Net2ADSyncServer

Handleiding 4.3

(26 oktober 2026)

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

Inhoudsopgave

Installatie en configuratie van de Net2ADSyncServer....3
Installatie....3
Werking....3
Synchronisatie regels....3
Configuratie....5
Net2....6
Tussentijds opslaan van de instellingen....7
De Active Directory instellingen....8
De AD-Net2 Synchronisatie instellingen....10
De AD kaart gegevens....12
Synchronisatie van Mifare kaartnummers naar de AD....14
De AD-Net2 Veldnaam relatie....15
Synchronisatietijd Instellingen....16
Synchronisatie met een vast interval....16
Synchronisatie op vaste tijden....17
De E-mail instellingen....18
SMTP....18
Azure/Entra....19
Fout- en/of activiteiten- rapportage....20
Licentie....21
Licentie soorten....21
Extra functionaliteit van een 'Ultimate' licentie....22
Autorisatie type....23
Speciale Instellingen....24
Gebruik van geneste AD groepen....28
De Evaluatie pagina....29
Het evaluatie proces....29
Getoonde informatie....29
Koppelen van AD gebruikers aan reeds bestaande Net2 gebruikers....31
Service Beheer....34
De Log instellingen....35
Overzicht van de afgeleide autorisaties....36

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.

Vanaf V4.0, is de applicatie compatibel met de **Net2 API interface** en niet meer met de SDK interface die in Net2 v7 is komen te vervallen. Om de Net2 API te activeren, kunt u de volgende handleiding volgen, welke tevens toelicht hoe u een trial of reguliere productlicentie kunt verkrijgen:

Handleiding voor het configureren van API producten

Werking

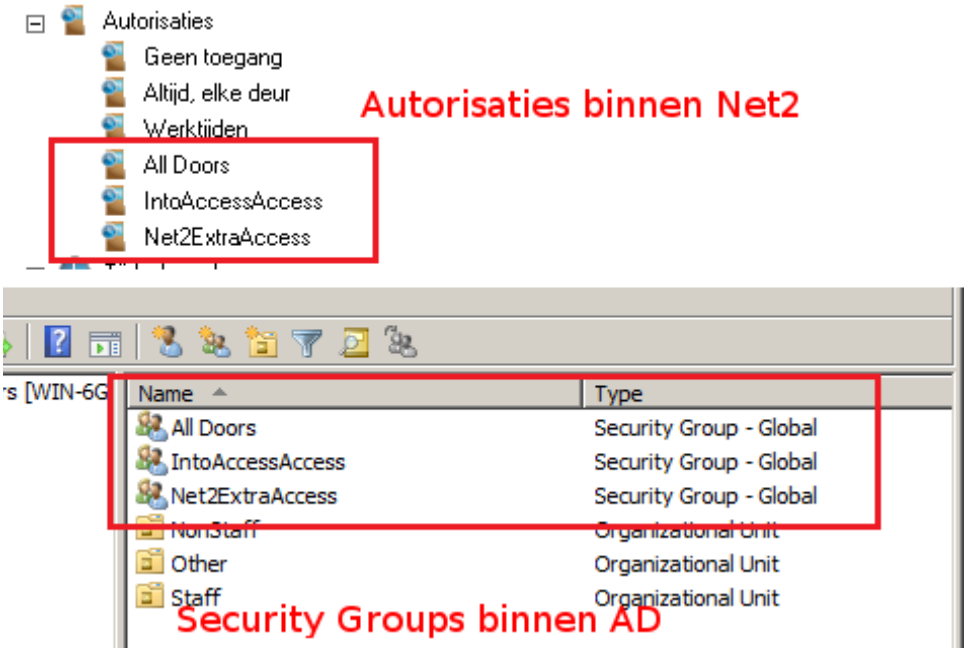
Deze applicatie is ontworpen vanuit het basis idee dat het beheer van alle medewerkers centraal gebeurt op de Active Directory server. Vanuit deze AD worden, initieel, alle relevante gegevens gekopieerd naar de Net2 database. Wijzigingen die daarna binnen de AD aangebracht worden, worden daarbij automatisch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

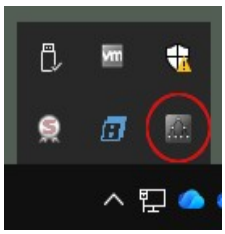
(*) Deze restrictie geldt niet voor de 'Ultimatief' versie. Meer details kunt u vinden onder het kopje 'licentie'.

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.

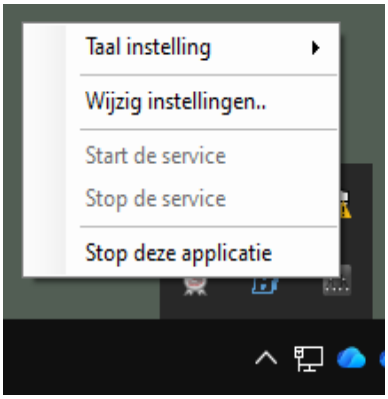
Configuratie

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 onderzoek van de taakbalk vestigen. (Zie Afbeelding 2.)



Afbeelding 2

Een klik met de rechter muisknop opent het hoofdmenu. (Zie Afbeelding 3.)



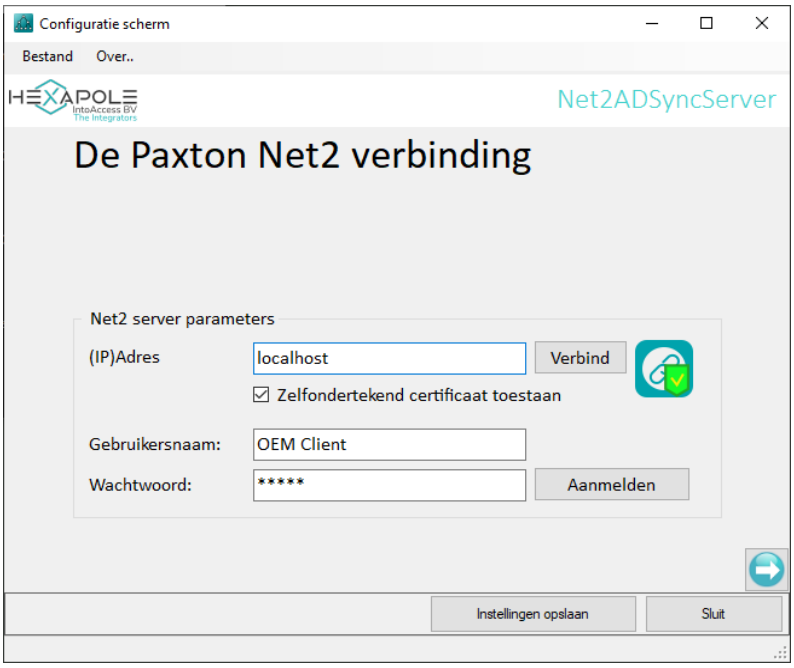
Afbeelding 3

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

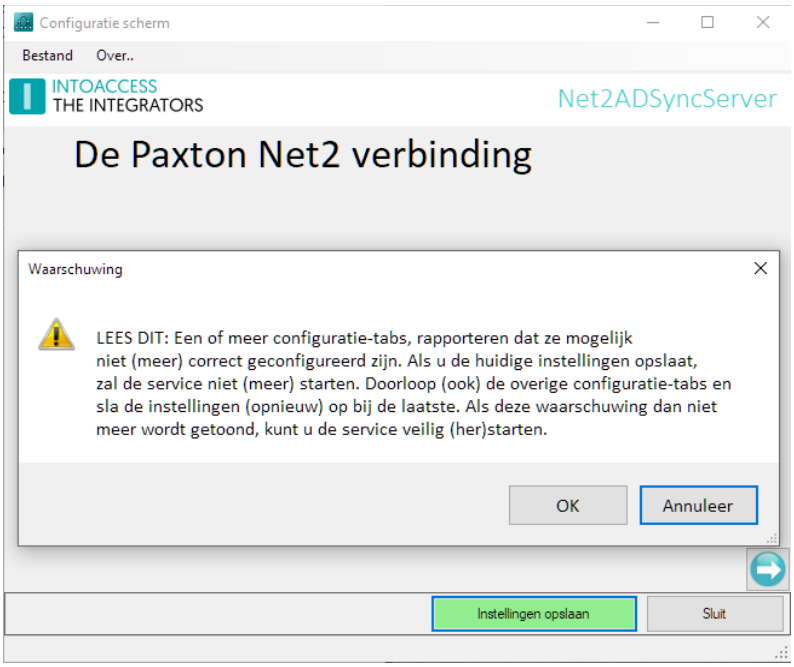
- Voer het (ip)adres in van de Net2 server. Als u de aanwezigheid app installeert op de Net2 server zelf, kunt u de 'localhost' waarde laten staan. Gebruik geen extern adapter ip adres in dat geval!!
- Sta een zelfondertekend certificaat toe, als bij het activeren van de Net2 API niet expliciet een officieel certificaat (uitgegeven door een certificaat autoriteit) is gebruikt.
- Klik op de verbind knop; als de verbinding slaagt zijn daarna de gebruikersnaam en het wachtwoord in te voeren.
- Voer een operator naam in waarmee u wilt dat de applicatie inlogt. Dit dient een operator te zijn met de “Systeembeheerder” rol (deze accounts vindt u onder “Net2 systeembeheerders” van de Net2 applicatie). We raden het gebruik van de ‘**OEM Client**’ aan, omdat deze niet onderhevig is aan de MFA. Als u MFA niet heeft ingeschakeld, mag het ook een andere gebruiker zijn. De ‘OEM Client’ gebruiker is standaard aanwezig op ieder Net2 systeem, maar zal nog wel even van een bij u bekend wachtwoord moeten worden voorzien.
- Voer het bijbehorende wachtwoord in.
- Klik op aanmelden.

Als alles goed gaat, zal er een bevestiging komen dat het aanmelden is gelukt en kunt u door naar het volgende configuratie-scherm, door op de pijl naar rechts te klikken.

