



INTOACCESS
THE INTEGRATORS



Net2SysLog

Handleiding 1.4

(8 augustus 2023)



Inhoudsopgave

Principe.....	3
Installatie.....	4
Configuratie.....	6
Net2 verbinding.....	8
Email instellingen.....	10
Webmail.....	10
SMTP.....	10
Email bestemming.....	10
Applicatie licentie.....	11
Syslog instellingen.....	12
Service beheer.....	14
Log instellingen.....	15
Gebeurtenissen classificatie.....	16
Critical.....	16
Alert.....	16
Error.....	16
Warning.....	17
Informational.....	17
Debug.....	18
Notice.....	18
Syslog service.....	19
UDP inschakelen.....	19
TCP inschakelen.....	19
Template.....	19
Herhaalde berichten.....	19



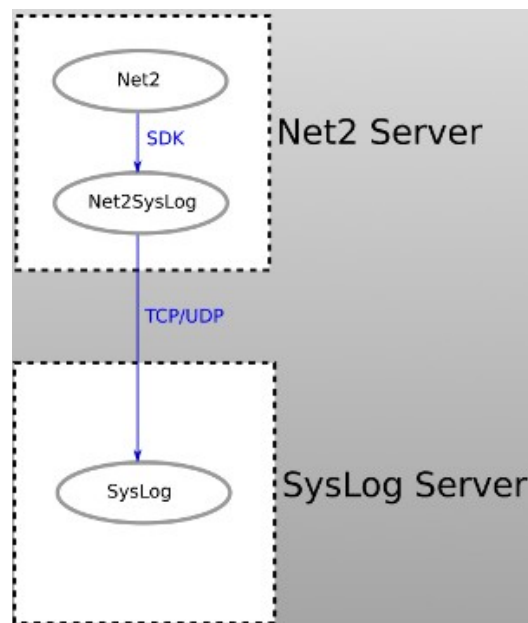
Principe

De manier waarop het programma werkt is als volgt:

Een achtergrond service welke periodiek de Paxton Net2 gebeurtenissen log controleert op nieuwe gebeurtenissen. Wanneer deze worden gevonden, stuurt de service ze door naar een syslog service naar keuze.

De service houdt (op disk) bij wat de laatst gelezen gebeurtenis was en zal dus na een herstart weer verder gaan waar het was gebleven.

RFC5424 syslog berichten worden ondersteund in zowel string als de meer formele gestructureerde data vorm.



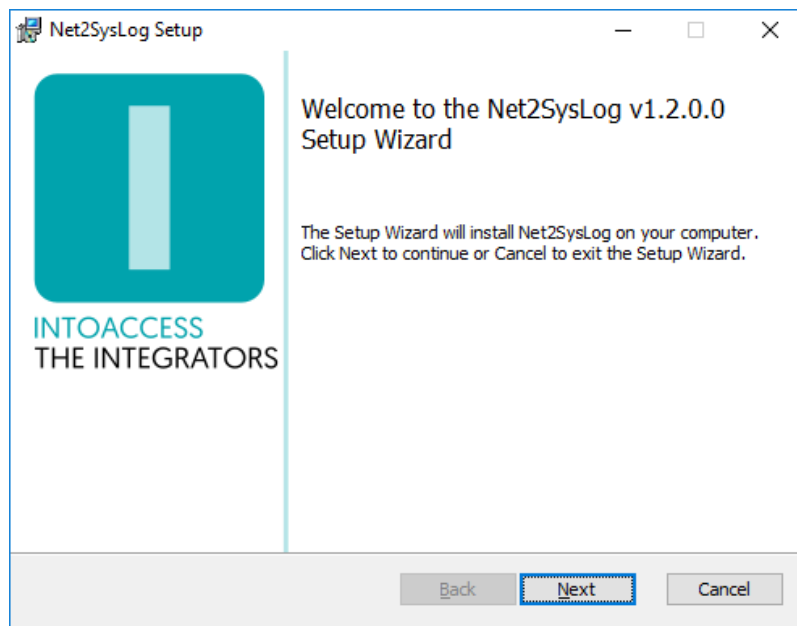
Afbeelding 1



Installatie

De applicatie kan worden geïnstalleerd, middels een enkel installatiebestand: Net2SysLog.msi

Het is niet noodzakelijk om de software op de Net2 server te installeren, maar we raden dit wel aan als meest robuuste configuratie.



