INTOACCESS
THE INTEGRATORS

Net2SysLog

Manual 1.4

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

Table of contents

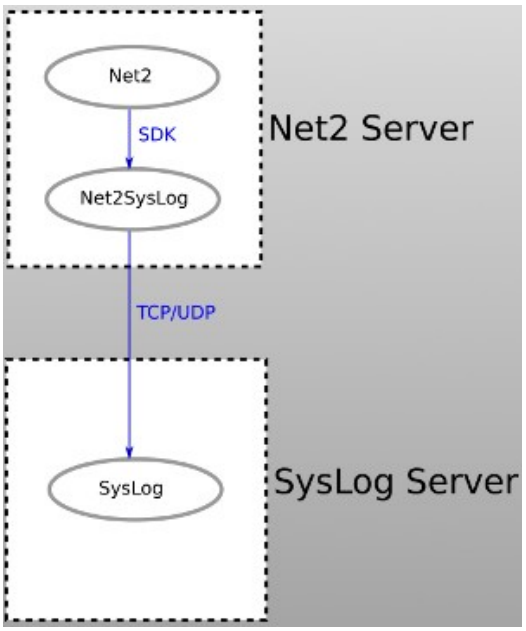
Principle

The way the program works is as follows:

A background service that periodically checks the Paxton Net2 event log for new entries and if it finds any, it sends it to a syslog service of choice.

It will keep track (persistent) of the event that was relayed last, so after a restart it will pick up where it ended.

It supports RFC5424 syslog messages using a plain message string as well as the more formal structured data format.



Afbeelding 1

Installation

The application can be installed, using a single setup file: Net2SysLog.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..

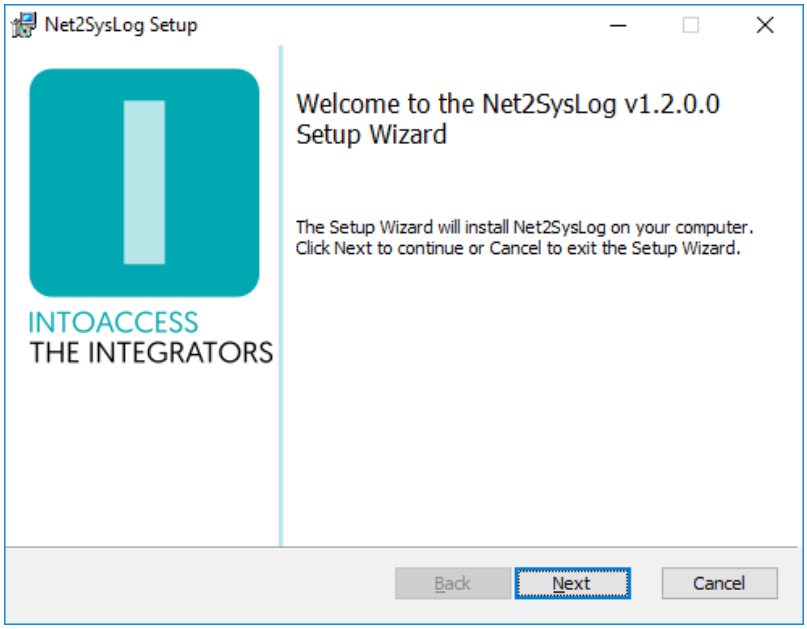


Image 2

The fist dialog window will display what application version you will install.

Note: the version number you see will most likely be different from the one displayed in 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.

