www.aras.nl
www.aras.be

Handleiding

MorphoManager i.c.m. Paxton Net2

Aanvullende informatie

Artikelnummer: BIO-MO-MANAGER

Versie: April 2023

ARAS SECURITY

Algemene informatie

Wijzigingen voorbehouden.

Kijk op onze support site http://support.aras.nl/ voor actueel nieuws en FAQ.

Voor technische ondersteuning:
E-mail: techhelp@aras.nl
Helpdesk: 0900 – 27 27 43 57

Inhoudsopgave

Inleiding

Voor beveiliging van ruimten met een zeer hoog risico brengt ARAS de vingerprint lezers van IDEMIA. Deze zorgen ervoor dat deuren niet geopend kunnen worden met een geleende, gevonden of gestolen pas. Er zijn modellen die alleen de vinger scannen, maar voor extra zekerheid zijn ook combinaties met paslezers en/of een pincodepaneel mogelijk. De biometrische lezers van IDEMIA bewijzen dat design wel degelijk gecombineerd kan worden met veiligheid. Door de onderscheidende algoritmes van IDEMIA blijven deze zelfs onder de meest uitdagende omstandigheden betrouwbaar identificeren.

Deze handleiding is enkel voor de SIGMA Lite & SiGMA Lite+ lezers van IDEMIA. Indien andere lezers gewenst zijn adviseren wij om contact op te nemen met de helpdesk van ARAS Security.

De installatie van Morpho Manager en Net2 worden beschreven elk in een losse handleiding, deze handleiding is enkel bedoelt voor de configuratie van Morpho Manager en de configuratie van Net2.

! LET OP !
De huidige SIGMA Lite & SIGMA Lite+ lezers zijn voorzien van een TLS encryptie, dit houdt in dat de werking van de kaartlezers anders is. TLS encryptie staat aan vanaf versie 4.12.0.

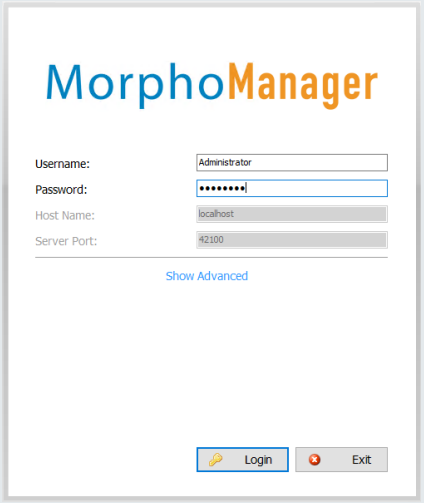
- Er dient altijd gebruik gemaakt te worden van de laatste versie Morpho Manager (versie 16.1.1.3 en hoger).
- De MBTB tool dient te beschikken over de laatste functionaliteiten (MBTB tool vanaf versie 4.6.13).
- Apparaten werken enkel in combinatie met TLS 1.2.
- Lokale configuratie op het apparaat is niet mogelijk.
- Thrift Commands (Integratie mogelijkheden) via RS485 zijn niet mogelijk (indien een integratie gewenst is, neem dan contact op met de helpdesk van ARAS Security.)

1. Basis configuratie

1.1. Login procedure

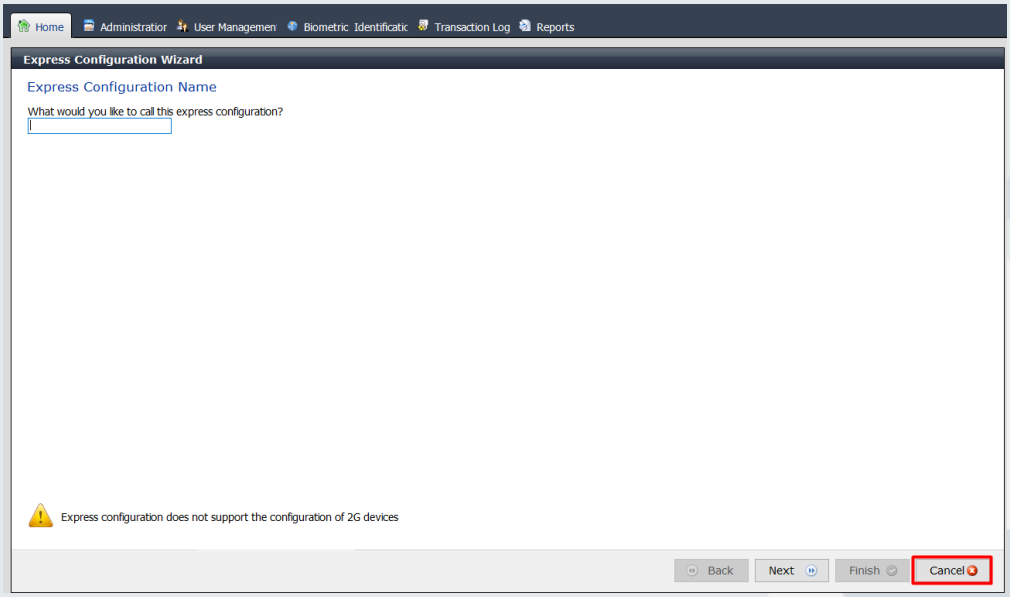
Zodra Morpho Manager is geïnstalleerd kan er ingelogd worden op de software.
De standaard logingegevens zijn:

Gebruikersnaam / Username: **Administrator**
Wachtwoord / Password: **password**



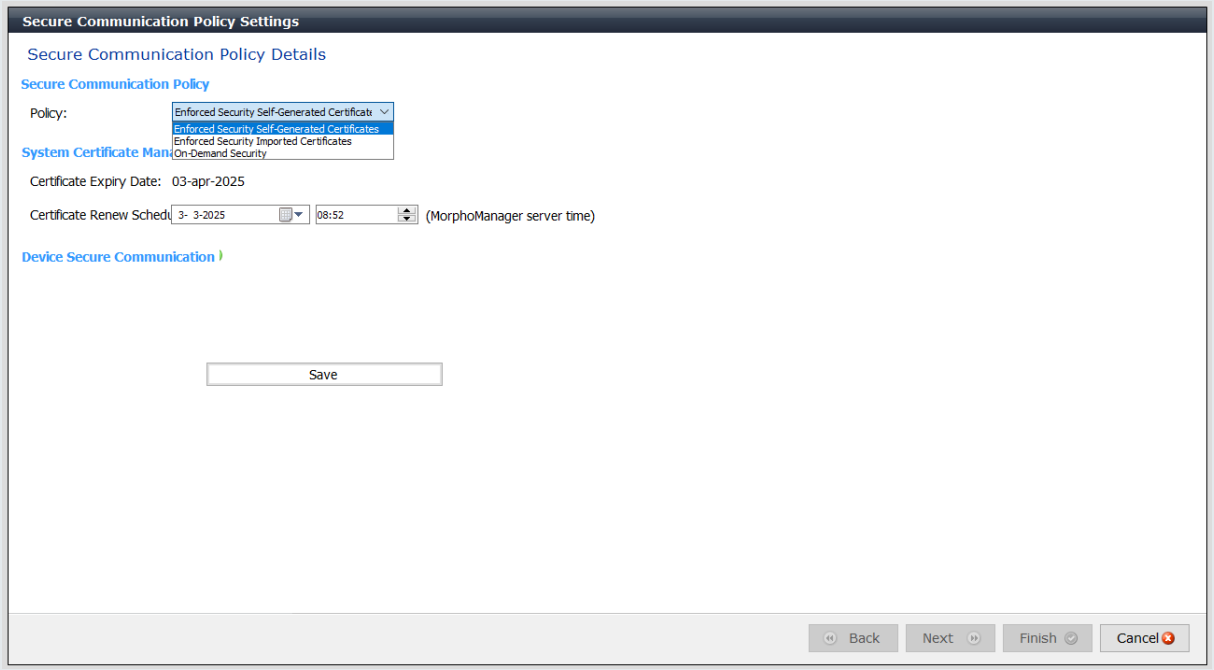
Vervolgens kan er op *Login* gedrukt worden.

Hierna verschijnt er een scherm voor de *Express Configuration*, klik hier op Cancel.



1.2. TLS Communicatie configureren

Nadat het scherm voor de Express Configuration is geannuleerd volgt het scherm voor de Secure Communication Policy. Hierin zijn er 3 mogelijkheden.



- Enforced Security Self-Generated Certificates
- Enforced Security Imported Certificates
- On-Demand Security

1.2.1. Enforced Security Self-Generated Certificates (aanbevolen)

Binnen deze optie genereerd de software zelf certificaten. Dit is de meest eenvoudige optie voor kleine systemen of voor systemen waarbij het niet van toepassing is dat er speciale/hoge certificaten vereist zijn.

1.2.2. Enforced Security Imported Certificates

Deze optie biedt de mogelijkheid om zelf certificaten in te laden, er zijn 2 certificaten benodigd (Authority.crt & Server.p12) om deze vervolgens in te laden en te converteren naar bestanden welke in de lezers geladen kunnen worden.

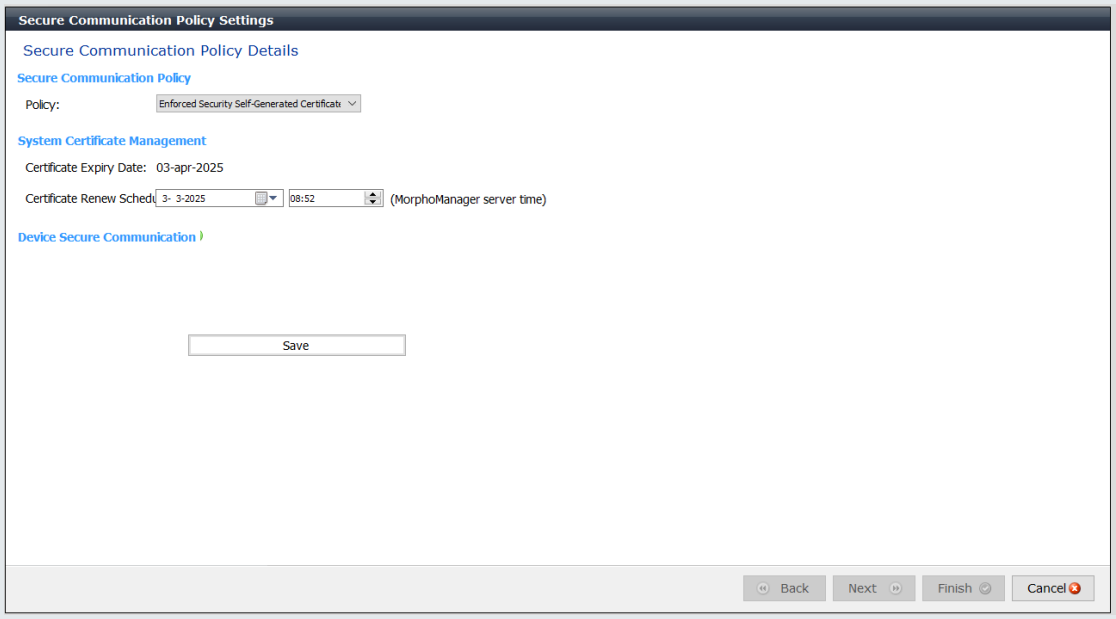
1.2.3. On-Demand Security

Dit is de meest onveilige optie. Indien gewenst wordt om deze optie te gebruiken adviseren wij om contact op te nemen met de helpdesk van ARAS Security.

