Stage ICT-infrastructure Soudal

Beschrijving van de realisatie

Bachelor in de Elektronica-ICT

Dries Janssen

Academiejaar 2021-2022

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

INHOUDSTAFEL

BEGRIPPENLIJST

In dit verslag komen een aantal technische begrippen en afkortingen aan bod. Om de context van dit document beter te begrijpen, is het aangeraden de begrippenlijst te doornemen. Hieronder staan de begrippen en afkortingen met hun betekenis:

Azure Active Directory (AAD):	cloud-based identity and access management service
Co-managed devices:	Co-management zorgt ervoor dat je Windows 10 devices kan managen door zowel gebruik te maken van Configuration Manager als Microsoft Intune
Hybrid exchange omgeving:	Opstelling die je toelaat om je lokale omgeving en de cloud omgeving samen te nemen als één enkele mail organisatie.
Conditional access:	Device of gebruiker moet aan bepaalde criteria voldoen om toegang te krijgen tot bedrijfsdata
Compliance policies:	Device of gebruiker moet aan bepaalde voorwaardes voldoen om compliant state te krijgen, anders krijgen ze non-compliant state.
Compliant:	Wanneer een user/device voldoet aan de compliance policies wordt de state hiervan "compliant"
Organizational Unit (OU):	Dit is een container binnen de Active Directory omgeving waar je op een georganiseerde manier users, groups en computers kan insteken en policies op kan zetten
Microsoft Intune:	Cloud-based service die de focus legt op mobile device management en mobile application management
System Center Configuration Manager (SCCM)	Klassieke on-premises oplossing voor het managen van computer systems.
Configuration profiles	Staan je toe om device restricties te maken en wijzigen.

INLEIDING

In dit verslag kan u de beschrijving van de realisatie terugvinden die verwezenlijkt is tijdens mijn stage bij Soudal. Deze stage is een verplicht opleidingsonderdeel binnen de professionele bacheloropleiding Elektronica-ICT. Deze dient succesvol afgerond te worden om te kunnen afstuderen.

Het onderwerp van de stage was initieel 'ICT Service Desk Medewerker', maar na een eerste sollicitatiegesprek bleek dit niet meer accuraat te zijn. Door veranderde bedrijfsprioriteiten is het onderwerp van de stage uitgebreid richting Service Desk Medewerker + Endpoint management.

Wegens de grootschaligheid van de IT-omgeving van Soudal (aantal computers, servers, eindgebruikers …), werkten wij met 2 studenten aan dezelfde stageopdracht. Dit is zowel individueel opdrachten uitvoeren als gecoördineerd in teamverband bepaalde zaken behandelen en uitrollen.

Bij de gemeenschappelijke onderwerpen waaraan we samenwerkten, hebben we onderling afgesproken het werk telkens gelijk te verdelen, waarbij we het aantal toestellen/gebruikers waarop iets moest gebeuren altijd ongeveer in de helft hebben opgesplitst.

Het gehele doel van deze stage is om eindgebruikers bij te staan, het beheren van data te centraliseren en te beveiligen en tot slot, de huidige infrastructuur up-to-date te houden.

De stageopdracht is een continu proces dat zich blijft verderzetten, ook na onze stage. In dit document kan u mijn bijdrage aan dit continue proces terugvinden.

1 OFF-BOARDING

Dit is een procedure binnen de IT-afdeling van bedrijven dat wordt uitgevoerd wanneer een medewerker, voor wat voor reden dan ook, beslist om het bedrijf te verlaten. (ontslag, pensioen, nieuwe job …)

Het doel van de off-boarding procedure is om toegang tot het bedrijfsnetwerk te ontzeggen en een back-up te maken van documenten, mailbox-inhoud en overige data. Door dit te doen, zorg je ervoor dat deze data niet zomaar verloren gaat en voorkom je dat de ex-medewerker nog toegang heeft tot het netwerk van Soudal.

Ik kreeg de opdracht om de off-boarding procedure uit te voeren op ex-medewerkers die het bedrijf onlangs hebben verlaten.

Dit behoorde niet tot het vaste takenpakket, maar werd aanzien als een zijdelingse opdracht. Desalniettemin een belangrijke taak die vooral bij aanvang van de stage werd uitgevoerd.

1.1 Off-boarding procedure

Het off-boarden van ex-medewerkers werd verwezenlijkt aan de hand van de bestaande off-boarding procedure die volgens de bedrijfsregels van Soudal is opgesteld.