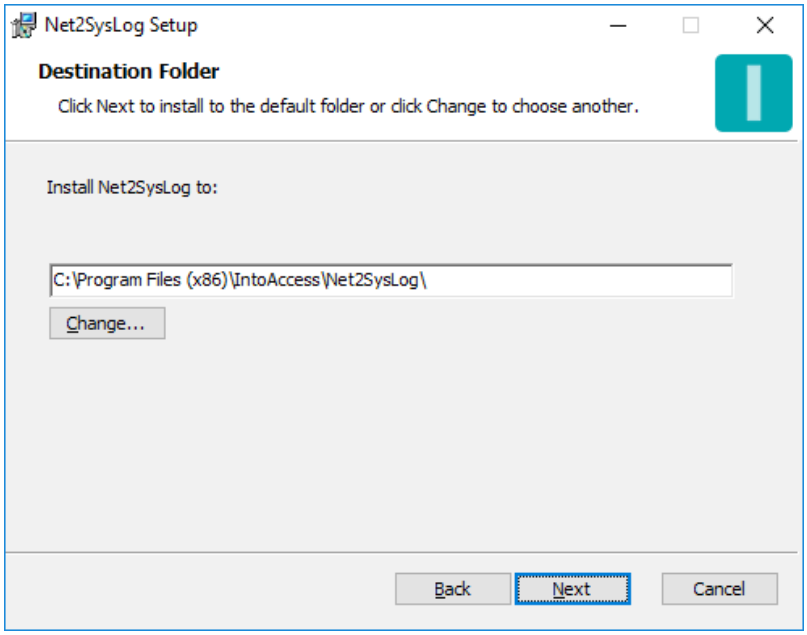


Image 3

The second dialog window shows where the application will be installed. The default value is typically fine.

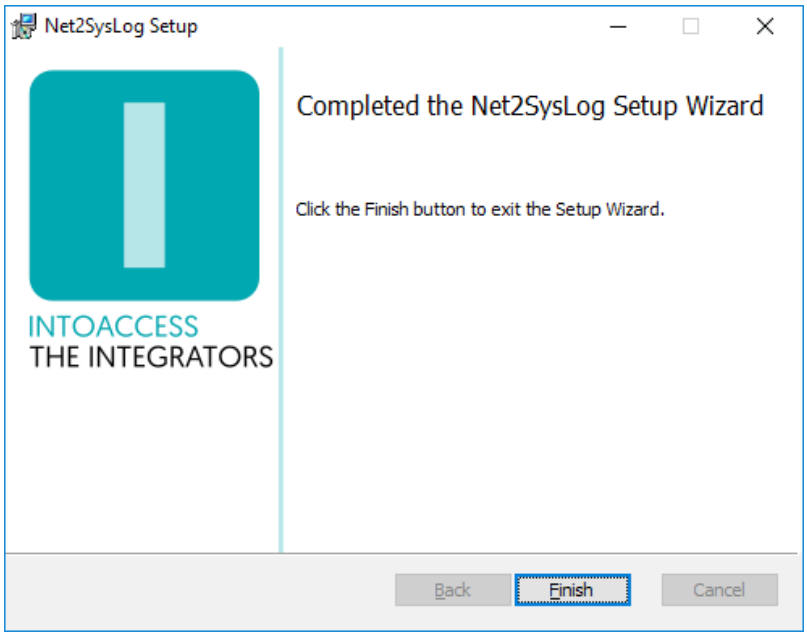


Image 4

The final dialog window will indicate whether the installation was successful.

Configuration

To help with the configuration, the *Net2SysLog manager* application is available and allows you to configure:

- how the application should connect to Net2;
- if you require emails of application starts/stops/errors;
- how the application should connect to a syslog daemon;
- what syslog message type to use;
- how and if non classified events should be relayed;

Image 5

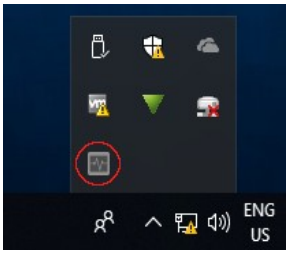


Image 7

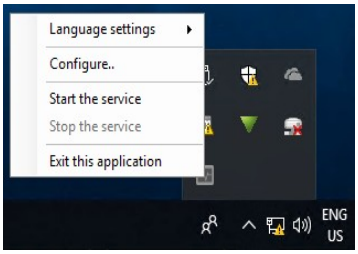


Image 6

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.

By right clicking on the tray icon, the following pop-up menu will appear (providing it is not opened already):

- 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. 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.

