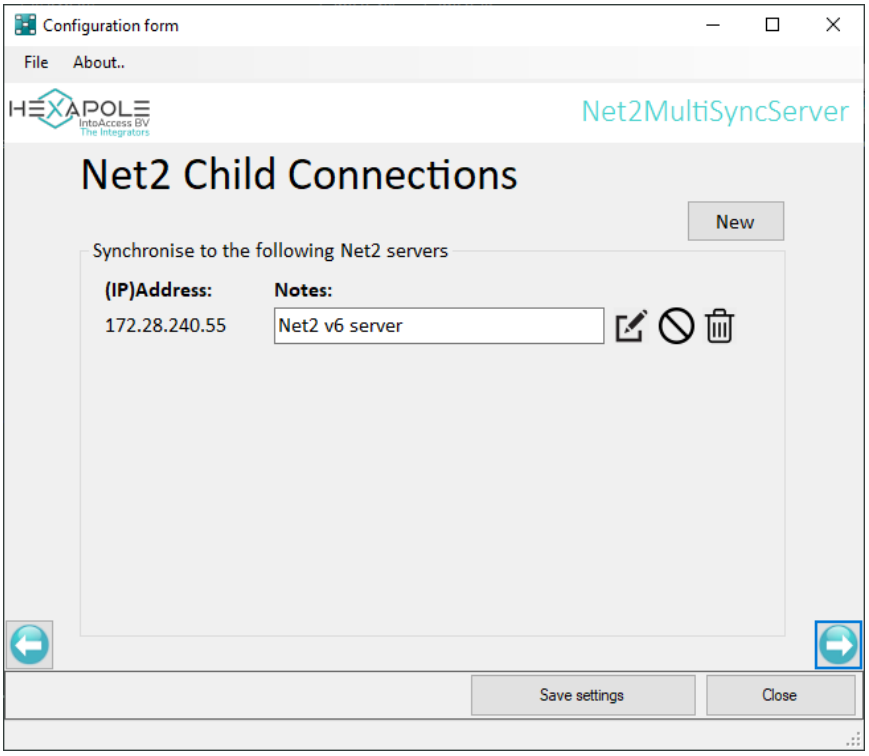


Image 6

Adding a child server is almost the same as configuring the connection to the main server. As a child server, it is possible to connect using either the SDK (v6.9 and below) or the API (v7+).

Please note: there is no default OEM Client account in the SDK versions. For this, you can use "system administrator" or a dedicated Net2 Operator account with system engineer rights.

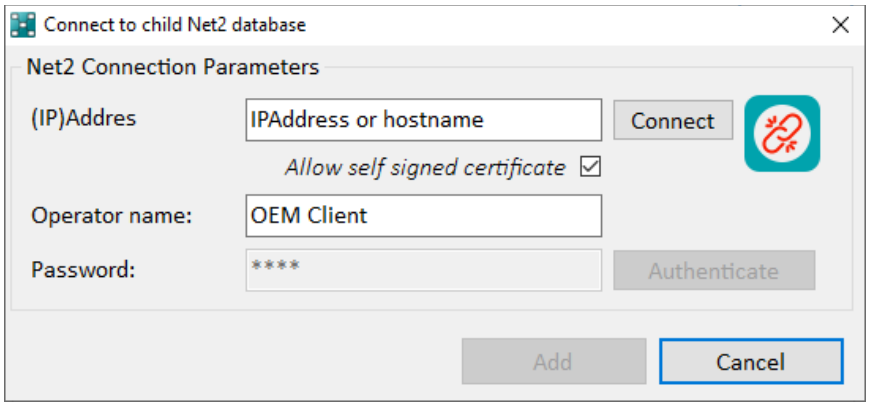


Image 7

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 8 and Figure 9)

Synchronization using a fixed interval

If you choose synchronization at a fixed interval, two fields can be entered. The actual interval time can be set here. The minimum interval time is 10 seconds; however, such a short interval is only necessary in very exceptional cases. A value of 300 seconds (5 min), or even higher, is more than sufficient in most cases.
In this case, synchronization will only take place during the selected schedule. Synchronization will therefore not take place outside of that schedule. The default schedule is the schedule that applies to all days. Schedules without times are not shown in the list.