Deze procedure kan je onderverdelen in 3 stappen. Het aanpassen van de instellingen op de mailbox. Zorgen voor de back-up van de nodige data die bijgehouden dient te worden en tot slot de nodige wijzigen aanbrengen in Active Directory.

a. Mailbox:

Voor het wijzigen van instellingen en attributen van de mailbox, maak ik gebruik van de **Microsoft Exchange Online Powershell Module**. Dit is een efficiënte manier van werken aangezien je met enkele lijnen code je hele mailbox kan configureren.

Bij het off-boarden van ex-medewerkers kan het zijn dat mails die nog steeds verstuurd worden naar de mailbox van deze persoon, doorgestuurd dienen te worden naar de vervanger of manager van de ex-medewerker.

Daarom is het belangrijk dat de instellingen van de mailbox aangepast dienen te worden. Eens het type aangepast is naar shared, kan je iemand anders koppelen aan de mailbox, zodat die de inkomende mails ook binnenkrijgt.

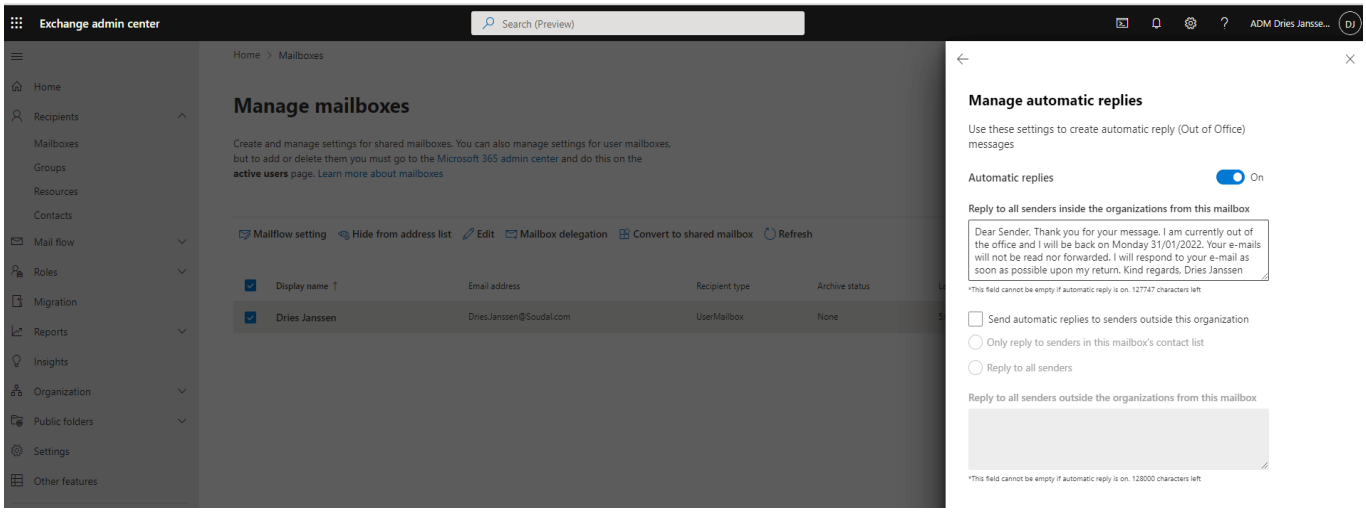
Onderstaande code toont dit principe aan:

```
JanssenD>Connect-EXOPSSession
JanssenD>Set-Mailbox dries.janssen@soudal.com -Type shared
JanssenD>Add-MailboxPermission dries.janssen@soudal.com -User "Vince Druyts"
-AccessRights Fullaccess
```

Wanneer er niemand gekoppeld dient te worden aan de mailbox van een ex-medewerker, kan je een automatische reply instellen.

De onderstaande afbeelding toont hoe je een automatische reply (= Out of Office) kan instellen voor een ex-werknemer. Wanneer je deze persoon dan bijvoorbeeld een e-mail zou sturen, krijg je deze automatische reply te zien. Op deze manier weet iedereen dat deze persoon niet langer bij Soudal werkt.

Dit kan je via Exchange admin center instellen via Others > Automatic replies.