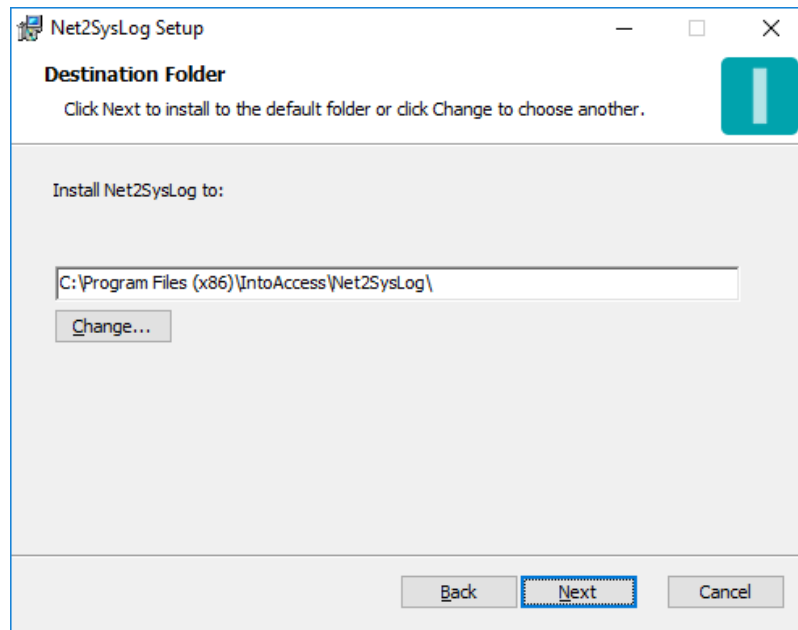
Afbeelding 2

Het eerste dialoogvenster zal aangeven welke applicatie-versie u gaat installeren. Noot: dit nummer zal bij u hoogstwaarschijnlijk anders zijn dan in Afbeelding 2.

Updates

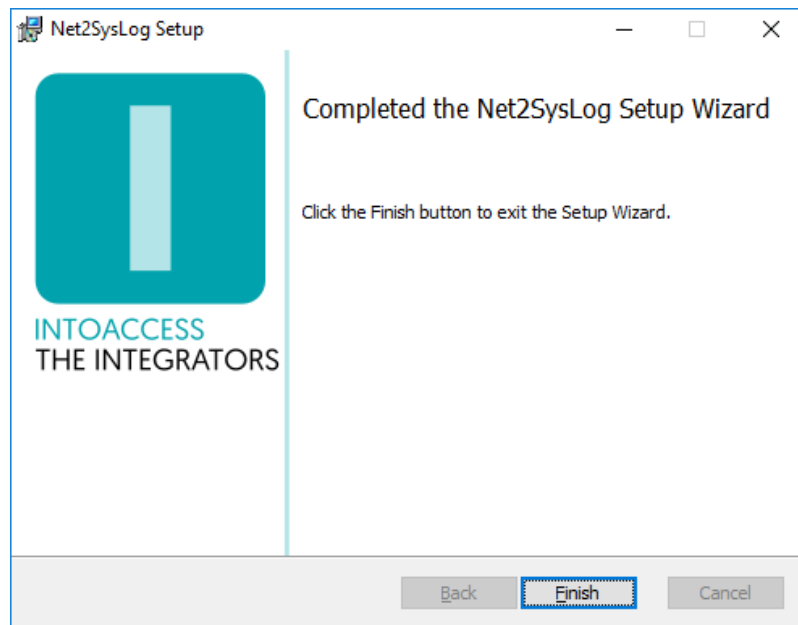
Hoewel een nieuwere versie een eventueel al aanwezige oudere versie zelf zou moeten vervangen, kun u voor de zekerheid ook eerst de bestaande applicatie de-installeren. De reeds bestaande configuratie instellingen worden daarbij niet verwijderd, dus na installatie van de nieuwe versie zou alles weer moeten werken, zonder opnieuw de configuratie-stappen uit te voeren.