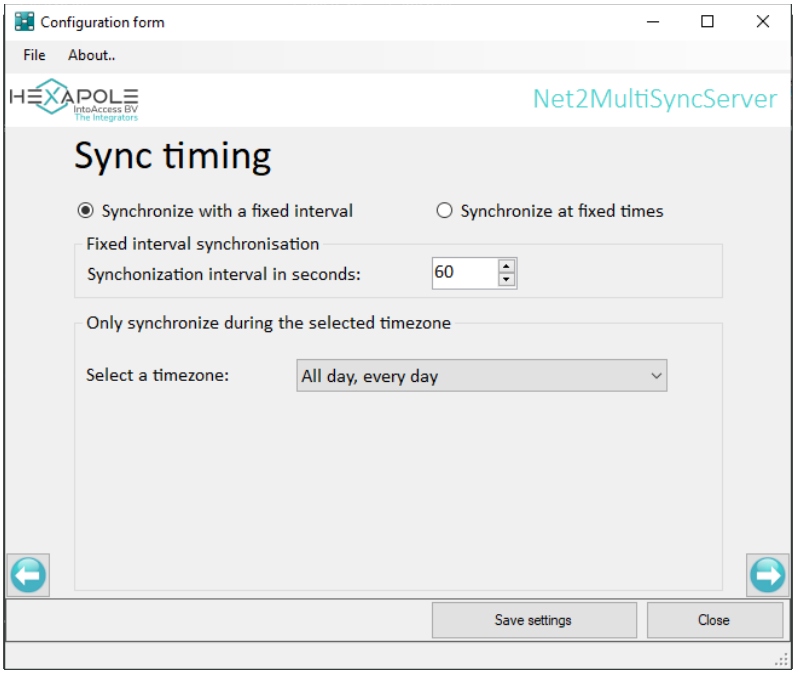


Figure 8

Synchronization at fixed times

If you choose daily synchronization at fixed times, the option to add one or more times is enabled. Clicking this button opens a new window, 'Enter a new time'. With this window open, you can enter multiple times by clicking the 'Add' button. Times that have already been entered can be removed by clicking the corresponding 'Remove' button.
With this setting, the application will perform a single synchronization pass at the specified times.

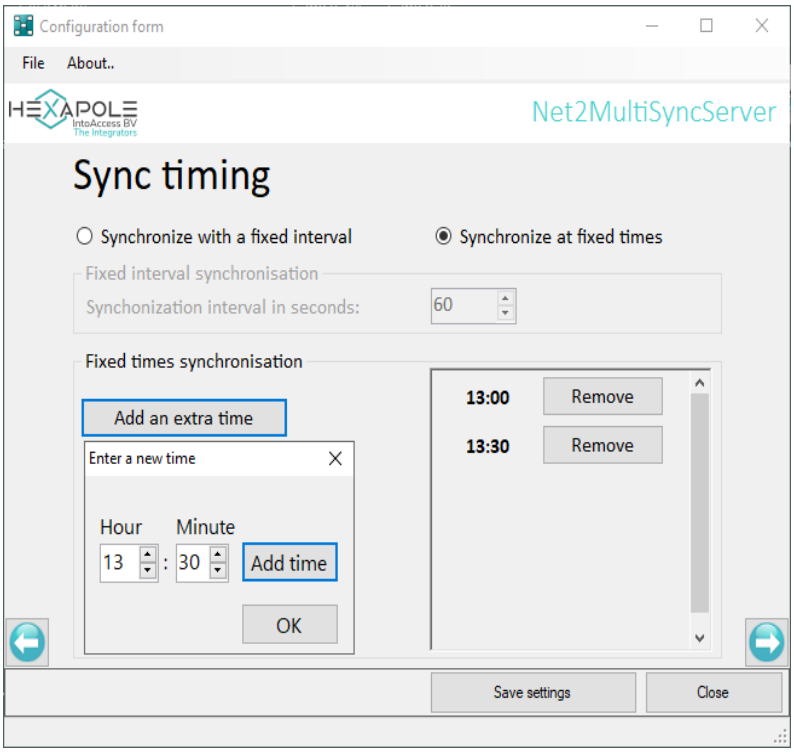


Figure 9

Sync Settings

There are multiple options that you can configure for the synchronization.