Tussentijds opslaan van de instellingen

De configuratie applicatie is opgebouwd uit een aantal afzonderlijke pagina's. De gegevens op al deze pagina's hebben een grote onderlinge afhankelijkheid. Zo zal het wijzigen van het adres van de Net2 server op de eerste pagina tot gevolg hebben dat gegevens op (bijna) alle overige pagina's niet langer meer geldig zijn. Het is daarom van belang om *altijd* alle pagina's te doorlopen. Pas daarna kunnen de gegevens op een consistente wijze kunnen worden opgeslagen.

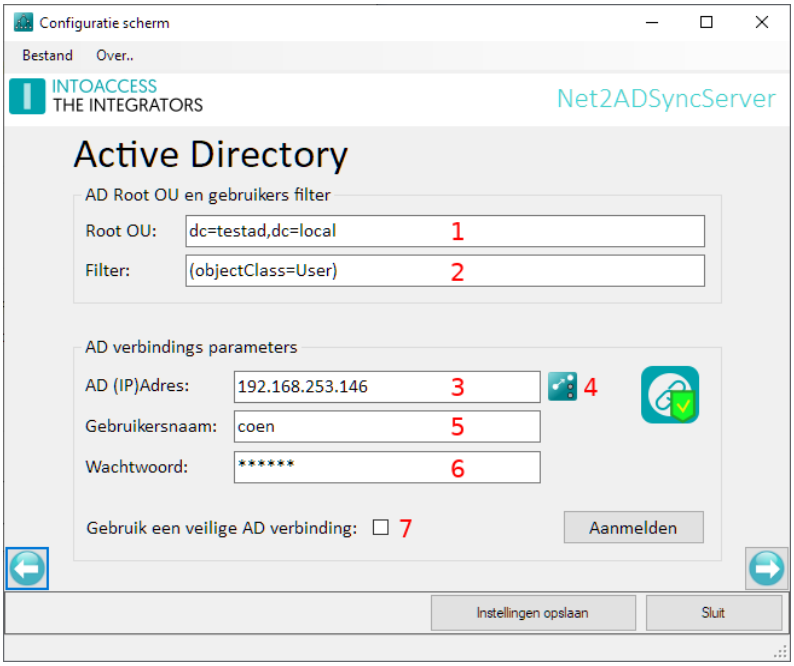
Tussentijds opslaan kan dus wel maar zal in veel gevallen leiden tot de waarschuwing zoals getoond in Afbeelding 5.



Afbeelding 5

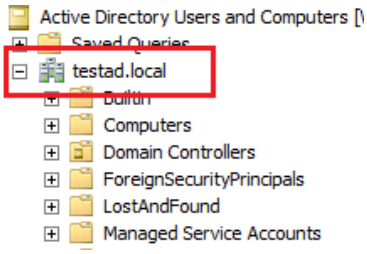
De Active Directory instellingen

Op deze pagina kunnen de parameters voor het opzetten van de verbinding met de AD server opgegeven worden. (Zie Afbeelding 6.)



Afbeelding 6

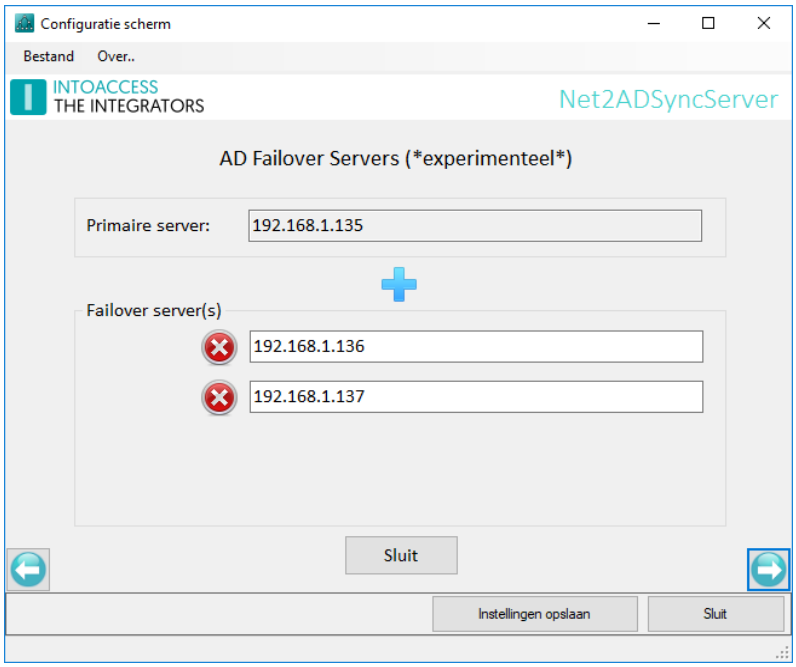
- Als eerste wordt gevraagd naar de 'Root OU'. (1). Vul in dit veld in ieder geval het volledige 'Domain Component' (dc) in. In het voorbeeld is de syntaxis opgegeven zoals die behoort bij de AD van Afbeelding 7. Indien alle medewerkers zich in een specifieke OU bevinden, dan zou deze hier ook opgenomen kunnen worden. Let er echter op dat dan ook de 'Security Groups' binnen deze OU staan omdat de applicatie deze anders niet zal kunnen vinden.



Afbeelding 7

- Het filter onder (2) wordt gebruikt bij het opvragen van de AD gebruikers. Ons advies is om deze standaardwaarde ongewijzigd te laten. Alleen in uitzonderlijke gevallen kan het noodzakelijk zijn om deze waarde 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. Als u op het icoon (4) aan de rechterzijde klikt, kunt u optioneel, 'failover' servers opgeven. (Zie Afbeelding 8.)

- De naam 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 8

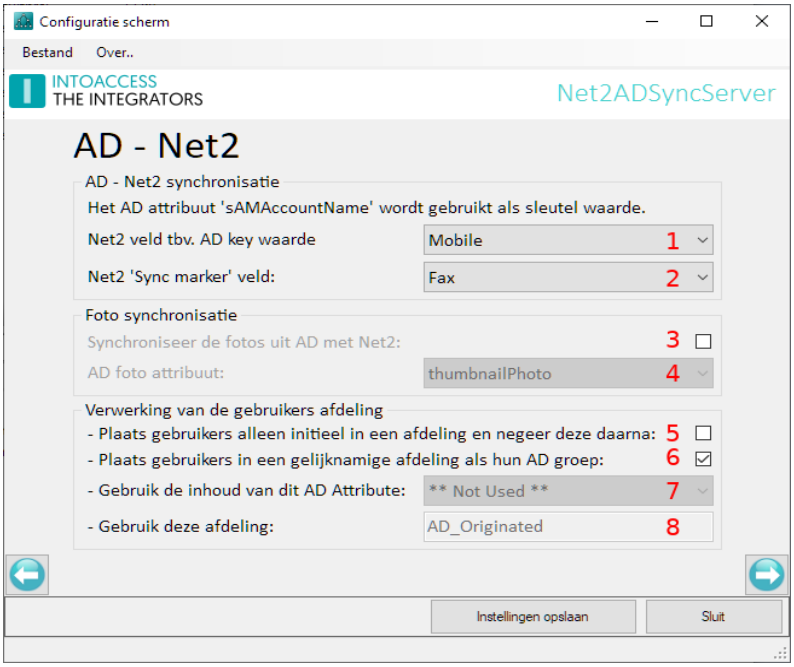
De AD-Net2 Synchronisatie instellingen

Deze pagina, (Zie Afbeelding 9.) heeft o.a. betrekking op de twee Net2 velden die gebruikt zullen gaan worden voor de opslag van zgn. ‘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, en in welk attribuut deze dan gevonden kunnen worden.

In het onderste gedeelte kan worden aangegeven op welke manier de ‘Afdeling’, waarin nieuwe medewerkers moeten worden geplaatst, bepaald kan worden. En tevens hoe hier daarna mee omgegaan moet worden.



Afbeelding 9

- 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.

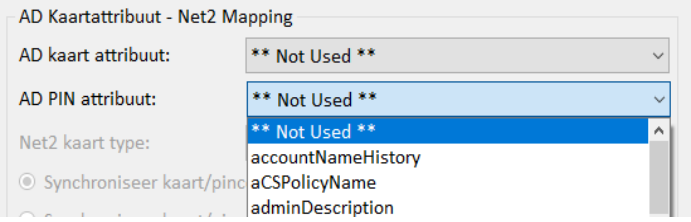
- Bij (5) kan worden aangegeven of de afdeling, waarin de gebruikers initieel zullen worden geplaatst, onderdeel moet blijven van het synchronisatieproces. Indien aangevinkt mogen de gebruikers handmatig naar een andere afdeling worden verplaatst zonder dat de applicatie de gebruikers weer teruggeplaatst (*1).
- (*1) *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. Gebruikers met een 'uitgeschakeld' (disabled) account kunnen wel in een andere afdeling worden geplaatst.*
- Als laatste wordt gevraagd naar de manier waarop de 'afdeling', waarin nieuwe gebruikers zullen worden geplaatst, gevonden kan worden.
  - 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

De pagina heeft betrekking op eventuele kaart-, PIN- , Telefoonnummers (Call ID's) of kentekens die vanuit de AD naar de Paxton database toe gesynchroniseerd moeten worden, of vice versa. (Zie Afbeelding 10.)

Afbeelding 10

- Kies onder (1) en (2) voor de optie: ''**Not Used**'', (Zie Afbeelding 11.), indien de AD géén kaart/PIN-/telefoon- nummers en/of nummerplaten bevat, (of moet gaan bevatten) en negeer de overige instellingen.

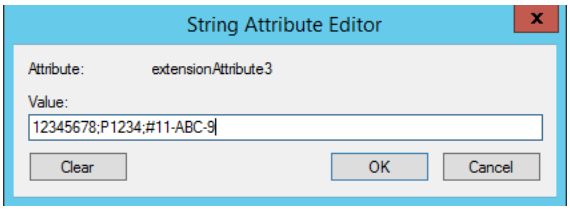


Afbeelding 11

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

  Kaarten, PIN-, telefoon- 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 '**#**'. Voor telefoonnummers is dat een **'T'**. 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. Deze moeten dan in de Active Directory als volgt worden opgegeven: (Zie Afbeelding 12.)