Afbeelding 3

Het tweede dialoogvenster laat zien waar de applicatie zal worden geïnstalleerd. De standaard waarde is daar doorgaans prima.



Afbeelding 4

Het laatste dialoogvenster geeft aan of de installatie is gelukt.



Configuratie

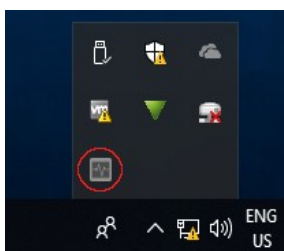
Als configuratie hulp, is de *Net2SysLog manager* beschikbaar, welke u in staat stelt om te configureren:

- hoe de applicatie met Net2 dient te verbinden;
- of u email wilt ontvangen over applicatie start/stop/fouten;
- hoe de applicatie moet koppelen aan een syslog service;
- wat voor syslog bericht type te gebruiken;
- hoe en of niet geclassificeerde gebeurtenissen moeten worden doorgegeven;

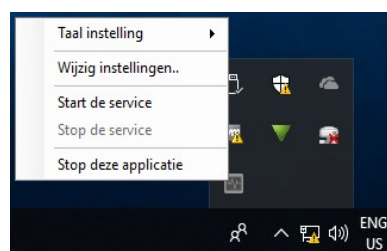
Bij het starten van de manager applicatie wordt een splash-screen getoond, waarna de applicatie onder normale omstandigheden verkleint tot een 'tray icon' in de rechter onder hoek van het scherm.



Afbeelding 5



Afbeelding 6



Afbeelding 7

Door rechts te klikken op het icoon, verschijnt een pop-up menu met diverse opties (mits het configuratie-scherm niet al is geopend).

- Taal instelling: Kies uw taal;
- Wijzig instellingen (eerst): Start de applicatie configuratie;
- Start de service: Start de service (dat kan pas na configuratie);
- Stop de service: Stop de service (dat kan pas na configuratie);



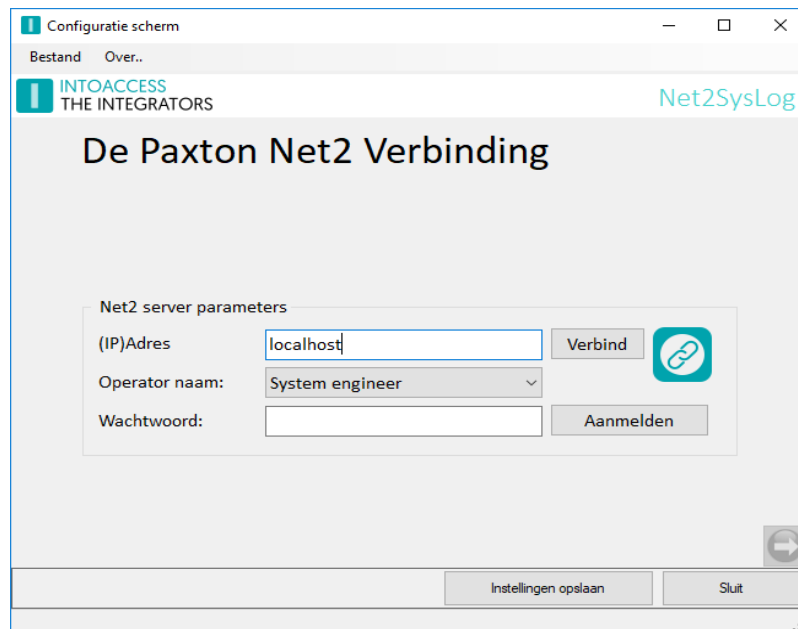
- Stop deze applicatie: Stop de manager applicatie.

De kleur van het icoon is overigens een indicatie van of de service draait. Wanneer de service (nog) niet draait, is de kleur grijs; wanneer de service draait, is het icoon gekleurd.



Net2 verbinding

De eerste configuratie-pagina is voor het definiëren van de Net2 verbinding. Wanneer u voor de eerste keer de configuratie start, zal dit enkele stappen vergen, maar nadat deze instellingen zijn opgeslagen, zal het bij een volgende keer automatisch verlopen.

