INTOACCESS
THE INTEGRATORS

IntoAccessWebServer

Manual 1.4

INTOACCESS B.V. THE INTEGRATORS
Strandweg 7B · 1976 BS · IJmuiden · The Netherlands
info@intoaccess.com · www.intoaccess.com · +31(0)255 700 227

Table of contents

Installation

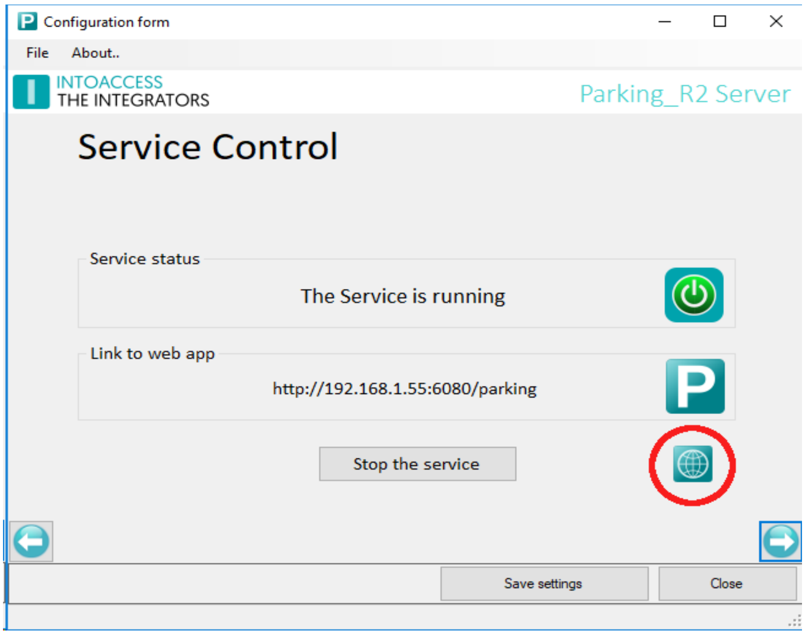
The application is typically installed automatically, together with all our web applications, like the PaxtonAttendanceWeb and Parking_R2. It is a ‘blind’ install, which allows/requires no user interaction.

After installation of one (or more) of the formerly mention applications, you will therefore also find the IntoAccessWebServer at the installed applications overview..

Configuration

In most cases, the existence of the IntoAccessWebServer will remain hidden. When however some more advanced web options need to be configured, the use of the IntoAccessWeb manager application is required.

The manager application does not come with a shortcut , but can be started using the manager of either the PaxtonAttendanceWeb or Parking_R2. At the "Service Control" tab, you will find a web symbol on the right hand side of the Start/Stop button, that will start the IntoAccessWebServer manager when you click on it.



Service Control

Service status: The Service is running

Link to web app: http://192.168.1.55:6080/parking

Image 1

This will first show the IntoAccess WebServer manager splash-screen, followed by the first configuration tab. If the application was already active, instead of the splash-screen, you will see a message stating that in instance of the application is already running. In that case you should see a tray icon in the right hand corder of the task bar, as displayed below. If you click on it with your right mouse button, a pop-menu will appear from which you can select "Configure"..