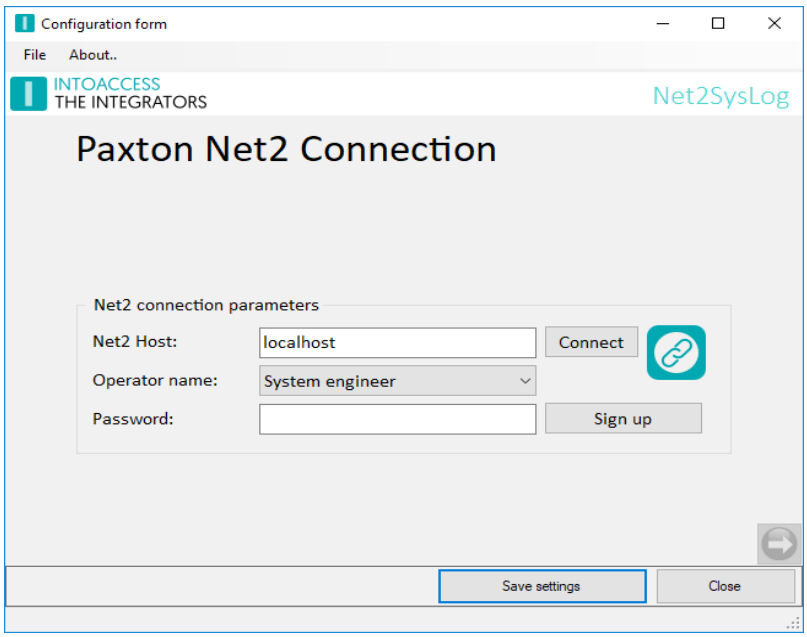


Image 8

- 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!!
- Click the Connect button; the application now tries to fetch the Net2 operators. (these users you can find under “Net2 operators” of the standard Net2 application)
- Select an operator with which the application should log on. It is required that this user has the “System Engineer” role.
- 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.

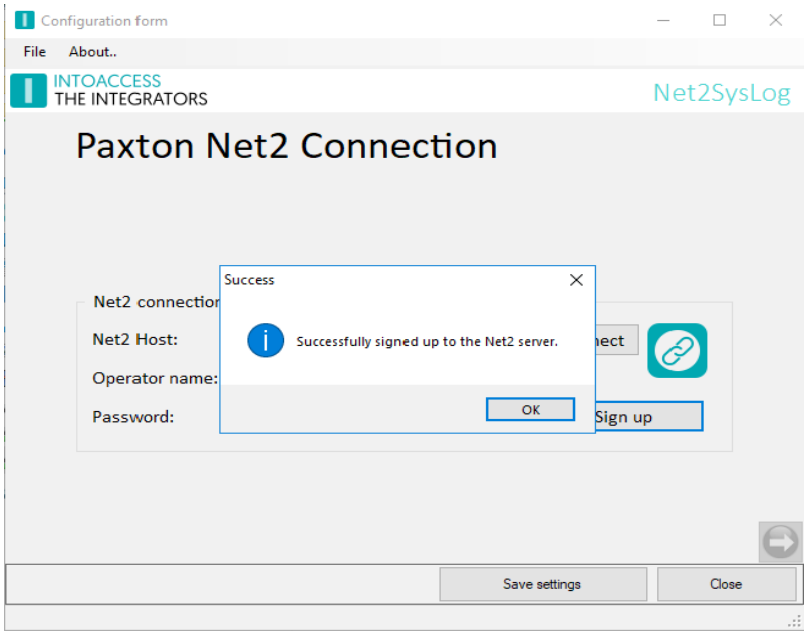


Image 9

After closing the success message, you can proceed to the next configuration window, by clicking on the right hand arrow.

Email 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 allow you to configure which SMTP server and port to use. If you select port 587, authenticated SMTP is also possible by supplying credentials.