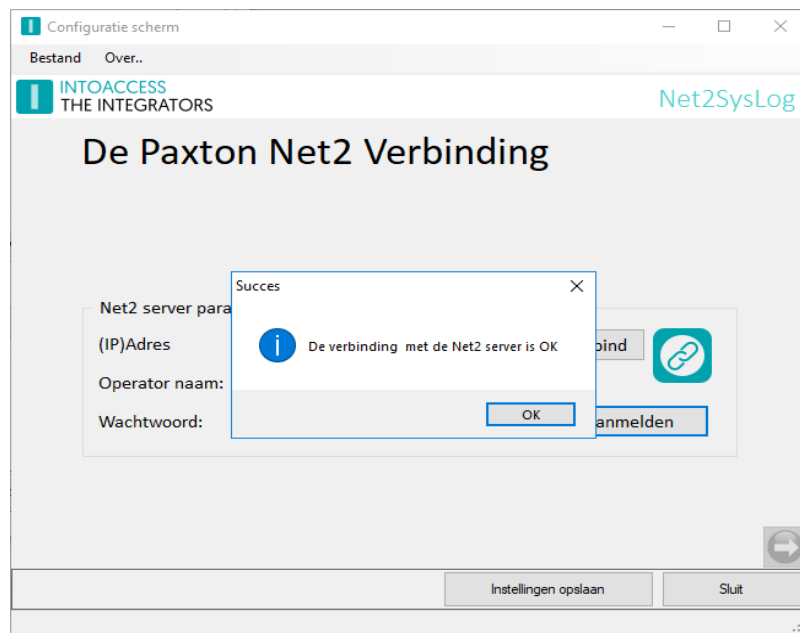


Afbeelding 8

- Voer het (ip)adres in van de Net2 server. Als u de aanwezigheid app installeert op de Net2 server zelf, kunt u de 'localhost' waarde laten staan. Gebruik geen extern adapter ip adres in dat geval!!
- Klik op de verbind knop; de app poogt nu bij Net2 de operators op te halen. (deze gebruikers vindt u onder “Net2 systeembeheerders” van de Net2 applicatie)
- Kies een operator waarmee u wilt dat de applicatie inlogt. Dit dient een operator te zijn met de “Systeembeheerder” rol.
- Voer het bijbehorende wachtwoord in.
- Klik op aanmelden.

Als alles goed gaat, zal er een bevestiging komen dat de verbinding is gelukt en de pijl in de rechter onder hoek van grijs naar gekleurd veranderen.





Afbeelding 9

U kunt nu naar het volgende configuratie-scherm, door op de pijl naar rechts te klikken.



Email instellingen

De email configuratie is optioneel en biedt de mogelijkheid om applicatie-meldingen naar een beheerder te laten sturen.

Dit is met name nuttig om vroegtijdig een indicatie te ontvangen dat er mogelijk iets mis is met de werking van de applicatie.

Webmail

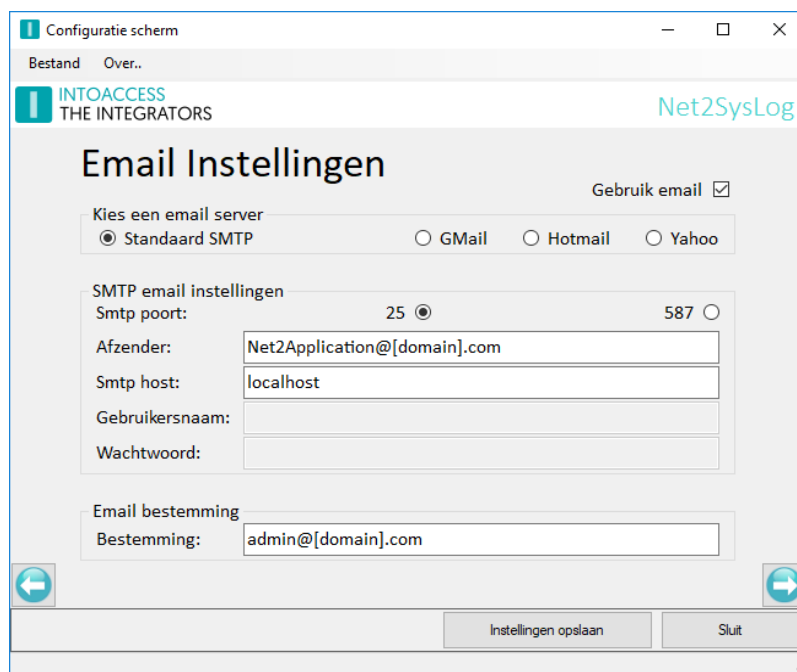
Voor het gebruik van webmail providers (zoals Gmail), kan het noodzakelijk zijn om de beveiliging te verlagen (provider account setting).