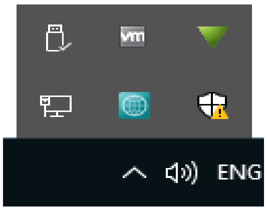


Image 3

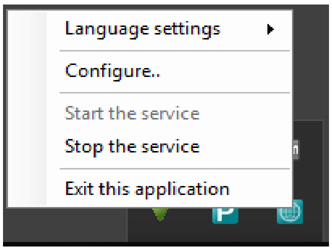


Image 2

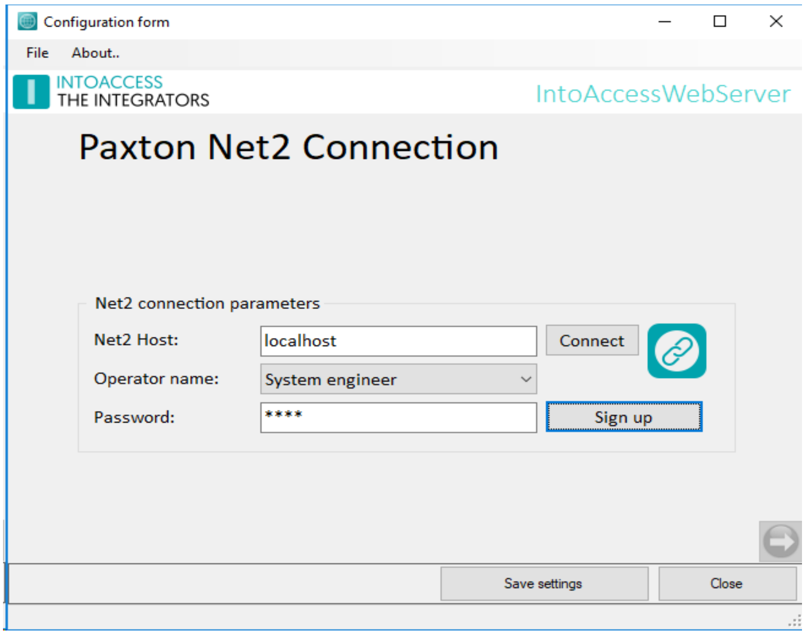
The menu option explained:

- Language settings: Select your preferred language;
- Configure: Start the configuration application;
- Start the service: Start the background service (only possible after configuration);
- Stop the service: Stop the background service (only possible after configuration);
- Stop this application: Stop the manager application.

The color of the tray-icon is an in indicator of the ‘running’ state of the service. If the service is not (yet) running, it is gray; when it is running it will be colored.

Net2 connection

The first configuration tab, allows you to define the Net2 connection parameters. When you start the configuration process for the first time, this will require a few steps. After these settings are stored however, the next time it will connect automatically.



Paxton Net2 Connection

Net2 connection parameters

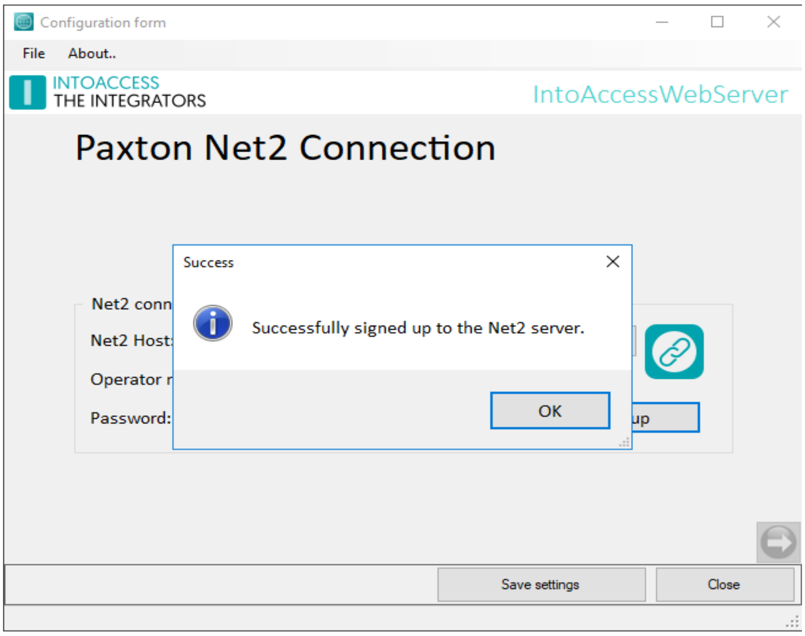
Net2 Host: localhost

Operator name: System engineer

Password: ****

Image 4

- Enter the (ip)address of the Net2 server. If you install the application on the Net2 server itself, you can keep the default 'localhost' value. Do not use an external adapter address in that case!!
- Click on the connect button; the application now attempts to fetch the list of operators from Net2. (these users can be found under “Net2 operators” in the Net2 application)
- Select an operator to use for the application logon. This needs to be an operator with the “System engineer” role.
- Enter the password of the selected operator.
- Click on the “Sign up” button.



Successfully signed up to the Net2 server.