1.2.4. Configureren van het TLS certificaat

In deze handleiding maken we gebruik van de optie Self-Generated Certificates. Dit om eenvoudig door de procedure te lopen, toch gebruik te kunnen maken van TLS zonder dat er kosten zijn voor certificaten.

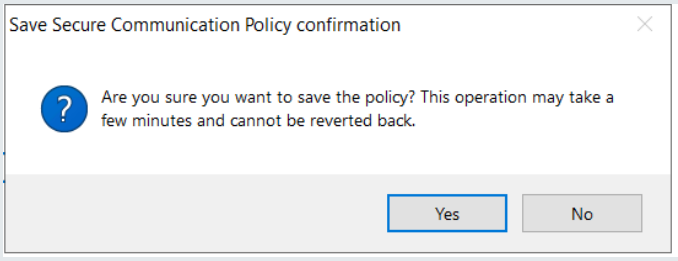
Selecteer bij Policy de Enforced Security Self-Generated Certificates.



Zodra deze is geselecteerd komt de software met een verloopdatum en een vernieuwdatum van het certificaat. Standaard is deze voor 2 jaar geldig.

Druk vervolgens op *Save* om de instellingen op te slaan.

Hierna komt een waarschuwingsmelding naar voren, dit om ervoor te zorgen dat de instellingen die gedaan worden het systeem te versleutelen met TLS encryptie.

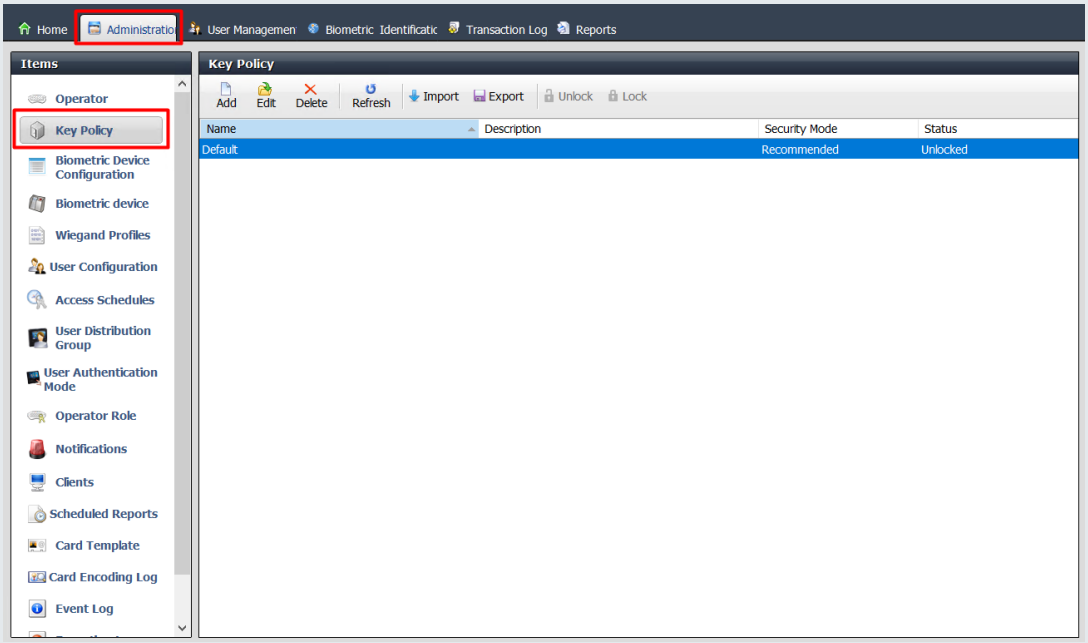


Klik binnen de waarschuwing op *Yes* om door te gaan, het systeem wordt her-geconfigureerd. Dit kan enkele minuten in beslag nemen. Zodra dit klaar is kan er op Finish gedrukt worden onderin het scherm.

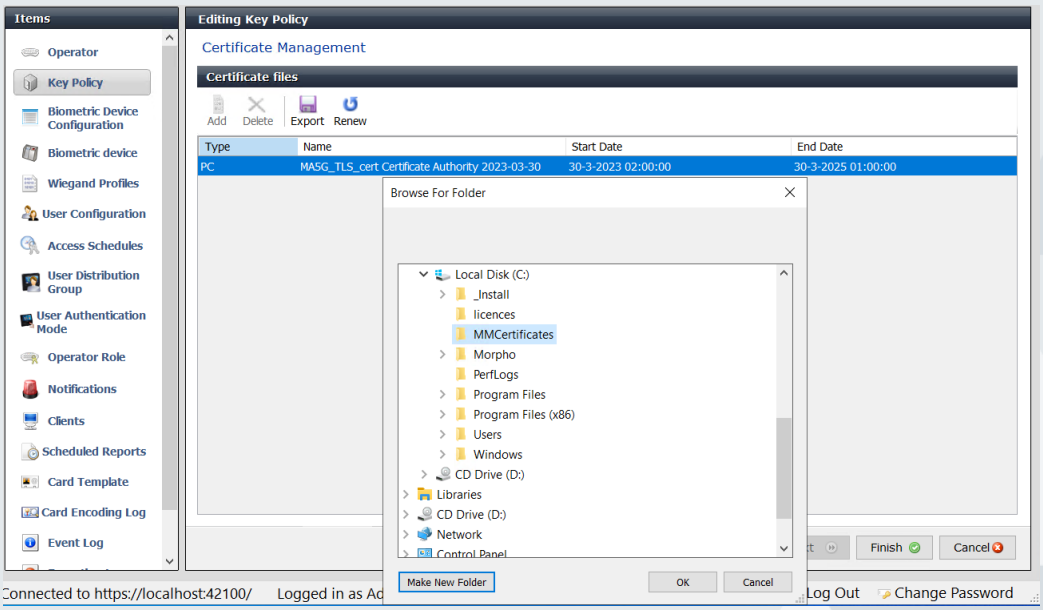
Nu is het systeem TLS versleuteld en kan het certificaat geconverteerd worden.

1.2.5. Certificaten opslaan

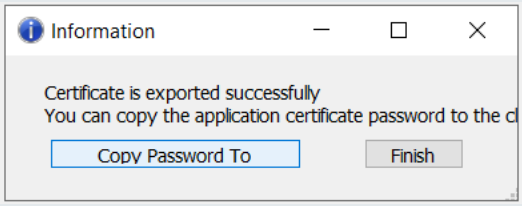
Om de certificaten te converteren zullen deze eerst geëxporteerd dienen te worden vanuit de software. De certificaten zijn te vinden onder Administration – Key Policy.



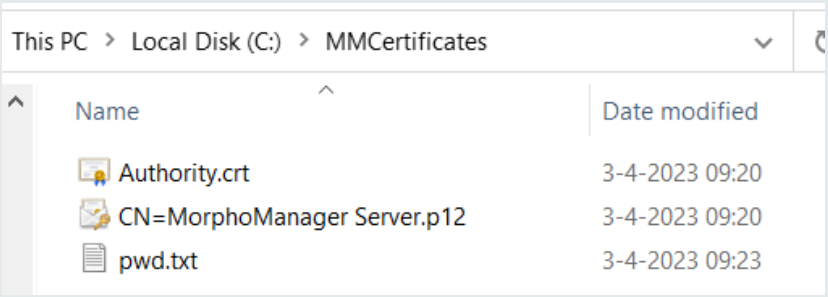
Klik vervolgens op *Edit* (bewerken) en druk 8x op *Next* (alle andere pagina's betreffen andere configuratie zaken waarbij we in deze handleiding niet op in gaan). Het scherm Certificate Management komt nu naar voren. Klik hier op Export en zorg ervoor dat de bestanden op de C:-schijf worden opgeslagen.



De software komt vervolgens met de melding dat de certificaten zijn opgeslagen. Deze zijn versleuteld met een wachtwoord. Dit is een zeer belangrijk wachtwoord, zorg ervoor dat deze wordt opgeslagen bij de certificaten (tijdens de installatie) en later eventueel op een logische plek zodat dit wachtwoord altijd bewaard blijft. Het wachtwoord kan eenvoudig gekopieerd worden met de knop *Copy Password To*.



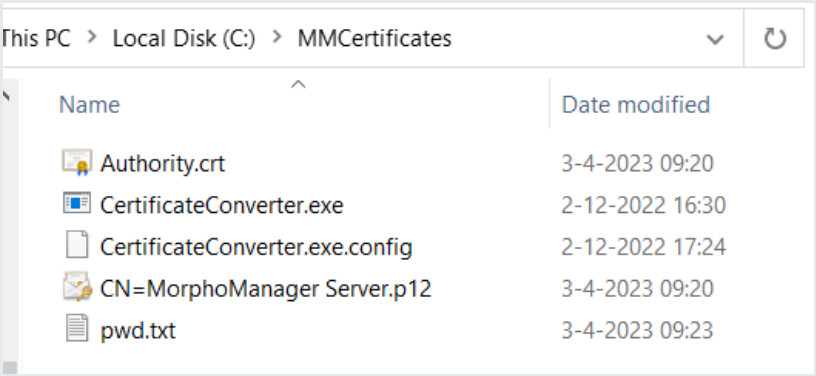
Voor nu slaan we hem op binnen dezelfde map als waar de certificaten staan.



1.2.6. Certificaten Converteren

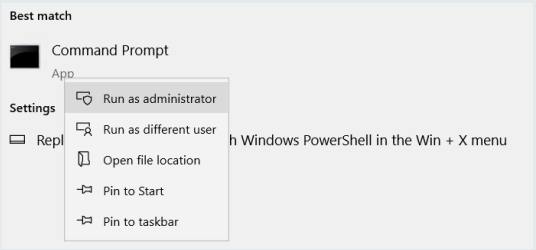
Nu de certificaten zijn opgeslagen kunnen deze geconverteerd worden naar bestanden welke gebruikt dienen te worden om de lezers te kunnen her-configureren zodra deze in Morpho Manager actief zijn geweest.

Stap 1. Kopieer vanaf de installatiemap of de USB stick de map CertificateConverter naar de map waar de certificaten zijn opgeslagen.

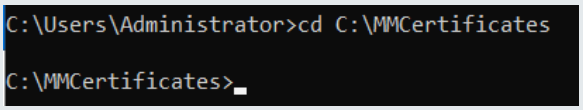


Nu alles compleet is kan de conversie beginnen.

Stap 2. Open hiervoor Opdrachtprompt in Administrator modus.



Stap 3. Ga binnen Opdrachtprompt als eerste naar de juiste map. Dit kan door het commando ‘cd’ gevolgd door de locatie.



Stap 4. Kopieer vanaf de installatiemap of de USB stick de inhoudt van het bestand ConversieScript.txt (pas eventueel het pad aan indien deze anders is dan deze handleiding.

Stap 5. Plak de inhoudt nu in Opdrachtprompt. En voer het uit door op de ‘Enter’-toets te drukken.