SMTP

The SMTP instellingen staan u toe een SMTP server en port te configureren. Indien u port 587 kiest, is geauthenticeerde SMTP mogelijk, waarbij u gebruikersnaam en wachtwoord kunt opgeven.

Email bestemming

Om gelijktijdig meerdere personen te adresseren, kunnen gescheiden door een ';' extra email adressen worden toegevoegd.

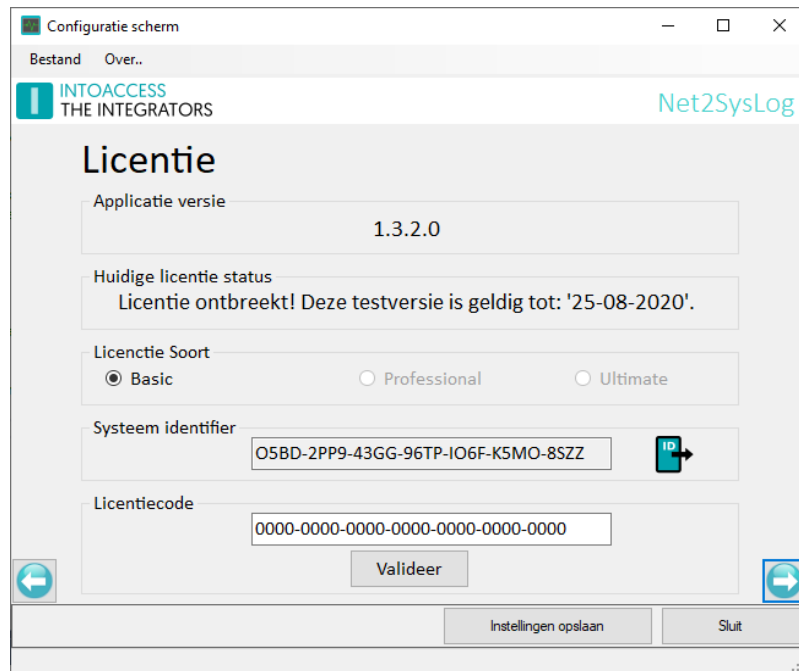


Afbeelding 10



Applicatie licentie

De proef/test versie zoals deze van de IntoAccess website kan worden gedownload, is volledig functioneel maar zal zonder licentie na een bepaalde datum niet meer werken.



Afbeelding 11

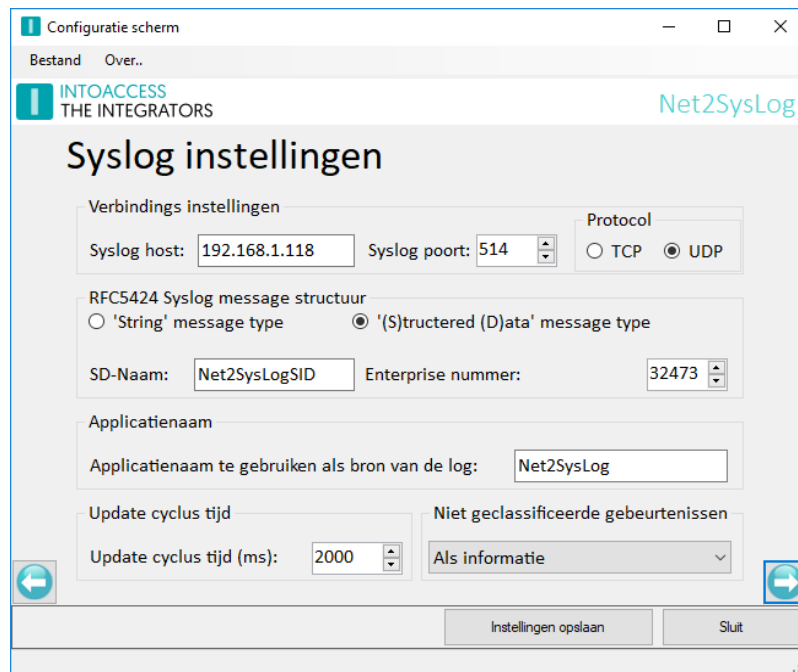
Na aanschaf van een licentie, kunt het "Systeem identifier" bestand exporteren (klik op het icoon) en aan IntoAccess (info@intoaccess.com) e-mailen, waarna u de licentiecode ontvangt.