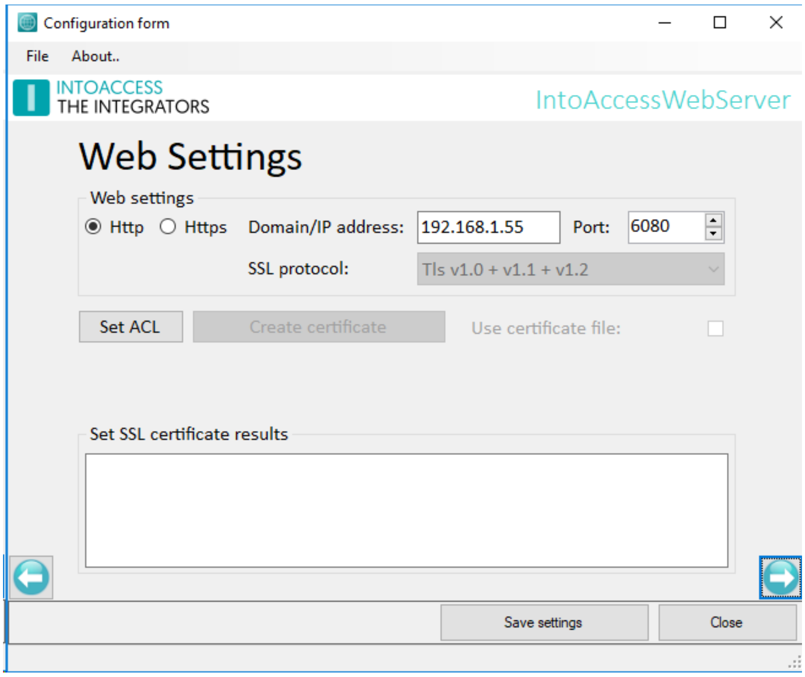
Image 5

If all goes well, a confirmation will appear that the application has successfully signed on and the arrow in the bottom right hand corner, will change from gray to colored.

You can now go to the next configuration tab, by clicking on this (right hand) arrow..

Web Settings

The config tab of the Web Settings, allow you to change the behavior of the HTTP web service:



Web Settings

Web settings

● Http ○ Https Domain/IP address: 192.168.1.55 Port: 6080

SSL protocol: Tls v1.0 + v1.1 + v1.2

Use certificate file: □

Set SSL certificate results

Image 6

By default, the protocol is set to HTTP, which is typically fine in a LAN environment and needs no further configuration. For access over public internet or networks of which it not can be guaranteed that they are safe, HTTPS can be switched on (S = secure).

HTTPS requires a few configuration steps, like providing a server certificate. There are a few ways of doing that:

– Use a ‘self signed’ certificate. The communication will be encrypted, but since the certificate is not issued by a ‘Certificate Authority’, browsers will not trust it and complain.

– Use an official certificate, issued by a ‘Certificate Authority’. For such a certificate, you typically also need to register a domain, with which the certificate will be associated.

The application supports both options. By clicking on the “Create certificate” button, the application will generate a ‘self signed certificate’, for the domain/IP address that was entered..

If you want to use an official certificate, your certificate provider will supply a .pfx file or a set of files with which you can create it. By selecting the “Use certificate file” option, you’ll get prompted to select provide the location of the pfx file.

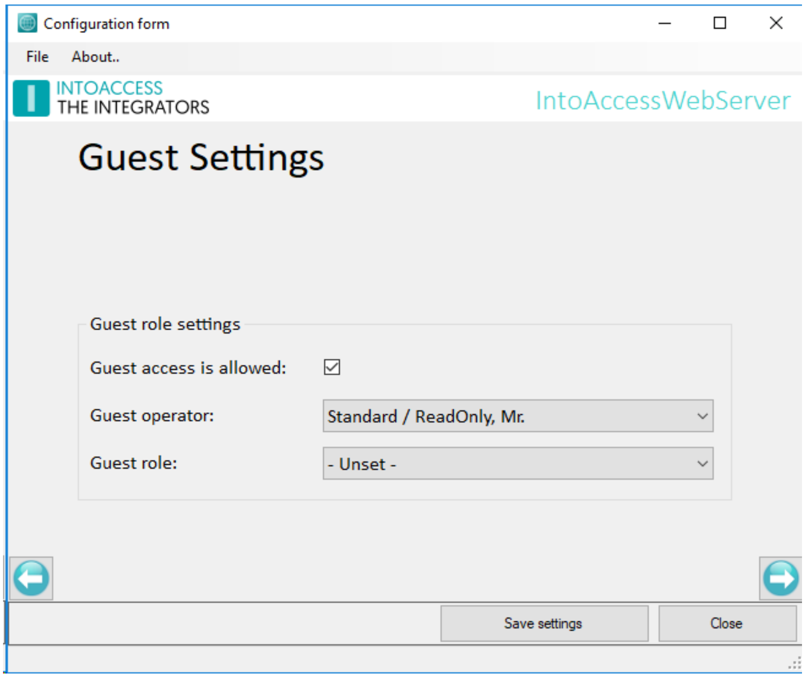
The supported SSL protocols are (also) only relevant when HTTPS is used and determine with which SSL protocols a browser is allowed to connect. Higher versions are typically safer than the lower ones, but it is possible that older browsers will fail to connect if you switch off the lower versions.