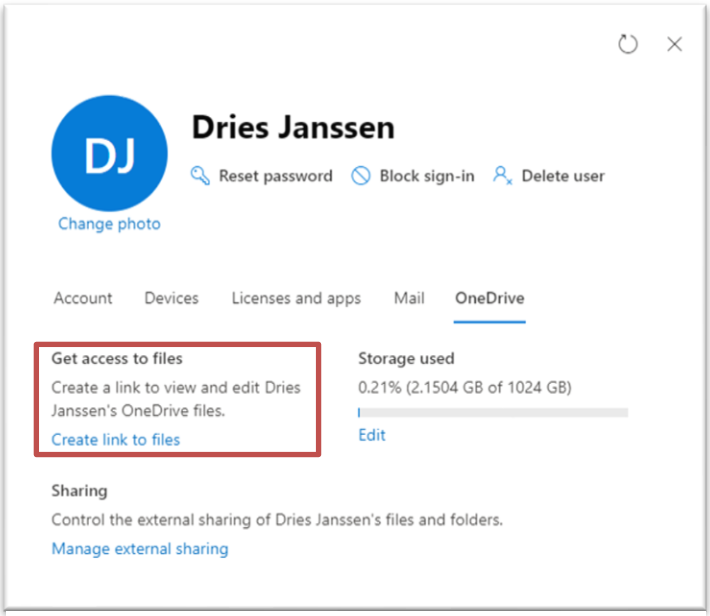
Afbeelding 1: configuratiescherm automatische replies.

b. Back-up:

In deze stap ga je een back-up maken van de OneDrive data. Deze dient vervolgens gekopieerd te worden naar de Soudal off-boarding Sharepoint site. Ook wordt er een back-up gemaakt van de Exchange mailbox omgeving.

Via Microsoft 365 admin center kan je met de zoekbalk naar de ex-werknemer zoeken. Eens je deze gevonden hebt, kan je in de OneDrive tab kiezen voor de optie 'Get access to files'. Deze optie genereert een link die verwijst naar de OneDrive data van deze persoon.

Van deze data wordt vervolgens een kopie gemaakt die je gaat exporteren naar de off-boarding site. Hier moet je enkel nog een folder creëren met de gegevens van de persoon die je aan het off-boarden bent.



Afbeelding 2: configuratiescherm voor back-up te maken van OneDrive data.

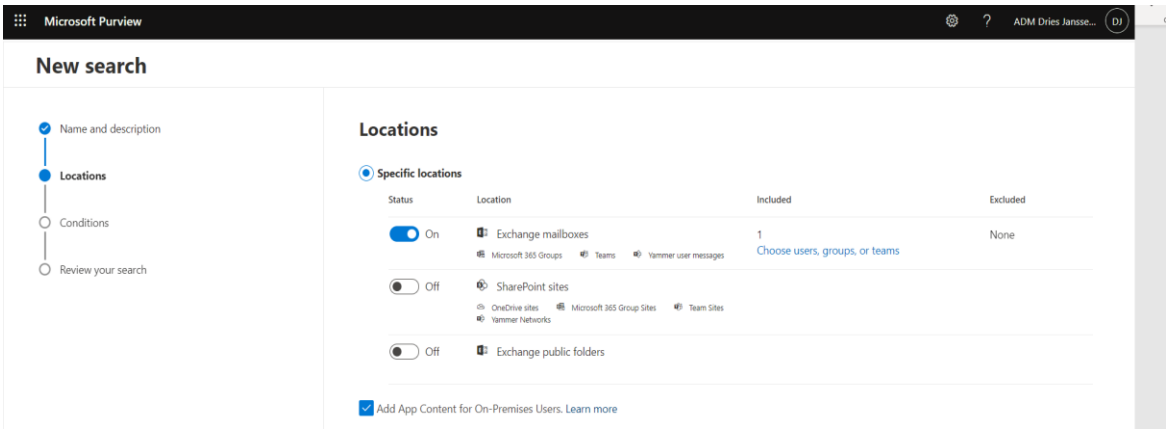
Nadat bovenstaande succesvol is uitgevoerd, kan je overgaan naar het maken van een back-up van de Exchange mailbox omgeving. In deze stap genereer je een PST-file, dit bevat items zoals events, contacten en e-mailberichten.

Via Microsoft Purview kan je een content search uitvoeren, hier zoek je de naam van de ex-werknemer voor wie het off-boarding proces dient uitgevoerd te worden.