Afbeelding 12

- Kies onder (2) 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 standaard niet toestaan dat er handmatig, of vanuit 'derden', andere kaarten aan een gebruiker worden toegekend. Als dit toch gewenst is kan bij (9) de optie worden aangevinkt om <u>andere kaart typen</u> te negeren.
- Indien het PIN nummer in een apart AD attribuut opgeslagen is kan dat worden opgegeven in (3). 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 (4). In dit geval mag een nummerplaat **niet** vooraf worden gegaan door een hashtag '#'.

Afbeelding 13

- Bij (6) en (7) 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 13), 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.

- U kunt er optioneel voor kiezen (15) om kaarten die als verloren gemarkeerd zijn, niet naar AD te synchroniseren (wat een PaperCut issue kan oplossen, als deze alleen het eerste kaartnummer uit AD leest).
- In Net2 mag een kenteken slechts aan één gebruiker worden toegewezen. Normaal gesproken zal de applicatie een foutmelding geven indien geprobeerd wordt om een zelfde kenteken aan meerdere gebruikers toe te kennen. In dat geval zal het kenteken ook bij beide gebruikers worden verwijderd. Dit verwijderen kan worden voorkomen door toe te staan (optie 10) dat meerdere gebruikers een kenteken delen. In dat geval zal het kenteken fysiek alleen aan de eerste gebruiker worden toegekend en zal de applicatie pogingen om het zelfde kenteken aan andere gebruikers toe te kennen negeren.
- De applicatie kan eventuele Mifare kaarten (11), 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 (13).
- In de meeste gevallen zal het nummer van de Mifare kaart in het Hexadecimale formaat zijn opgeslagen, vink in dat geval (12) aan.
- Bij (14) wordt de optie geboden om de applicatie een foutmelding te laten versturen, (zie ook bij e-mail instellingen), indien er 'toegangsmiddelen' ontbreken bij één 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 Faxton 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.*

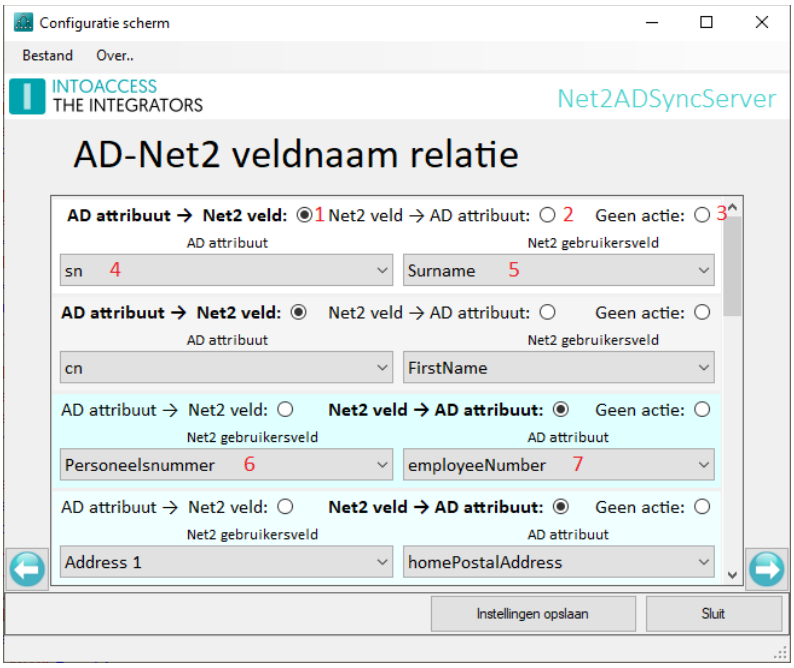
Zodra er een nieuw, of aangepast, Mifare kaartnummer wordt gedetecteerd, zal deze in de AD worden aangepast. De daarop volgende synchronisatieslag zal de applicatie het aangepaste Mifare kaartnummer weer als Paxton kaartnummer synchroniseren naar Paxton toe.

De AD-Net2 Veldnaam relatie

Deze pagina biedt de mogelijkheid om meerdere AD attribuut waarden op te nemen in het synchronisatieproces. (Zie Afbeelding 14.)

In **alle gevallen** moet het Net2 veld: 'Surname' van een waarde worden voorzien.

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



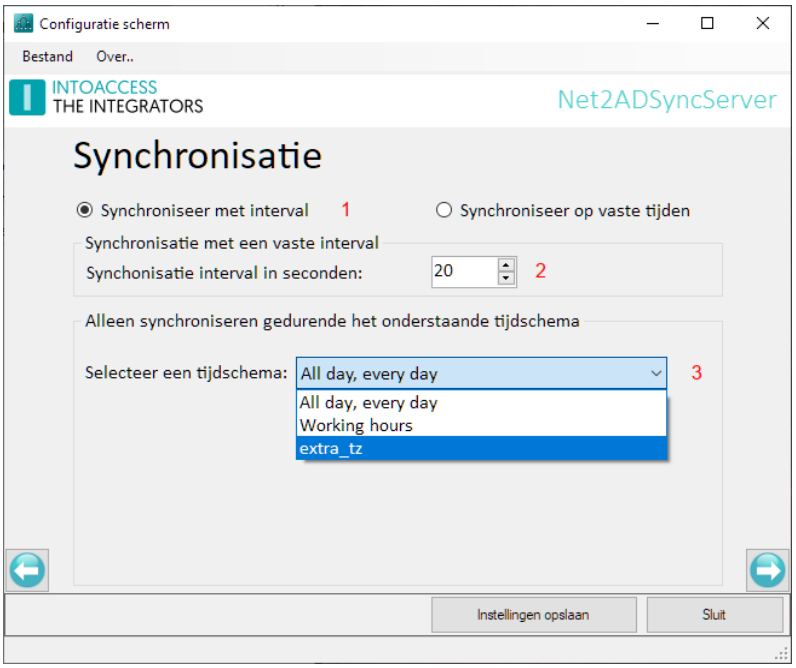
Afbeelding 14

Doorloop de volgende stappen als er ook andere velden gesynchroniseerd moeten worden:

- 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 gebruikersveld 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.

Synchronisatietijd Instellingen

Deze pagina, (Zie Afbeelding 15 en Afbeelding 16), biedt de mogelijkheid om de applicatie de synchronisatie uit te laten voeren met een vaste interval, of dagelijks op vaste tijden.



Afbeelding 15

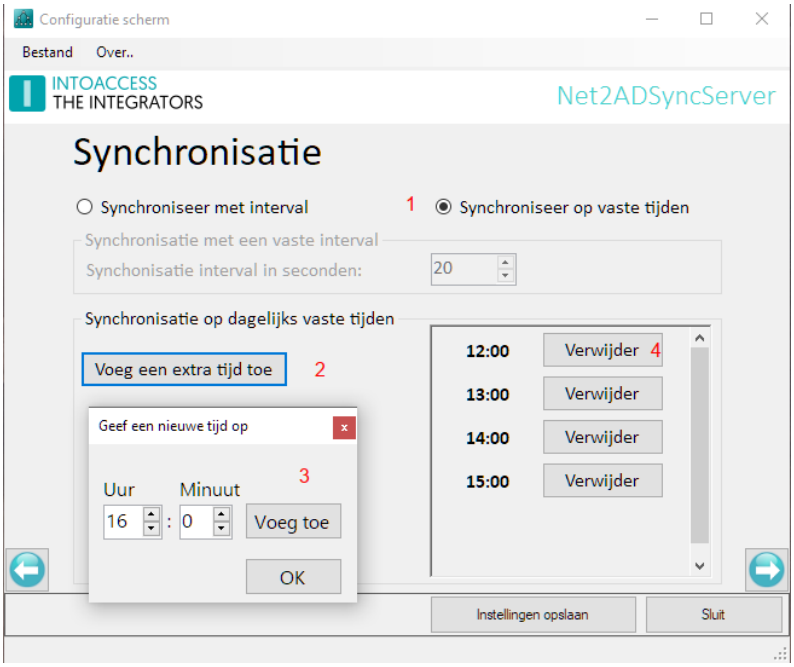
Synchronisatie met een vast interval

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.
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). (Zie Afbeelding 16.) 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 16

De E-mail instellingen

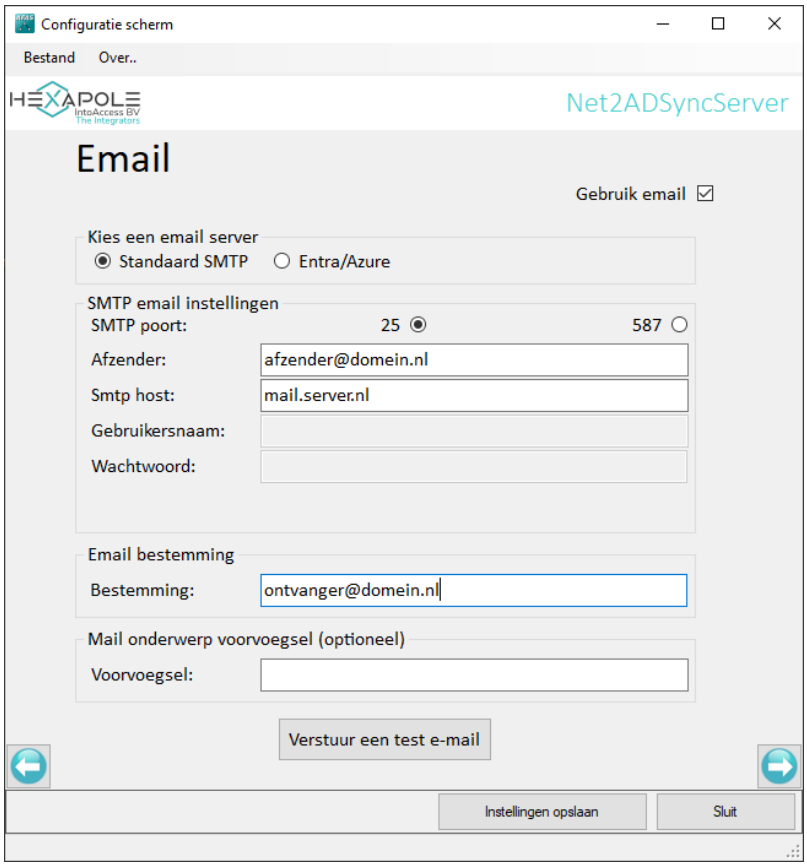
De email configuratie is standaard optioneel en biedt de mogelijkheid om applicatie-meldingen naar een beheerder te laten sturen.