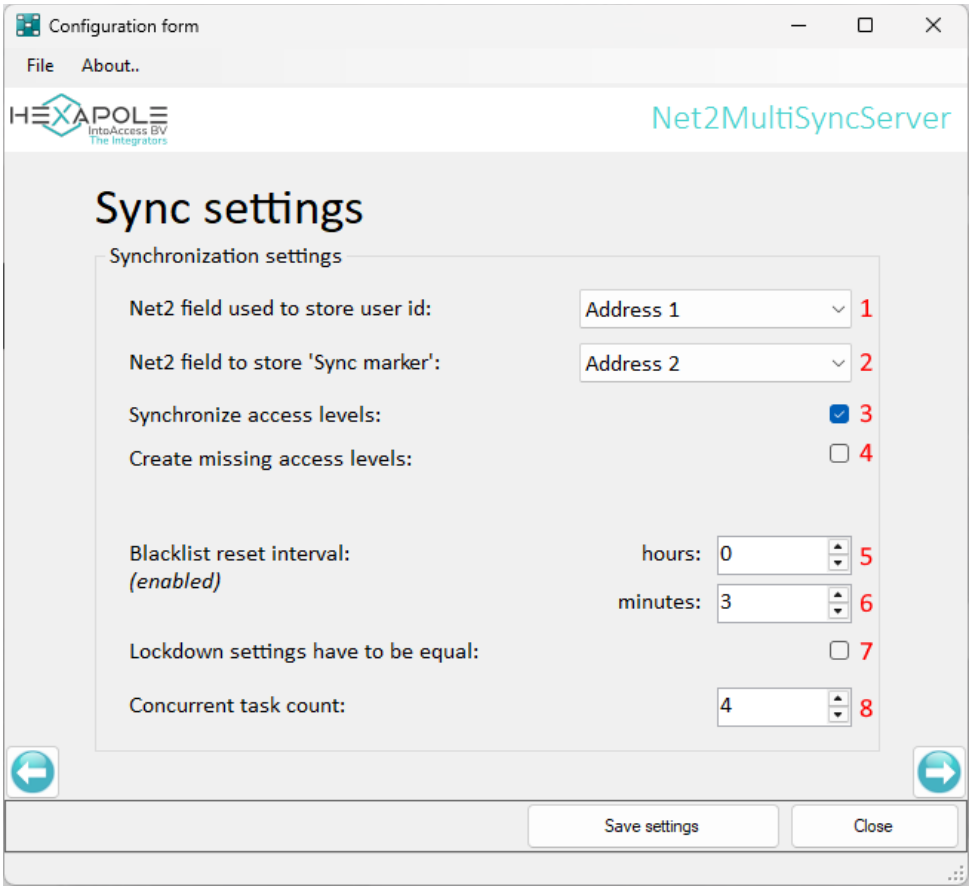


Image 10

The main server contains users that are synchronized to the child servers. In order to connect the user from the main server to the user in the child server, the user id from the main server has to be stored in a Net2 field on the child server. You can choose which Net2 field should be used for storing this unique id number (1).
Please keep in mind that, depending on which field you choose, the value in that Net2 field on the main server will not be synchronized to the child server.

It is also required that the synchronized users in the child server will get a 'sync marker', which will be stored in a Net2 field of choice (2). This marker tags the user as a user that has to be kept in sync with the corresponding user on the main server.
P*lease keep in mind that, depending on which field you choose, the value in that Net2 field on the main server will not be synchronized to the child server.*

You can enable or disable the synchronization of access levels for users (3). If access levels are not synchronized, the access levels can be configured separately for the child servers. If access levels are synchronized, the application will check if the access levels exist. In case of advanced access levels, the combination of access levels has to be allowed on the child server. If not, the child server will be blacklisted and you will have to solve any problems with the access levels.

It is possible to have all access levels that exist on the main server, automatically created on the child servers (4), if not present yet. Beware that these access levels will be created **without rights** and have to be manually 'populated'.

If you don't want to restart the service every time an error occurs on one of the child servers, you use the automatic reset functionality for the blacklist (5/6). The interval describes how often the blacklist will be reset. When the reset is enabled and you are making use of the mail functionality, mails about errors will be sent once a day. If no reset is applied, e-mails are sent when an error is encountered.