Ook hier gaat een folder aangemaakt worden, de naamgeving hiervoor is:

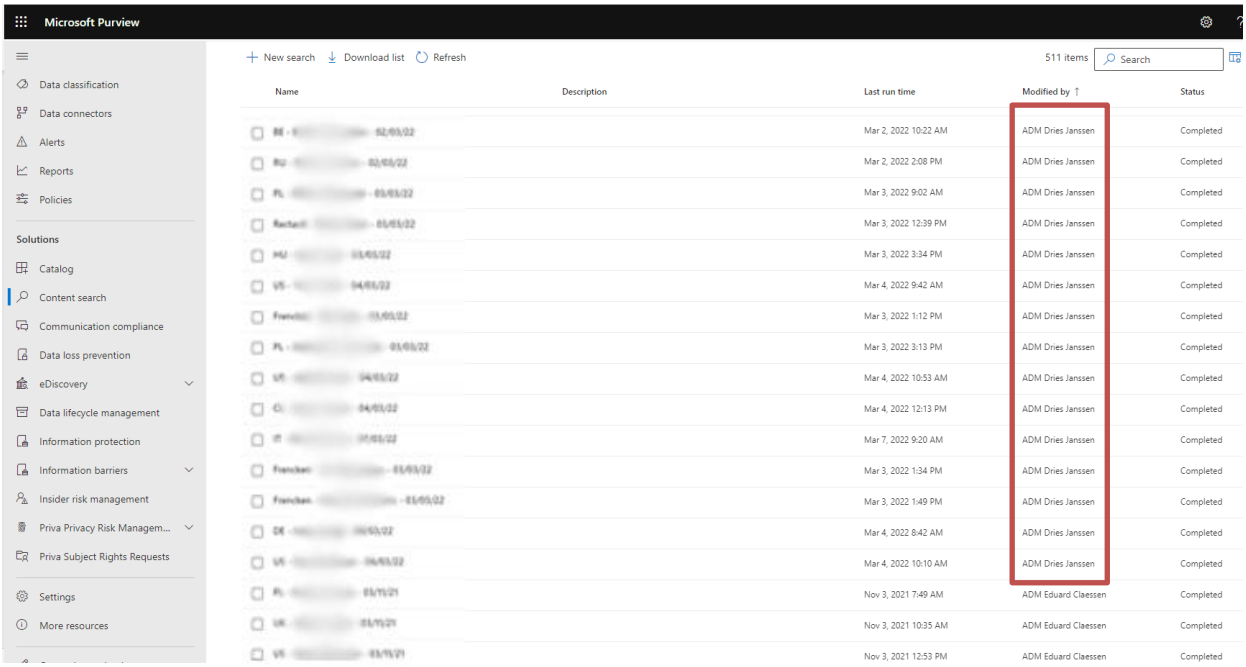
“LANDCODE – NAAM – DATUM”.

Op onderstaande afbeelding zie je het configuratiescherm waar je de scope van de back-up specifieert. In dit geval de Exchange mailbox van de ex-medewerker. Deze ex-medewerker duid je bijkomend aan in de include sectie.



Afbeelding 3: configuratiescherm voor het genereren van mailbox PST-file.

Na het doorlopen van de wizard gaat de PST-file aangemaakt worden in de folder met de naamgeving gespecifieerd in de eerste stap van de wizard. Daarna exporteer je deze PST-file ook naar de Soudal off-boarding Sharepoint site. Dit kan door het selectievakje aan te vinken en de optie “exporteren naar” aan te duiden.



Afbeelding 4: Overzicht van ex-medewerkers die off-boarding proces doorlopen hebben.

c. Active Directory:

Onderstaande stappen dienen tot slot nog uitgevoerd te worden om de off-boarding af te ronden. Deze gebeuren op de Domain Controller (DC).

Je gaat ervoor zorgen dat de ex-medewerkers geen toegang meer krijgen tot het Soudal netwerk. Voor beveiligingsredenen worden de login gegevens van deze ex-medewerkers dus gedeactiveerd. Dit kan je doen door de Dial-in opties te wijzigen naar "Deny access". Department gerelateerde groepen en groepen waar licenties zoals die van Office365 aan gekoppeld zijn, worden afgenomen. Enkel de 'domain user' groep mag behouden worden. Dit is een Globale groep die standaard alle users binnen het domain bevat.