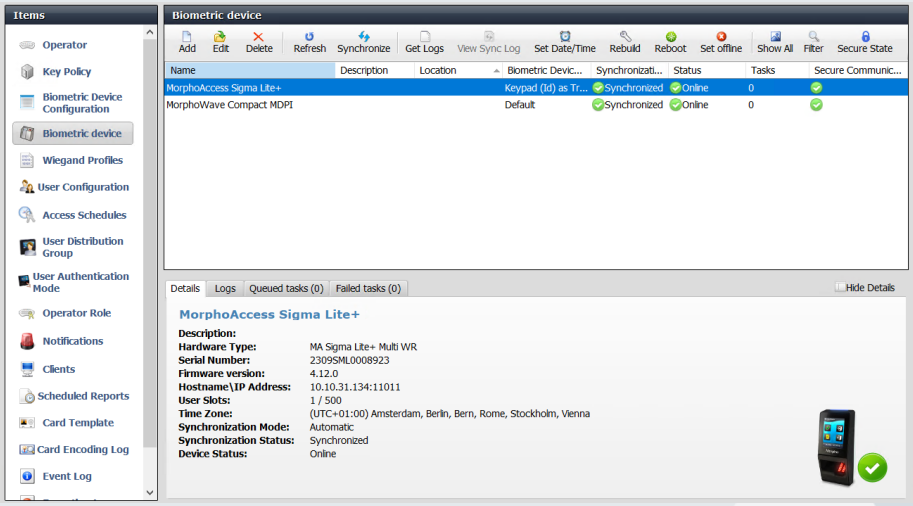
Stap 6. Zodra dit is afgerond geeft Opdrachtprompt de melding dat het is gelukt, nu staan er in de map waar de certificaten staan 2 extra bestanden met als extensie .pem (MACI_full.pem & TerminalCA.pem)

Deze certificaten zijn benodigd om een verbinding te maken met de lezers inclusief te certificaten. Zoals te zien is in hoofdstuk 2.2 de handleiding ‘Gebruikershandleiding SIGMA Lite & SIGMA Lite+’.

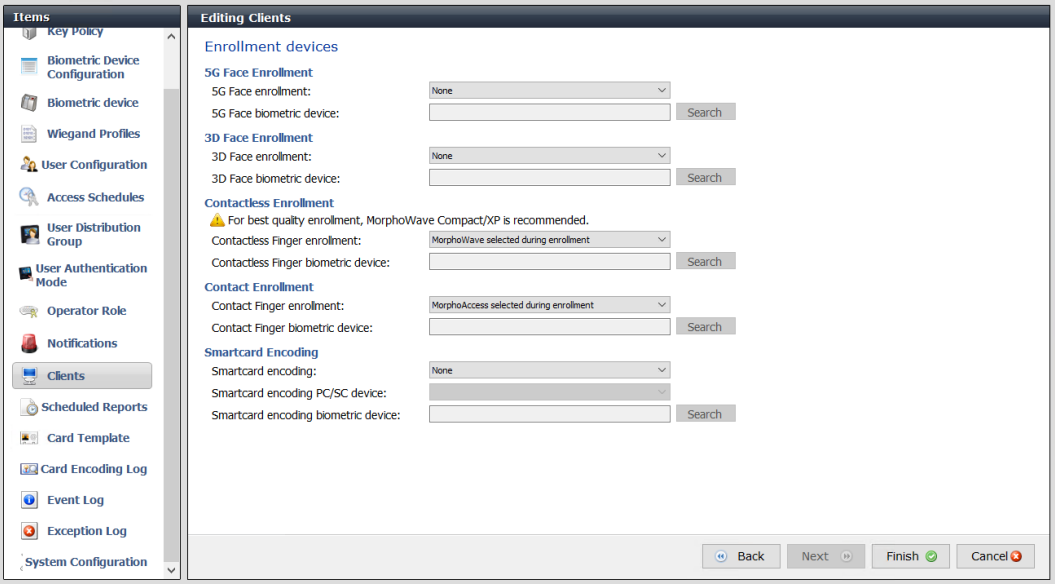
Wanneer dit is afgerond kunnen Opdrachtprompt en de map waar het certificaat worden gesloten.

1.3. Lezers toevoegen aan het systeem

Nu de certificaten zijn gemaakt, en de certificaten zijn geëxporteerd kunnen er lezers aan het systeem worden toegevoegd. Dit kan in MorphoManager Onder Administration - Biometric Device, hier staan alle lezers welke in het systeem zijn toegevoegd en of deze verbinding hebben met de software.

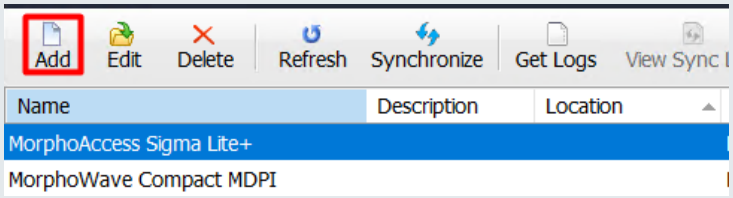


Eerst zal de instelling voor de client bepaald dienen te worden. Dit om in te stellen hoe gebruikers zich in een later stadium zichzelf gaan inleren. Ga hiervoor naar *Administration – Clients* en klik op *Edit*. Op de laatste pagina kunnen de apparaten worden geselecteerd welke gaan dienen om in te kunnen leren. In het voorbeeld hieronder is gekozen dat de lezer geselecteerd gaat worden tijdens het aanmaken van de persoon.



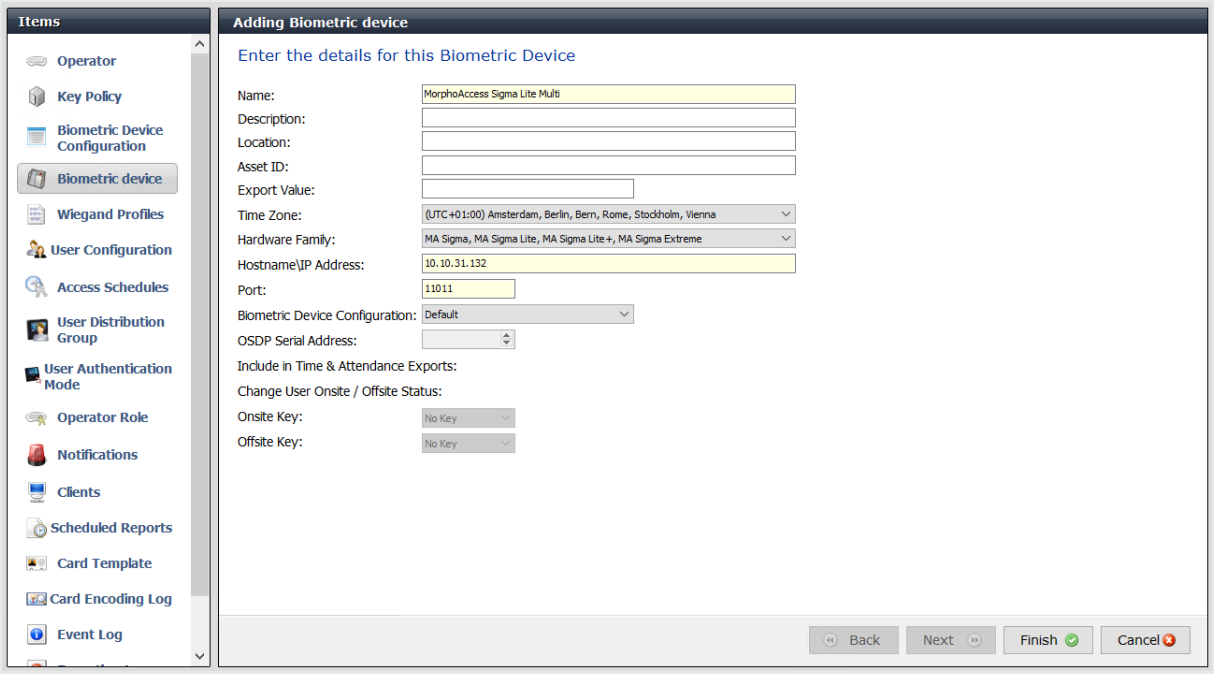
1.3.1. Lezer configureren

Om een lezer toe te voegen dient er op *Add* geklikt te worden.



Er verschijnt nu een scherm om een nieuwe lezer toe te voegen, vul de volgende gegevens in;

- Naam - Dit kan een locatiebenaming zijn waar de lezer zich bevindt *(bijvoorbeeld Technische ruimte A.10.1*).
- Time Zone – Zet deze tijdzone naar de gewenste tijdzone (*bijvoorbeeld UTC+01:00*).
- Hardware Family – Dit is geheel afhankelijk van het type lezer (in de meeste gevallen zal dit de MA Sigma, MA Sigma Lite, MA Sigma Lite+ en MA Sigma Extreme zijn).
- Hostname / IP Address – Vul hier het IP adres van de lezer in
- Biometric Device Configuration – Zet deze voor nu op Default (Dit zullen we later aanpassen).



Wanneer alle gegevens zijn ingevuld kan er op *Finish* geklikt worden. De kaartlezer gaat verbinding maken met de software en synchroniseren. Binnen het synchronisatieproces zal ook het certificaat worden gekoppeld. De lezer zal zich dan ook een aantal keer herstarten om de juiste configuratie te laden.

1.3.2. Leesprofiel configureren

Omdat er is gekozen om samen met Paxton te werken zijn er twee mogelijkheden beschikbaar.

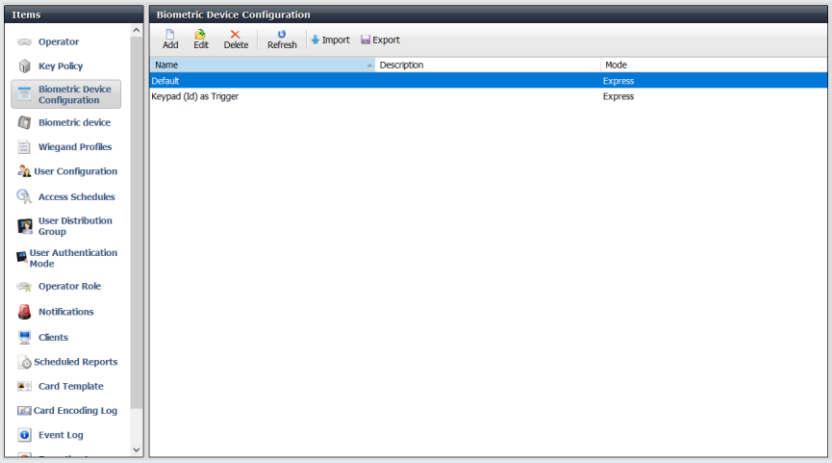
- ENKEL vinger (Biometric ONLY)
- Vinger + PIN (Keypad (ID) as trigger)

Hieronder wordt beschreven hoe dit geconfigureerd kan worden.