Let op: de Systeem Identifier is verschillend per PC en daardoor ook de benodigde licentie code.



Syslog instellingen

In dit configuratie scherm kunt u definiëren hoe Net2 gebeurtenissen worden doorgegeven aan de syslog service:

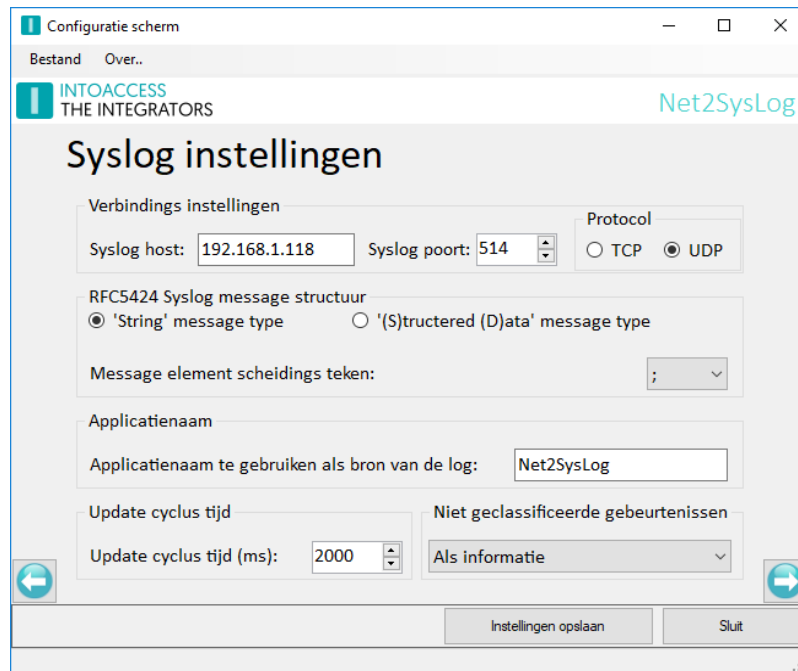


Afbeelding 12

- Verbindings instellingen:
 - Configureer het ip adres of computer naam van de computer waarop de syslog service draait;
 - Kies een poort nummer (514 is de standaard);
 - Kies een protocol (hangt af van uw syslog configuratie);
- RFC5424 Syslog message structuur:
 - Als u kiest voor het 'Structured Data' bericht type, kunt u een naam en nummer opgeven die in dit bericht worden opgenomen. Noot: het msg veld zal worden gevuld met de Net2 gebeurtenis index, opdat de syslog service niet alle berichten als identiek beschouwt. (zie ook Herhaalde berichten)
 - Als u kiest voor het string bericht type (zie Afbeelding 13), kunt u kiezen welk scheidingsteken dient te worden gebruikt voor de veld=waarde combinaties.
- Applicatie naam:
 - De applicatie naam die zal worden doorgegeven aan de syslog service. (deze naam wordt ook opgenomen in het onderwerp van e-mail notificaties).
- Update cyclus tijd:
 - De tijd in milliseconden, tussen opeenvolgende checks op nieuwe Net2 gebeurtenissen.