Het attribuut msExchRecipientTypeDetails dient ook gewijzigd te worden naar code "34359738368". Hiermee maak je in AD duidelijk dat het wel degelijk een shared mailbox is. Dit is nodig omdat Soudal werkt met een Hybrid Exchange omgeving. Het commando dat in stap **a** werd uitgevoerd om een mailbox shared te maken gebeurde in Exchange Online (EXO) om problemen te voorkomen moet je dus ook Exchange On-Premise duidelijk maken dat dit een shared mailbox is. Hierdoor passen we dit attribuut aan.

Voor een duidelijk overzicht te behouden binnen de AD-omgeving, worden ook de nodige velden aangepast en verwijderd. Zo schrijf je telkens een descriptie bij het user-profile van de persoon die in het off-boarding proces zit. Deze descriptie vermeldt door wie het account gedeactiveerd is (initialen) en op welke datum dit gebeurd is. Overige gegevens zoals telefoonnummer, manager, job titel … worden verwijderd.

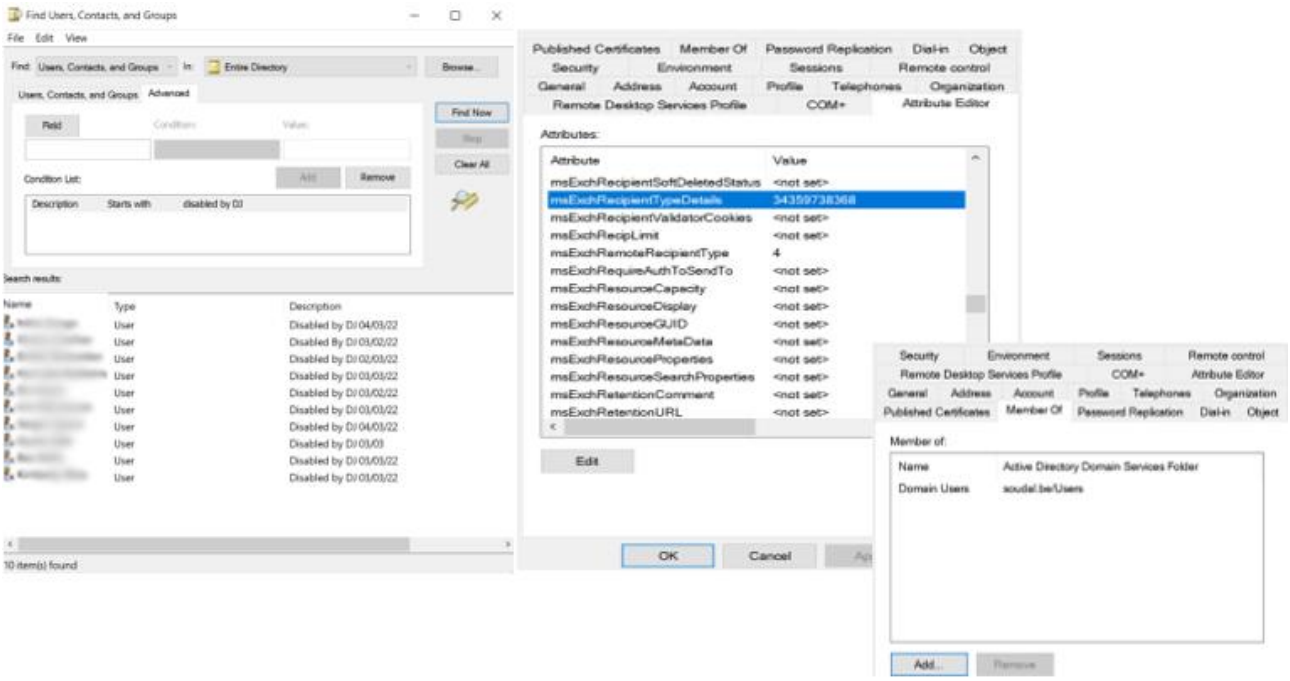
Tot slot verplaats je de gebruiker naar een off-boarding Organizational Unit (OU) binnen zijn desbetreffende organisatie. Gebruikers van Spanje komen dus bijvoorbeeld niet in dezelfde off-boarding OU terecht als die van België. Dit is voor de organisatiestructuur duidelijk te houden en heeft verder geen betekenis.

Nog belangrijk om te vermelden, de stappen **a** en **b** dienen eerst uitgevoerd te worden alvorens de licenties, die gekoppeld zijn aan de AD-groepen, worden afgenomen. Anders kan je bijvoorbeeld geen back-up meer maken van de OneDrive data als je de Office365 licenties al hebt afgenomen.