By default the web server will 'listen' on TCP/IP port 6080, but you can change that. If you opt to use HTTPS, the default port will change to 6443. The official ports for HTTP and HTTPS are 80 and 443. The application deviates from that, to prevent conflicts with possible other web services on your system. You can however select a port that is most convenient for you.

The ACL button offers the possibility to update the Windows Access Control List with the selected options. It registers which applications are allowed to listen on what port.

Guest Settings

If you want to allow the application to be used without logging in, you can select here that guest access is allowed and with what rights. On the url you can then use the url parameter **guest=yes** to log in automatically.



Guest Settings

Guest role settings

Guest access is allowed: ☑

Guest operator: Standard / ReadOnly, Mr.

Guest role: - Unset -

Image 7

You can select either a guest operator or a guest role. The role option has however become problematic for use with the Parking_R2. This has to do with the way that rights are defined in PaxtonAttendanceWe and Parking_R2.

- PaxtonAttendanceWeb: rights based on an operator role.

  Allocating a role to a guest is sufficient to allow this guest access to the application.
- Parking_R2: richts based on an operator

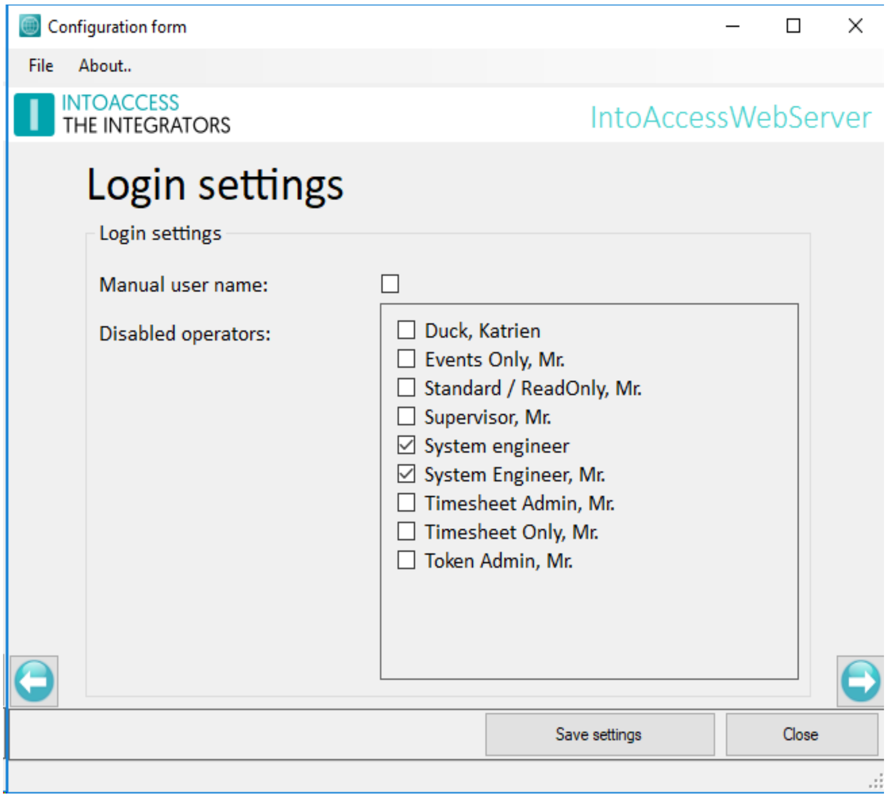
  Allocation a role is **insufficient**, because the Parking_R2 application, requires an operator with rights linked to it..

Bottom line: we advise to use the Guest operator option , since that works for both the PaxtonAttendanceWeb as well as the Parking_R2. A guest will mimic the selected operator in that case, where it does not matter if you disable that operator in the next config tab. It is a good idea to create a dedicated ”guest” operator in Net2, to keep better track of the rights it gets.

Login Settings

To enhance security, which can be required when using the web interface over the public internet, you can indicate if a user name should be entered manually (opposed to getting a list of operators to select from).

Someone trying to gain access illegally, will than need to know both user name and password.