Mail destination

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

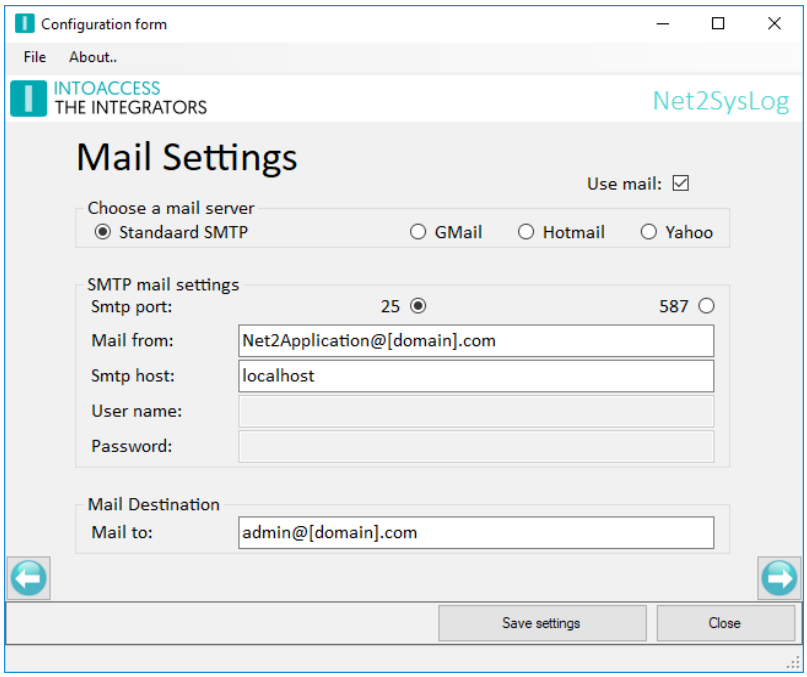


Image 10

Application license

The trial/test version as it can be downloaded from the IntoAccess website, is fully functional but will stop working after a certain date when it is not licensed.

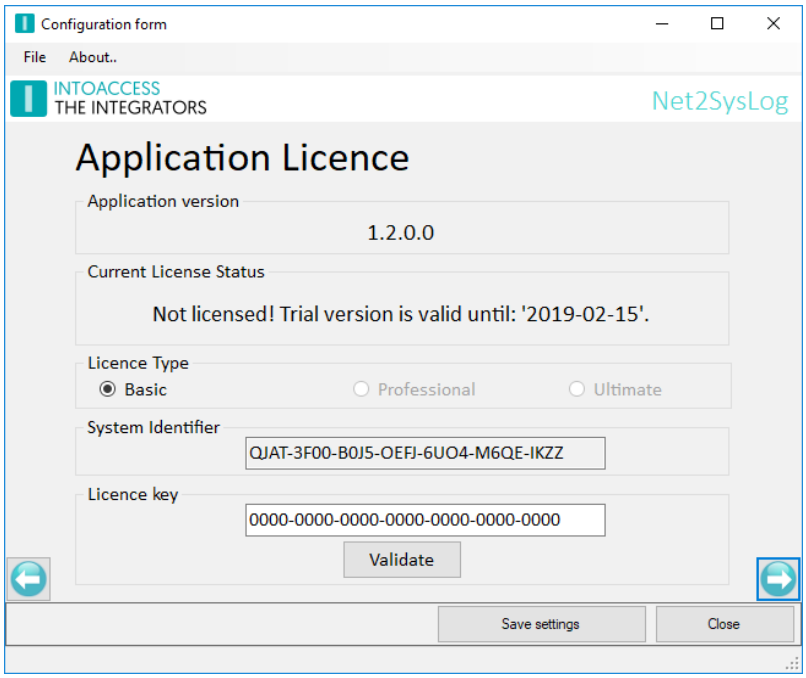


Image 11

After buying a license, you can copy the “System identifier” into an email or send a screenshot to IntoAccess and receive your license code.

Note: the System identifier differs per PC and therefore also the required license code.

Syslog settings

In this configuration window, you can define the way in which Net2 events are relayed to a syslog server:

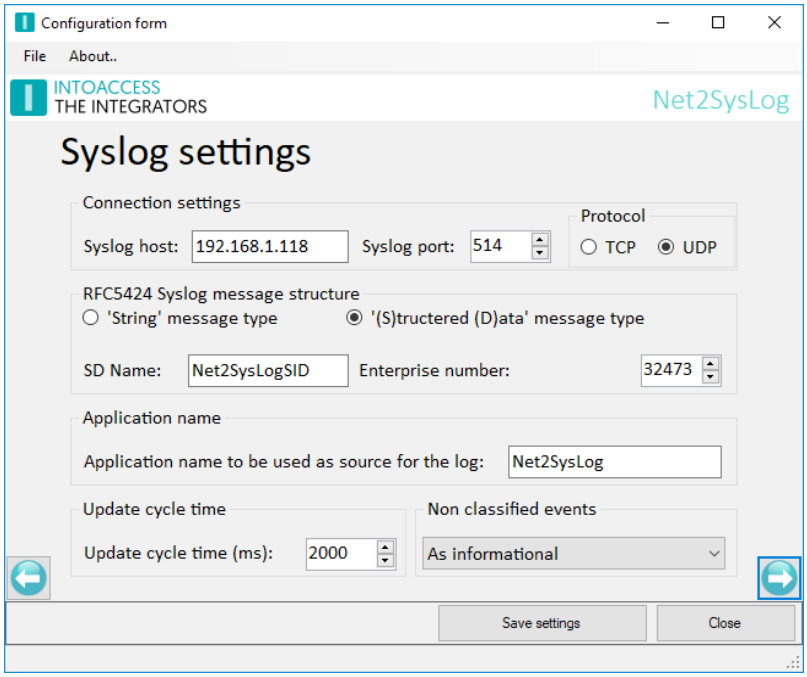


Image 12

- Connection settings:
  - Set the ip address or the host name of the computer that runs the syslog daemon;
  - Pick a port number (514 is the standard);
  - Pick a protocol (depends on your syslog config);
- RFC5424 Syslog message structure:
  - If you opt for the structured data, you can enter a name and number that will be incorporated in the data. Please note that the msg field will be populated with the Net2 event id, in order to prevent the syslog daemon from considering all messages the same. (also see Repeated messages)
  - If you opt for the string type (see Image 13), you have to select a separator character for the field=value combinations.
- Application name:
  - The application name that will be reported to the syslog daemon.
- Update cycle time:
  - The time in milliseconds, between subsequent checks of the Net2 event logs.

- Non classified events:
  - Select how and if you want non classified events to be relayed to the syslog daemon. Non classified events are typically events that do not indicate that something is wrong or need to be reported on. (also see Event classification)