Deze taak werd voornamelijk bij aanvang van de stage uitgevoerd. De reden hierachter is omdat er dringend licenties vrijgemaakt diende te worden. Deze licenties waren nog gebonden aan ex-medewerkers die hier niets mee zijn.

Door het off-boarding proces te doorlopen, komen er terug licenties vrij, deze kunnen op hun beurt toegekend worden aan andere werknemers.

Onderstaande afbeelding toont enkele configuratieschermen binnen de AD-omgeving die het eindresultaat aantonen.



Afbeelding 5: eindresultaat off-boarding procedure in Active Directory

1.2 Off-boarding site opschonen

Soudal heeft een bepaald aantal Sharepoint sites waar zij hun off-boarding data op bijhouden. Dit gaat, zoals vorig hoofdstuk uitgelegd, meestal over OneDrive-bestanden en mailboxinhoud van de ex-werknemers.

Deze data wordt gemiddeld tussen de 1-3 jaar bijgehouden. Het geheugen op deze sites is niet oneindig, dus dienen deze sites regelmatig 'opgekuist' te worden.

Offboarding site 1, was op het moment van onze stage al geruime tijd volledig in gebruik betreffende de opslagcapaciteit. Off-boarding site 1 heeft betrekking tot data van ex-medewerkers die tussen 2018 en 2021 het bedrijf verlaten hebben.

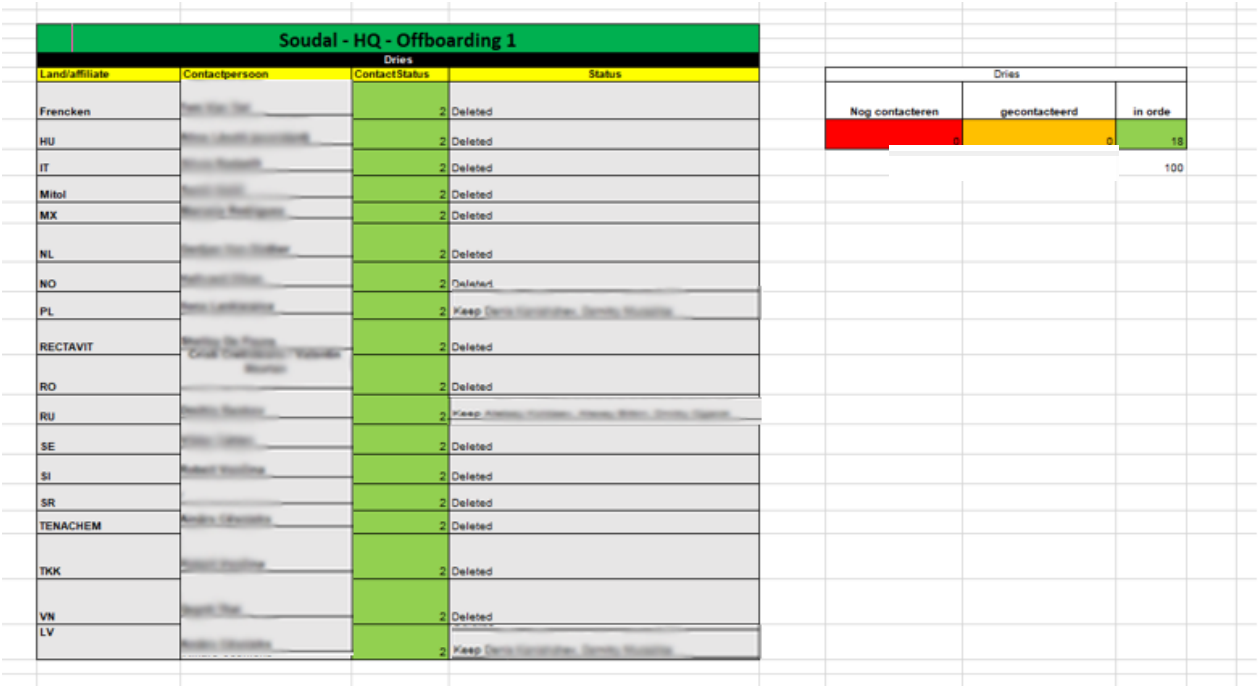
Aangezien off-boarding site 1 betrekking had tot ongeveer 35 landen/affiliaties, heb ik er 18 voor mijn rekening genomen.