Login settings

Login settings

Manual user name: □

Disabled operators:

- □ Duck, Katrien
- □ Events Only, Mr.
- □ Standard / ReadOnly, Mr.
- □ Supervisor, Mr.
- ☑ System engineer
- ☑ System Engineer, Mr.
- □ Timesheet Admin, Mr.
- □ Timesheet Only, Mr.
- □ Token Admin, Mr.

Image 8

Within this context, having an operator with a standard name (like System engineer), still betrays a user name to a possible hacker. To prevent that, the application allows you to select which operators are blocked from using the web interface.

The blocking of access is functionally unrelated to showing a list of operators or not. You can choose to block certain operators and still allow the use of a dropdown list to select the user/operator.

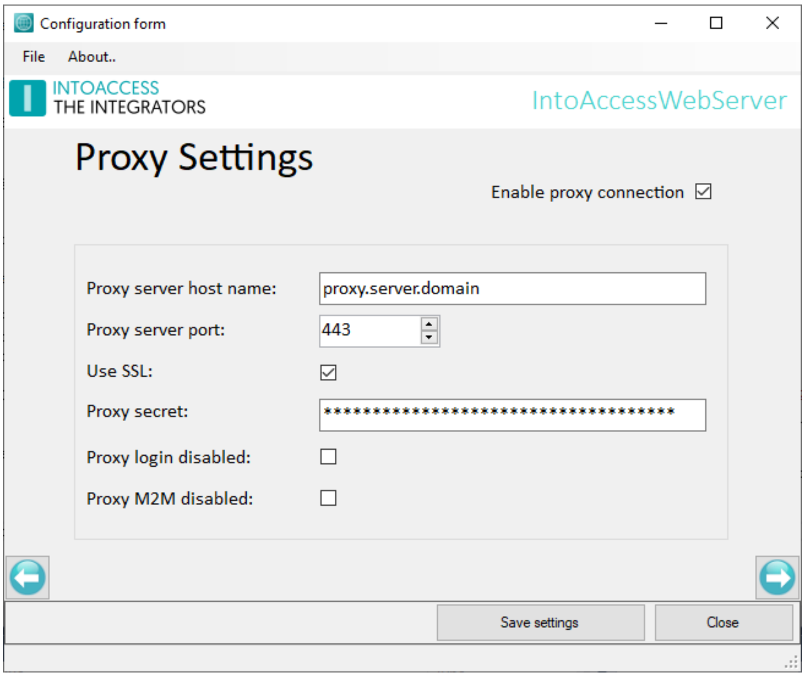
Proxy Settings

To access the web service **publicly** (instead of just over the LAN), there are a number of options. The (technically) simplest method, is to create a 'hole' in the firewall that separates the LAN from the public internet and use 'port forwarding' to connect the public port (for which the 'hole' was made) to the server/port where the IntoAccessWebServer is listening on.

Not all network administrators are happy with such a set up, since that requires the server to be placed in a DMZ.

An alternative and slightly safer form is the use of an HTTP(S) server met proxy capabilities, like Apache or IIS. These will act as intermediary between the public internet and the IntoAccessWebServer.

The third option is a form where IntoAccessWebServer itself connects to a proxy server in the cloud, from where the web application can be accessed. This will only require HTTPS traffic to pass from the LAN to the outside world, which is allowed by most companies. The config tab below allows you to configure this connection.



Proxy Settings

Enable proxy connection ☑

Proxy server host name:	proxy.server.domain
Proxy server port:	443
Use SSL:	☑
Proxy secret:	************************************
Proxy login disabled:	□
Proxy M2M disabled:	□

Image 9

- The proxy server host name, is the domain name of the host where the proxy server is running.
- The proxy server port, is the TCP/IP port at which the proxy server listens. Since 'outside' connection are typically only allowed on port 443, we advise you not to change this.
- Use SSL, allows you to use HTTPS instead of HTTP. This also is a requirement for unhindered traffic to the outside world and also offers encryption.
- The proxy secret is a string with which the IntoAccessWebServer identifies itself at the proxy server as a legitimate web service. Without this secret, the proxy server will not accept the connection as coming from a web service.
- The 'back end' applications (that are exposed through the IntoAccessWebServer), can be blocked from also being exposed via the proxy. By disabling the 'Proxy login', apps like PaxtonAttendenceWeb and Parking_R2 will no longer be exposed.
- A special type of back end, is the machine to machine (M2M) type. This can be separately blocked from exposure via the proxy. **Please not that disabling both the login as well as the M2M exposure, will render the proxy connection useless.**