One of the features of Net2 is that you can enable or disable a lock down. This option is found in the server configuration tool under 'Features' > 'Security Lockdown integration'.
If you want the lock down settings to be the same on the main server and the child servers, you should check this option (7). A child server will be blacklisted when the settings don't match.
Please note that the service only checks if the Net2 feature is enabled or disabled. In order for a lock down to work, certain Triggers and Actions also have to be configured. In other words: this check does not guarantee that a lock down is actually possible if a child server has the feature enabled.

The concurrent task count (8) is intended for multi-threading purposes. With a concurrent task count of 1, the synchronization is performed synchronously and all child servers are synchronized one by one.
With a concurrent task count of 2 or higher (max 12), x child servers are synchronized at the same time. This results in a faster full sync cycle.
Note: This feature reserves and starts multiple threads on the system CPU. Take the number of CPU cores of your system into account.



Mail Settings

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

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.

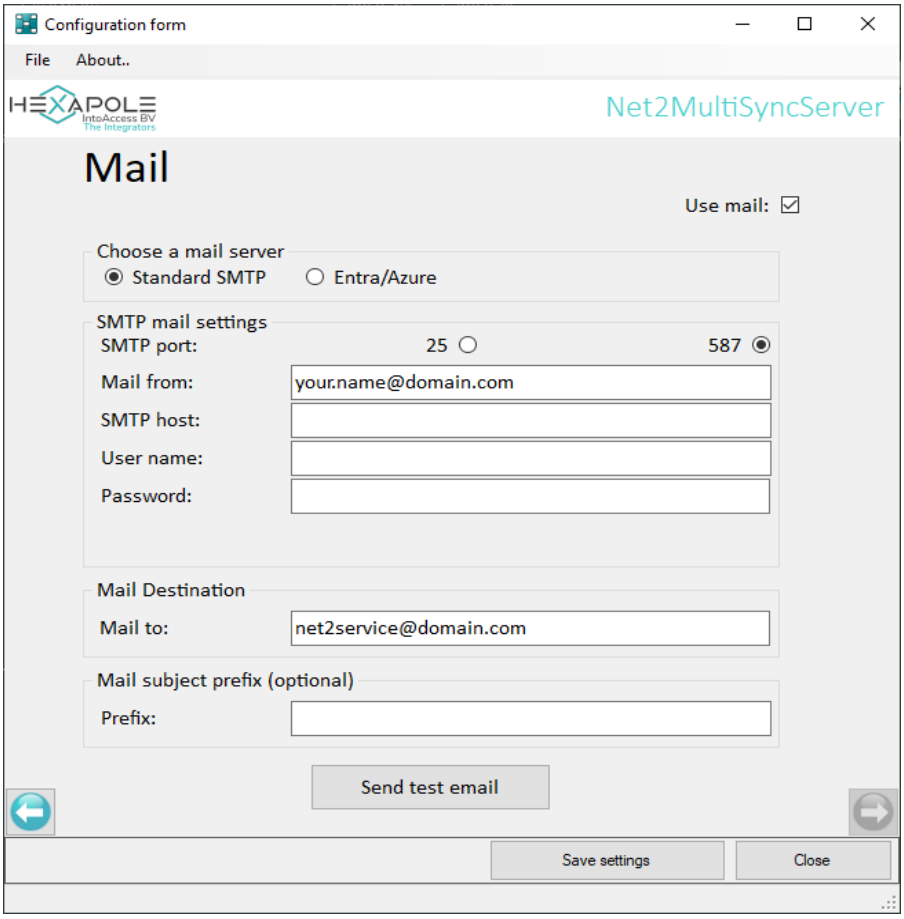


Image 11

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.