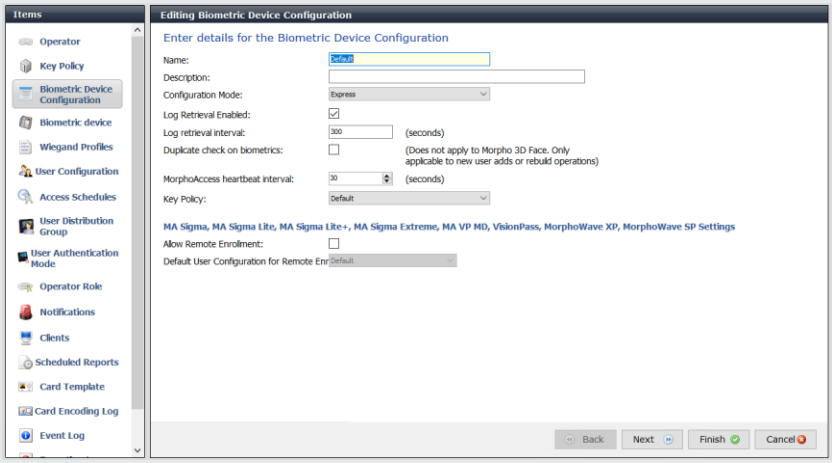
1.3.2.1. ENKEL vinger (Biometric ONLY)

Standaard werkt dit in Morpho al, met wat kleine aanpassingen zal dit ook met Net2 werken. Voor de volledigheid zal dit wel uitgelegd worden in de handleiding.

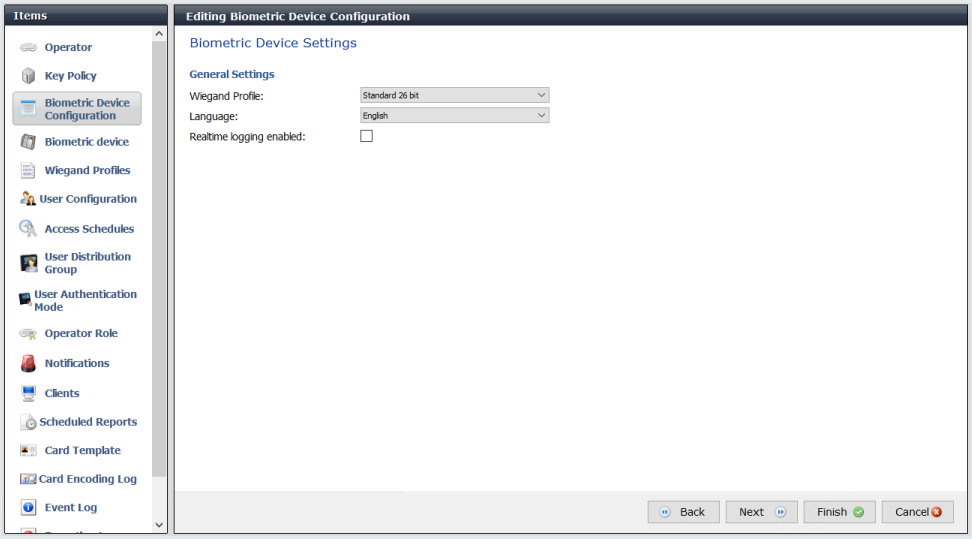
Alvorens de lezer geconfigureerd wordt is er een *Biometric Device Configuration* template beschikbaar genaamd ‘Default’. Deze kan worden ingezien onder *Configuration - Biometric Device Configuration*. Klik hiervoor op bewerken om de configuratie in te zien.



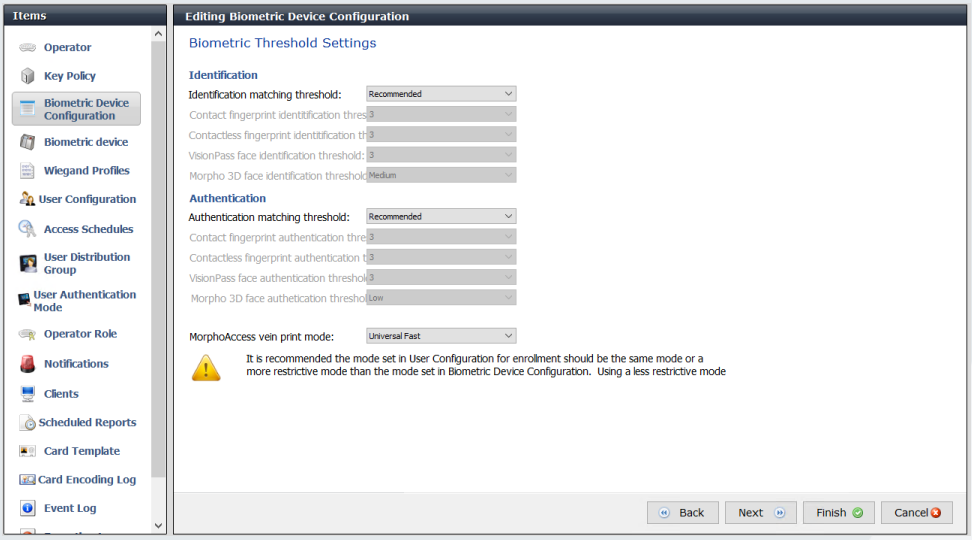
Op de eerste pagina is onder andere de Key Policy geconfigureerd voor de TLS versleuteling. Op deze pagina zullen er geen aanpassingen zijn. En kan er dus op *Next* geklikt worden.



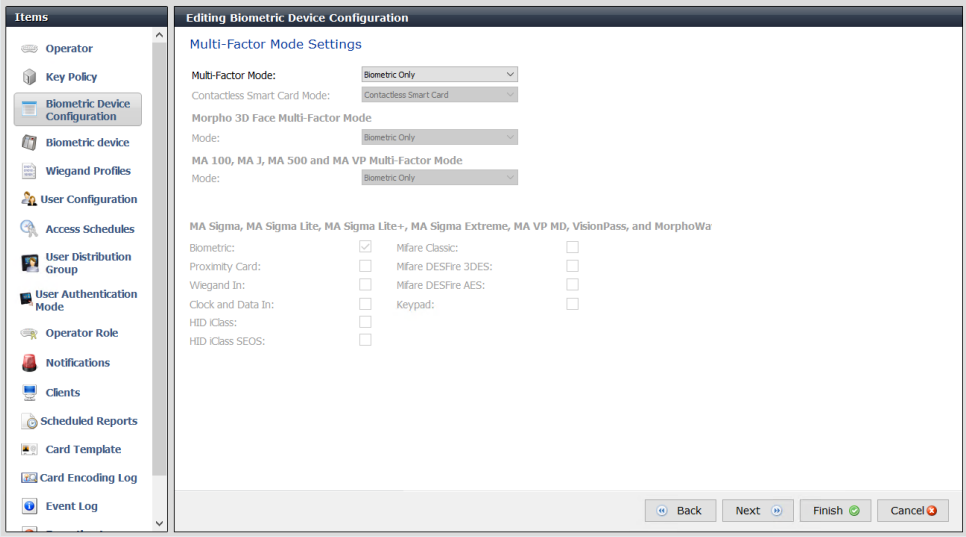
Op de volgende pagina is het kaartformaat te vinden, om het systeem te laten werken met Net2 dient het Wiegand profiel omgezet te worden naar *Standard 26 bit*. Zodra dit is gedaan kan er op *Next* geklikt worden.



Na het kaartformaat goed te hebben gezet volgt de pagina voor de gevoeligheid van de lezer. Wanneer de lezer zal worden gebruikt met vingers die slecht te lezen zijn kan dit hier veranderd worden. Standaard staan deze instellingen op Recommended. We adviseren het om deze instelling zo te laten staan en eerst te kijken wat de leesbaarheid van de vingers is alvorens deze instelling wordt aangepast. Klik hier ook weer op *Next* om verder te gaan.

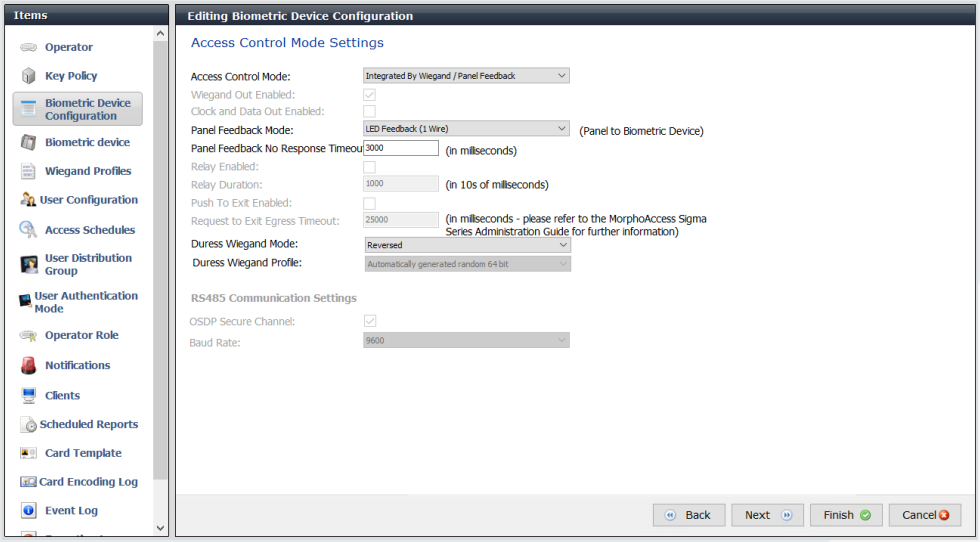


Hierna kan de modus ingesteld worden. Voor de configuratie ENKEL vinger is het voldoende om Biometric Only toe te passen. Klik zonder aanpassingen te doen op Next om verder te gaan.



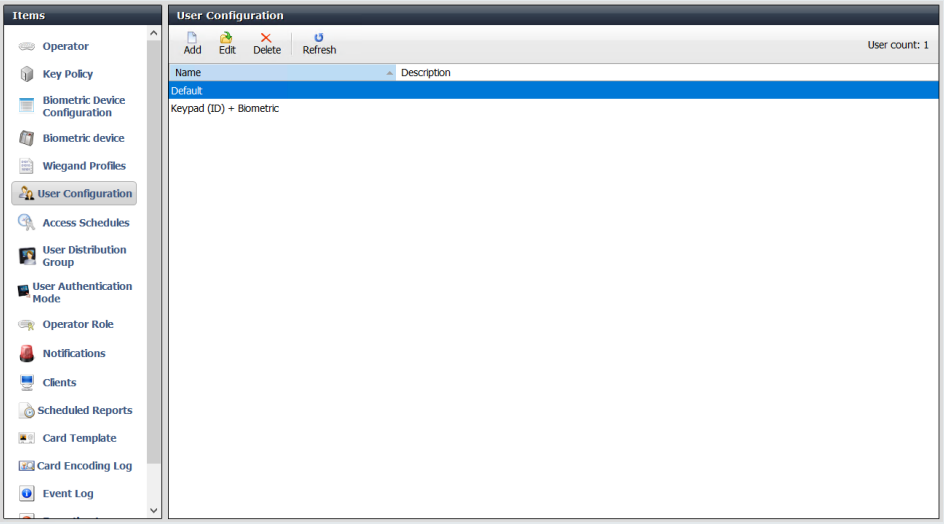
Vervolgens kan er geconfigureerd worden wanneer de lezer toegang geeft op basis van de LED sturing. Zonder deze instelling zal de lezer altijd toegang geven zodra de lezer de vinger herken, ook als de persoon niet in het toegangscontrolesysteem staat. Het is dus noodzakelijk dat dit wel geconfigureerd zal gaan worden. Hieronder de instellingen;

Access Control Mode – **Integrated by Wiegand / Panel Feedback**
LED Feedback Mode – **LED Feedback (1 Wire)**
Panel Feedback No Response Timeout – **3000ms**



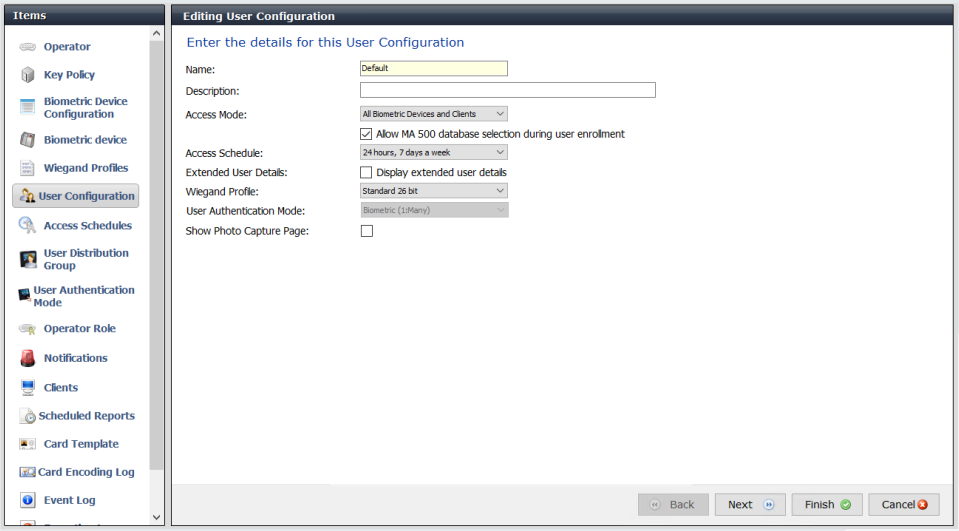
Zodra dit is ingesteld kan er op *Finish* geklikt worden, de overige instellingen zijn niet van toepassing voor de configuratie met Net2.