The proxy server

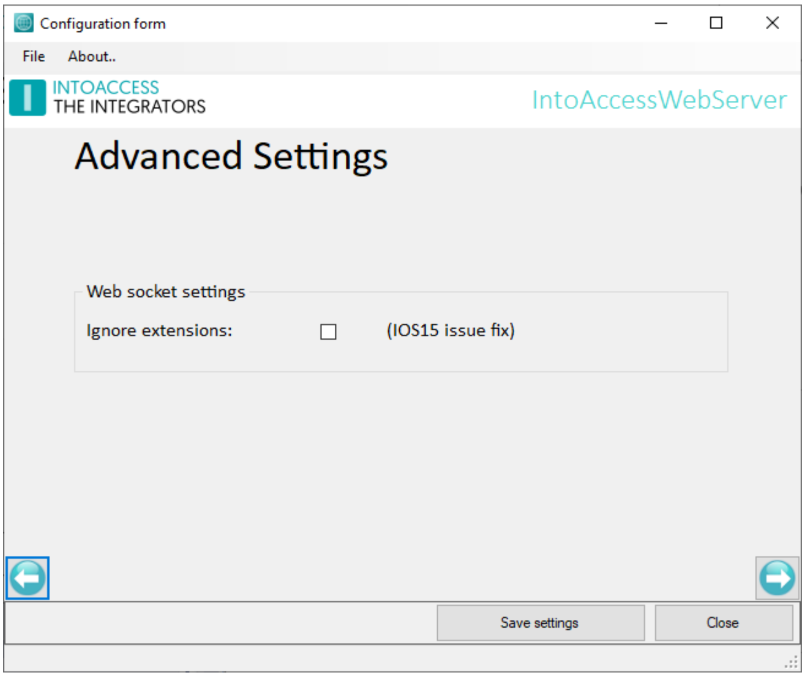
The proxy server, from which the web interface is presented on the public internet, is a service offered by IntoAccess. In its simplest form, the customer can request a <customer>.intoaccess.nl sub domein, where the web interface can be offered. In this case, IntoAccess will take care of registering the (sub)domain and the HTTPS certificate.

Optionally, the service can also use a domain that the customer registers themself. This requires that the customer makes sure that the domain 'resolves' to the proper IntoAccess server address and also supplies the HTTPS certificate for that domain.

Please contact us for a price indication of the periodic costs of the proxy service.

Advanced Settings

This tab contains settings that should typically be left unchanged, unless you experience some issue.



Advanced Settings

Web socket settings

Ignore extensions: □ (IOS15 issue fix)

Image 10

If you set the Web socket server to ignore 'extensions' it will respond to a browser client that asks for any compression method (deflate), that this is not supported. Due to some bug in (early?) IOS15 Safari versions, this may be required in order to get the web application to work properly.

The setting itself is not IOS specific, so possibly it will also help with any other browser that causes issues. The drawback is that you lose any traffic compression, which is normally not a very big price to pay.

If it it just one IOS/Safari device that you want to behave properly, you can also try to disable the following Safare setting: "Advanced/Experimental Features/NSURLSession WebSocket". This will cause Safari to request the deflation method 'x-webkit-deflate-frame', which is not supported in any case, effectively also disabling compression (but now only for this client).

Mail Settings

The email configuration is optional and offers the possibility to have application messages sent to a system administrator.

This is specifically useful as an early warning system that the application is not functioning correctly.