De geadresseerde(n) in deze configuratie-pagina, zullen alleen e-mails krijgen als er iets iets fout gaat bij de synchronisatie. In een volgend configuratie-scherm kunnen echter ook de berichten die naar de eindgebruiker gaan geconfigureerd worden. (deze gebruiken dezelfde server instellingen)

SMTP

De 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. U kunt overwegen om een gratis webmail account te gebruiken (zoals Gmail), maar deze aanbieders maken het in toenemende mate lastiger (of onmogelijk) om SMTP te gebruiken via hun servers.

SMTPS (poort 465) wordt niet ondersteund.



Afbeelding 17

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

Azure/Entra

Het is ook mogelijk om SMTP met OAuth2 via Azure/Entra te gebruiken. Daarvoor zal dan een App registratie gemaakt moeten waarbij deze handleiding wordt gevolgd: Entra Handleiding.

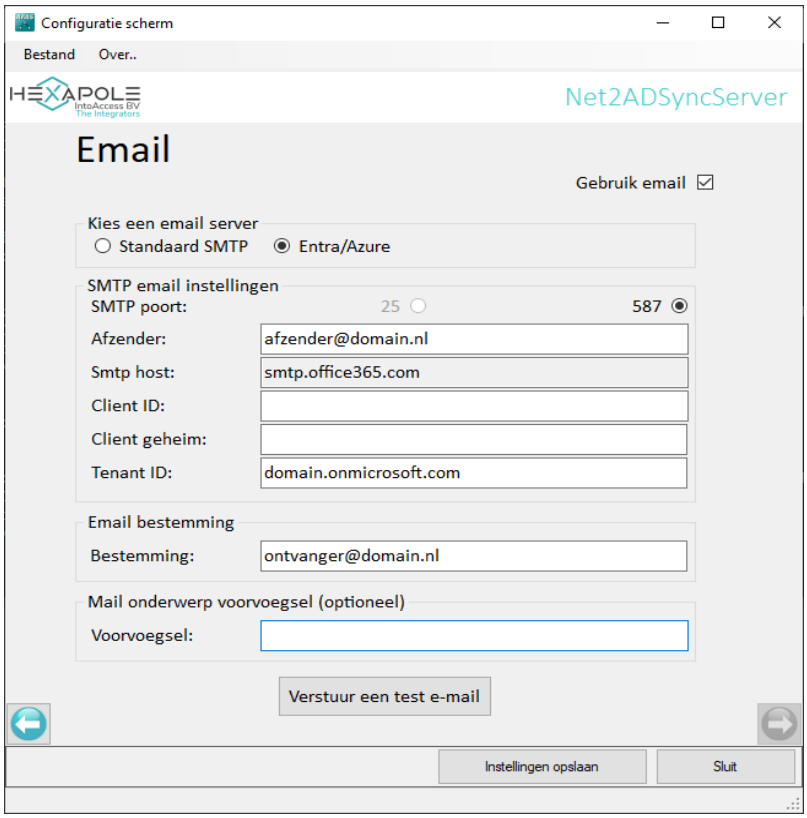
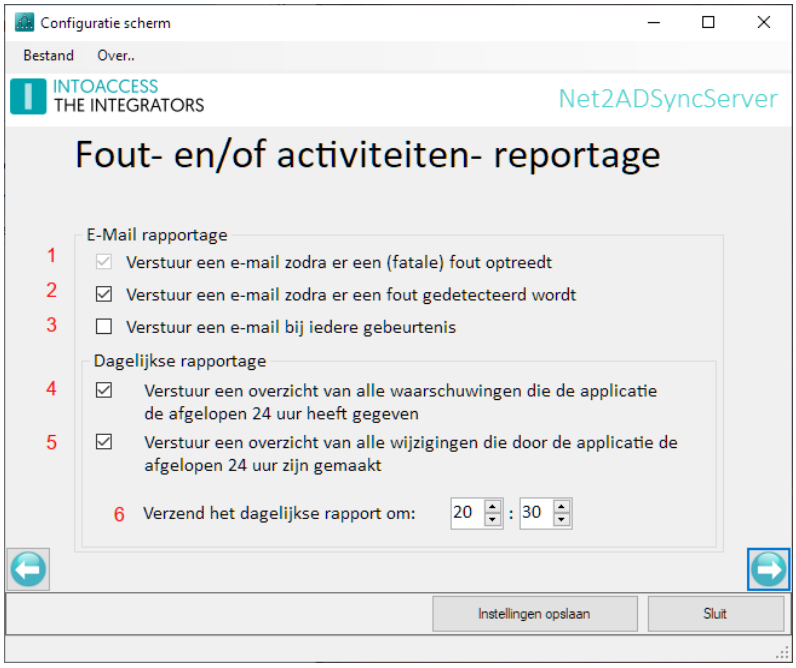


Image 18

De Azure/Entra Tenant ID kan worden ingegeven als domein of als GUID.

Fout- en/of activiteiten- rapportage

Indien op de vorige pagina de optie om email te kunnen versturen is geactiveerd kan op deze pagina, (Zie Afbeelding 19.) opgegeven worden wat voor soort berichten er gewenst zijn.



Afbeelding 19

- In alle gevallen (1) zal er een email verzonden worden op het moment dat er binnen de applicatie een fout is opgetreden waarvan de applicatie niet zelf van kan herstellen.
- Indien gewenst (2) kunnen ook problemen gemeld worden die de werking van de applicatie niet (langdurig) zullen verstoren.
- Eventueel kan er (3) ook een email verzonden worden bij iedere aanpassing die door de applicatie gemaakt wordt, of ieder bij ieder probleem dat door de applicatie gedetecteerd wordt.

Aanvullend daarop kan de applicatie ook dagelijks een rapportage mailen.

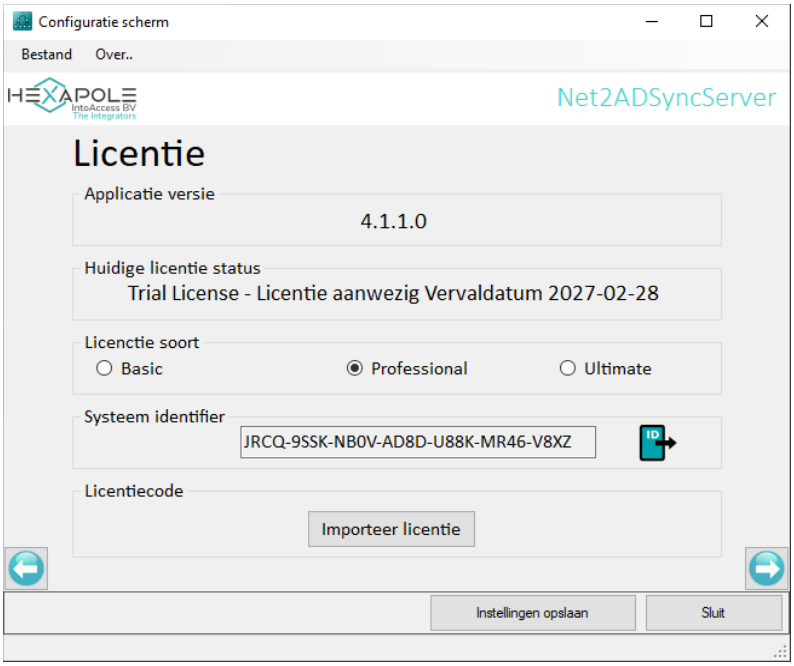
- Bij (4) kan de optie geactiveerd worden om dagelijks op een vaste tijd een overzicht te versturen van alle waarschuwingen die de applicatie de afgelopen heeft verzameld.
- De optie bij (5) zorgt ervoor dat de applicatie dagelijks een rapport verstuurd met daarin alle wijzigingen die de afgelopen 24 uur zijn gemaakt.

Bij (6) kan het tijdstip worden opgegeven waarop het rapport verzonden moet worden.

Licentie

De software zoals deze van de IntoAccess website kan worden gedownload, is volledig functioneel maar zal zonder API of (trial) productlicentie nog niet werken. In de volgende handleiding wordt de te volgen procedure nader toegelicht:

Handleiding voor het configureren van API producten



Afbeelding 20

Licentie soorten

- 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).

Extra functionaliteit 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.

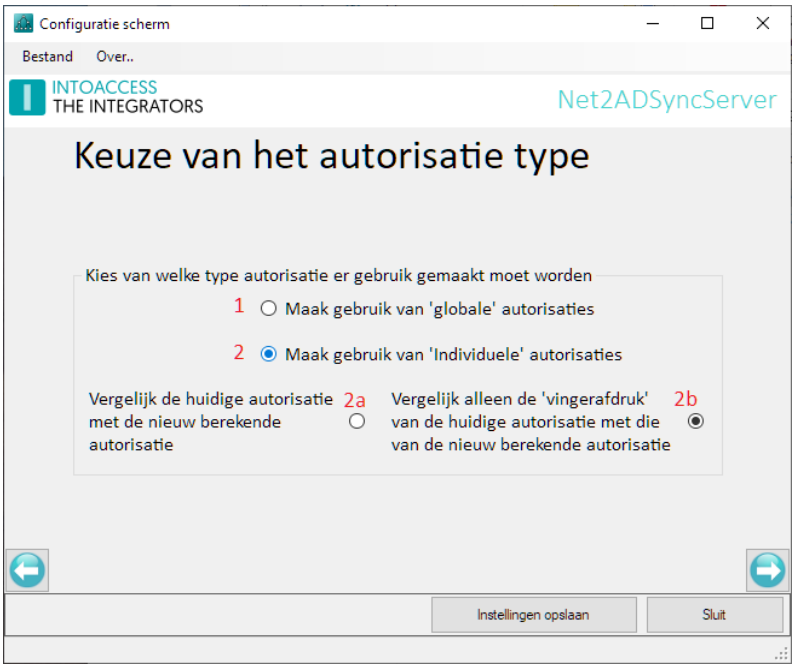
De applicatie gaat er daarbij vanuit dat bij overlappende deuren de minst restrictieve tijdzone leidend is. Indien dat noodzakelijk is, maakt de applicatie daarbij ook een nieuwe tijdzone aan.

