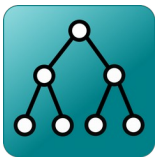
INTOACCESS
THE INTEGRATORS



Net2ADSyncServer

Handleiding 2.11

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

Index

Installatie en configuratie van de Net2ADSyncServer

Installatie

De Net2ADSyncServer applicatie wordt geïnstalleerd met behulp van een enkel Windows Installatie bestand (*.msi) De gehele installatie bestaat uit een 'manager' applicatie, welke speciaal bedoeld is voor het configureren van de eigenlijke service, en de synchronisatie service zelf.

Werking

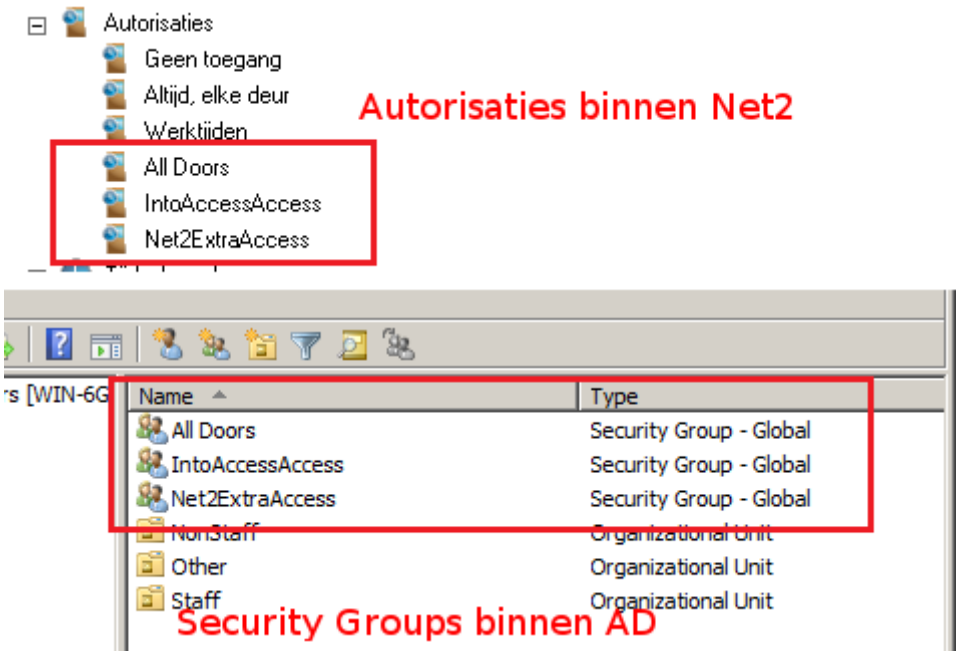
Deze applicatie is ontworpen vanuit het basis idee dat het beheer van alle medewerkers centraal gebeurt op de Active Directory server. Vanuit deze AD worden, initieel, alle relevante gegevens gekopieerd naar de Net2 database. Wijzigingen die daarna binnen de AD aangebracht worden, worden daarbij automatisch ook doorgevoerd in de Net2 database.

Versie 2.x ondersteunt ook het synchroniseren van kaart en/of pincodes, en speciaal aangewezen gebruikersvelden, **naar de AD**.

Synchronisatie regels

De Net2ADSyncServer applicatie gaat, voor de synchronisatie, uit van de volgende regels:

In AD moeten er één of meer 'Security Groups' bestaan, **waarvan de naam overeenkomt** met een 'Autorisatie' binnen Net2. Zie afbeelding 1.



Afbeelding 1

Gebruikers die binnen AD lid zijn van één* van deze 'Security Groups' zullen automatisch naar Net2 gesynchroniseerd worden, en de gelijknamige autorisatie toegekend krijgen. Optioneel kunnen er ook 'extra' gegevens worden gesynchroniseerd, waaronder ook eventuele Kaart/badge nummers.

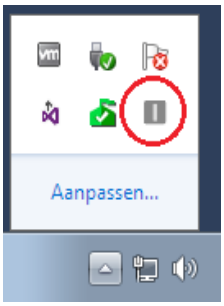
(*) Deze restrictie geldt niet voor de 'Ultimate' versie. Meer details kunt u vinden onder het kopje 'licentie'.

Verder gelden de volgende regels voor de synchronisatie:

- AD gebruikers die geen lid zijn van een van deze speciale 'Security Groups' worden niet gesynchroniseerd.
- Gebruikers, die voor de installatie van de applicatie reeds in Net2 aanwezig waren, worden door de applicatie genegeerd. De Manager applicatie zal hier wel een waarschuwing over geven omdat het gevaar bestaat dat deze gebruikers dubbel in Net2 terecht zullen komen indien deze gebruikers ook in AD voorkomen. Dit kan een serieus probleem opleveren indien deze gebruikers reeds over een kaart/badge beschikken. Het aanmaken van een badge/kaart voor deze nieuw in te brengen gebruikers zal dan fout gaan.

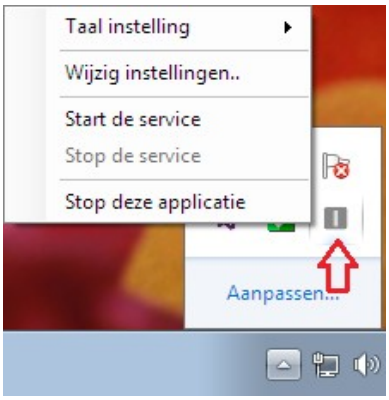
Configuratie

Het configureren van de Net2ADSyncServer applicatie moet gebeuren met behulp van de bijgeleverde 'Manager applicatie' (Net2ADSyncService Manager). Deze applicatie zal bij het opstarten gedurende een aantal seconden een melding geven en zich daarna in het systeemvak in de rechter onderhoek van de taakbalk vestigen. Zie afbeelding 2.



Afbeelding 2

Een klik met de rechter muisknop opent het hoofdmenu. Zie afbeelding 3.



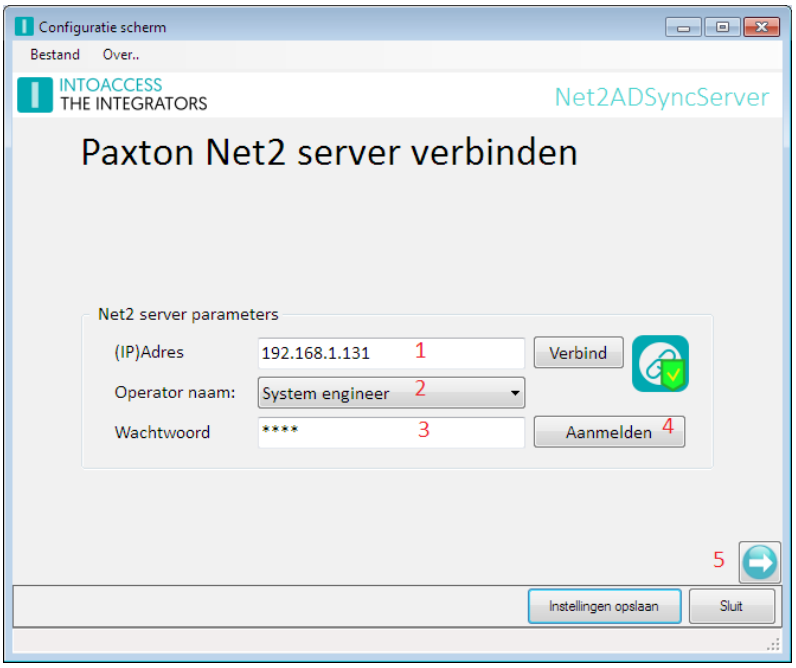
Afbeelding 3

Het kan zijn dat de applicatie in eerste instantie een Engelstalig menu laat zien, dit kan worden aangepast door 'Nederlands' te kiezen bij de menu optie 'taalinstellingen' /'Language settings'.

Zolang de applicatie nog niet geconfigureerd is, zijn de menu opties voor het starten en stoppen van de service niet actief. Kies als eerste de menu optie: 'wijzig de instellingen eerst..'

Net2

De applicatie opent met het scherm waarmee de instellingen voor de verbinding met de Net2 server kunnen worden opgegeven. Zie afbeelding 4.



Afbeelding 4

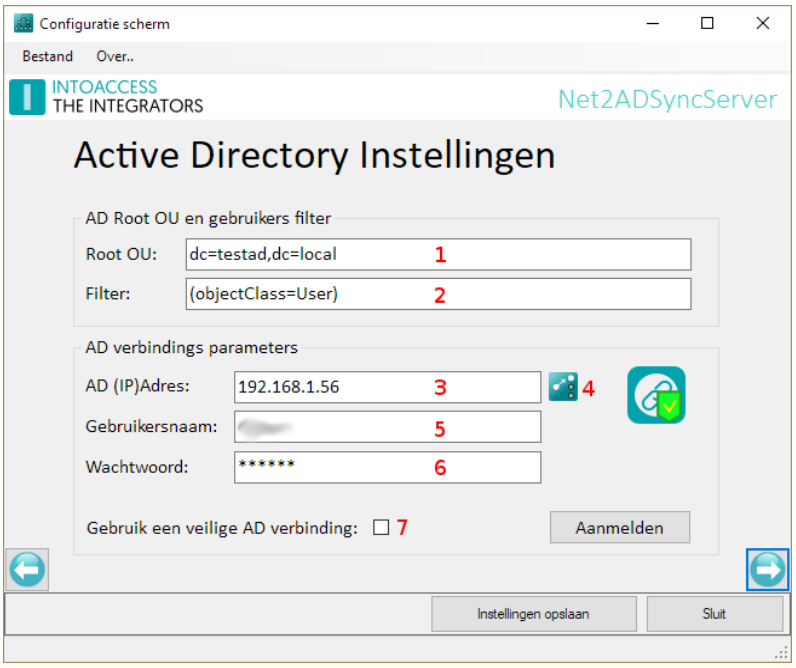
- Als eerste zal het (IP) adres van de PC gevraagd worden waarop de Paxton Net2 server is geïnstalleerd (1). Dit mag het IP adres zijn, of de netwerk naam van de betreffende machine. Indien deze applicatie op dezelfde machine is geïnstalleerd kan het beste 'localhost' als adres worden opgegeven.

  Klik na het opgeven van het adres op 'Verbind'. Hierna zal de applicatie proberen om een verbinden met de Net2 server op te bouwen en, als dat gelukt is, een lijst met ‘Net2 Systeem beheerders' ophalen. Deze worden daarna in de middelste ‘drop-down’ lijst getoond.
- Kies hier de gewenste beheerder (2) en voer daarna zijn/haar wachtwoord in. Het standaard wachtwoord voor de systeembeheerder, 'Net2', staat standaard ingevuld (3).
- Klik daarna op de knop '*Aanmelden*' (4). Als de verbinding opgezet kan worden, wordt hier een melding over gegeven en wordt de 'pijltjes-knop' rechtsonder actief. (5)

Er wordt een zo adequaat mogelijke foutmelding gegeven indien er in dit proces iets fout gaat.