Nu de configuratie voor het apparaat is ingericht kan het profiel voor de gebruikers gemaakt worden op basis van enkel de vinger (Biometric ONLY). Ga hiervoor naar *Administration – User Configuration*. En klik op *Edit* om de Default configuratie aan te passen.



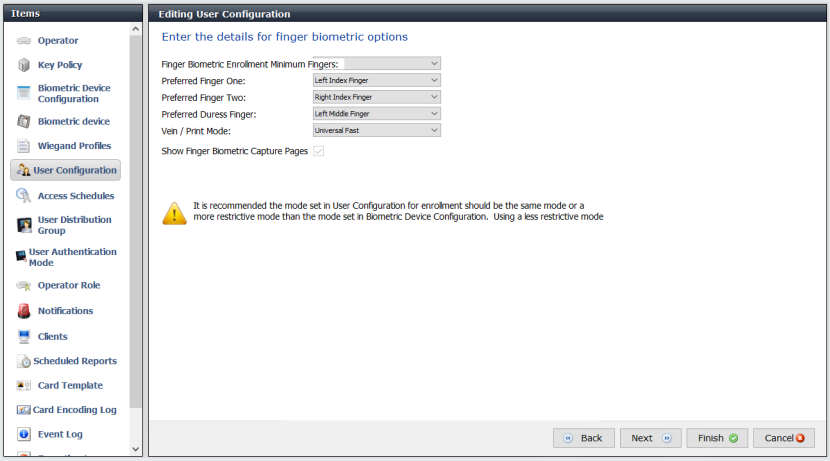
Op het eerste scherm hoeven we enkel het wiegand profiel aan te passen naar *Standard 26 bit* om een werking met Net2 te kunnen maken. Daarnaast vinken we de optie *Show Photo Capture Page* uit. Gezien Morpho een doorgeef systeem is naar Net2 hoeven hier geen foto's in geplaatst te worden.

Los vinden we op deze pagina ook de User Authentication Mode, gezien standaard de optie enkel vinger al werkt hoeven we dit ook niet aan te passen. Daarnaast is deze optie bij het bewerken van een template ook niet beschikbaar om aan te passen.



Vervolgens klikken we op *Next* om verder te gaan.

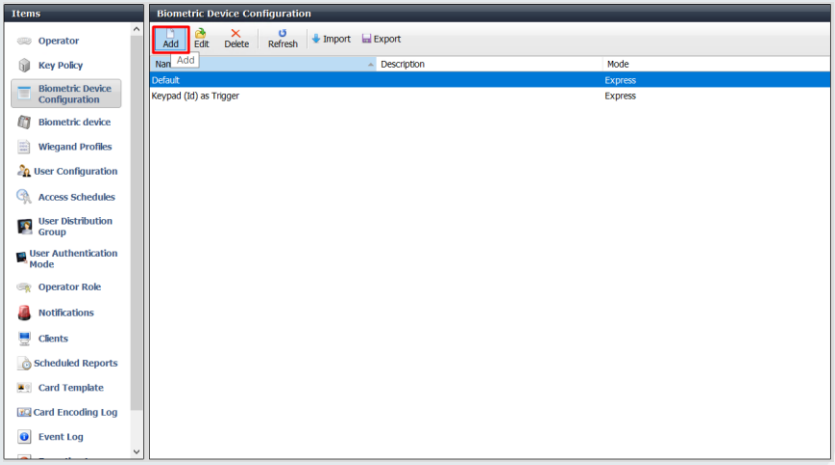
Op de volgende pagina kan er aangegeven worden hoeveel vingers er minimaal ingeleerd dienen te worden. We adviseren dit op standaard 2 te laten staan. Dit omdat het wel eens voorkomt dat een persoon zijn wijsvinger in het systeem heeft gezet en er vervolgens een pleister op heeft zitten doordat deze is opengehaald. Vandaar adviseren we dus ook om 2 vingers in te leren zodat een persoon altijd toegang kan krijgen. Alle vingers inleren is ook mogelijk.



Vervolgens drukken we op Finish. (de overige pagina's configureren andere type kaartlezers zoals de MorphoWave en de VisionPass.

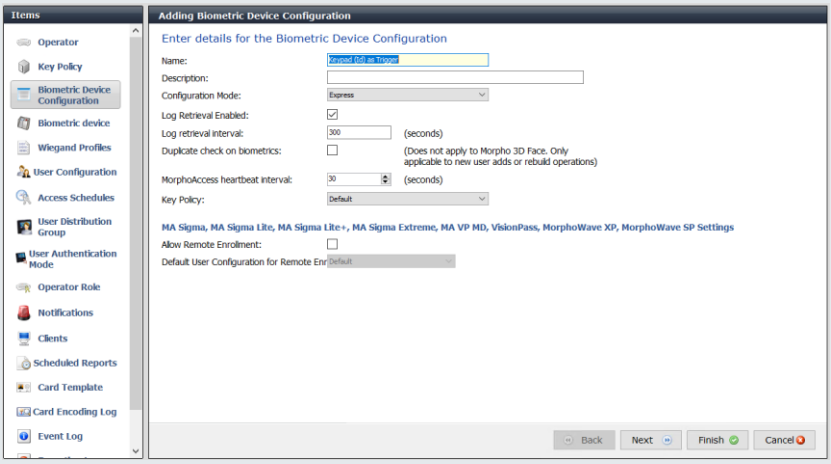
1.3.2.2. Vinger + PIN

Om dit juiste te configureren dienen er een aantal andere zaken geconfigureerd te worden dan bij alleen vinger. Hiervoor zal eerst een nieuwe configuratie voor de lezer gemaakt dienen te worden. Dit kan onder Configuration – Biometric Device Configuration. Klik hiervoor op Add om een nieuwe configuratie te maken.

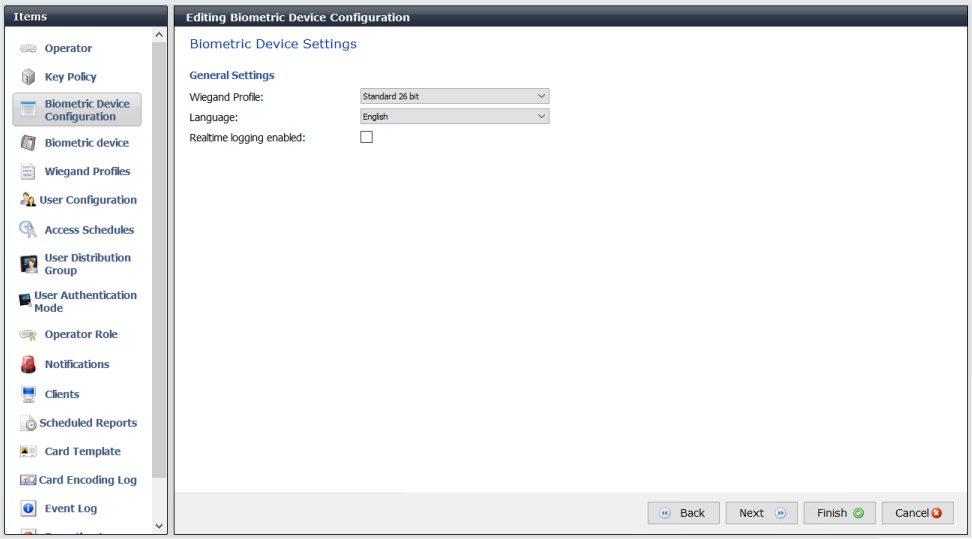


Het is wenselijk om de naam van de configuratie een juiste naam te geven. Als voorbeeld zal de template *Keypad (Id) as Trigger* heten. Het Id van gebruiker zal dan dienen als de pincode voor de kaart. Er zal dan eerst een pincode ingedrukt dienen te worden om vervolgens een vinger aan te kunnen bieden.

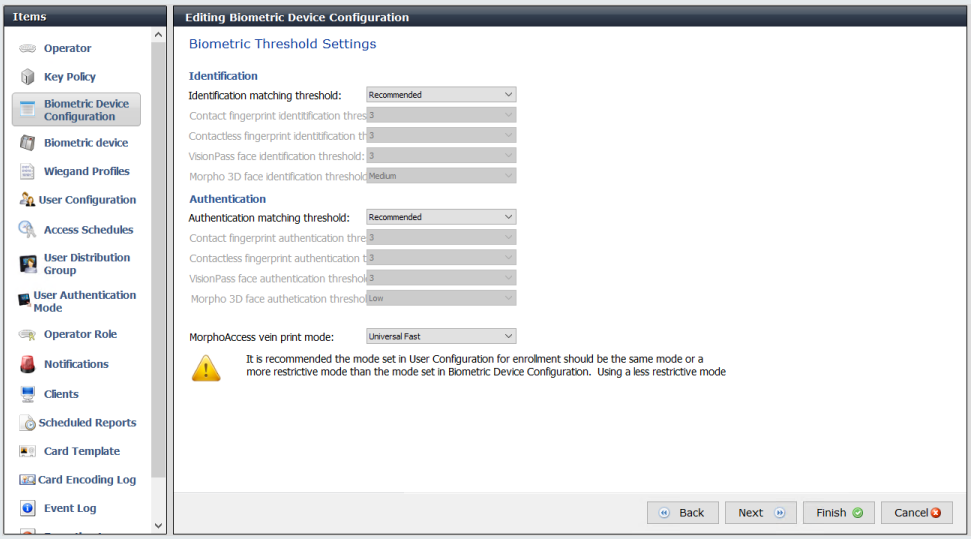
Naast de benaming is hier ook de Key Policy te vinden voor de TLS versleuteling. Deze kan op Default blijven staan als dit niet is aangepast. Vervolgens kan er op *Next* geklikt worden.