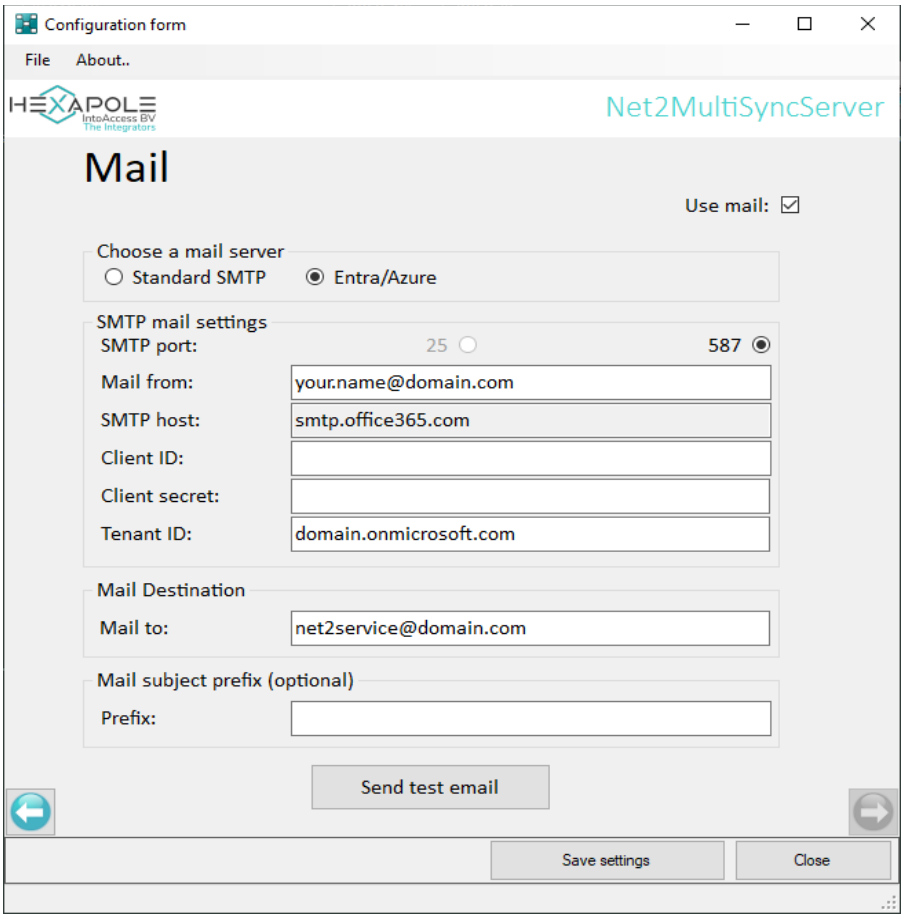


Image 12

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

Application Licence

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

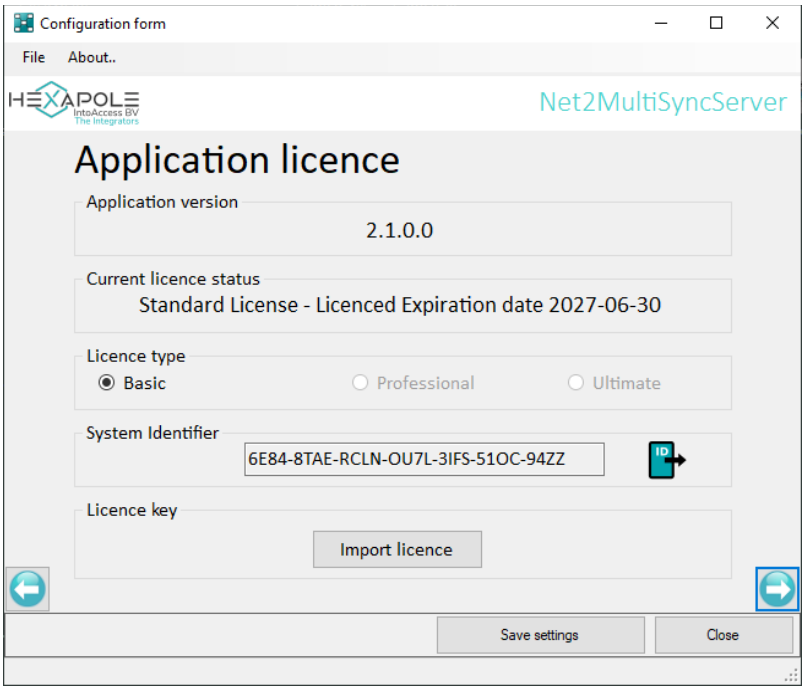


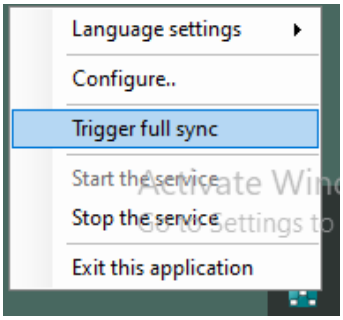
Image 13

Service API settings

The Service API is used to perform an on-demand runnow sync pass. This can be triggered using the following Curl command:

curl -i -k -X POST -u user:password -d '{}' https://localhost:6091/api/v1/runnow

In addition, this sync pass can also be triggered from the Tray Icon of the manager application, via the "trigger full sync" option.