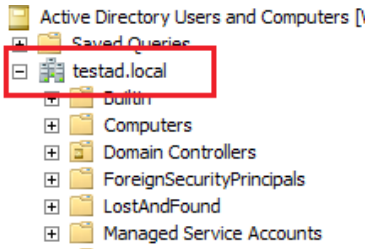
De Active Directory instellingen

Op deze pagina kunnen de parameters voor het opzetten van de verbinding met de AD server opgegeven worden. Zie afbeelding 5.



Afbeelding 5

- Als eerste wordt gevraagd naar de 'Root OU'. (1). Vul in dit veld in ieder geval het volledige 'Domain Component' (dc) in. In het voorbeeld is de syntaxis opgegeven zoals die behoort bij de AD van afbeelding 6. Indien alle medewerkers zich in een specifieke OU bevinden, kan deze hier ook opgenomen worden.

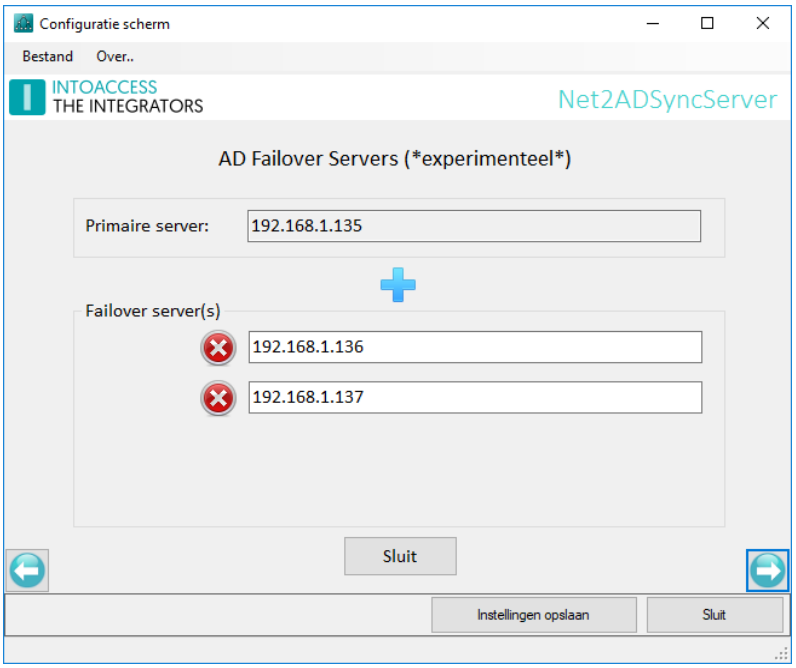


Afbeelding 6

- Het filter onder (2) wordt gebruikt bij het opvragen van de AD gebruikers. Alleen in uitzonderlijke gevallen kan het voordeel opleveren om dit filter aan te passen.
- Vervolgens wordt er gevraagd om het AD (IP) adres van de server (3). Ook hier geldt weer dat er een IP adres, of een netwerknaam, opgegeven kan worden. Indien u op het icoon (4) aan de rechterzijde klikt, kunt u optioneel, 'failover' servers opgeven. Zie afbeelding 7. Noot: dit is een experimentele optie.
- De gebruiker, waar in veld (5) om gevraagd wordt, zal gebruikt worden om de applicatie aan te melden bij de AD. Als er alleen gegevens **van** de AD **naar** Net2 toe gesynchroniseerd hoeven te worden is het voldoende als deze gebruiker alleen 'leesrechten' heeft.

- Geef bij veld (6) het wachtwoord van deze gebruiker op.

  Alle wachtwoorden worden versleuteld opgeslagen in het configuratiebestand.
- Indien het noodzakelijk is om een beveiligde verbinding (LDAPS, poort 636) te gebruiken, kunt u deze optie aanvinken (7). Houd er rekening mee dat de AD server in dat geval een geldig SSL certificaat dient te hebben.



Afbeelding 7

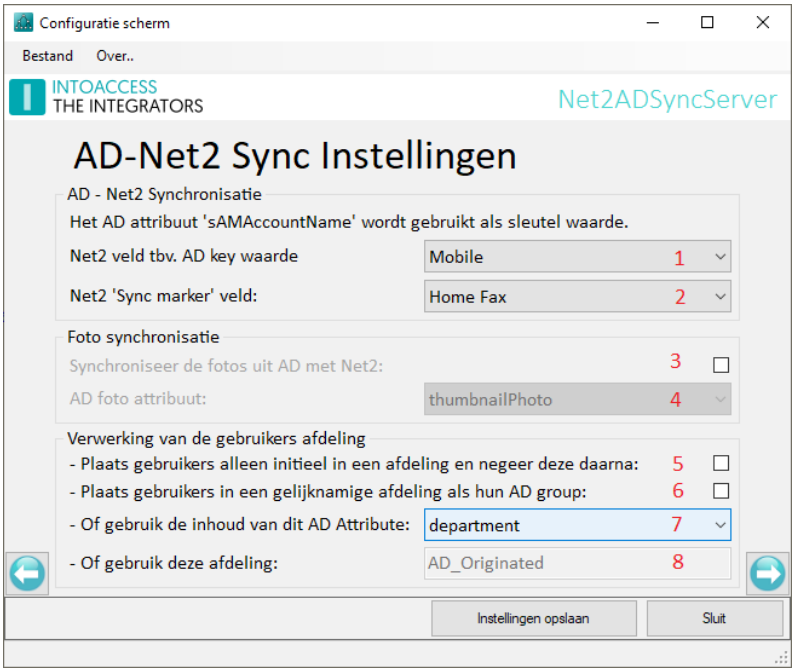
De AD-Net2 Synchronisatie instellingen

Deze pagina, zie afbeelding 8, heeft o.a. betrekking op de twee Net2 velden die gebruikt zullen gaan worden voor de opslag van ‘meta informatie’ ten behoeve van het synchronisatieproces zelf. De applicatie gebruikt de AD waarde 'sAMAccountName' als 'sleutel' voor het uniek identificeren van de medewerkers. Deze waarde moet daarom altijd bij de andere gegevens van de betrokken medewerker worden opgeslagen.

Daarnaast zal de applicatie nog een ander veld gebruiken om aan te geven dat de gegevens van de desbetreffende medewerker beheerd worden door de applicatie. Medewerkers waarbij het betreffende veld leeg is (of een andere waarde bevat), zullen door de applicatie genegeerd worden.

In het met middelste kader wordt de mogelijkheid geboden om ook foto’s vanuit AD naar Net2 te synchroniseren.

In het onderste gedeelte kan worden opgegeven in welke Net2 afdeling (‘Department’) de gesynchroniseerde medewerkers zullen worden geplaatst.



Afbeelding 8

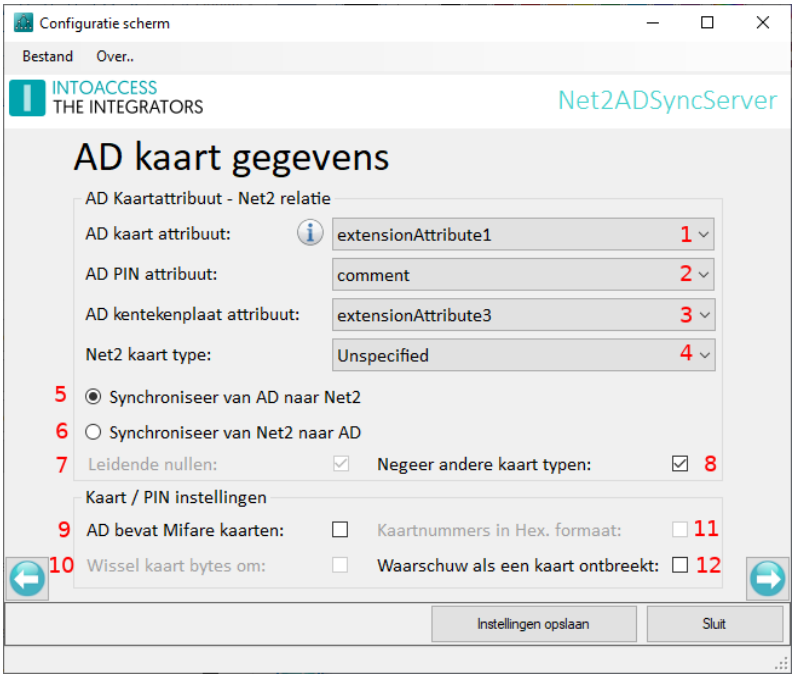
- Als eerste wordt gevraagd naar het Net2 gebruikers veld waar de 'sAMAccountName' waarde in moet worden opgeslagen (1). Kies hiervoor een van de velden die niet voor een ander doel gebruikt gaan worden.
- Het volgende veld zal gebruikt worden voor de opslag van de 'marker' waarde (2). Dit veld zal gevuld worden met de tekst: “AD_SYNCED”.
- Middels het zetten van een vinkje bij (3) kan worden aangegeven dat ook eventueel in AD aanwezige foto’s moeten worden gesynchroniseerd naar Net2. Als dit inderdaad gewenst is, dan kan bij (4) aangegeven worden welk AD attribuut gebruikt wordt voor de opslag van de foto’s.
- Bij (5) kan worden aangegeven of de afdeling, waarin de gebruikers initieel zullen worden geplaatst, onderdeel moet blijven van het synchronisatieproces. Indien aangevinkt mogen de

gebruikers handmatig naar een andere afdeling worden verplaatst zonder dat de applicatie de gebruikers weer terugplaatst. Op pagina ‘Speciale Instellingen’ kan worden opgegeven dat gebruikers die niet langer meer voorkomen in de AD in een speciale afdeling moeten worden geplaatst. Deze instelling heeft een hogere prioriteit dan deze. Gebruikers met een ‘uitgeschakeld’ (disabled) account kunnen wel in een andere afdeling worden geplaatst.

- Vervolgens wordt gevraagd naar de naam van de 'afdeling' waar de nieuwe gebruikers zullen worden geplaatst.
- Hier kan de keuze worden gemaakt tussen een afdeling met de zelfde naam als de toegewezen autorisatie. (6), of
- Een afdeling waarvan de naam is opgeslagen in een van de AD attributen. (7)
- Een specifieke afdeling (8).

Afdeling zullen door de applicatie worden aangemaakt, zowel bij (7) als bij (8) indien deze nog niet bestaan.

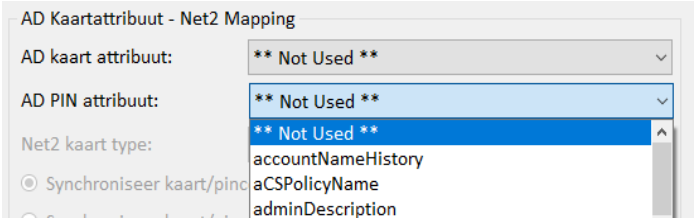
De AD kaart gegevens



Afbeelding 9

De pagina heeft betrekking op eventuele kaart-, PIN- of kentekens die reeds in AD aanwezig zijn, of naar de AD toe gesynchroniseerd moeten worden. Zie afbeelding 9.