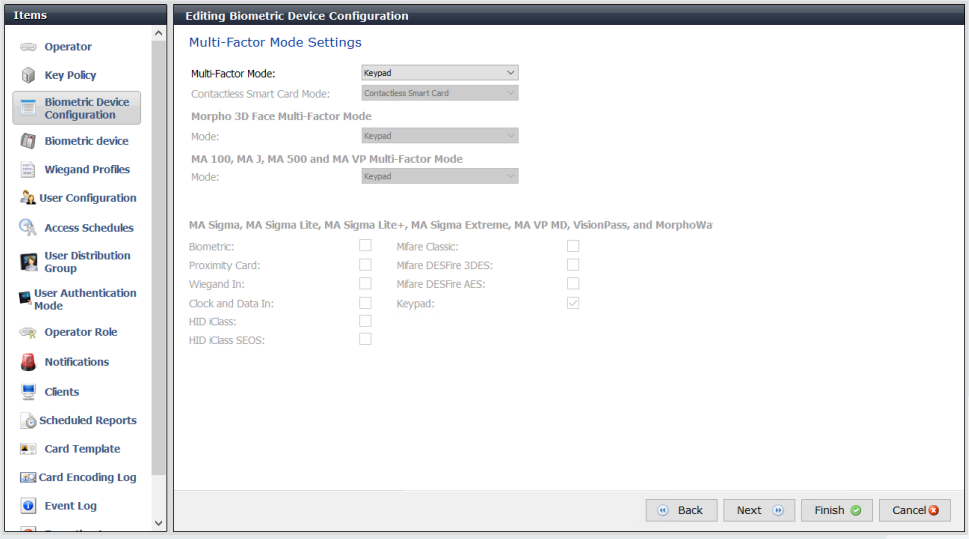
Op de volgende pagina is het kaartformaat te vinden, om het systeem te laten werken met Net2 dient het Wiegand profiel omgezet te worden naar *Standard 26 bit*. Zodra dit is gedaan kan er op *Next* geklikt worden.



Na het kaartformaat goed te hebben gezet volgt de pagina voor de gevoeligheid van de lezer. Wanneer de lezer zal worden gebruikt met vingers die slecht te lezen zijn kan dit hier veranderd worden. Standaard staan deze instellingen op Recommended. We adviseren het om deze instelling zo te laten staan en eerst te kijken wat de leesbaarheid van de vingers is alvorens deze instelling wordt aangepast. Klik hier ook weer op *Next* om verder te gaan.

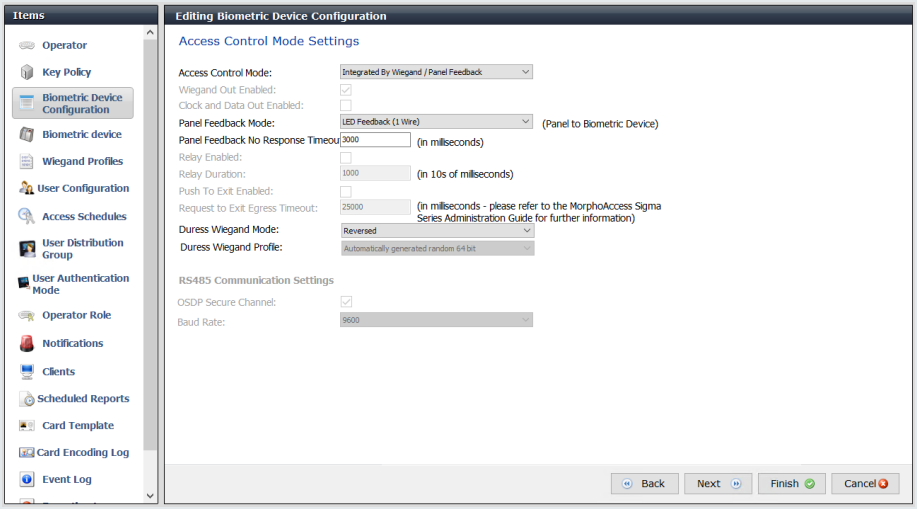


Hierna kan de modus ingesteld worden. Voor de configuratie Vinger + PIN is het voldoende om Keypad toe te passen als Multi-Factor Mode. Klik vervolgens op Next om verder te gaan.



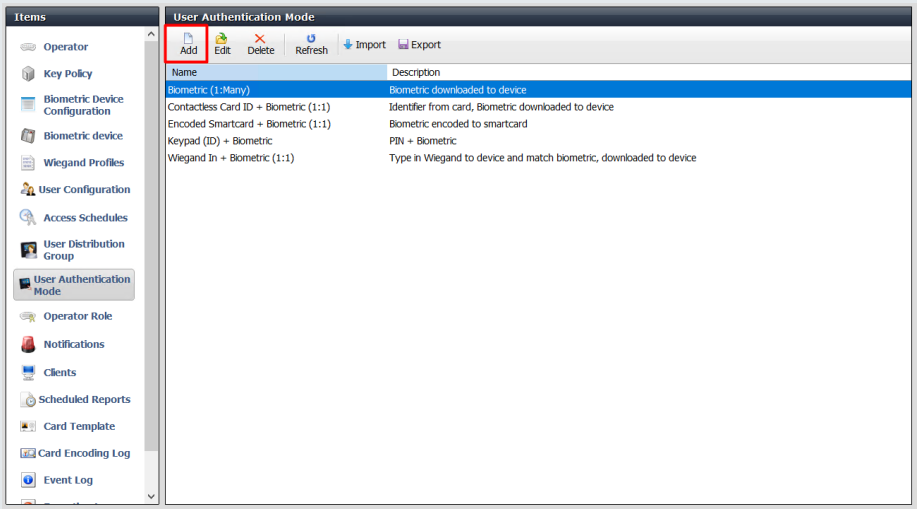
Vervolgens kan er geconfigureerd worden wanneer de lezer toegang geeft op basis van de LED sturing. Zonder deze instelling zal de lezer altijd toegang geven zodra de lezer de vinger herken, ook als de persoon niet in het toegangscontrolesysteem staat. Het is dus noodzakelijk dat dit wel geconfigureerd zal gaan worden. Hieronder de instellingen;

Access Control Mode – **Integrated by Wiegand / Panel Feedback**
LED Feedback Mode – **LED Feedback (1 Wire)**
Panel Feedback No Response Timeout – **3000ms**

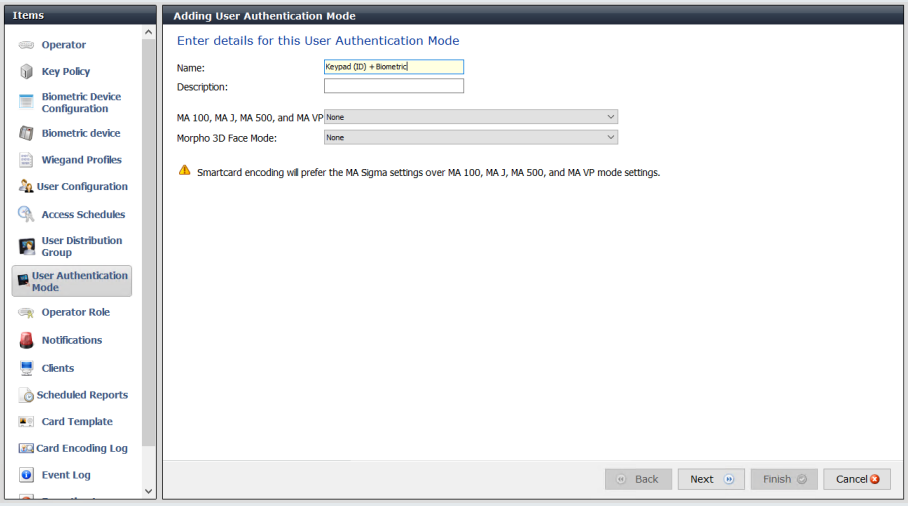


Zodra dit is ingesteld kan er op *Finish* geklikt worden, de overige instellingen zijn niet van toepassing voor de configuratie met Net2.

Nu de configuratie voor het apparaat is ingericht kan het profiel voor de gebruikers gemaakt worden op basis van Vinger + PIN. Eerst zal er een nieuwe authenticatie mode aangemaakt dienen te worden. Ga hiervoor naar Administration – User Authentication Mode en voeg een nieuwe mode toe.

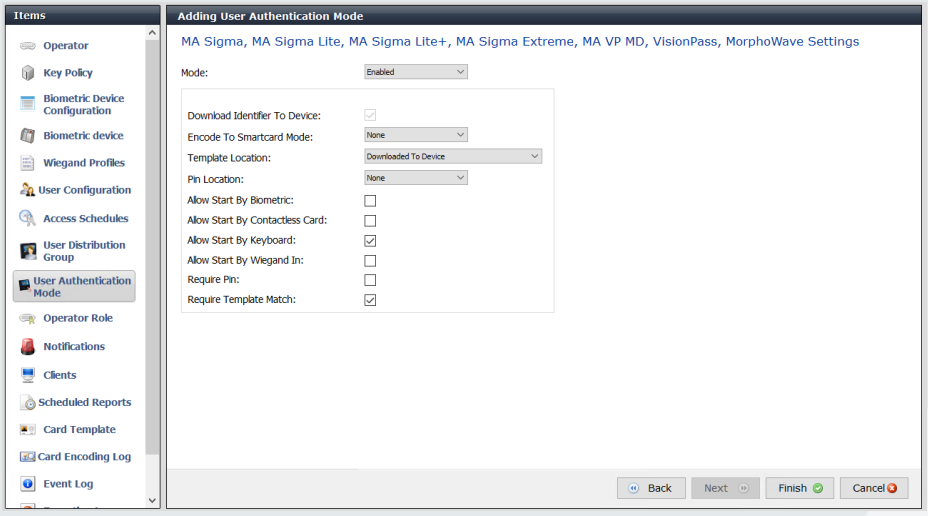


Geef ook hier weer de template een logische benaming, een voorbeeld hiervan is Keypad (ID) + Biometric. Klik vervolgens op *Next*.