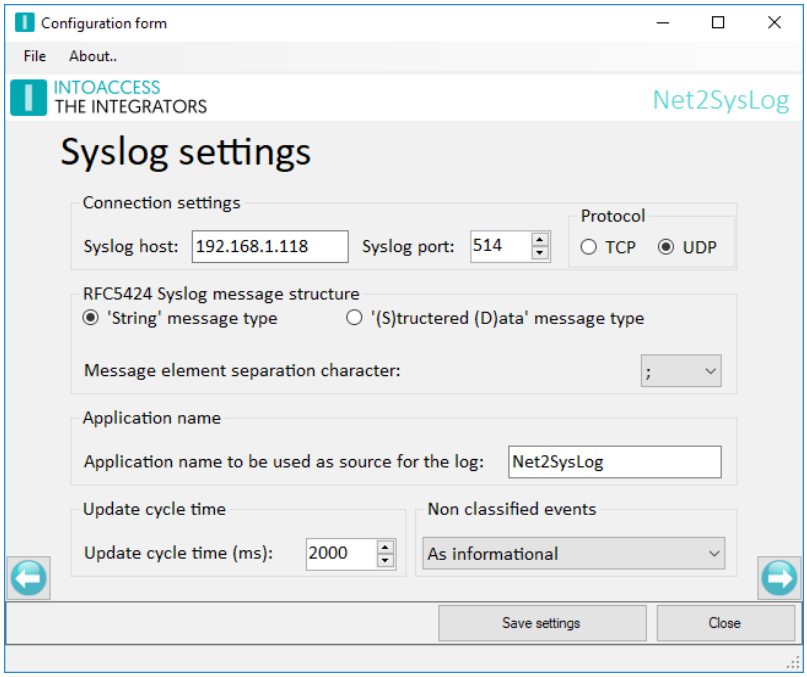


Image 13

Service Control

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

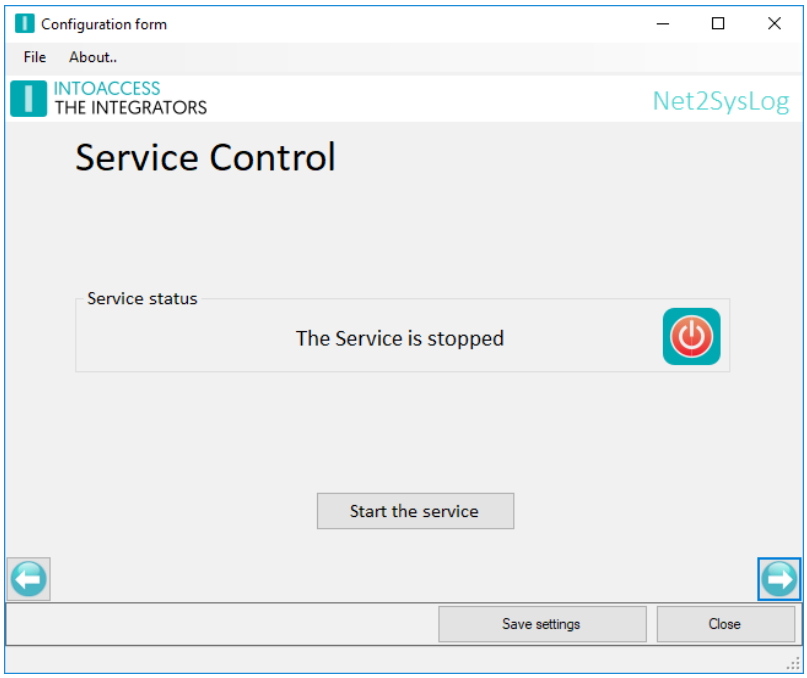


Image 14

Other ways to start and stop the service are:

- Using the tray icon pop-up menu;
- Using the Windows service manager (look for “Net2SysLog”);

Log settings

This page, see image 15, offers the possibility to review the last (max. 500) lines of the log file. The application will log its 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.

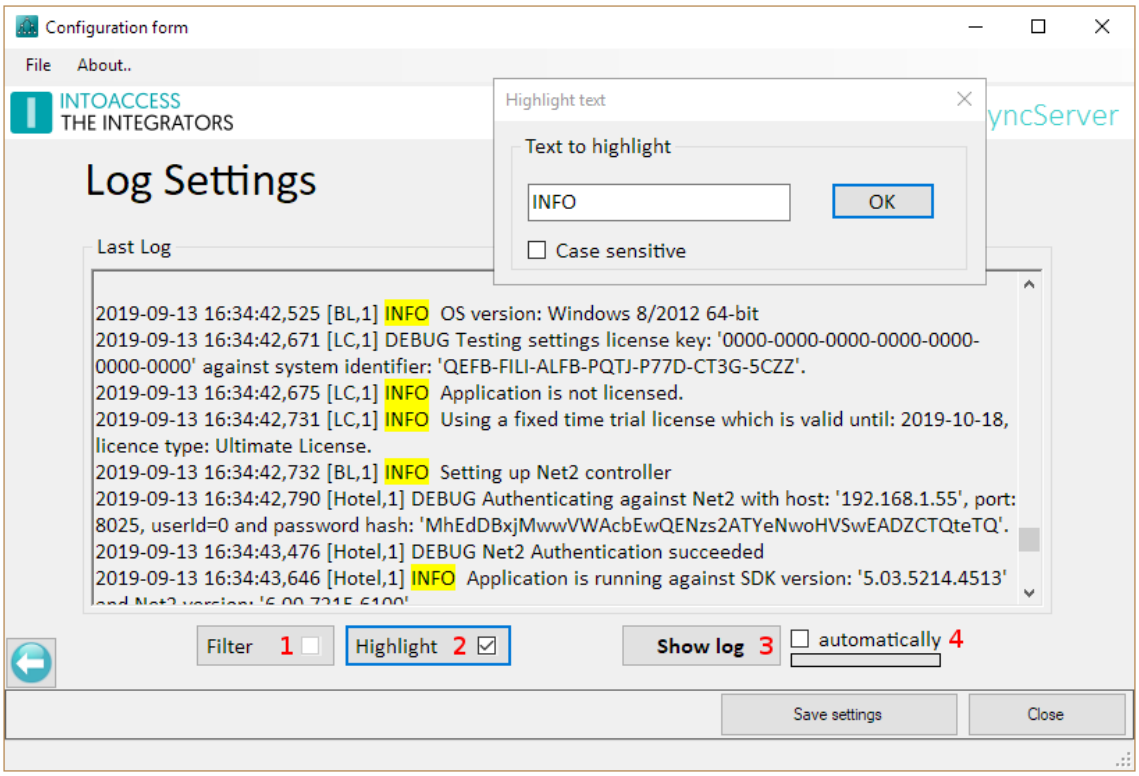


Image 15

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\Net2SysLog

Event classification

In this chapter you will find the applied Net2 event classification. All remaining events are considered “Non classified”.