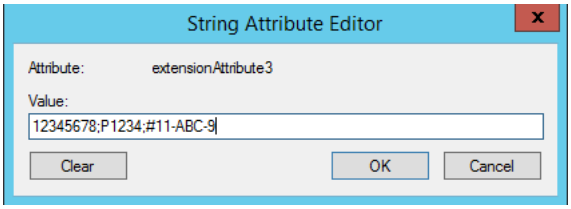
- Kies onder (1) en (2) voor de optie: ''**Not Used**'', zie afbeelding 10, indien de AD géén kaart/ PIN-nummers/nummerplaten bevat, (of moet gaan bevatten) en negeer de overige instellingen.



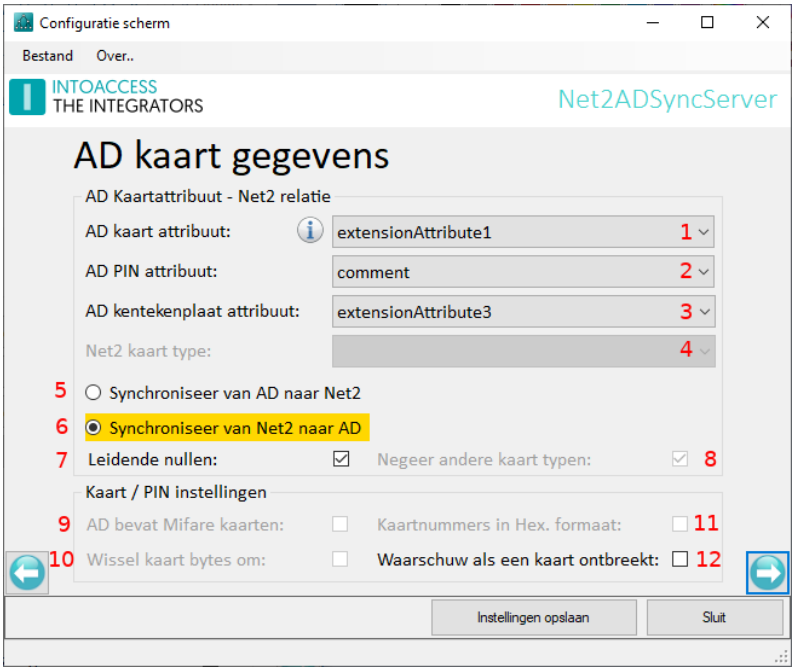
Afbeelding 10

- Kies het AD attribute dat in AD gebruikt wordt voor de opslag van het kaart/PIN-nummer/nummerplaat (1).

  Kaarten, PIN-nummers en nummerplaten kunnen in aparte AD attributen worden opgeslagen en/ of in één enkel gecombineerd veld. In het laatste geval moet het PIN nummer vooraf worden gegaan door de letter '**P**' en voor de nummerplaten is dat een hekje/hashtag '**#**'. De waarden worden gescheiden van het kaartnummer door een scheidingsteken (<komma>, <punt-komma>, <spatie> of een <tab>). De onderlinge volgorde is daarbij niet van belang.
- Voorbeeld: een gebruiker heeft een kaart met nummer 12345678, een pincode met nummer 1234 en een nummerplaat met nummer 11-ABC-9. De waarde voor het kaart attribuut in Active Directory moet dan als volgt worden opgegeven:



- Indien het PIN nummer in een apart AD attribuut opgeslagen is kan dat worden opgegeven in (2). In dit geval mag het PIN nummer **niet** vooraf worden gegaan door de letter 'P'.
- Indien de nummerplaten in een apart AD attribuut zijn opgeslagen, kan dat worden opgegeven in (3). In dit geval mag een nummerplaat **niet** vooraf worden gegaan door een hashtag '#'.
- Kies onder (4) het kaarttype dat gebruikt wordt. Kies 'Unspecified' indien het gebruikte kaarttype niet in de lijst voorkomt. Als het kaart attribuut op iets anders staat dan '**Not Used**', zal de applicatie niet toestaan dat handmatig of vanuit derden andere kaarten worden toegevoegd, tenzij bij (8) wordt aangevinkt om andere kaart typen te negeren.



Afbeelding 11

- Bij (5) en (6) kan worden aangegeven of kaart/PIN informatie **naar-** of **vanuit-** de AD gesynchroniseerd moet worden.
- Het wordt duidelijk aangegeven als de keuze wordt gemaakt om kaart/PIN informatie **naar** de AD toe te synchroniseren, zie afbeelding 11, juist om te voorkomen dat deze optie onbedoeld geselecteerd wordt.
- Vink de optie 'Leidende nullen' aan als het kaartnummer '123' als '00000123' in de AD moet verschijnen.

- De applicatie kan eventuele Mifare kaarten (9), zowel de 4 bytes 'Classic', als de 7 bytes 'DESFiRE' kaarten, automatisch converteren naar de nummers zoals die door Paxton gebruikt worden. De lengte van de Mifare kaartnummer wordt automatisch herkend.
- In een enkel geval zijn de afzonderlijke 'bytes' van het Mifare kaartnummers onderling omgewisseld, zet in dat geval het vinkje bij (10).
- In de meeste gevallen zal het nummer van de Mifare kaart in het Hexadecimale formaat zijn opgeslagen, vink in dat geval (11) aan.
- Onder (12) wordt de optie geboden om de applicatie een foutmelding te laten versturen, (zie ook bij e-mail instellingen), indien de kaart-/badge gegevens ontbreken van een of meer medewerkers.

Synchronisatie van Mifare kaartnummers naar de AD

De optie om kaart/PIN nummers naar de AD te synchroniseren heeft, bij gebruik van Mifare kaarten, de beperking dat alleen het Paxton kaartnummer wordt gesynchroniseerd en niet het Mifare kaartnummer zelf. Dit kan ondervangen worden door het Mifare kaartnummer in een van de Net2 gebruikersvelden op te slaan. Dit veld kan dan met het gewenste AD attribuut gesynchroniseerd worden (zie ook de paragraaf: 'AD-Net2 veldnaam relatie'). Eventueel is het dan ook nog mogelijk om dit zelfde AD attribuut weer als 'bron' te laten fungeren voor het kaartnummer in Paxton.

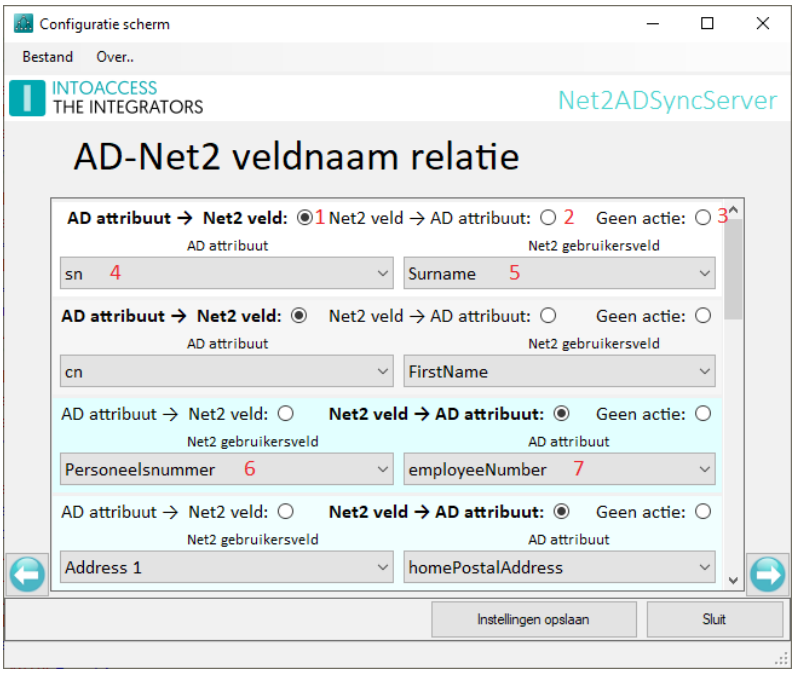
Concreet zou dit als volgt ingesteld kunnen worden:

- *Het Mifare kaartnummer wordt opgeslagen in Net2 gebruikersveld 'Personeelsnummer';*
- *Het 'Personeelsnummer' veld wordt gesynchroniseerd met AD attribute 'extensionAttribute1';*
- *Het zelfde 'extensionAttribute1' wordt als 'AD kaart attribuut' geselecteerd;*
- *Bij de kaart/PIN instellingen wordt aangegeven dat het een Mifare kaart betreft.*

Zodra er een nieuw, of aangepast, Mifare kaartnummer wordt gedetecteerd, zal deze in de AD worden aangepast. De daarop volgende synchronisatieslag zal de applicatie het aangepaste Mifare kaartnummer weer als Paxton kaartnummer synchroniseren naar Paxton toe.

De AD-Net2 Veldnaam relatie

Deze pagina biedt de mogelijkheid om meerdere AD attribuut waarden op te nemen in het synchronisatieproces. Zie afbeelding 12.



Afbeelding 12

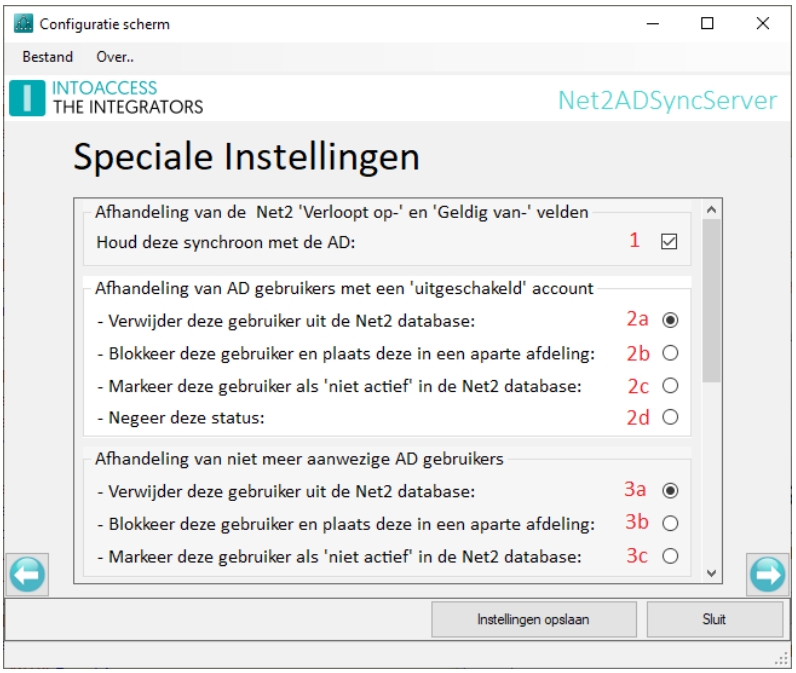
In alle gevallen moet het Net2 veld: 'Surname' opgenomen zijn in deze lijst.

Als absoluut minimum volstaat het als alleen de AD waarde 'sAMAccountName' wordt toegewezen aan het veld Surname. Zie paragraaf: “AD-Net2 Synchronisatie instellingen”.