Afbeelding 14

Use the options to determine how the Service API can be accessed:

- Disabled – the Service API is switched off.
- Local – the Service API is only accessible from the local machine.
- All – the Service API is accessible from any network location.

Port- Specify the SSL port that the Service API should listen on.

Certificate File - Click this field to select the SSL certificate (.pfx) file that should be used to secure the Service API connection.
By default, a self-signed certificate (.pfx) is already imported and can be used for this purpose.

Certificate Password- Enter the password belonging to the selected certificate file.
By default, the password for the self-signed certificate is already filled in.

Check Certificate- Click this button to verify that the selected certificate file and password are valid.

Username / Password- Use the Net2 operator for this.

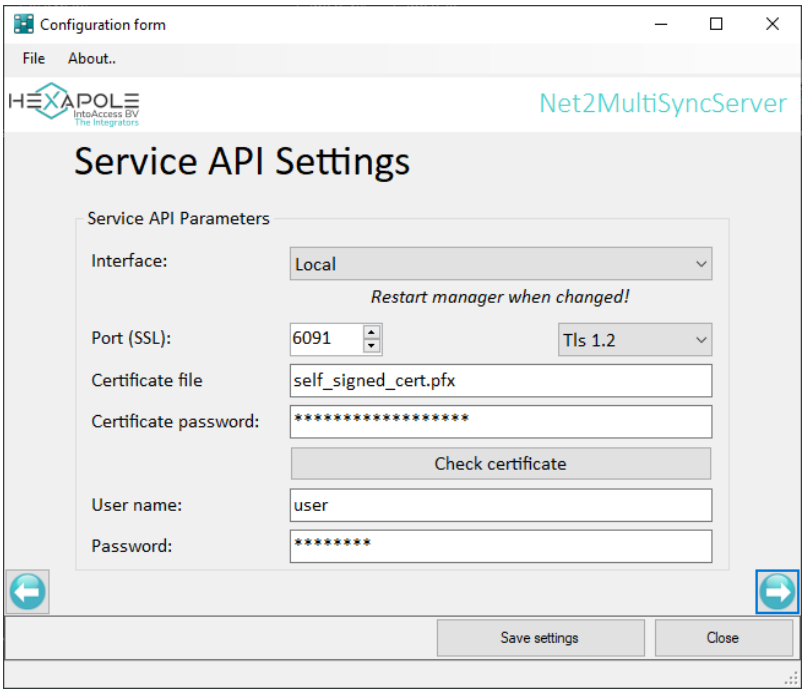


Image 15

Service Control

The service control window offers a way to stop and start the background service.