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.

Autorisatie type

Nieuw in versie 3 is de mogelijkheid om in plaats van 'globale' autorisaties gebruik te maken van 'individuele' autorisaties. Deze mogelijkheid is echter exclusief beschikbaar, en ook alleen zinnig, voor gebruikers die van de 'Ultimate' functionaliteit gebruik maken. (Zie Afbeelding 21.)



Afbeelding 21

Het gebruik van 'globale' autorisaties is het meest inzichtelijk. Bezwaar van deze methodiek is echter dat Paxton het maximum aantal autorisaties dat gecreëerd kan worden gelimiteerd heeft tot 255. Dit probleem speelt met name in situaties met veel toegangspunten waarbij ook een gedifferentieerd toegangsbeleid gewenst is.

Deze limiet kan nu omzeild worden door gebruik te maken van 'Individuele' autorisaties. Deze autorisatie vorm kent geen limiet op het aantal autorisaties dat gebruikt mag worden.

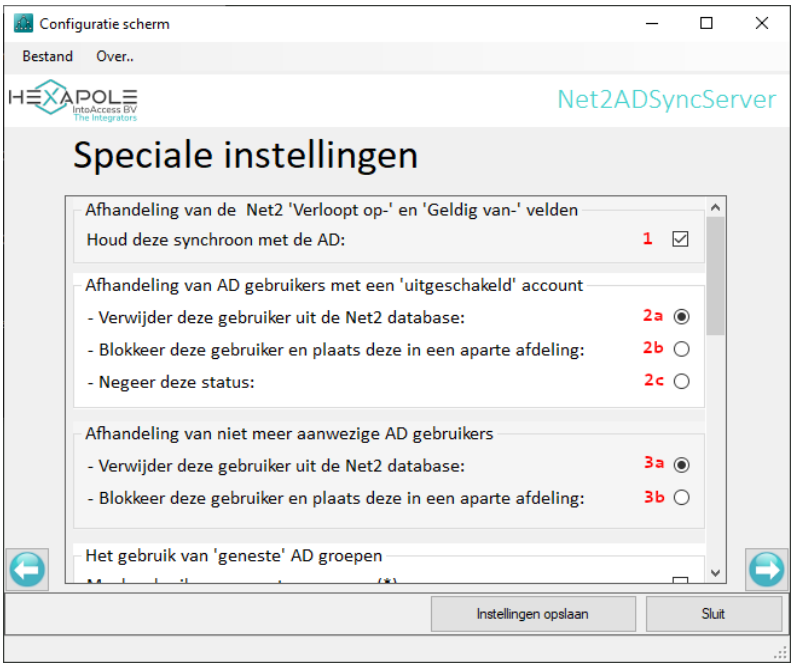
In beide gevallen geldt dat er wel een absolute limiet bestaat op het aantal verschillende tijdzones, 64, dat aangemaakt kan worden.

Bij het gebruik van 'individuele' autorisaties kan gekozen worden voor het, per gebruiker, vergelijken van de berekende autorisatie met de reeds toegekende autorisatie. Deze methode is het veiligst maar ook de meest arbeidsintensieve methode. (2a)

Als alternatief kan er ook gekozen worden voor het vergelijken van een 'vingerafdruk' van de berekende autorisatie met de opgeslagen 'vingerafdruk'. Deze methode is aanmerkelijk sneller maar is alleen veilig als gegarandeerd kan worden dat de autorisatie van een gebruiker nooit handmatig gewijzigd zal worden. (2b)

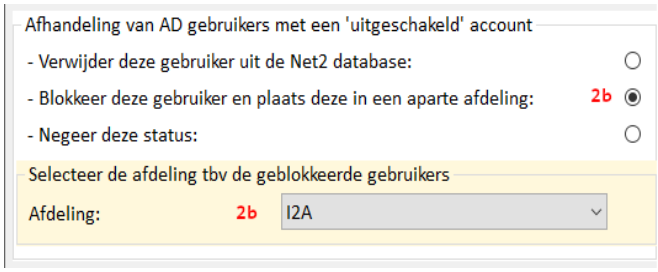
Speciale Instellingen

Deze pagina, (Zie Afbeelding 22 t/m Afbeelding 25), 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 22

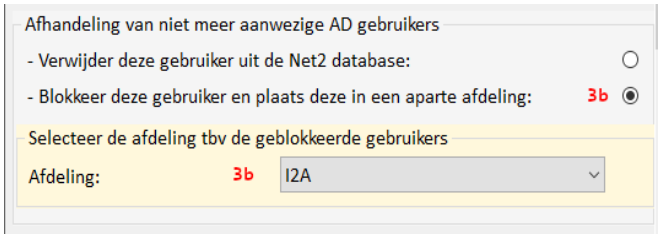
- Als het vinkje bij (1) gezet is worden de 'Geldig van-' en 'Verloopt op-' Net2 gebruikers velden synchroon gehouden met de 'whenCreated' en 'accountExpires' AD attributen. Bij het verwijderen van het vinkje kunnen deze velden apart worden ingesteld in Net2. Nieuw ingebrachte gebruikers zullen dan alleen initieel van de 'whenCreated' en 'accountExpires' waarden worden voorzien.
- Bij (2a..2c) 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 23.)



Afbeelding 23

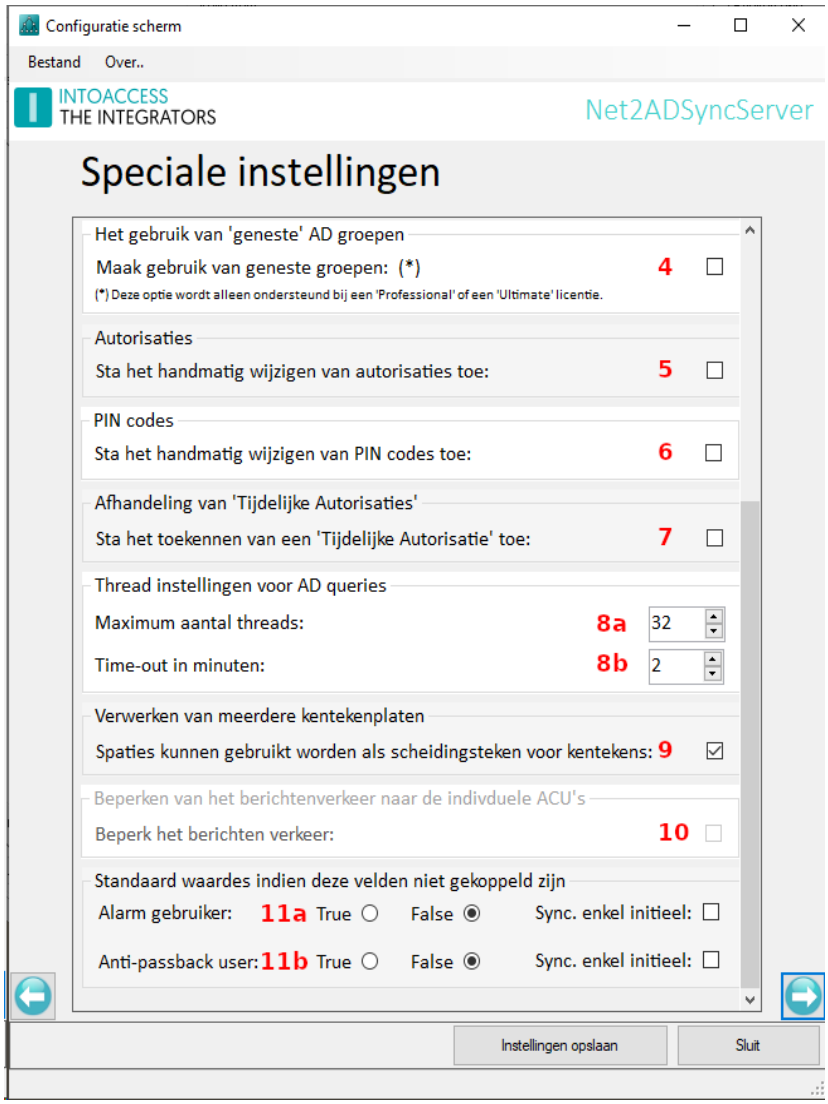
- Optie (2c) biedt de mogelijkheid om deze AD status volledig te negeren. Gebruikers met een 'uitgeschakeld' AD account worden dan hetzelfde verwerkt als gebruikers met een ingeschakeld account.

- Bij (3a..3b) 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 24.)



Afbeelding 24

- Bij (4), (Zie Afbeelding 25.) wordt de mogelijkheid geboden om in AD van 'geneste' groepen gebruik te maken.