- Kies als eerste de ‘bron’ of het ‘doel’ van de synchronisatie bij (1) of (2).
- De optie (1) biedt de mogelijkheid om een AD attribuut te synchroniseren met een Net2 gebruikers veld waarbij het AD attribuut leidend is.
  - Kies in dit geval het gewenste AD attribuut bij (4) en het gewenste Net2 gebruikers veld bij (5).
- De optie bij (2) biedt de mogelijkheid om een Net2 gebruikers veld met een AD attribuut te synchroniseren waarbij het Net2 veld leidend is.
  - Kies in dit geval bij (6) het gewenste Net2 veld en bij 7 het gewenste AD attribuut.
- Selecteer ‘Geen actie’ (3) om een veld uit het synchronisatieproces te verwijderen.

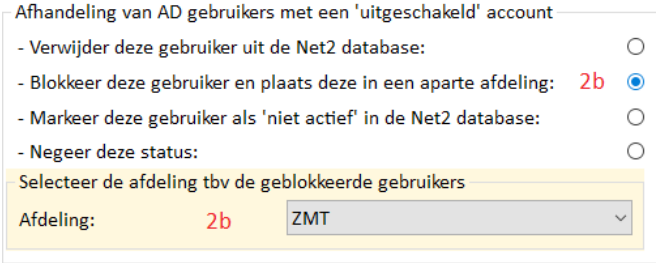
Speciale Instellingen

Deze pagina, zie afbeeldingen 13 t/m17, biedt de mogelijkheid om een afwijkende waarde in te stellen voor enkele van de basisparameters. In de meeste gevallen zullen de reeds ingestelde waarden voldoen, slechts in uitzonderingsgevallen kan het gewenst zijn om hier een afwijkende waarde in te stellen.



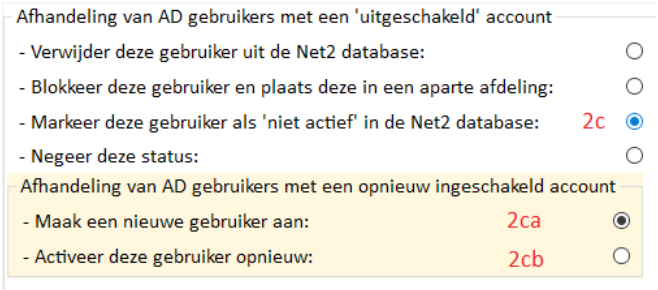
Afbeelding 13

- Als het vinkje bij (1) gezet is worden de ‘Geldig van-’ en ‘Verloopt op-’ Net2 gebruikers velden synchroon gehouden met de ‘whenCreated’ en ‘accountExpires’ AD attributen. Bij het verwijderen van het vinkje kunnen deze velden apart worden ingesteld in Net2. Nieuw ingebrachte gebruikers zullen dan alleen initieel van de ‘whenCreated’ en ‘accountExpires’ waarden worden voorzien.
- Bij (2x) kan worden ingesteld hoe de applicatie moet omgaan met gebruikers waarvan het account in AD is uitgeschakeld (‘disabled account’).
  - Standaard (2a) zullen deze gebruikers worden verwijderd uit Net2.
  - De optie (2b) zorgt ervoor dat deze gebruikers geblokkeerd worden en tevens in een aparte afdeling worden geplaatst. Indien deze optie wordt geselecteerd wordt tevens de mogelijkheid geboden om de betreffende afdeling te selecteren. Zie afbeelding 14



Afbeelding 14

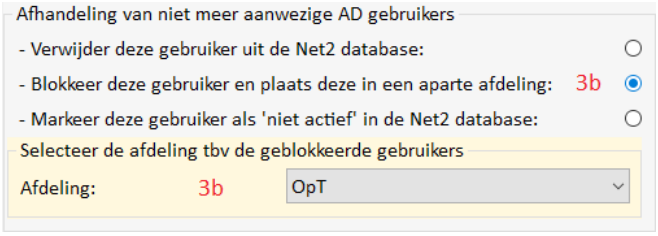
- Bij (2c) biedt de optie om de gebruiker te markeren als ‘niet actief’ binnen Net2. Gebruikers met deze status hebben geen toegangsrechten en zijn niet zichtbaar binnen Net2. De historie van dergelijke gebruikers blijft wel bestaan. Indien deze optie gekozen wordt wordt tevens gevraagd, zie afbeelding 15, wat er moet gebeuren indien een dergelijke gebruiker weer opnieuw ‘ingeschakeld’ wordt.



Afbeelding 15

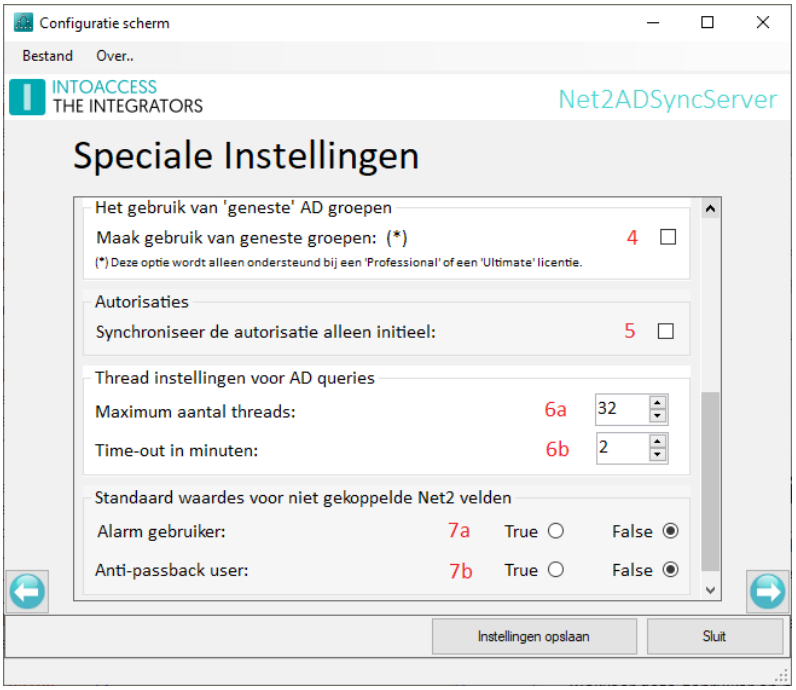
  - Indien de optie (2ca) gekozen wordt zal op dat moment een geheel nieuwe gebruiker worden aangemaakt.
  - Bij optie (2cb) wordt de betreffende gebruiker weer opnieuw actief gemaakt.
- Optie (2d) biedt de mogelijkheid om deze AD status volledig te negeren. Gebruikers met een ‘uitgeschakeld’ AD account worden dan hetzelfde verwerkt als gebruikers met een ingeschakeld account.

- Bij (3x) kan worden opgegeven hoe de applicatie moet omgaan met gebruikers die niet langer meer aanwezig zijn in AD.
  - Normaal gesproken (3a) worden deze gebruikers uit de Net2 database verwijderd. Bezwaar van het volledig verwijderen van een gebruiker is dat daarmee ook de volledige historie van deze gebruiker wordt verwijderd.
  - Als alternatief kan deze gebruiker ook geblokkeerd worden en in een aparte afdeling worden geplaatst. Indien deze optie wordt geselecteerd wordt tevens de mogelijkheid geboden om de betreffende afdeling te selecteren. Zie afbeelding 16



Afbeelding 16

  - Als laatste wordt ook de optie geboden (3c) om deze gebruiker alleen op ‘inactief’ te zetten.

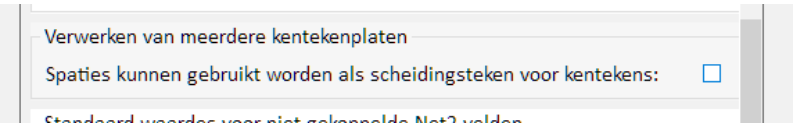


Afbeelding 17

- Bij (4), zie afbeelding 17, wordt de mogelijkheid geboden om in AD van ‘geneste’ groepen gebruik te maken.

  (Voor meer informatie over de inzet van geneste groepen zie het kopje ‘Gebruik van geneste AD groepen’ op de volgende pagina).
- Autorisaties worden alleen initieel gezet als het vinkje bij (5) staat aangevinkt. Dat betekent dat enkel bij het aanmaken van de gebruiker in Net2, de autorisatie wordt gesynchroniseerd. Daarna kan men een andere autorisatie toekennen aan de gebruiker, zonder dat dit door de synchronisatie wordt beïnvloed. Deze instelling wordt genegeerd voor gebruikers met een uitgeschakeld (disabled) account, en gebruikers die niet langer meer voorkomen in de AD en die in een aparte afdeling geplaatst moeten worden. (Zie 2b en 3b)
- De gegevens worden zo effectief mogelijk opgehaald uit de Active Directorty. De applicatie voert hiervoor veel taken gelijktijdig uit. In sommige gevallen, bijvoorbeeld bij oude machines, kan dit tot problemen leiden. In zulke gevallen kan het aantal threads (grofweg het aantal gelijktijdige processen) worden beperkt. Bij (6a) en (6b) kunnen aanpassingen worden gedaan om de applicatie voor uw situatie zo optimaal mogelijk te laten lopen.
- Als elke gebruiker in Net2 het inbraaksysteem in- en/of uit- moet kunnen schakelen, of de anti-passback regels in acht moet nemen, dan kan bij (7a) of (7b) een vinkje worden gezet. Dit werkt alleen als er geen AD veld is gekoppeld voor deze Net2 velden in het scherm ‘AD-Net2 veldnaam relatie’.

In versie 2.13.9 is de optie toegevoegd om het gebruik van spaties als scheidingsteken tussen kentekens uit te schakelen. (zie afbeelding: 18)

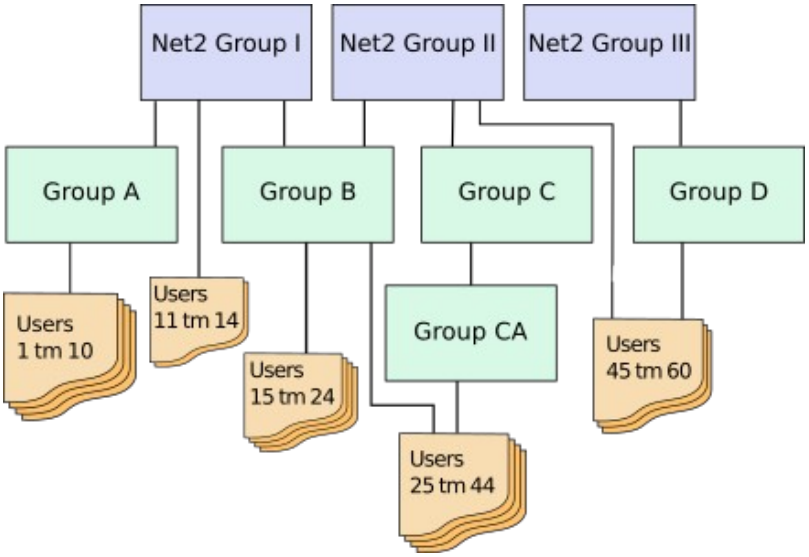


Afbeelding: 18

Deze optie is speciaal toegevoegd voor de Engelse markt. In tegenstelling tot Nederland is een spatie daar een legitiem karakter in het kenteken.