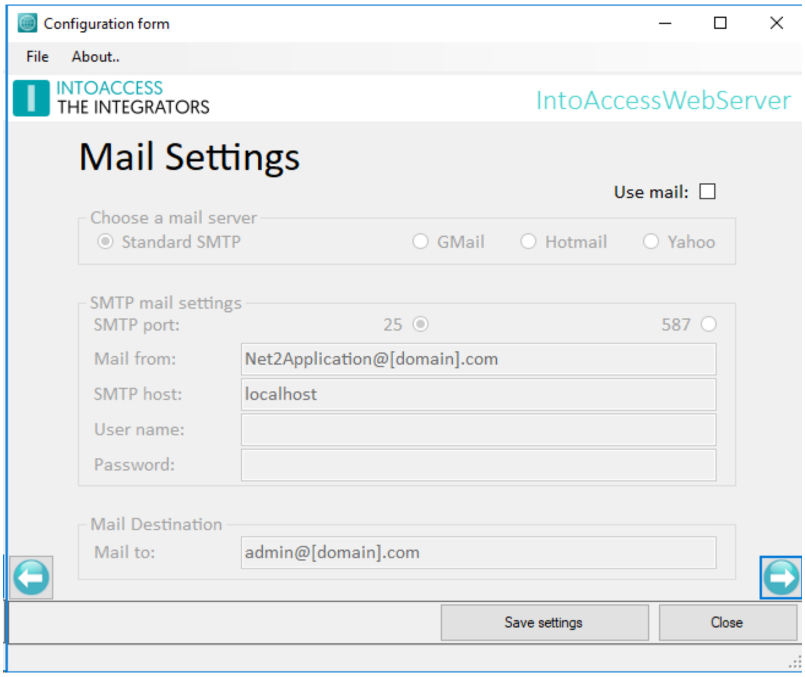
Webmail

To use web mail providers (like Gmail), it may be required to lower the security settings of the mail account.

SMTP

The SMTP settings, currently do not offer any encryption or authentication support. Its use is therefore only only advised on a LAN environment.

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



Mail Settings

Use mail: □

Choose a mail server
● Standard SMTP ○ GMail ○ Hotmail ○ Yahoo

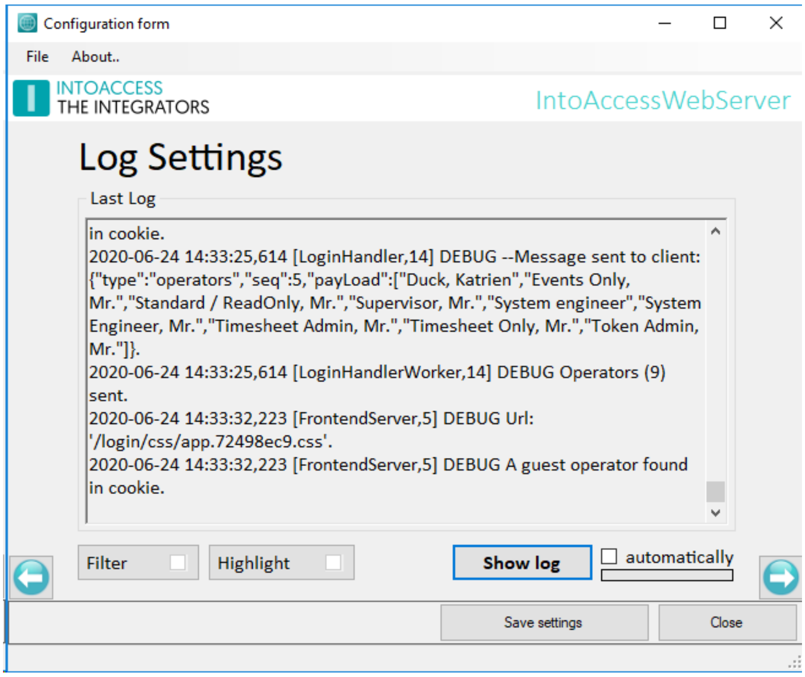
SMTP mail settings
SMTP port: 25 ● 587 ○
Mail from: Net2Application@[domain].com
SMTP host: localhost
User name:
Password:

Mail Destination
Mail to: admin@[domain].com

Image 11

Configure and view the logging

This window offers the possibility to view the last (max. 500) lines of the log file. The application logs very detailed which actions it conducts. You have the option to filter and highlight text from the logs. When filtering, only log lines containing the filter text are shown. When highlighting, the matching text will be highlighted with a yellow color. Select the checkbox to enable/disable the filter or highlight. If you want the logs to be updated automatically, which can be helpful when the service is running, you can check the checkbox at ‘automatically’. Any new logs will be added to the log overview every five seconds.



```
in cookie.
2020-06-24 14:33:25,614 [LoginHandler,14] DEBUG --Message sent to client:
{"type":"operators","seq":5,"payLoad":["Duck, Katrien","Events Only,
Mr.","Standard / ReadOnly, Mr.","Supervisor, Mr.","System engineer","System
Engineer, Mr.","Timesheet Admin, Mr.","Timesheet Only, Mr.","Token Admin,
Mr."]}.
2020-06-24 14:33:25,614 [LoginHandlerWorker,14] DEBUG Operators (9)
sent.
2020-06-24 14:33:32,223 [FrontendServer,5] DEBUG Url:
'/login/css/app.72498ec9.css'.
2020-06-24 14:33:32,223 [FrontendServer,5] DEBUG A guest operator found
in cookie.
```

Image 12

Especially when you encounter an issue, the log file can contain very important information (also for an end user).