Afbeelding 25

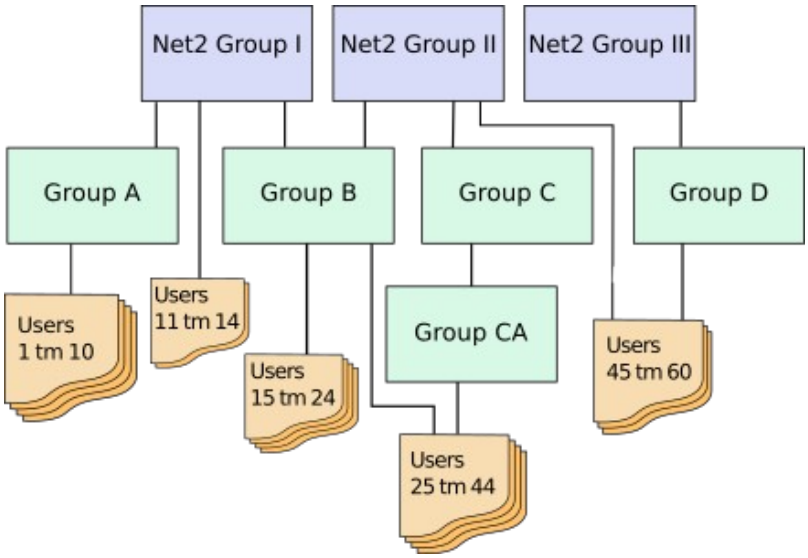
- (*Voor meer informatie over de inzet van geneste groepen zie het kopje 'Gebruik van geneste AD groepen' op pagina: 28*).
- Als het vinkje bij (5) gezet is worden autorisaties alleen initieel toegekend. Dat betekent dat enkel bij het aanmaken van een nieuwe medewerker in Net2 de autorisatie wordt overgenomen uit AD. Daarna mag er handmatig een andere autorisatie worden toegekend aan de betreffende medewerker zonder dat deze door het synchronisatieproces wordt teruggezet. Deze instelling wordt genegeerd voor medewerkers met een uitgeschakeld (disabled) account, en medewerkers die niet langer meer voorkomen in de AD en die in een aparte afdeling geplaatst moeten worden. (Zie 2b en 3b)
- Als het vinkje bij (6) gezet is worden pin codes alleen initieel toegekend. Dat betekent dat enkel bij het aanmaken van een nieuwe medewerker in Net2 de pin code wordt overgenomen uit AD. Daarna mag er handmatig een andere pin code worden toegekend aan de betreffende

medewerker zonder dat deze door het synchronisatieproces wordt teruggezet. Let op dat u deze optie moet aanvinken, wanneer u er voor kiest om kaart nummers vanuit AD te synchroniseren, maar handmatige pin codes wilt toestaan. Daar een kaart attribuut ook toestaat dat er een pin code bij wordt opgenomen (zoals P1234), dient u expliciet te configureren dat handmatig wijzigen van pin codes is toegestaan, om te voorkomen dat de sync applicatie deze verwijdert wanneer er geen pin code wordt gevonden in het kaart attribuut.

- In Paxton kan aan een medewerkers een 'Tijdelijke Autorisatie' toegekend worden. Normaal gesproken zal de applicatie deze, bij de eerstvolgende synchronisatie ronde, weer terug zetten naar de originele autorisatie. Als het vinkje bij (7) is gezet dan zal de applicatie 'tijdelijke autorisaties' respecteren. Dit biedt de mogelijkheid om medewerkers, tijdelijk, een andere autorisatie toe te kennen dan zij volgens de instellingen van de AD zouden mogen hebben. De gegevens worden zo effectief mogelijk opgehaald uit de Active Directory. De applicatie voert hiervoor veel taken gelijktijdig uit. In sommige gevallen, bijvoorbeeld bij oude PC's, kan dit tot problemen leiden. In zulke gevallen kan het verstandig zijn om het aantal 'threads' (grofweg het aantal gelijktijdige processen) te beperken. Bij (8a) en (8b) kunnen aanpassingen worden gedaan om de applicatie voor uw situatie zo optimaal mogelijk te laten lopen. In de praktijk zal het echter **zelden nodig zijn** om deze instelling aan te passen.
- Sinds versie 2.13.9 is de optie toegevoegd om het gebruik van spaties als scheidingsteken tussen kentekens in- of uit- te schakelen. (Optie 9) Deze optie is speciaal toegevoegd voor de Engelse markt. In tegenstelling tot Nederland is een spatie daar een legitiem karakter in een kenteken.
- Bij (10) wordt de optie geboden om het netwerkverkeer naar de individuele ACU's te beperken. Deze optie is bedoeld voor systemen met véél ACU's (> 30) waarbij de gegevens van alle medewerkers verstuurd moeten worden, bv bij de initiële synchronisatie slag. Deze optie is alleen van belang bij het gebruik van individuele autorisaties.
- Als medewerkers in Net2 het inbraaksysteem in- en/of uit- moet kunnen schakelen, of de anti-passback regels in acht moet nemen, dan kan bij (11a) of (11b) 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'. De optie om deze waarde alleen initieel te zetten biedt de mogelijkheid om deze waarde later handmatig aan te passen. Een waarde alleen initieel synchroniseren, betekent feitelijk alleen bij het aanmaken van een gesynchroniseerde gebruiker. In tegenstelling tot de standaard waarden, zal de 'Sync, enkel initieel' optie ook werken als er een AD veld is gekoppeld. Als de waarde echter van Net2 naar AD gaat, is het alleen initieel synchroniseren impliciet (instelling genegeerd). Bij de aanmaak van de gebruiker zal het attribuut de de waarde uit AD krijgen, waarna deze handmatig kan worden aangepast en naar AD gesynchroniseerd wordt.

Gebruik van geneste AD groepen

Hieronder is deze mogelijkheid nader uitgewerkt. (Zie Afbeelding 26.)



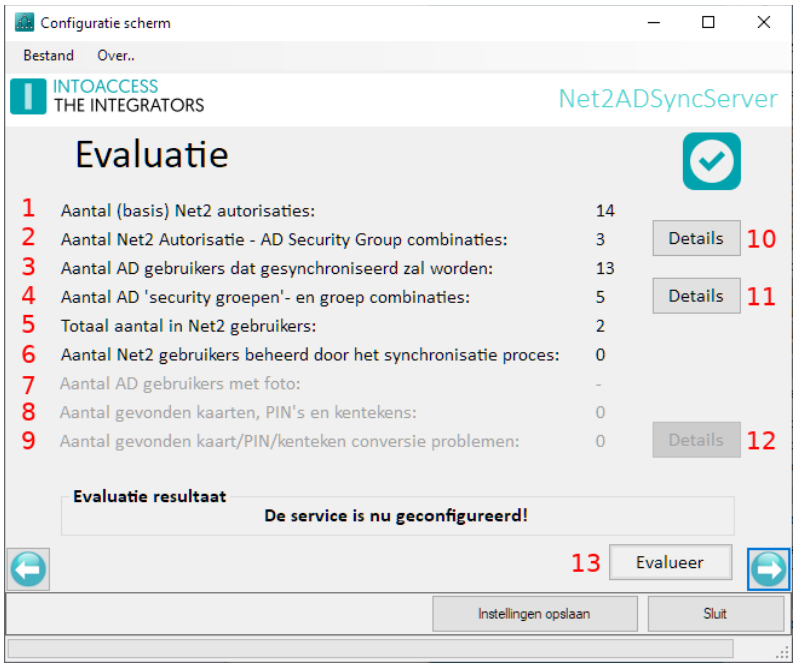
Afbeelding 26

- 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 medewerkers: 'Users 1 tm 10' zijn via 'Group A' lid van 'Net2 Group I'. Deze medewerkers 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 medewerkers ook niet gesynchroniseerd worden.
- De medewerkers: 'Users 11 tm 14 zijn direct lid van 'Net2 Group I'. Deze medewerkers zullen in het synchronisatie proces worden opgenomen, ongeacht de instelling voor het gebruik van geneste groepen.
- De medewerkers: 'Users 15 tm 24 zijn via 'Group B' zowel lid van 'Net2 Group I' als van 'Net2 Group II'. Deze medewerkers zullen een autorisatie toegewezen krijgen die de verzamelde rechten bevat van autorisatie 'Net2 Group I' en 'Net2 Group II'.
- De medewerkers: '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'. medewerkers mogen dus via verschillende wegen lid zijn van een, aan een Net2 gerelateerde, autorisatie groep;
- De medewerkers: '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 medewerkers hier lid zijn van meer dan één (aan een Net2 autorisatie gerelateerde) groep.

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 27.)



Afbeelding 27

Het evaluatie proces

Na het indrukken van de '*Evalueer*' knop (13) zal de applicatie zowel de medewerkers uit AD, als uit Net2 verzamelen. Het zal dit doen volgens dezelfde regels als het synchronisatie process.

Getoonde informatie

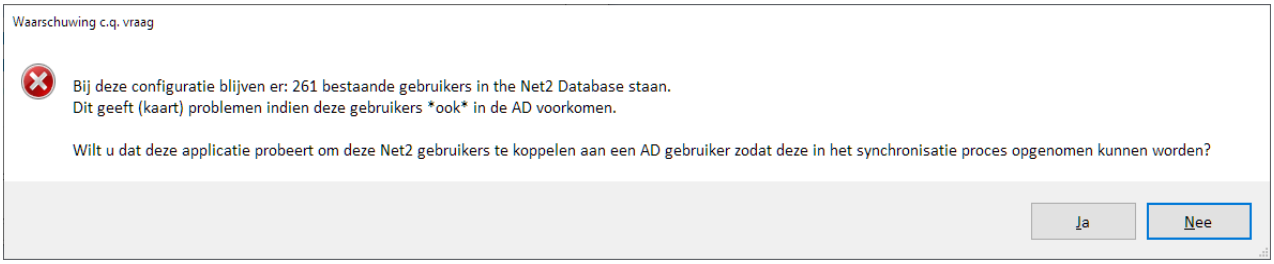
- Bij (1) zal het aantal, in Net2 gevonden autorisaties getoond worden. Indien er van een 'Ultimate' licentie gebruik wordt gemaakt, en de applicatie al een keer actief is geweest, kan het zijn dat er al één of meerdere 'afgeleide' autorisaties in Net2 aanwezig zijn. Deze zullen hier dan niet worden 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 (10) en (11) bieden de mogelijkheid om de gevonden waarden te inspecteren.

- 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. Er zal een waarschuwing getoond worden als dit gedetecteerd wordt.
- 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 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 (8) wordt het aantal in de AD gevonden kaarten, PIN's en kentekens getoond.
- Bij (9) wordt het aantal fouten getoond die zijn opgetreden tijdens de verwerken van de kaarten, PIN's en/of kentekens. De selectie van een onjuist kaarttype (Mifare/Paxton) is een veel voorkomende oorzaak van dit soort fouten. (Zie pagina: '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 (12).
- De regels/knop bij (8), (9) en (12) zijn 'grijs' indien er geen gebruik gemaakt wordt van de mogelijkheid om kaarten te synchroniseren.