Gebruik van geneste AD groepen

Hieronder is deze mogelijkheid nader uitgewerkt. Zie afbeelding 19.



- Afbeelding 19

- In dit voorbeeld vertegenwoordigen de AD security groepen: 'Net2 Group I' t/m 'Net2 Group III' de groepen waarvan een gelijknamige autorisatie aanwezig is in Net2.
- De AD groepen: 'Group A t/m Group CA' zijn 'gewone' security groepen, dit zijn dus groepen zonder tegenhanger in Net2.
- De gebruikers: 'Users 1 tm 10' zijn via 'Group A' lid van 'Net2 Group I'. Deze gebruikers zullen nu in het synchronisatie proces worden opgenomen en binnen Paxton de autorisatie 'Net2 Group I' krijgen. Als er géén gebruik gemaakt wordt van geneste groepen zullen deze gebruikers ook niet gesynchroniseerd worden.
- De gebruikers: 'Users 11 tm 14 zijn direct lid van 'Net2 Group I'. Deze gebruikers zullen in het synchronisatie proces worden opgenomen, ongeacht de instelling voor het gebruik van geneste groepen.
- De gebruikers: 'Users 15 tm 24 zijn via 'Group B' zowel lid van 'Net2 Group I' als van 'Net2 Group II'. Deze gebruikers zullen een autorisatie toegewezen krijgen die de verzamelde rechten bevat van autorisatie 'Net2 Group I' en 'Net2 Group II'.
- De gebruikers: 'Users 25 tm 44 zijn zowel via de groepen 'Group CA' → 'Group C', als via 'Group B' lid van de 'Net2 Group II'. Daarnaast zijn zij, via de 'Group B' ook nog lid van 'Net2 Group I'. Gebruikers mogen dus via verschillende wegen lid zijn van een, aan een Net2 gerelateerde, autorisatie groep;
- De gebruikers: 'Users 45 tm 60' zijn direct lid van 'Net2 Group II' en via 'Group D' ook lid van 'Net2 Group III'.

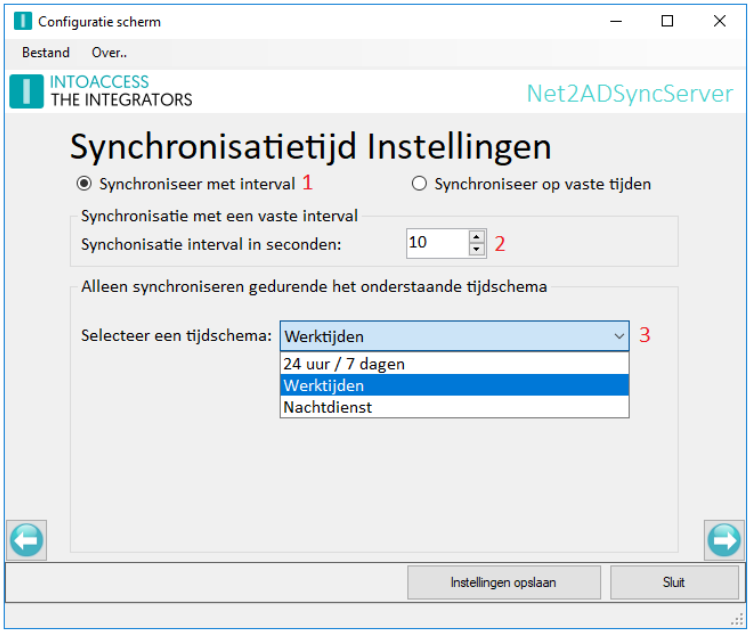
Let erop dat dit voorbeeld een 'Ultimate' licentie vereist omdat de gebruikers hier lid zijn van meer dan één (aan een Net2 autorisatie gerelateerde) groep.

Synchronisatietijd Instellingen

Deze pagina, zie afbeelding 20 en 21, biedt de mogelijkheid om de applicatie de synchronisatie uit te laten voeren met een vaste interval, of dagelijks op vaste tijden.

Synchronisatie met een vast interval

Indien men kiest voor synchronisatie met een vaste interval (1), kunnen twee velden worden ingevoerd. De werkelijke intervaltijd kan worden ingesteld bij (2). De minimale intervaltijd is 10 seconden, een dergelijke kleine intervaltijd is echter alleen in zeer uitzonderlijke gevallen noodzakelijk. Een waarde van 300 seconden (5 min), of zelfs nog groter, is in de meeste gevallen ruim voldoende.



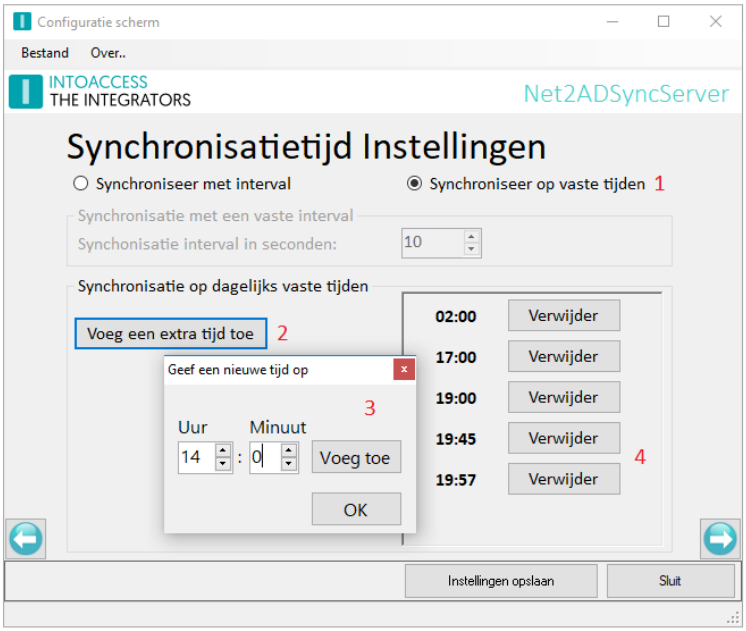
Afbeelding 20

In dit geval zal de synchronisatie alleen plaats vinden gedurende het geselecteerde tijdschema. Er zal dus **geen** synchronisatie plaatsvinden buiten het betreffende tijdschema. Het default tijdschema is het tijdschema dat alle dagen geldt. Tijdschema's zonder tijden worden niet in de lijst (3) getoond.

Synchronisatie op vaste tijden

Indien men kiest voor synchronisatie dagelijks op vaste tijden (1), dan is de optie om één of meer tijden toe te voegen ingeschakeld (2). Na het klikken op deze knop wordt een nieuw venster 'Geef een nieuwe tijd op' (3) geopend. U kunt, met dit venster geopend, meerdere tijden opgeven door op de knop '*Voeg toe*' te drukken. Reeds ingevoerde tijden kunnen worden verwijderd door op de bijbehorende knop '*Verwijder*' (4) te drukken.

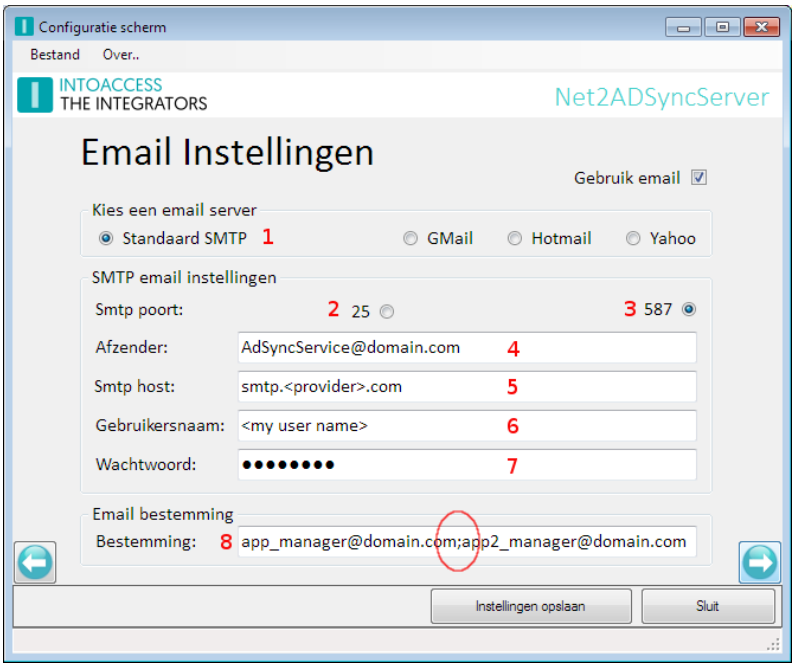
Met deze instelling zal de applicatie een enkele synchronisatie slag uitvoeren op de opgegeven tijden.



Afbeelding 21

De E-mail instellingen

Deze pagina, zie afbeelding 22, biedt de mogelijkheid om de applicatie zodanig te configureren dat eventuele problemen gemeld kunnen worden via e-mail. Dit is van belang omdat de applicatie als een 'Windows service' draait, en dus niet over de mogelijkheid beschikt om een melding op het scherm te tonen. Daarnaast zal de applicatie éénmaal per 24 uur een rapport verzenden met daarin alle wijzigingen die de laatste 24 uur zijn doorgevoerd.



Afbeelding 22

De applicatie kan gebruik maken van een SMTP server (1), of van een Webmail account voor het versturen van e-mailberichten. Indien gebruik gemaakt moet worden van een Webmail account verdient het de voorkeur om hiervoor een apart account aan te maken. Voor dit account moeten dan de beveiligingsregels op minimaal worden ingesteld.

Qua instelling is er geen verschil tussen het gebruik van een webmail account en een SMTP server welke gebruik maakt van STARTTLS (poort 587).

Let op: het SSL/TLS protocol wordt niet ondersteund.

Bij gebruik van een interne mailserver kan poort 25 worden geselecteerd. De applicatie zal berichten dan onversleuteld verzenden.

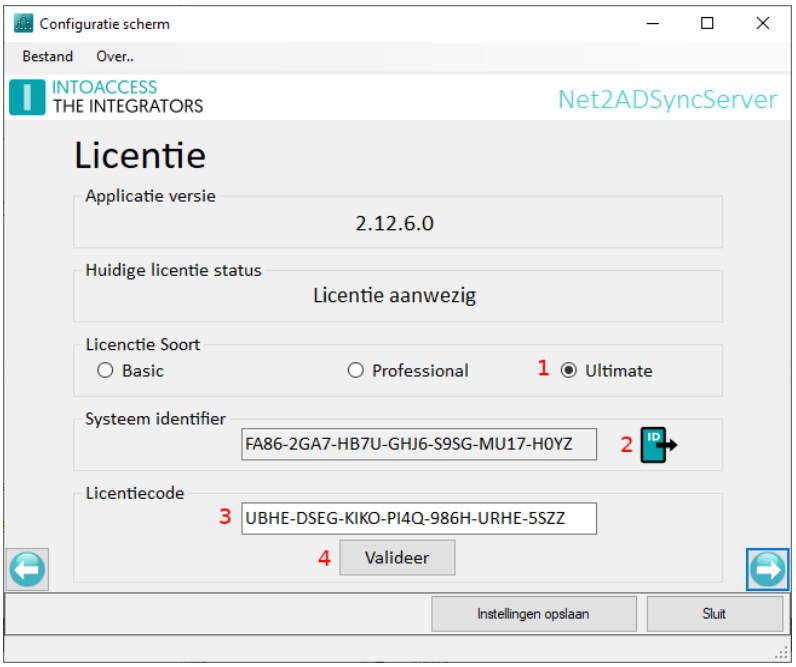
- Geef bij (4) het afzender adres op;
- Geef bij (5) het adres op van de SMTP server;
- De velden voor het ingeven van de gebruikersnaam (6) en het wachtwoord (7) zijn alleen relevant als er van een beveiligde verbinding over poort 587 gebruik gemaakt wordt;
- Geef bij (8) op welke perso(o)n(en) er allemaal op de hoogte gehouden moeten worden. Er kunnen hier meerdere e-mailadressen worden opgegeven. Deze moeten van elkaar zijn gescheiden door een 'punt-komma'.