Er verschijnt nu een scherm om de modus in te stellen. Neem hiervoor onderstaande instellingen over;

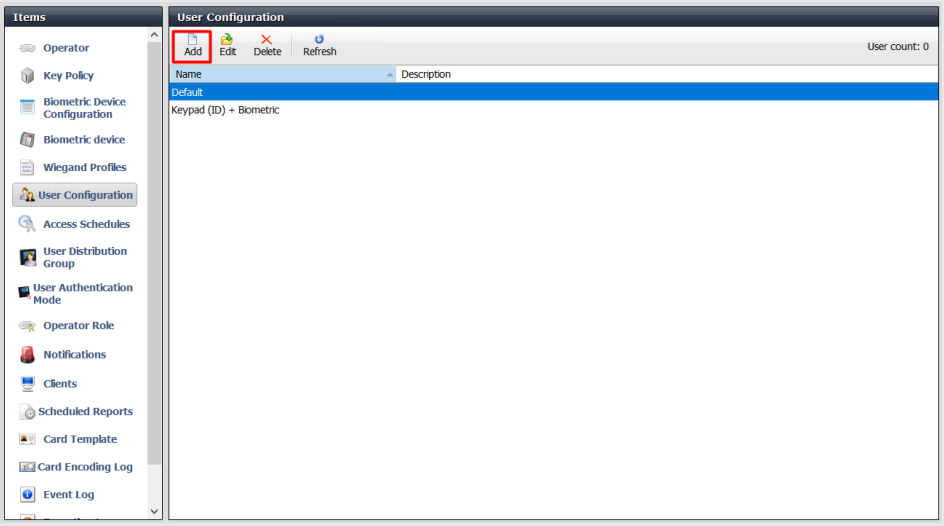
Mode: Enabled
Download Identifier To Device: Checked
Template Location: Download To Device
Allow Start by Keyboard: Checked
Require Template Match: Checked



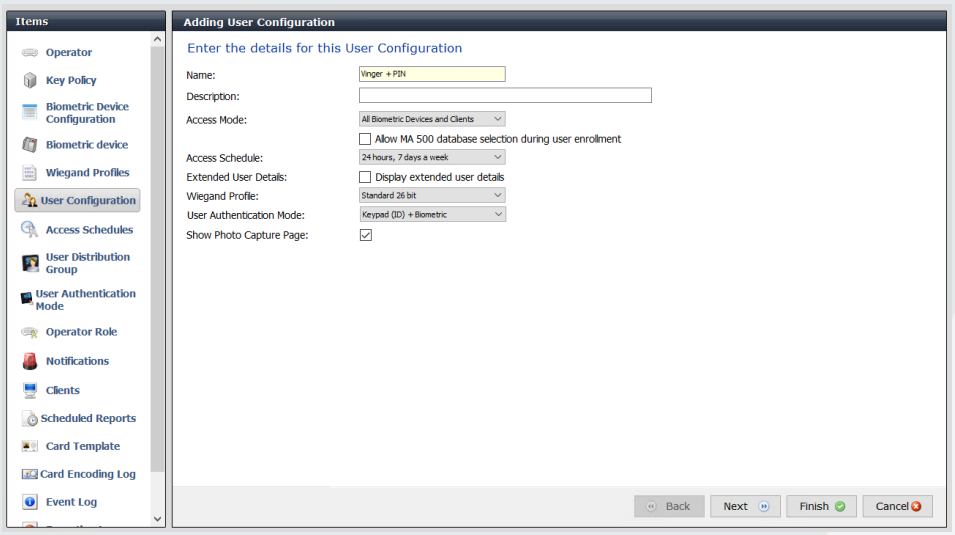
Druk Hierna op *Finish* om dit op te slaan.

Nu kan de User Configuratie aangemaakt worden om dit aan de personen te kunnen koppelen tijdens het aanmaken hiervan.

Ga hiervoor naar *Administration – User Configuration*.
En klik op *Add* om een nieuwe configuratie aan te maken.

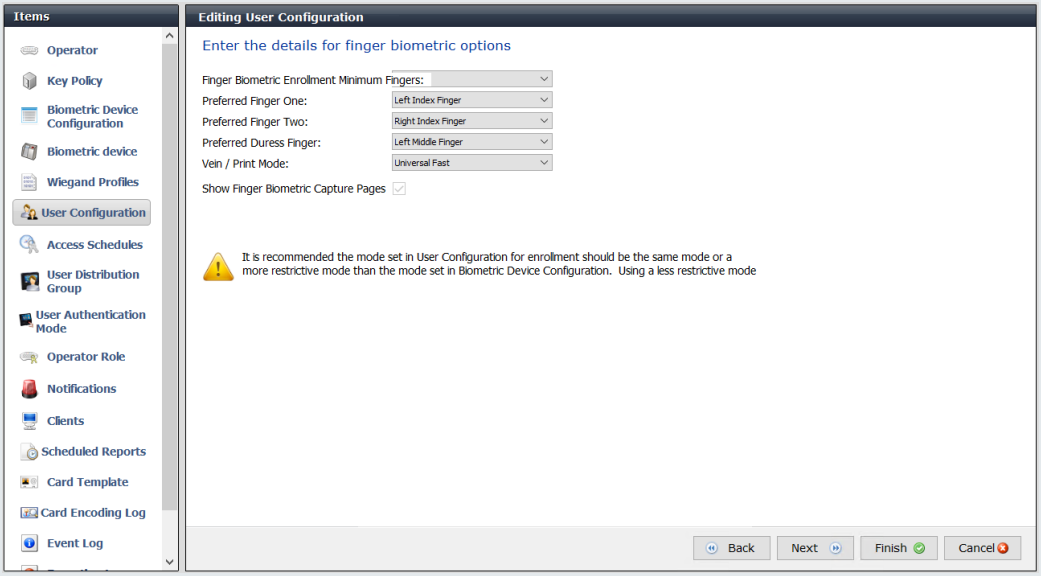


Geef op het eerste scherm een logische benaming zoals bijvoorbeeld ‘Vinger + PIN’. Verder passen we het wiegand profiel aan naar *Standard 26 bit* om een werking met Net2 te kunnen maken.
De User Authenticatie Mode is zojuist aangemaakt en kan worden geselecteerd.
Daarnaast vinken we de optie *Show Photo Capture Page* uit. Gezien Morpho een doorgeef systeem is naar Net2 hoeven hier geen foto’s in geplaatst te worden.



Vervolgens klikken we op *Next* om verder te gaan.

Op de volgende pagina kan er aangegeven worden hoeveel vingers er minimaal ingeleerd dienen te worden. We adviseren dit op standaard 2 te laten staan. Dit omdat het wel eens voorkomt dat een persoon zijn wijsvinger in het systeem heeft gezet en er vervolgens een pleister op heeft zitten doordat deze is opengehaald. Vandaar adviseren we dus ook om 2 vingers in te leren zodat een persoon altijd toegang kan krijgen. Alle vingers inleren is ook mogelijk.



Vervolgens drukken we op Finish. (de overige pagina's configureren andere type kaartlezers zoals de MorphoWave en de VisionPass.

1.4. Montage & Configuratie Net2

Morpho Manager is nu klaar voor gebruik, voordat er personen worden toegevoegd zal eerst Net2 ook ingericht dienen te worden. In deze handleiding zal de volledige configuratie van Net2 worden overgeslagen. Wel zal er uitgelegd worden hoe de lezer dient te worden aangesloten en dient te worden geconfigureerd.

1.4.1. Montage

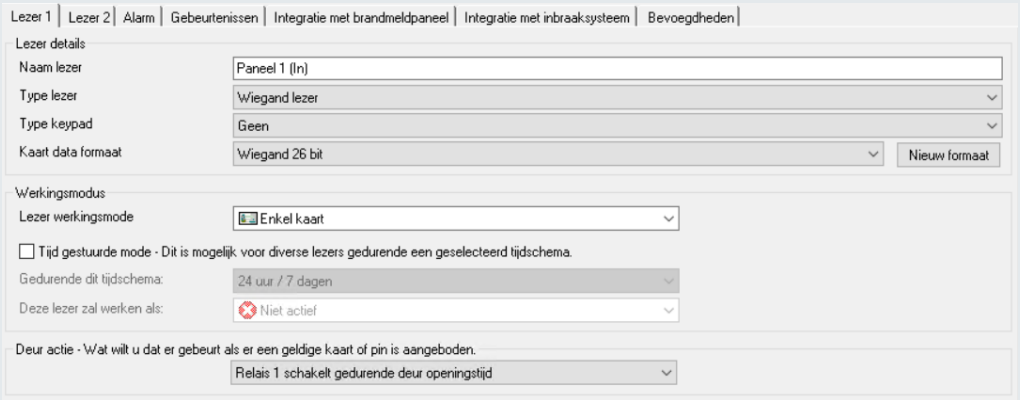
Gezien de lezers via het netwerk zijn aangesloten waarbij de spanning over PoE gaat hoeft de 12V niet te worden aangesloten.

Kaartlezer	**Net2 centrale**	
Power +12v (rood)	12V (rood)	niet aansluiten indien PoE actief
Power GND (zwart)	0V (zwart)	niet aansluiten indien PoE actief
Wiegand_OUT0 (groen)	D0 (geel)	
Wiegand_OUT1 (wit)	D1 (blauw)	
Wiegand_GND (zwart/rood)	0V (zwart)	
Wiegand_LEDOUT1 (blauw)	LED (groen)	

1.4.2. Configuratie

Wanneer Net2 volledig is geconfigureerd en er is bepaald welke ‘deuren’ een lezer van IDEMIA krijgen kan dit geconfigureerd worden. Ga hiervoor naar het desbetreffende paneel in Net2. Selecteer de gewenste Lezer en verander onderstaande instellingen;

Type lezer: Wiegand lezer
Type keypad: Geen
Kaart data formaat: Wiegand 26 bit
Lezer werkingsmode: Enkel kaart

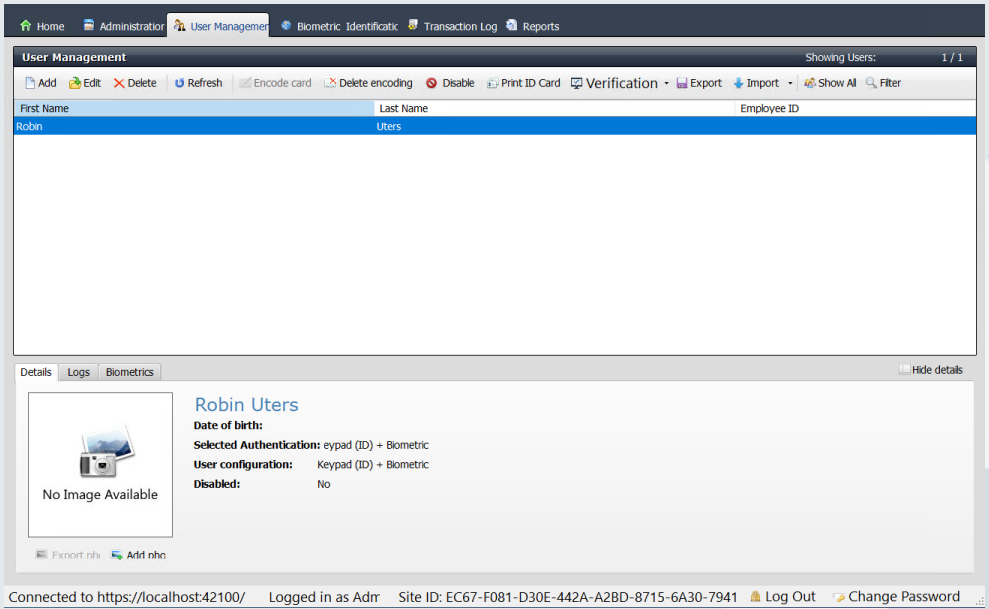


Druk vervolgens op Uitvoeren om de instellingen op te slaan.