Koppelen van AD gebruikers aan reeds bestaande Net2 gebruikers

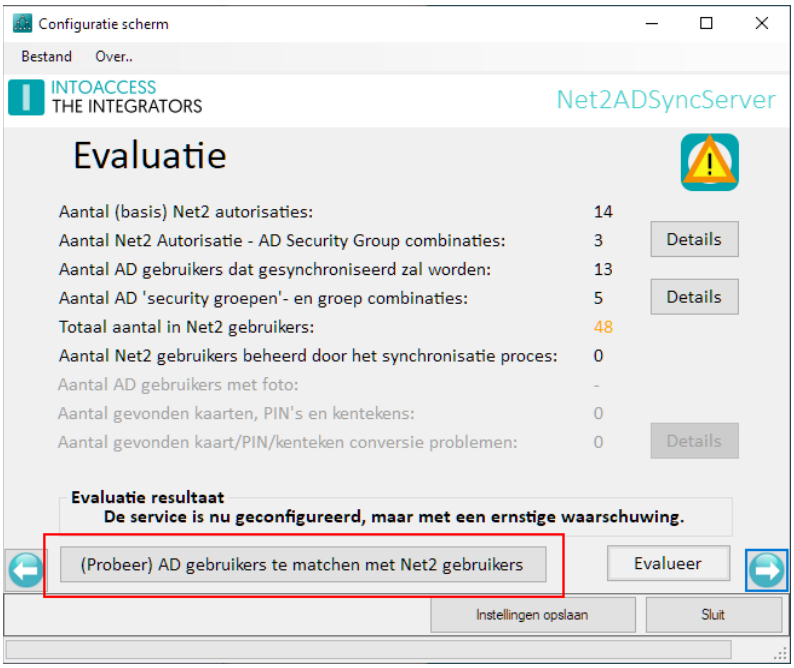
Sinds versie 2.15.0 wordt de mogelijkheid geboden om reeds bestaande Net2 gebruikers op te nemen in het synchronisatie proces.

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 28.)



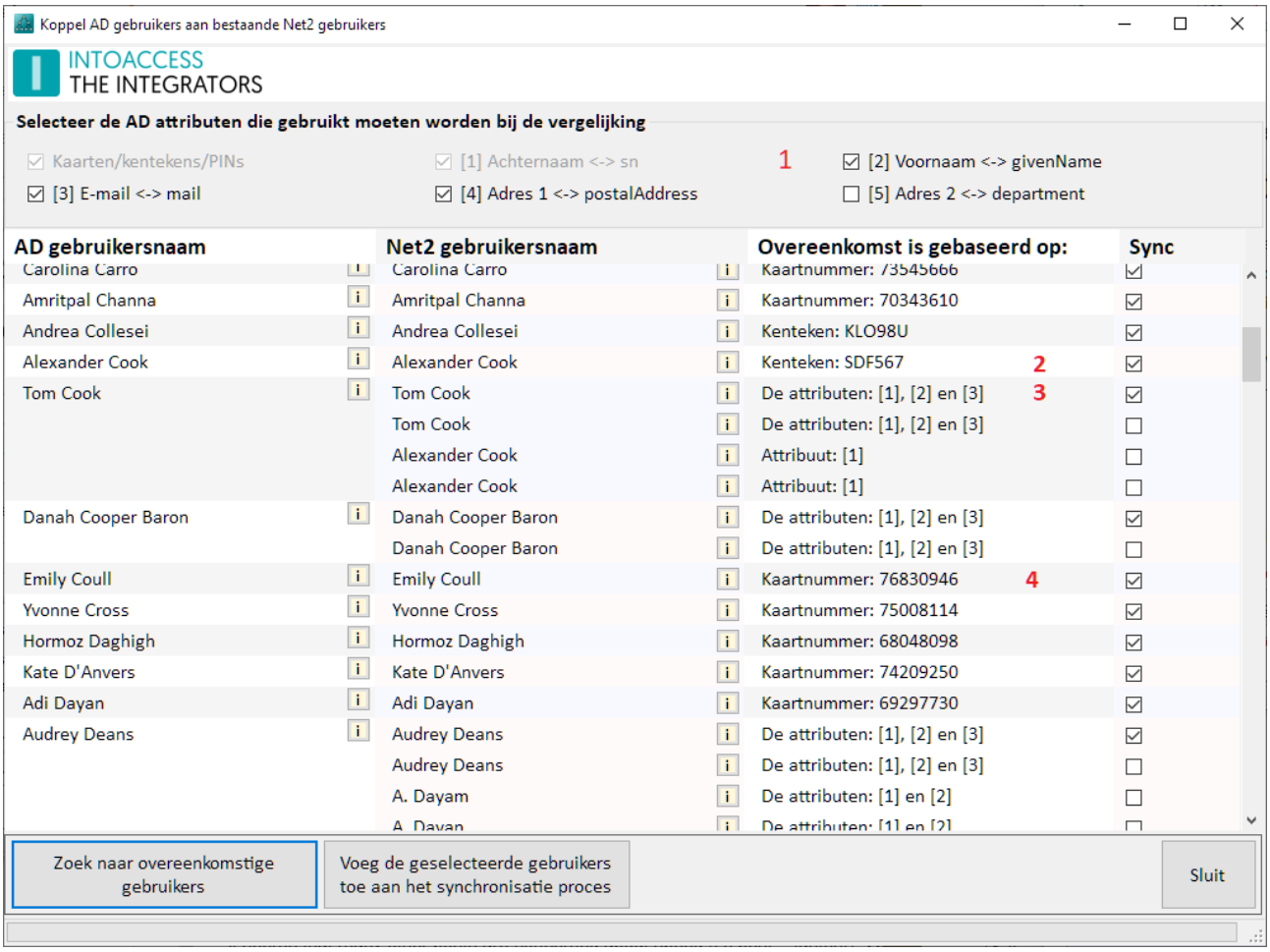
Afbeelding 28

Indien dit inderdaad gewenst is wordt er een extra knop vrijgeschakeld waarmee het koppel proces gestart kan worden. (Zie Afbeelding 29.)



Afbeelding 29

Na het indrukken van de '*(Probeer) AD gebruikers te matchen met Net2 gebruikers*' knop wordt er een nieuw scherm geopend. (Zie Afbeelding 30.), (In eerste instantie nog zonder zoekresultaten).

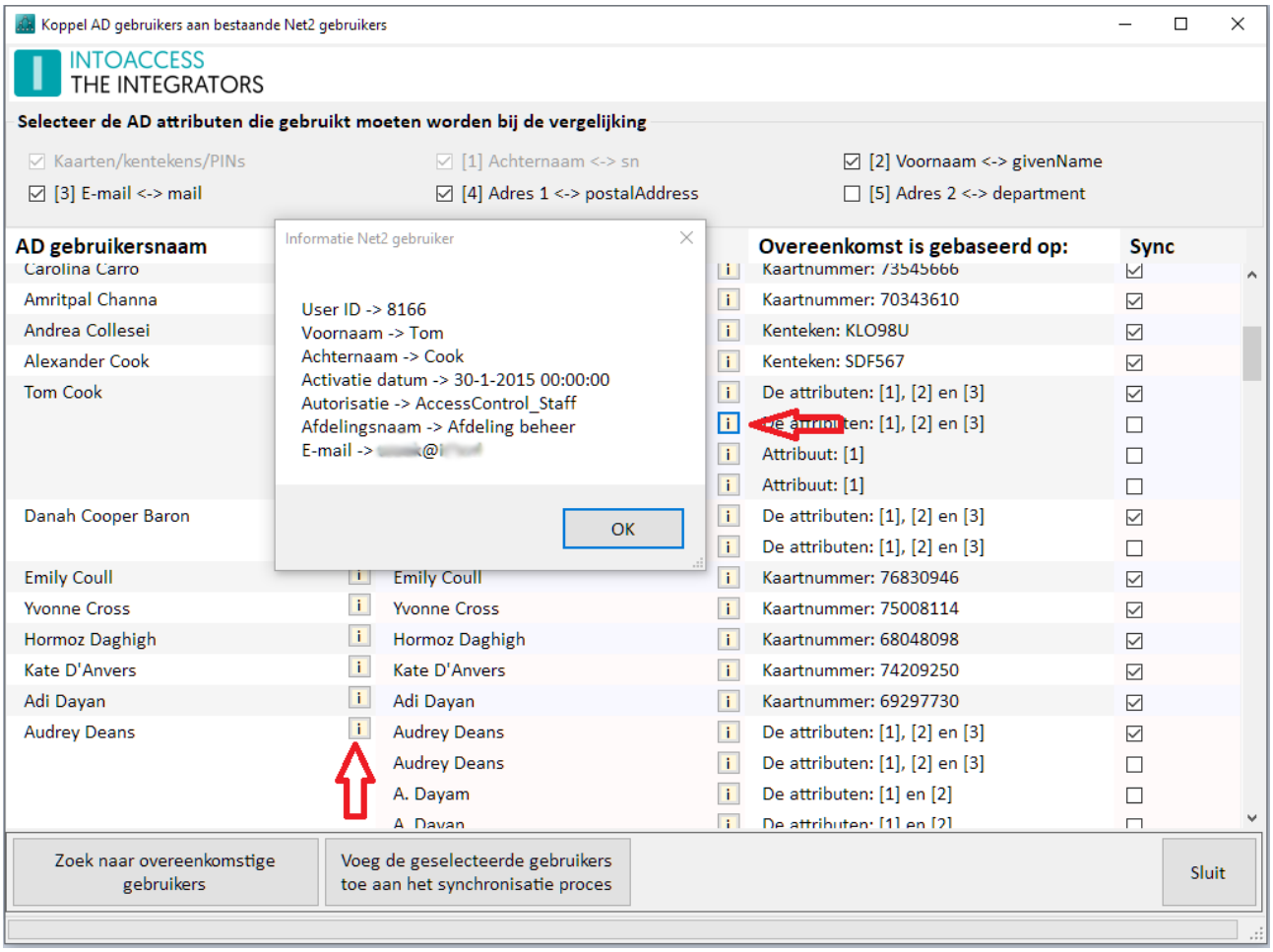


Afbeelding 30

- 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 31.)