Licentie

Deze pagina biedt de mogelijkheid om de gewenste licentie in te stellen, en deze, na aanschaf bij IntoAccess BV, te valideren. Zie afbeelding 23.

Een licentie kan direct bij IntoAccess besteld worden. Stuur daarvoor een mailtje naar info@intoaccess.com met daarin de bedrijfsnaam, factuuradres en het Btw-nummer.

Een licentie is gebonden aan de machine waarop de applicatie is geïnstalleerd, maar is verder onbeperkt geldig. Nieuwere versies van de applicatie zijn vrij te gebruiken voor bestaande licentiehouders.



Afbeelding 23

- Kies bij (1) de gewenste licentie;
  - Een 'Basic' licentie volstaat indien er niet meer dan 100 medewerkers worden gesynchroniseerd tussen AD en Net2 en de totale configuratie over niet meer dan 25 deuren beschikt.
  - Een 'Professional' licentie maakt dat de applicatie zonder deze restricties zal werken.
  - Een 'Ultimate' licentie zorgt er voor dat de applicatie ook de inzet van meerdere AD 'Security Group – Net2 Autorisatie' combinaties ondersteunt. De applicatie zal in dergelijke gevallen zelf, per combinatie, een nieuwe Net2 autorisatie aanmaken of hergebruiken. Deze functionaliteit lijkt op de Paxton “Geavanceerde Bevoegdheden” (maar dan beter).
- Licenties zijn gekoppeld aan de ‘System Identifier’ zoals die getoond worden bij (2). Bij aanschaf van een licentie, zal om de export file (klik op het icoon om deze te maken) worden gevraagd.
- De ontvangen licentiecode kan bij (3) worden ingegeven en vervolgens door op de ‘*Valideer’* knop (4) te drukken worden gecontroleerd.

Extra functionaliteit bij aanschaf van een ‘Ultimate’ licentie.

Hieronder vindt u een uitgewerkt voorbeeld van het inzet van gecombineerde autorisaties, zoals die mogelijk gemaakt wordt bij de aanschaf van een ‘Ultimate’ licentie.

In Net2 zijn de volgende autorisaties aangemaakt:

- ‘Basis toegang’, in deze autorisatie zijn de toegangsrechten opgenomen die aan alle medewerkers toegekend kunnen worden. Bv. de toegang via de hoofdingang, de centrale hal, de fietsenstalling en afdeling 'A' en 'B' maar deze laatste twee alleen onder werktijden.
- ‘Afdeling A’, in deze autorisatie zijn alleen de toegangsrechten opgenomen die toegang geven tot afdeling 'A' maar dan van 's morgens 05:00 tot 's avonds 22:30 .
- ‘Afdeling B’, in deze autorisatie zijn alleen de toegangsrechten opgenomen die 24x7 toegang geven tot afdeling 'B'.

In AD zijn gelijknamige security groepen aangemaakt.

Alle medewerkers die in AD lid gemaakt zijn van de groep: ‘Basis toegang’ krijgen daarmee de toegangsrechten toegekend zoals die gedefinieerd zijn in de ‘Basis toegang’ autorisatie in Net2.

Medewerkers die over de extra toegangsrechten moeten beschikken, zoals die zijn vastgelegd in de autorisatie ‘Afdeling A’, kunnen nu ook lid gemaakt worden van de AD groep: ‘Afdeling A’.

De applicatie zal nu in Net2 een nieuwe autorisatie aanmaken waarbij de toegangsrechten van beide oorspronkelijke autorisaties zijn gecombineerd en deze toekennen aan de medewerkers die lid zijn van beide groepen. Effectief gezien betekent dit dat deze medewerkers op dat moment de toegangsrechten hebben tot de centrale hal, de fietsenstalling, en afdeling ‘B’, zoals die gedefinieerd is door de ‘Basistoegang’ autorisatie, en toegang tot ‘Afdeling A’ zoals gedefinieerd door de autorisatie ‘Afdeling A’.

Aanvullend daarop kunnen medewerkers die 24x7 toegang moeten hebben tot ‘Afdeling B’ ook lid gemaakt worden van deze AD groep.

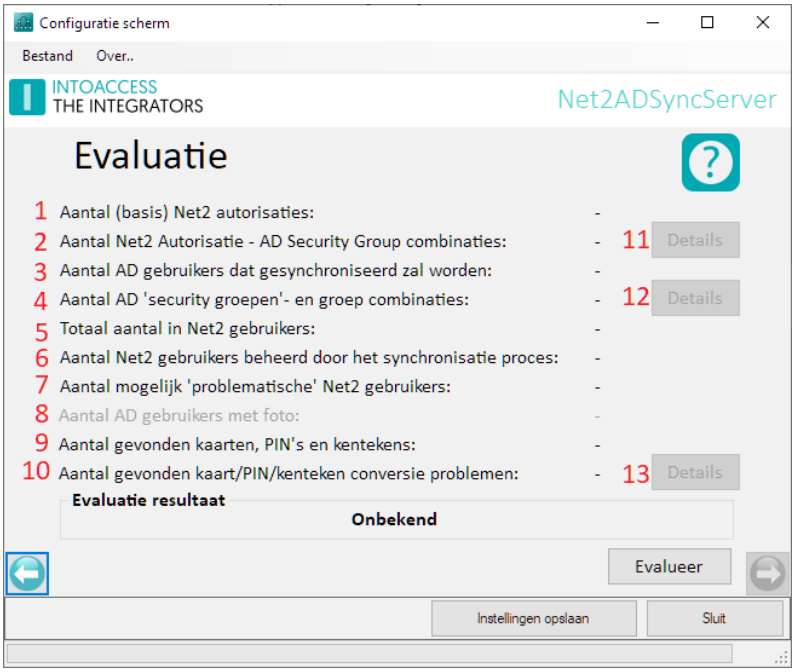
De applicatie gaat er daarbij vanuit dat bij overlappende deuren de minst restrictieve tijdzone leidend is. Indien dat noodzakelijk is, maakt de applicatie daarbij ook een nieuwe tijdzone aan.

De ‘Professional’ licentie vereist, in dit geval, dat alle gecombineerde autorisaties vooraf handmatig zijn aangemaakt; er moet dus een ‘Basis’ , Basis+A, Basis+B en een Basis+A+B autorisatie worden aangemaakt. Dit geldt ook voor de security groepen binnen de AD. Als er een aanpassing gemaakt moet worden in de ‘Basis’ autorisatie, dan moet deze ook in alle afgeleide autorisaties doorgevoerd worden, met de bijbehorende risico’s van fouten. De ‘Ultimate’ licentie ondervangt dit probleem door alle afgeleide autorisaties geheel zelf te beheren.

Het aantal groepen dat op deze manier gecombineerd kan worden, is in principe niet gelimiteerd. De enige beperking die voor dit systeem geldt, is dat het totaal aantal autorisaties (de basis autorisaties en de berekende autorisaties) niet groter mag zijn dan 255. Dit is het maximum aantal autorisaties dat Paxton ondersteunt.

De Evaluatie pagina

Deze pagina biedt de mogelijkheid om alle eerder opgegeven instellingen te evalueren. Doel van deze pagina is eventuele configuratiefouten in een zo vroeg mogelijk stadium te ondervangen. Deze evaluatie zal geen wijzigingen aanbrengen in Net2 (en ook niet in AD). Er kan dus zonder risico geëxperimenteerd worden met de instellingen. Zie afbeelding 24.



Afbeelding 24

Na het indrukken van de '*evalueer*' knop zal de applicatie zowel de medewerkers uit AD, als uit Net2 verzamelen.

- Bij (1) zal het aantal, in Net2 gevonden autorisaties getoond worden. Indien er van een 'Ultimate' licentie gebruik wordt gemaakt, en de applicatie al een keer actief is geweest, kan het zijn dat er al één of meerdere 'afgeleide' autorisaties in Net2 aanwezig zijn. Deze zullen hier dan niet worden getoond.
- Bij (2) wordt het aantal overeenkomstige 'AD Security Group – Net2 autorisatie' paren getoond. Deze waarde is van belang omdat alleen de medewerkers in AD die in deze groep(en) voorkomen, gesynchroniseerd zullen worden.
- Het aantal AD medewerkers dat in deze groep(en) voorkomt wordt bij (3) getoond.
- Bij (4) wordt het aantal 'AD Security Group – Net2 autorisatie' combinaties getoond. Dit mag alleen afwijken van het aantal zoals dat getoond wordt bij (2) indien er gebruik gemaakt wordt van een 'Ultimate' licentie.

  De knoppen (11) en (12) bieden de mogelijkheid om de gevonden waarden te tonen.
- Bij (5) wordt het totaal aantal reeds in Net2 aanwezige medewerkers getoond. Let erop, dat als er reeds medewerkers in Net2 aanwezig zijn, en die **niet** onder beheer van de synchronisatieproces vallen en **wèl** in de AD voorkomen, dit, in het gunstigste geval, zal leiden tot dubbelingen in Net2, en in het slechtste geval tot kaart/badge nummer conflicten.

- Bij (6) wordt het aantal medewerkers getoond die reeds beheerd worden door het synchronisatieproces. Initieel zal dit altijd nul zijn.
- Bij (7) wordt het aantal 'problematische' medewerkers getoond. Dit betreft medewerkers waarvan het veld dat dient voor de opslag van de 'sAMAccountName' reeds van een waarde is voorzien, terwijl de betreffende medewerker niet is opgenomen in het synchronisatieproces.

  Of een medewerker in het synchronisatieproces is opgenomen, wordt bepaald door de waarde van het gebruikersveld dat is aangewezen om de Net2 Sync 'marker' waarde te bevatten. Zie ook (2) in afbeelding 8.
- Bij (8) wordt het aantal medewerkers getoond die voorzien zijn van een foto.