Het is niet aan mij om te beslissen welke data bijgehouden dient te worden, daarom heb ik altijd eerst de contactpersoon gecontacteerd. Dit kan bijvoorbeeld de manager geweest zijn of de verantwoordelijke van de ex-werknemer.

Voor de landen/affiliaties waar ik verantwoordelijk voor was, heb ik een Excel-bestand gemaakt ter opvolging van deze 'opkuis'. Dit bevatte de contactpersoon, contact status en de status over wat er mocht gebeuren met deze data. Onderstaande afbeelding toont hoe ik dit heb aangepakt en opgevolgd.

Elk contactpersoon is ofwel via mail of Teams gecontacteerd geweest. In dit bericht werd er vermeld van welke persoon of personen er nog data werd bijgehouden en of deze nog bijgehouden moest worden.

Indien dit niet het geval was, mocht de folder met naam van deze persoon verwijderd worden van Offboarding site 1.



Soudal - HQ - Offboarding 1			
	Dries		
Land/affiliate	Contactpersoon	ContactStatus	Status
Frencken		2	Deleted
HU		2	Deleted
IT		2	Deleted
Mitol		2	Deleted
MX		2	Deleted
NL		2	Deleted
NO		2	Deleted
PL		2	Keep
RECTAVIT		2	Deleted
RO		2	Deleted
RU		2	Keep
SE		2	Deleted
SI		2	Deleted
SR		2	Deleted
TENACHEM		2	Deleted
TKK		2	Deleted
VN		2	Deleted
LV		2	Keep

Dries		
Nog contacteren	gecontacteerd	in orde
0	0	18
		100

Afbeelding 6: Excel-file met opvolging van landen/affiliaties Offboarding site 1.

2 SYMANTEC MIGRATIE

In dit deel wordt er meer uitleg gegeven over het migratieproces van Symantec antivirus naar Windows Defender. Deze migratie is essentieel aangezien de huidige Symantec licenties verlopen tegen eind juni en niet verlengt zullen worden.

Hierdoor dient er een vervanging geïmplementeerd te worden voor Symantec, zodat devices niet zonder virusscanner komen te zitten. Deze keuze was vooraf reeds bepaald, namelijk Windows Defender in combinatie met Defender for Endpoint (D4E).

2.1 Verwijderen Symantec

De scope van deze migratie beperkt zich tot alle co-managed client devices. Dit staat gelijk aan ongeveer 360 devices waarop Symantec verwijderd moet worden.

Voor deze migratie succesvol te doen verlopen, dienen er bepaalde stappen uitgevoerd te worden. Dit proces verloopt in een 4-tal stappen. Elke stap wordt uitgevoerd op een bepaalde server.

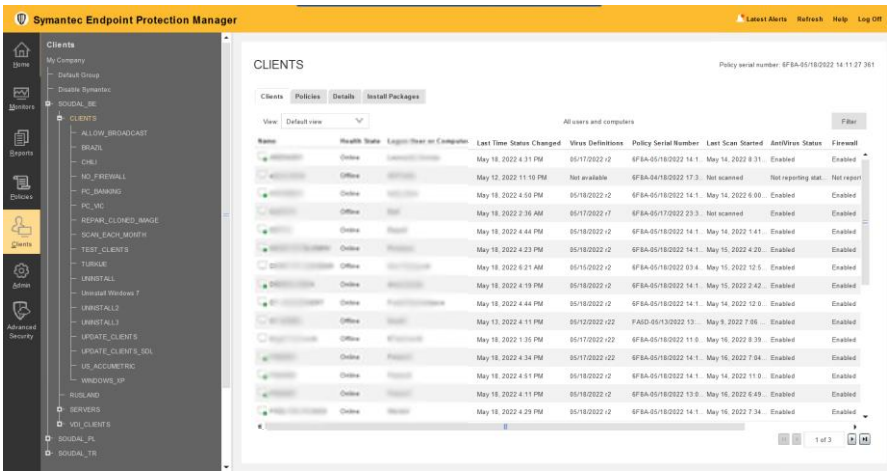
Zo komen onder meer de Symantec-server, de Domain Controller (DC) als de SCCM-server aanbod. Tot slot zal er ook nog een deel via Intune verlopen, dit gaat voornamelijk over het toekennen van groepen en het nut hiervan.

Het is niet de bedoeling dat Symantec handmatig device per device gaat worden verwijderd, maar deze migratie gaat aan de hand van scripts in bulk uitgevoerd worden. We spreken hier over 36 devices per keer. Mocht er ergens iets verkeerd lopen in dit proces, dan blijft de schade beperkt.