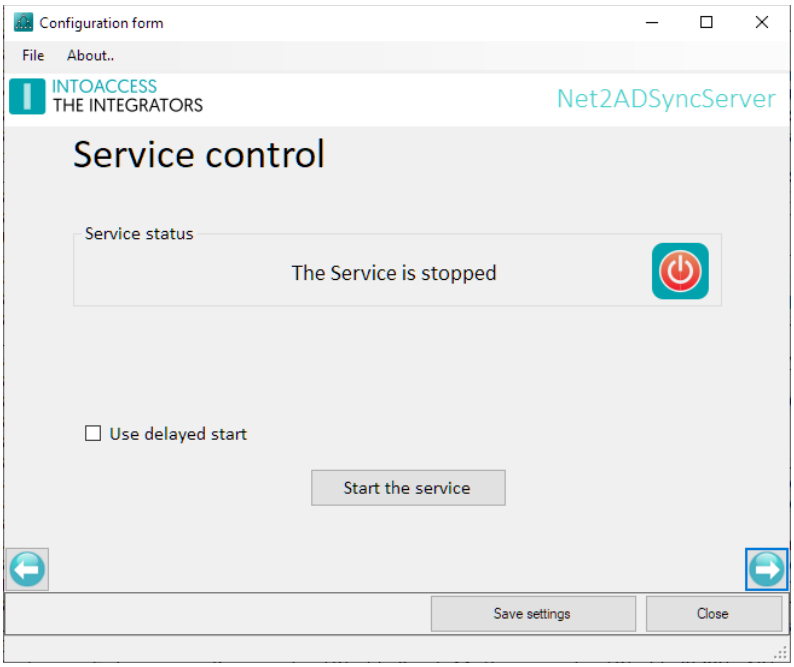


Afbeelding 31

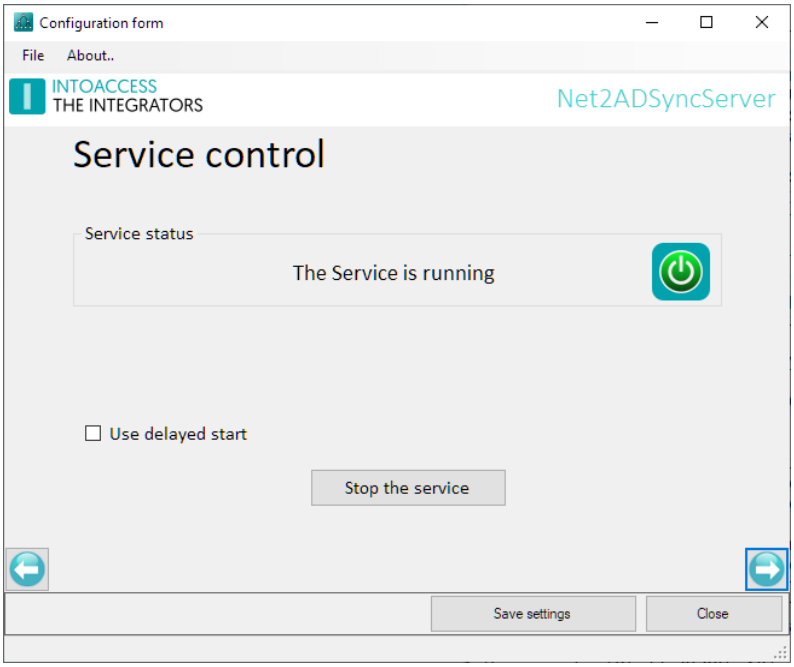
Na het indrukken van de '*Voeg de .. proces*' knop zullen de geselecteerde gebruikers worden opgenomen in het synchronisatie proces. Daartoe zullen de beide velden zoals benoemd bij (1) en (2) in hoofdstuk: 'De AD-Net2 Synchronisatie instellingen' op bladzijde 8, gevuld worden met de 'sAMAccountName'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

Service Beheer

Deze pagina, (Zie .Afbeelding 32 en Afbeelding 33), 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: 35 ('Log instellingen'). De laatste logmeldingen die hier getoond worden geven inzicht in de reden waarom de service niet start.



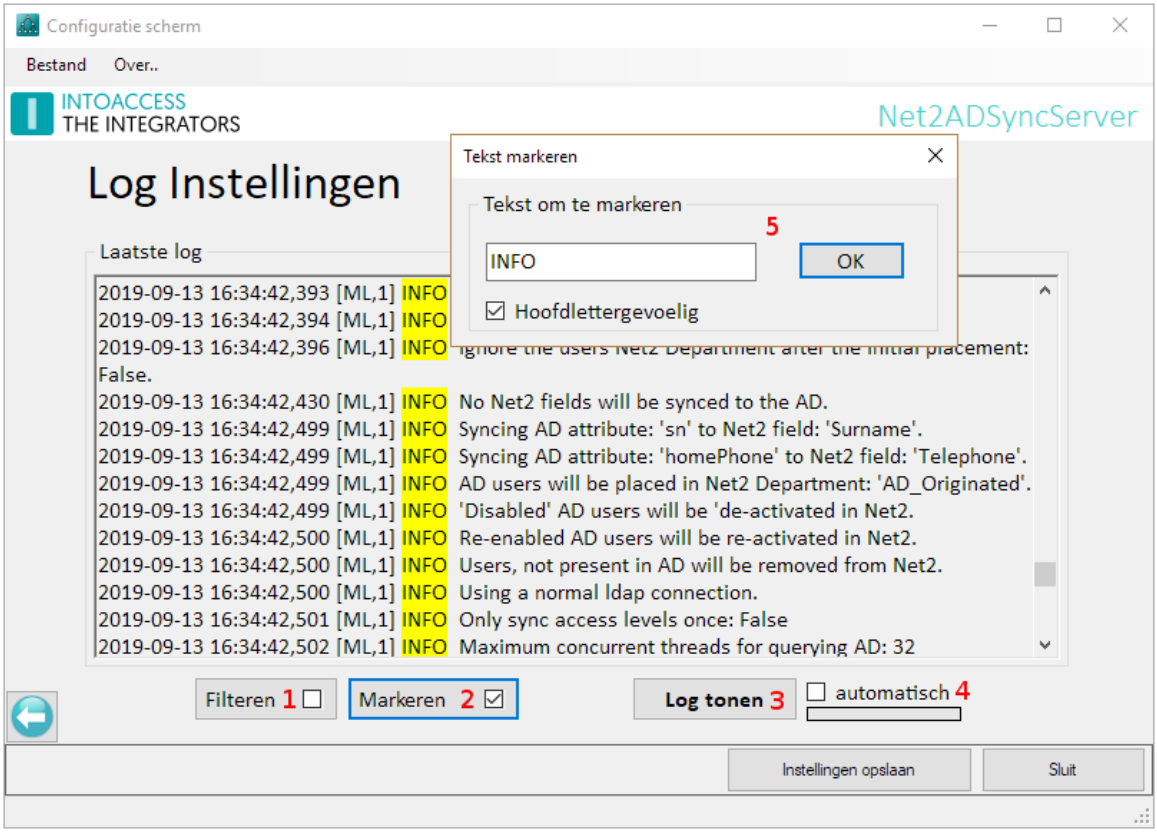
Afbeelding 32



Afbeelding 33

De Log instellingen

Deze pagina, (Zie Afbeelding 34.), biedt de mogelijkheid om de laatste (max. 500) regels uit de logfile te bekijken. De applicatie logt zeer gedetailleerd welke stappen er allemaal doorlopen worden. Mocht de applicatie met een onverwacht probleem geconfronteerd worden dan kan, met behulp van deze logfile, de oorzaak vaak snel worden gevonden.



Afbeelding 34

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.

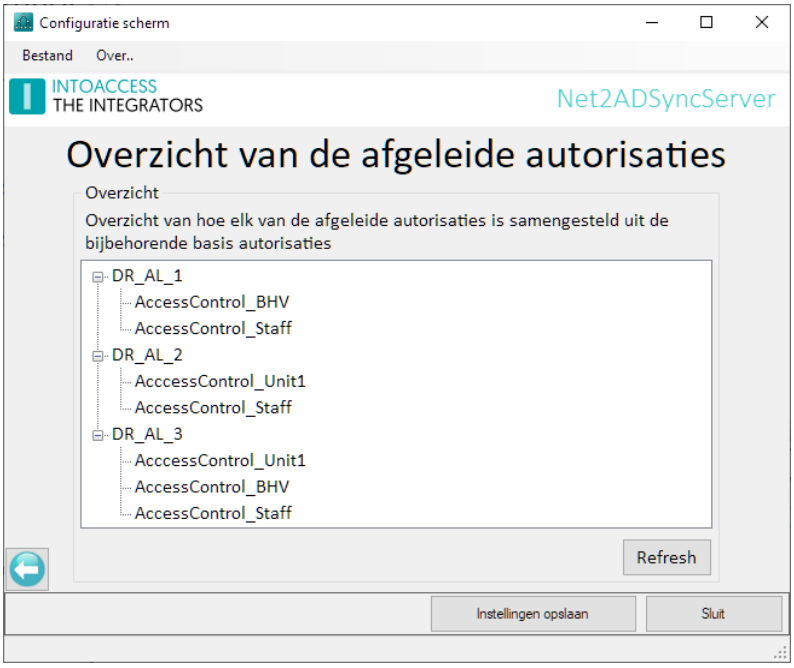
De logfile zelf bevindt zich in de folder: c:\IntoAccess\Logging\Net2ADSyncServer\

Overzicht van de afgeleide autorisaties

Op deze pagina (Zie Afbeelding 35) kan een overzicht worden getoond van de opbouw van de door de applicatie gegenereerde autorisaties (de DR_AL_<n> autorisaties). Van ieder van deze afgeleide autorisaties is te zien uit welke 'basis' autorisaties deze is opgebouwd.

Deze pagina wordt alleen getoond indien:

- Er gebruik gemaakt wordt van een 'Ultimate' licentie;
- Het gebruik van 'globale' autorisaties is geselecteerd;
- De applicatie al eerder minimaal één afgeleide autorisatie heeft aangemaakt;



Afbeelding 35

Handleiding Net2ADSyncServer
Versie 4.3