- Niet geclassificeerde gebeurtenissen:
 - Kies hoe en of niet geclassificeerde gebeurtenissen worden doorgegeven aan de syslog service. Niet geclassificeerde gebeurtenissen zijn doorgaans gebeurtenissen die geen fouten aangeven of gerapporteerd moeten worden. (zie ook Gebeurtenissen classificatie)

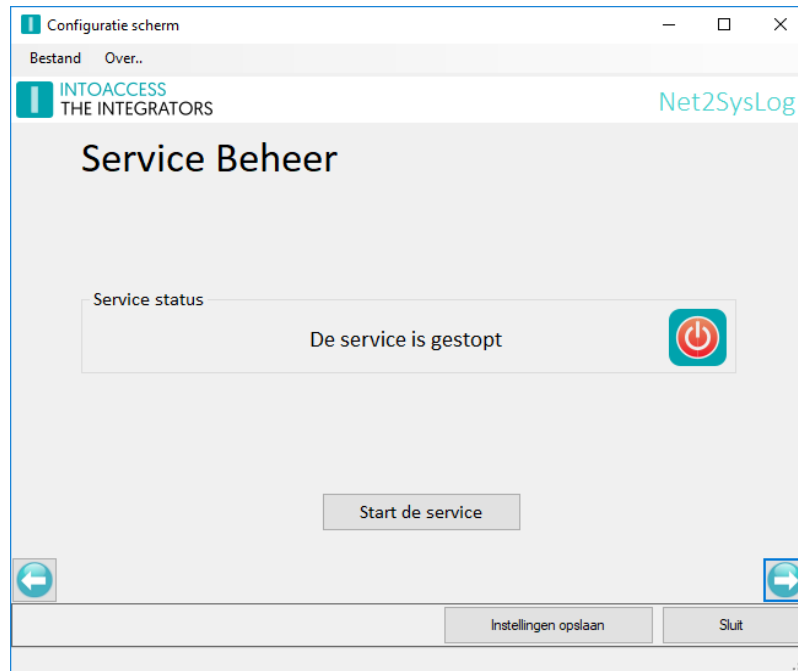


Afbeelding 13



Service beheer

De service beheer pagina biedt de mogelijkheid om achtergrond service, die de periodieke import uitvoert, te stoppen en starten.



Afbeelding 14

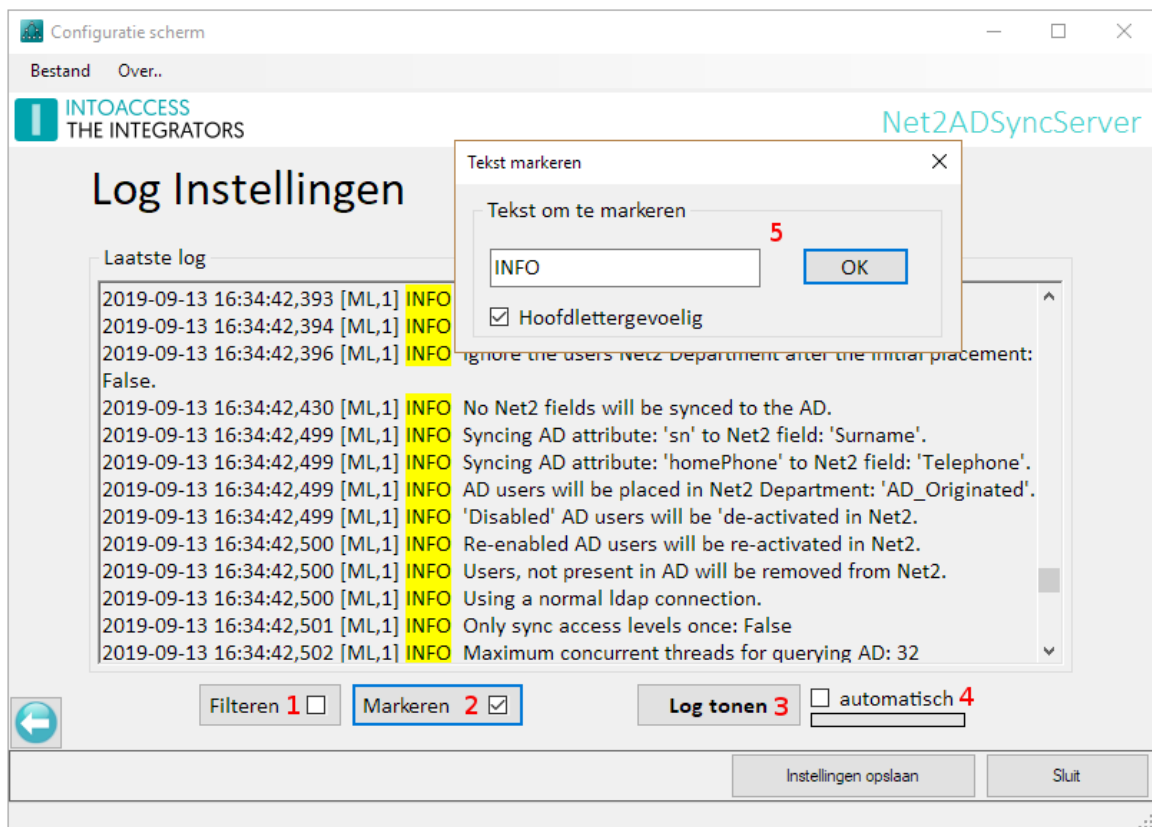
De overige manieren waarop de service kan worden gestart en gestopt zijn:

- Het tray icon pop-up menu;
- De Windows service manager (zoek "Net2SysLog");

Log instellingen

Deze pagina, zie afbeelding 15, biedt de mogelijkheid om de laatste (max. 500) regels uit de logfile te bekijken. De applicatie logt zeer gedetailleerd welke stappen de applicatie allemaal doorloopt. Mocht de applicatie met een onverwacht probleem geconfronteerd worden dan kan, met behulp van deze logfile, de oorzaak vaak snel worden gevonden.

Het loont zeker de moeite om even naar de laatste regels in deze logfile te kijken als de applicatie niet wil starten, of anderszins onverwacht gedrag vertoont.



Afbeelding 15

Deze pagina biedt ook de mogelijkheid om de logfile op bepaalde termen te filteren (1) en/of bepaalde termen te markeren (2). Een voor de hand liggende 'filter term' zou bijvoorbeeld het woord "ERROR" of "WARN" kunnen zijn. Als de applicatie goed werkt zouden beide termen niet voor mogen komen in de logfile.

Optie (4) biedt de mogelijkheid om de logfile automatisch met een vaste interval opnieuw te laden.

De log file(s) zelf bevinden zich in de folder:

c:\IntoAccess\Logging\Net2SysLog



Gebeurtenissen classificatie

In dit hoofdstuk vindt u de toegepaste Net2 gebeurtenissen classificatie. Alle overige gebeurtenissen worden als “Niet geclassificeerd” beschouwd.

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 permitted 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 service

Hoewel dit buiten de scope van dit document valt, biedt dit hoofdstuk wat informatie over de syslog configuratie op een Ubuntu server.

Zelfs als u een ander systeem gebruikt, zou dit nuttig kunnen zijn.

Op Ubuntu, heet de syslog service rsyslog en heeft zijn configuratie in het `/etc/rsyslog.conf` bestand en enige `*.conf` bestanden in de `/etc/rsyslog.d/` map.

UDP inschakelen

Om het UDP protocol in te schakelen, voeg de volgende regels toe (of haal de commentaar tekens weg):

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

TCP inschakelen

Om het TCP protocol in te schakelen, voeg de volgende regels toe (of haal de commentaar tekens weg):

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

Template

De standaard bericht template, zal gestructureerde data niet weergeven. Om deze (en andere) data ook te kunnen zien, kunt u het standaard template op de volgende manier aanpassen:

Voeg een nieuwe template definitie regel toe:

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

Wijzig de gebruikte template (origineel uitgecommentarieerd):

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

Herhaalde berichten

De syslog service kan herhalende berichten onderdrukken, waarvan de velden `msg`, `hostname`, `procid` and `appname` gelijk zijn. U kunt dit gedrag in of uit schakelen, middels de volgende instelling:

```
$RepeatedMsgReduction off/on
```





Handleiding Net2SysLog
Versie 1.4