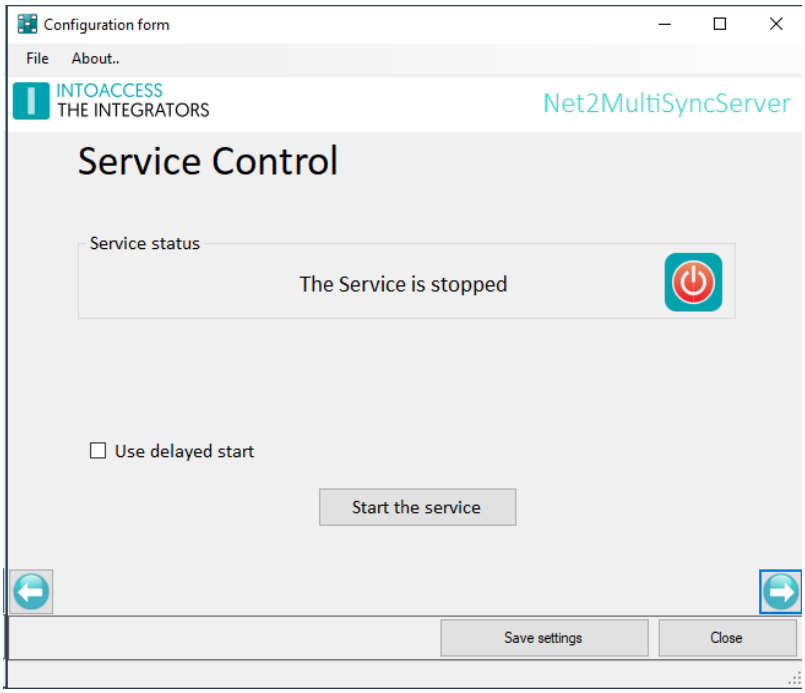


Image 16

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.

By default, the Net2MultiSyncServer has a service dependency on Net2, in order to make sure that it will only start after Net2 is up and running. This dependency can cause problems with some Net2 configuration tools, that attempt to restart the Net2 service. Temporarily switching off the Net2MultiSyncServer is typically enough to use the tools without issues. If this is inconvenient for you, you can select the **Use delayed start** option, which will remove the Net2 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.

Log Settings

This page, 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.

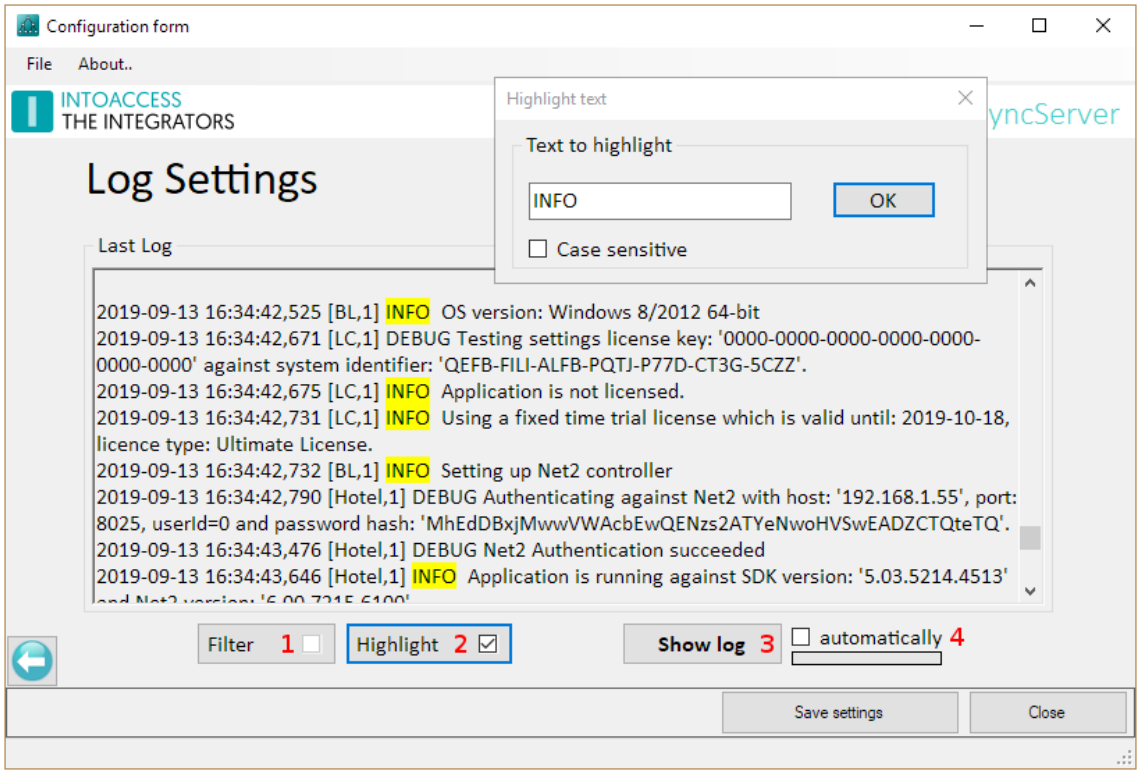


Image 17

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 files are located in the folder:

c:\IntoAccess\Logging\Net2MultiSyncServer

Manual Net2MultiSyncServer
Version 2.1