1.5. Persoon toevoegen

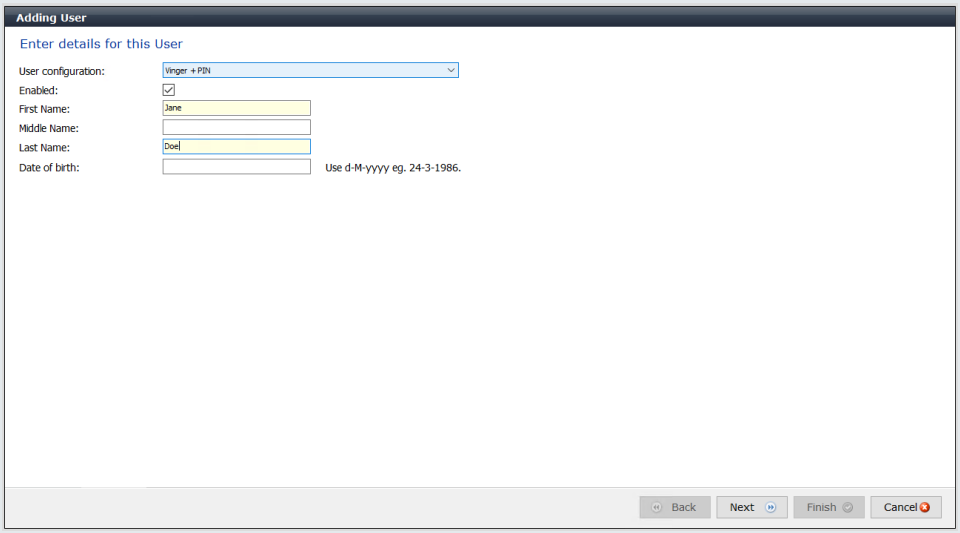
Om een persoon toe te voegen aan Morpho Manager en Net2 zullen er 2 handelingen gedaan dienen te worden. De persoon zal eerst toegevoegd dienen te worden in Morpho Manager en hierna in Net2.

Ga hiervoor naar Morpho Manager en klik op User Management

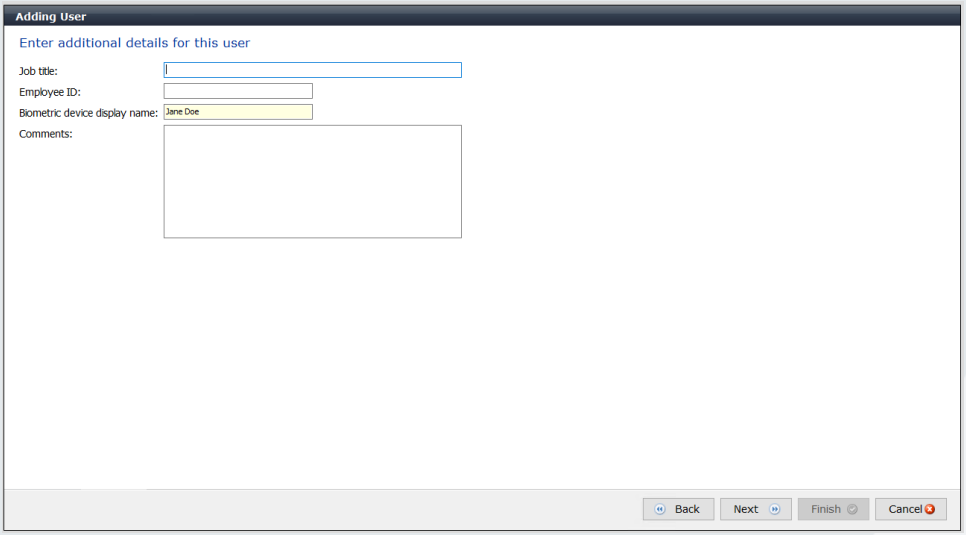


Klik vervolgens op *Add* om een nieuw persoon toe te voegen.

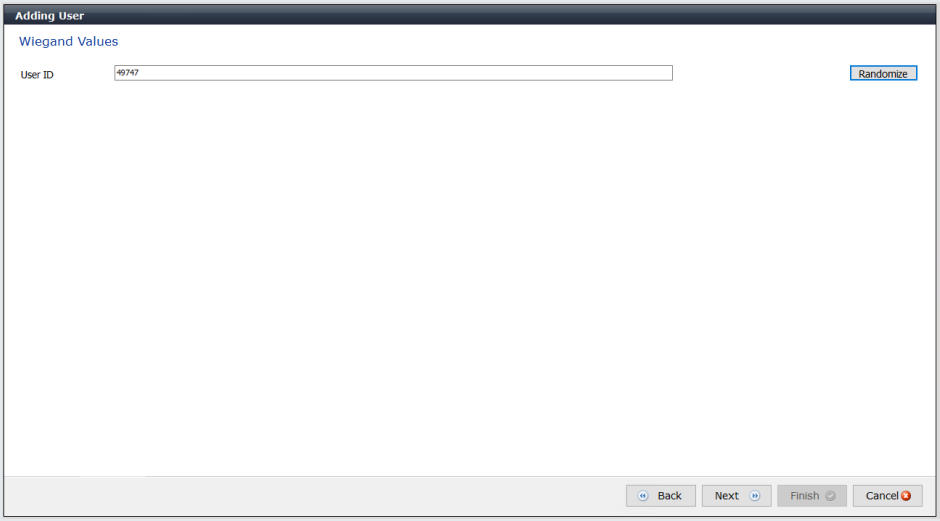
In deze handleiding zijn er 2 soorten templates aan bod gekomen, afhankelijk van welke er is gekozen is deze zichtbaar in het dropdown menu bij *User Configuration*. Selecteer hier de gewenste configuratie. Vul vervolgens de voornaam en achternaam in. (Dit kunnen ook de voorletter en achternaam zijn). En klik op *Next*.



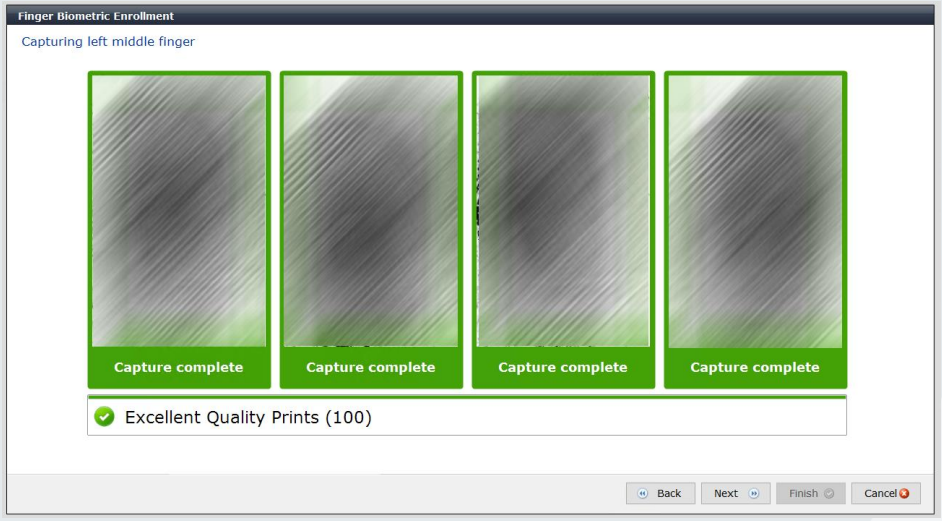
Op de volgende pagina kunnen eventueel extra details worden ingevuld, gezien Morpho Manager een doorgeef systeem is laten we dit leeg.



Hierna kan de pincode / User ID worden gegenereerd. Dit kan handmatig ingevuld worden met 5 cijfers of via de knop willekeurig worden aangemaakt. We adviseren om een willekeurige code te nemen. Dit gezien het een pincode / toegangscode is voor het gebruik van de lezer. Klik vervolgens op *Next* om door te gaan. Onthoudt deze code goed. Dit is de pincode voor de gebruiker en tegelijkertijd dient deze code ook in Net2 te worden opgeslagen als kaarthouder.

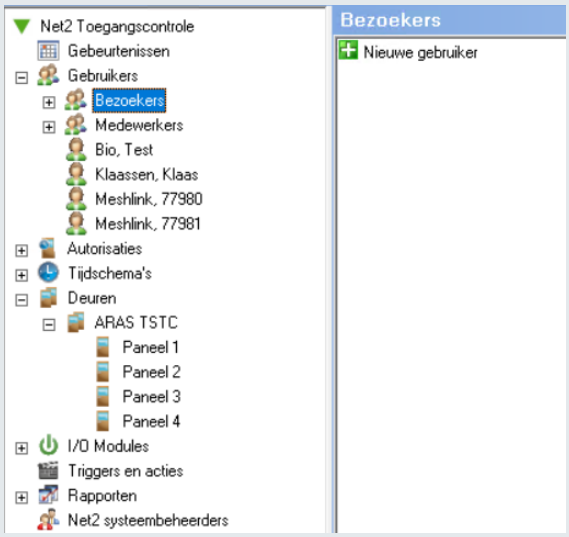


Nu kunnen de vingers worden ingeleerd. Afhankelijk van de situatie kunnen de lezers zelf dienen als inleer optie maar er zijn ook USB apparaten hiervoor beschikbaar. Klik eerst op een vinger welke dient te worden ingeleerd. Dit hoeven niet perse de 3 vingers te zijn welke knipperen in het scherm. Wel is het verstandig om 2 van de 3 vingers te doen.

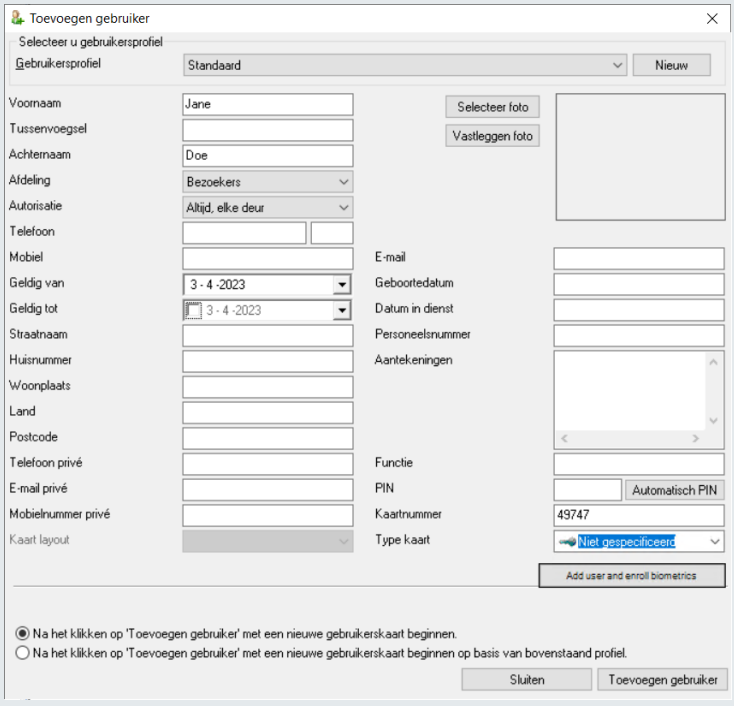


Deze procedure volgt 2 maal. Eventueel kan onderin het scherm vinger 1 en vinger 2 aangepast worden. Zodra dit is gedaan kan er op *Finish* gedrukt worden. Nu de persoon is toegevoegd kan deze ook in Net2 worden toegevoegd aan het systeem.

Ga hiervoor naar Net2 en dan naar Gebruikers om een gebruiker toe te voegen.



Klik op + Nieuwe gebruiker en voer hier de gegevens in van de gebruiker, geef deze persoon hier ook de juiste autorisatie. Het kaartnummer is het nummer welke zojuist is Morpho Manager is ingevuld en het type kaart is Niet gespecificeerd.



Zodra deze gebruiker is toegevoegd kan deze stap herhaald worden voor alle andere personen en kan het systeem gebruikt gaan worden.