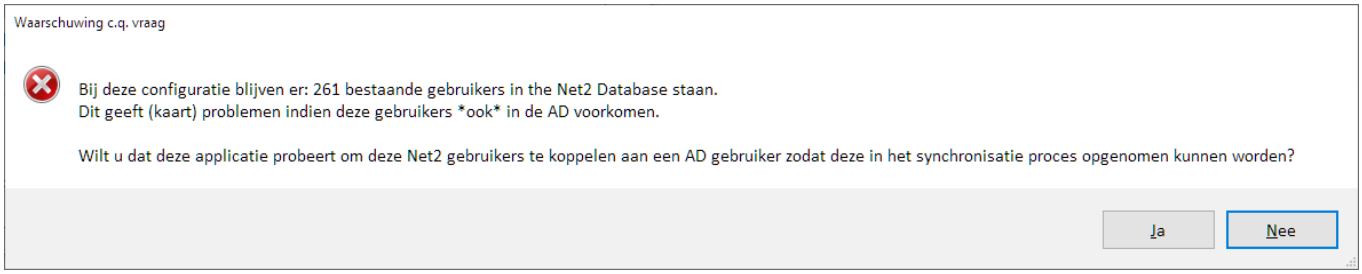
  Deze regel zal ‘grijs’ zijn indien er geen gebruik gemaakt wordt van de mogelijkheid om foto’s te synchroniseren.
- Bij (9) wordt het aantal in de AD gevonden kaarten, PIN’s en kentekens getoond.
- Bij (10) wordt het aantal fouten getoond die zijn opgetreden tijdens de verwerken van de kaarten, PIN’s en kentekens. De selectie van een onjuist kaarttype (Mifare/Paxton) is een veel voorkomende oorzaak van dit soort fouten. (Zie pagina 10, AD kaart gegevens.) Een andere mogelijke oorzaak is de keuze van het verkeerde AD attribuut. De gevonden fouten worden getoond na het indrukken van knop (13).

  De regels/knop bij (9), (10) en (13) zijn ‘grijs’ indien er geen gebruik gemaakt wordt van de mogelijkheid om kaarten te synchroniseren.

Koppelen van AD gebruikers aan reeds bestaande Net2 gebruikers

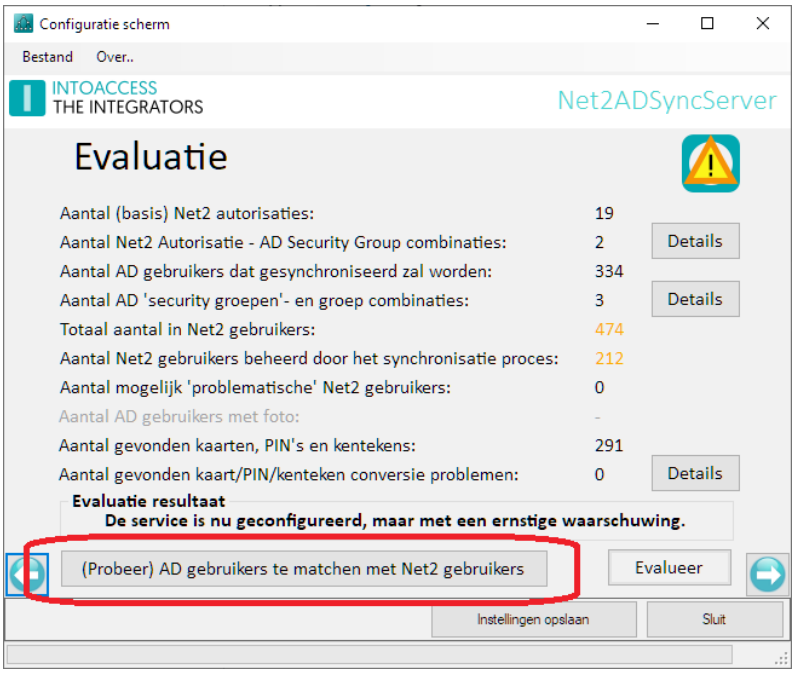
Sinds versie 2.15.0 wordt de mogelijkheid geboden om reeds bestaande Net2 gebruikers op te nemen in het synchronisatie proces.

Als tijdens het evaluatieproces meer dan een bepaald percentage gebruikers wordt gevonden, die wel in Paxton staan maar niet in het synchronisatieproces zijn opgenomen, zal de toepassing vragen of het wenselijk is ze te koppelen. Zie afbeelding: 25.



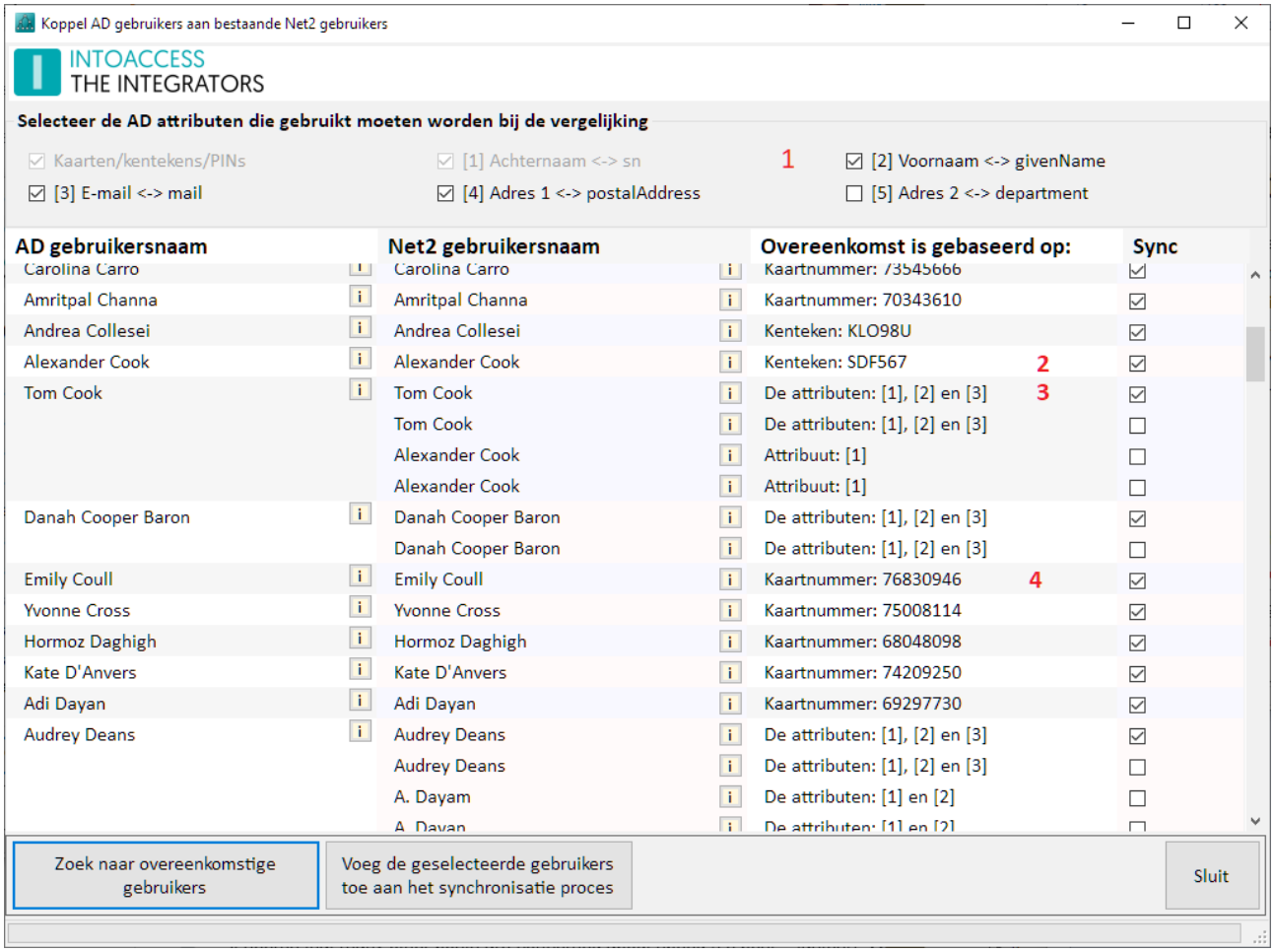
Afbeelding: 25

Indien dit inderdaad gewenst is wordt er een extra knop vrijgeschakeld waarmee het koppel proces gestart kan worden. Zie afbeelding 26.



Afbeelding 26

Na het indrukken van de '*(Probeer) AD gebruikers te matchen met Net2 gebruikers*' knop wordt er een nieuw scherm geopend. Zie afbeelding 27, (echter nog zonder het zoekresultaat).

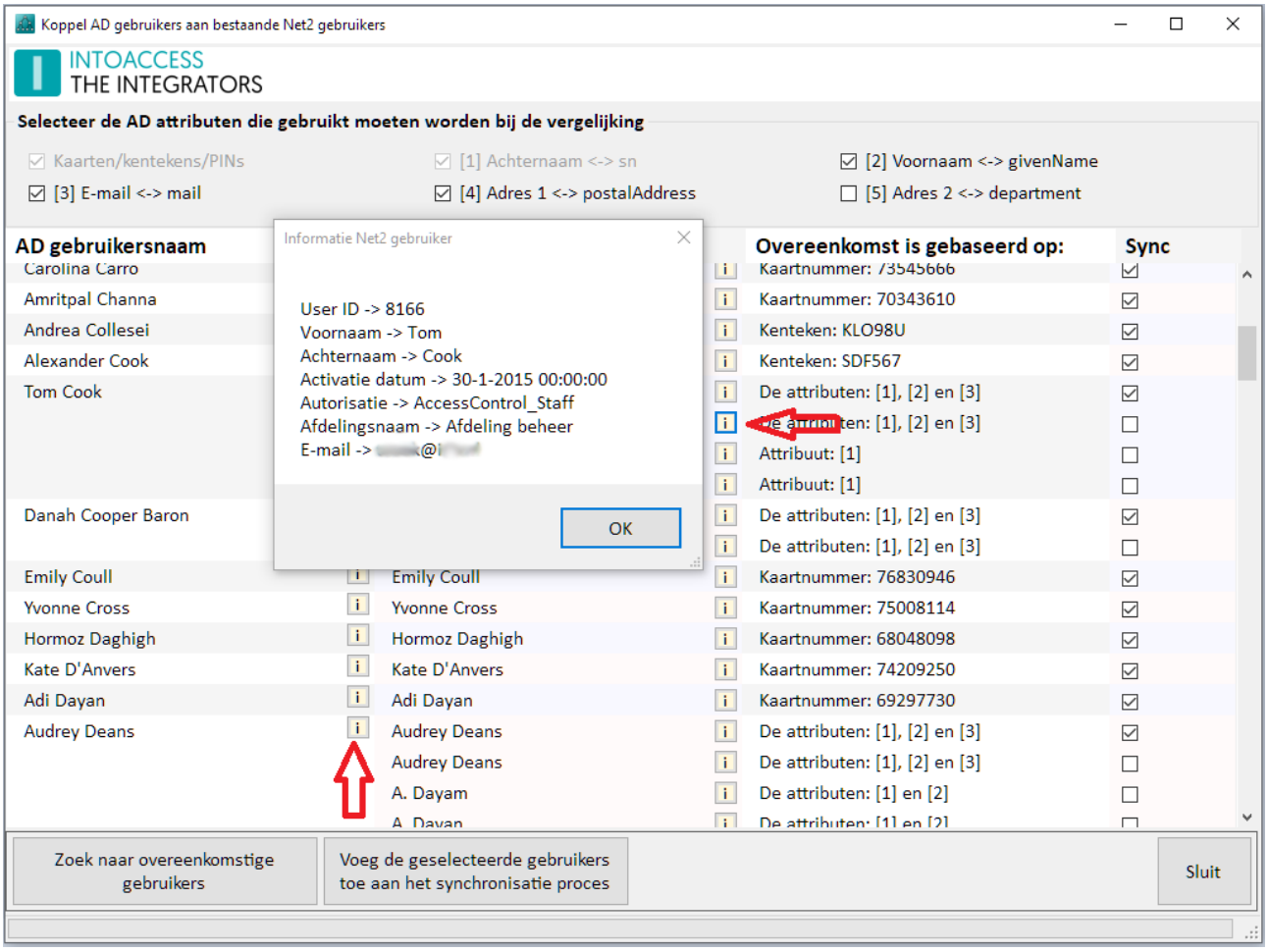


Afbeelding 27

- Kies als eerste bij (1) de velden/attributen die in het zoekproces moeten worden opgenomen.
- De achternaam zal altijd in dit proces worden opgenomen, en kan dus ook niet worden gedeselecteerd, dit geldt ook voor kaarten, PIN codes en kentekens indien deze zijn opgenomen in het synchronisatie proces (*). De andere velden zijn optioneel. Als deze velden overeenkomstige gegevens bevatten maakt dat het selectie proces nauwkeuriger.