Lines in log files all have the same format:

- *Date time [name,id] DEBUG | INFO | WARN | ERROR log message*.

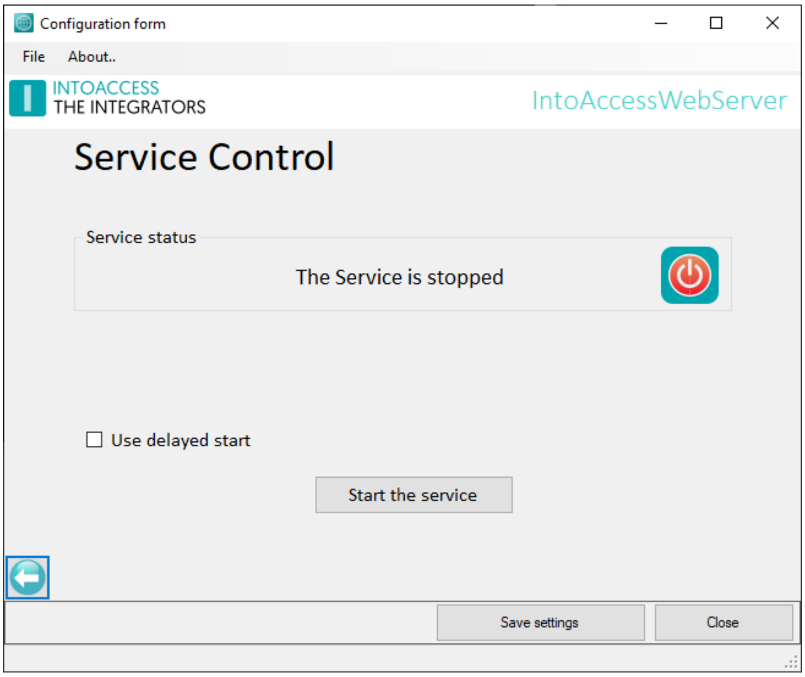
Pay attention to WARN and/or ERROR messages. These are typically the most indicative of the cause of problems.

The web server log file is located here:

c:\IntoAccess\Logging\IntoAccessWebServer

Service Control

The service control window (also) offers a way to stop and start the service.



The Service is stopped

☐ Use delayed start

Image 13

Other ways to stop/start the services are:

- The tray icon pop-up menu
- The Windows service manager

By default, the IntoAccessWebServer 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 IntoAccessWebServer 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.

The web service application 'listens' on **all** interfaces and can be tested by going to the following url, if the web settings are not changed from their default value:

http://localhost:6080/

Error situations

This chapter offers some pointers for those situations where the installation fails or the application malfunctions.

The application will not install

Try to uninstall any older versions of the application, using the Windows software manager.

The remove any files that are left behind in the installation directories. If you are using a 32 bit Windows version, the path will not include the “ (x86)”:

- c:\Program Files (x86)\IntoAccess\IntoAccessWebServer

Try to install the application again.

The service will not start

Take a look at the application log file, using the manager application.

In case the log points to a port conflict (another app is using port 6080), alter the port number to one that is still free, save the settings and (re)start the application.

The web application can not be accessed

The service starts without a problem, but the website can not be accessed.

- Be aware of the fact that a 'localhost' address can only be accessed from the PC that is running the attendance service.
- If you have non standard firewall software installed, check if the tcp/ip port (default 6080) is open for external access.

The web application shows “Incompatible browser”

The application has detected that your browser seems to be incompatible with the attendance software. Please check if there are updates available for your browser, install these and try again.

At this page you can check which browsers are compatible:

https://caniuse.com/#feat=es5

The web application has a distorted layout

Your browser may be incompatible, even though the application did not detect this. See “Incombatible browser” solution.

Other

If the previous pointers did not help to solve the issue, please gather the log files of the IntoAccessWebServer application, place these in a zip file and send it to the support department. Please also add a detailed problem description.

The relevant log files you can (normally) find here:

- C:\IntoAccess\Logging\IntoAccessWebServer\

Manual IntoAccessWebServer
Version 1.4