Critical

```
91,   // Mains failed
102,  // Mains restored
721,  // Cannot lock
723,  // Battery critically low
```

Alert

```
75,  // Intruder alarm
76,  // Intruder alarm on partition
85,  // Fire alarm input
90,  // Tamper
92,  // Door forced
94,  // Reader tamper
95,  // Duress code
96,  // Keypad hacker
103,  // Tamper restored
```

Error

```
5,   // Real time clock error
8,   // Checksum failure
97,  // Input short
98,  // Input cut
99,  // Input voltage substitution
141,  // Door not unlocked following call
500,  // ACU not responding
502,  // Check communications interface
510,  // IO board not responding
513,  // IO board firmware update failed
514,  // Could not connect to IO board
515,  // Could not configure IO board
557,  // Server error
559,  // Add ACU Error
561,  // Send message failed
568,  // Object Changed Without Event Showing In Event Viewer
578,  // Firmware upgrade error
590,  // Lockdown activated by user with network instruction
700,  // Event table corrupted
```

```
701,  // Flash CRC changed
702,  // EEprom CRC changed
703,  // Invalid session
711,  // Queued events lost
720,  // Cannot unlock
```

Warning

```
1,    // Control unit reset
4,    // Real time clock set
61,   // Door not opened
50,   // Reader not active
83,   // Silence alarm
86,   // Fire door
93,   // Door left open
112,  // Access Denied - Lockdown in Progress
120,  // Door Lockdown Activated
142,  // Call not answered
300,  // Lockdown Activated
301,  // Lockdown Reset
302,  // Application Launched
520,  // Net2 Air Bridge disconnected
553,  // Backup failed
555,  // Archive failed
560,  // Server warning
591,  // Lockdown reset by user with network instruction
708,  // Factory reset started
722,  // Low battery
725,  // Communications failure signal strength too low
726,  // "Communications warning,  signal strength is low"
```

Informational

```
16,   // Access denied
17,   // Access denied
20,   // Access permited token only
21,   // Access permitted token + pin
22,   // Access permitted token + pin + code
23,   // Access denied - invalid token
24,   // Access denied - invalid PIN
25,   // Access denied - invalid code
26,   // Access permitted pin only
27,   // Access permitted code only
28,   // Door opened
```

```
29,   // Door relock
31,   // Access denied - ANPR
33,   // ACU APB cleared
87,   // PIN not valid
88,   // Token not valid
111,  // Access denied
121,  // Door Lockdown Reset
137,  // Summer time clocks forward
138,  // Summer time clocks backward
501,  // ACU online
552,  // Backup succeeded
554,  // Archive succeeded
558,  // Add ACU
706,  // Compact started
707,  // Compact complete
724,  // Battery level updated
750,  // Inactive bank erase complete
```

Debug

```
710,  // Nano Debug information
```

Notice

```
80,   // Firmware updated
89,   // Keypad time out
122,  // Set Door Open Time
503,  // Scheduled wake up
504,  // Handle wake up
511,  // IO board online
512,  // IO board firmware update succeeded
516,  // IO board settings updated
521,  // Net2 Air Bridge reconnected
551,  // Alarm actioned
709,  // Factory reset complete
```

Syslog daemon

Although it falls outside of the scope of this document, this chapter offers some information on the syslog daemon configuration on an Ubuntu server.

Even if you are using a different system, it may offer some help.

On Ubuntu, the syslog daemon is called rsyslog and has its configuration in the /etc/rsyslog.conf file and any additional *.conf files in the /etc/rsyslog.d/ directory.

Enable UDP

To enable the UDP protocol, add (or uncomment) the following lines:

```
module(load="imudp")
input(type="imudp" port="514")
```

Enable TCP

To enable the TCP protocol, add (or uncomment) the following lines:

```
module(load="imtcp")
input(type="imtcp" port="514")
```

Template

The default message template, will not display any structured data. In order to see this (and other) data as well, you can alter the default template like this:

Add a new template definition line:

```
$template MyTemplate,"%TIMESTAMP% %HOSTNAME% %APP-NAME%: pri=%pri%,slp=%syslogpriority%,slf=
%syslogfacility%,slt=%syslogtag%,msg=%msg%,data=%STRUCTURED-DATA%\n"
```

Alter the template used (original commented out):

```
#$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
$ActionFileDefaultTemplate MyTemplate
```

Repeated messages

The syslog daemon can suppress repeated message that have the same msg, hostname, procid and appname fields. You can switch this behavior on and of with the following setting:

```
$RepeatedMsgReduction off/on
```

Manual Net2SysLog
Version 1.4