  (*) Kaarten, PIN codes en kentekens worden alleen gebruikt indien deze gesynchroniseerd moeten worden vanuit de AD naar Net2.
- Na het indrukken van de '*Zoek naar overeenkomstige gebruikers*' knop worden de gevonden gebruikers getoond. (Indien aanwezig)
- Per AD gebruiker kan er slechts één Net2 gebruiker worden geselecteerd. De applicatie zal hierop controleren voordat de gebruikers in de database gekoppeld kunnen worden.
- De applicatie zal als eerste proberen om gebruikers te koppelen op basis van overeenkomstige kentekens, kaart en/of PIN nummers. Indien er een overeenkomstige waarde is gevonden wordt er verder geen aandacht meer besteed aan de naam van de gebruiker, of de waarde van de overige velden.

- Indien er geen overeenkomstige waarden gevonden kunnen worden, of indien er geen gebruik gemaakt wordt van kaart/PIN/kenteken synchronisatie, zal de applicatie proberen gebruikers te linken op basis van op elkaar lijkende achternamen. Van de daarbij gevonden reeks worden daarna de overige velden met elkaar vergeleken. De reeks met de grootste rij overeenkomsten wordt dan standaard geselecteerd.
- Indien het 'Voornaam' veld onderdeel is van het vergelijkingsproces zal de applicatie ook proberen om eventuele voorletters op te nemen in de vergelijking. Dus 'J. Jansen' zal dan bijvoorbeeld matchen met 'Jan Jansen'.
- De meest rechtse kolom geeft aan op welke grondslagen de gevonden persoon werd geselecteerd.
- Met behulp van de 'beige' *i*-knopjes kan detail informatie worden opgevraagd over de betreffende persoon. Zie afbeelding 28.

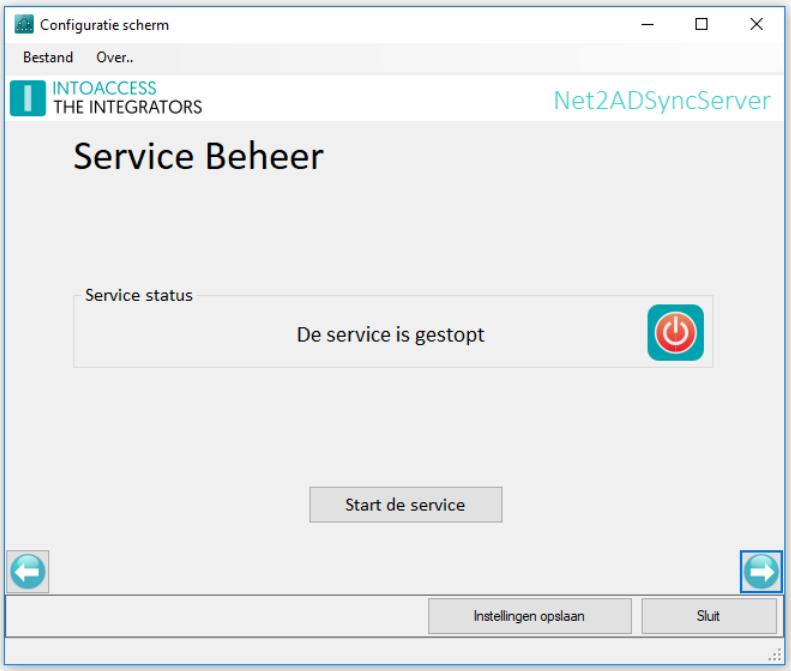


Afbeelding 28

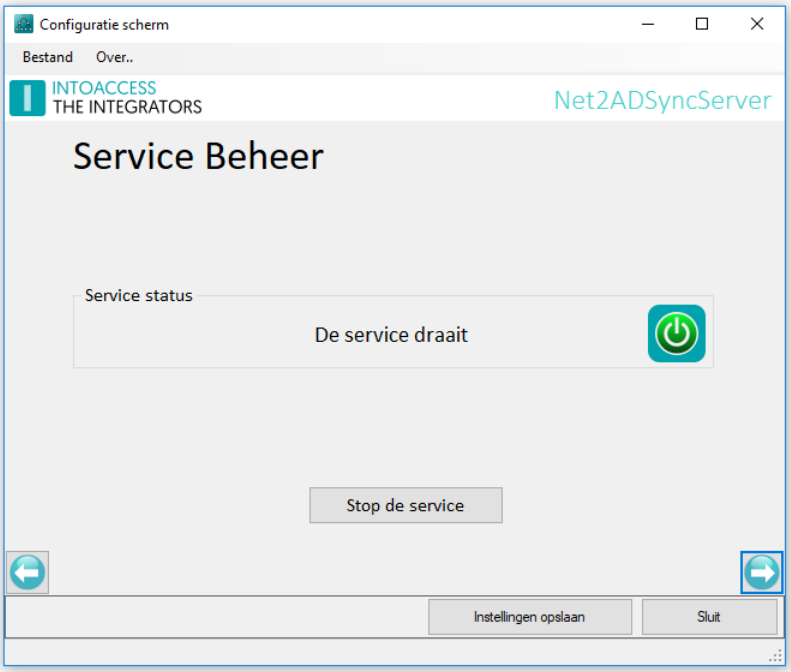
Na het indrukken van de '*Voeg de .. proces*' knop zullen de geselecteerde gebruikers worden opgenomen in het synchronisatie proces. Daartoe zullen de beide velden zoals benoemd bij (1) en (2) in hoofdstuk: 'De AD-Net2 Synchronisatie instellingen' op bladzijde 8, gevuld worden met de 'sAMAccountName' en de juiste 'marker waarde'.

Service Beheer

Deze pagina, zie afbeelding 29 en 30, biedt de mogelijkheid om de eigenlijke service te starten en te stoppen. Als de service niet start na het klikken op '*Start de service*', kijk dan bij de pagina 'Log instellingen'. De laatste logmeldingen die hier getoond worden geven inzicht in de reden waarom de service niet start.



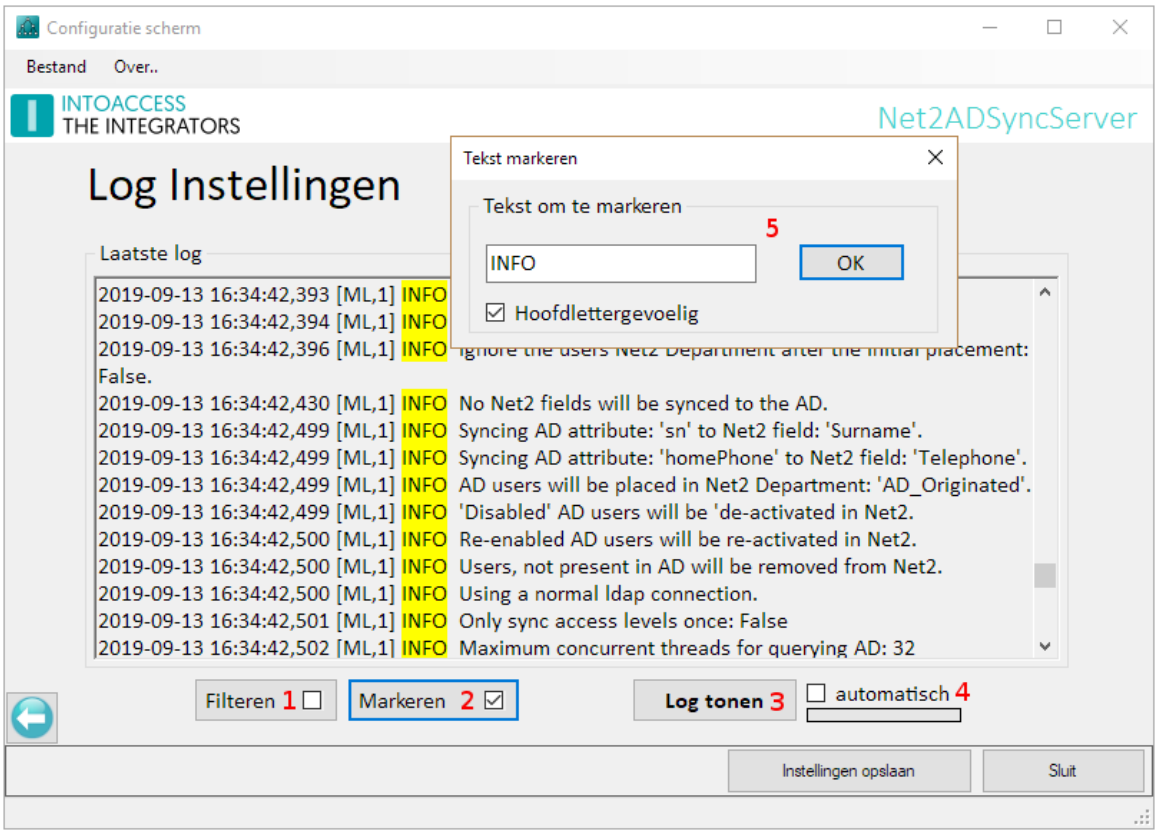
Afbeelding 29



Afbeelding 30

De Log instellingen

Deze pagina, zie afbeelding 31, 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.



Afbeelding 31

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.

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 logfile zelf bevindt zich in de folder: c:\IntoAccess\Logging\Net2ADSyncServer\

INTOACCESS
THE INTEGRATORS

Handleiding Net2ADSyncServer
Versie 2.11

Alle informatie en specificaties zijn correct op het moment van publicatie, maar kunnen zonder voorafgaande kennisgeving worden gewijzigd.
April 2021