2.1.1 Symantec Endpoint Protection Manager

De Symantec-server is de server waarop Symantec Endpoint Protection Manager (EPM) geïnstalleerd staat. Hierop dienen nog enkele instellingen gewijzigd te worden alvorens het verwijder-proces kan worden gestart.

Onderstaande foto toont het clients overzicht van Symantec-EPM. Hierin staan alle clients en servers waarop Symantec geïnstalleerd staat. Ook diegene dat buiten de scope van de migratie vallen.

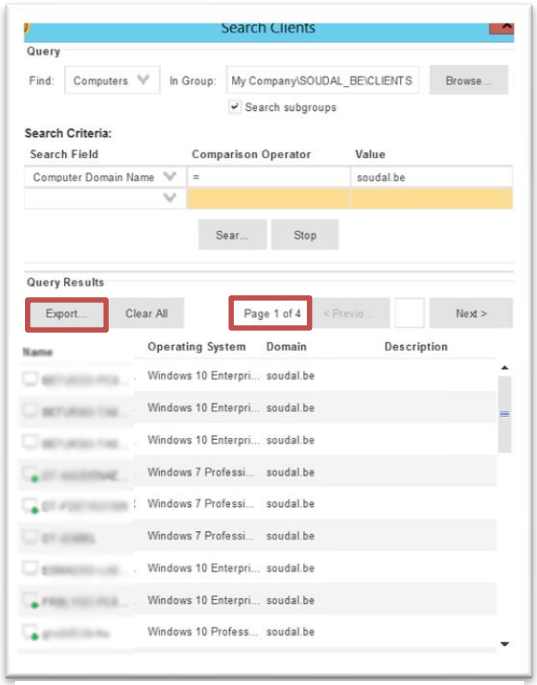


Afbeelding 7: overzicht Symantec Endpoint Protection Manager

Zoals eerder aangekaart was de scope van de migratie beperkt tot de "Co-managed" client devices. Hierdoor is het noodzakelijk om een zoekfilter toe te passen op computer domain name, met de waarde "soudal.be" om deze devices te verkrijgen.

De devices die ik terugkreeg met deze query heb ik vervolgens naar de 'uninstall' folder verplaatst.

Bijkomend werden ook nog alle query results geëxporteerd naar een Excel-bestand. Deze Excel-file, die alle device names bevat, wordt op de SCCM en DC server gebruikt om bijkomende scripts op uit te voeren. Dit wordt aangehaald in de verdere stappen.



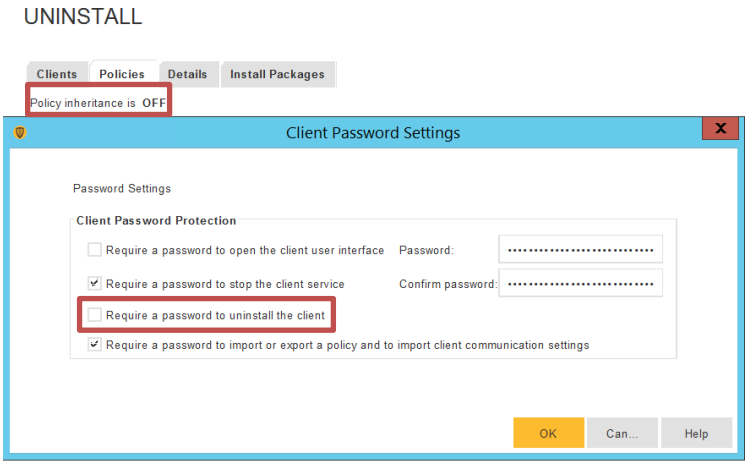
Afbeelding 8: zoekfilter voor co-managed devices

Ik heb 5 pagina's geëxporteerd die steeds 36 devices bevatten. Te samen goed voor 180 devices. De overige devices heb ik voor de andere stagiair overgelaten. Dit wil ook zeggen dat ik de scripts die dadelijk aangekaart worden, ook 5x heb uitgevoerd, 1 keer per groep van 36 devices.

Op de parent-group folder binnen EPM staan policy settings die gelden voor alle onderliggende child-groups en hun desbetreffende devices in die groups. Hierdoor wordt er onder meer een passwoord gevraagd als je handmatig Symantec zou willen uninstallen.

Voor security redenen is dit heel goed, maar dit zou betekenen dat je deze taak niet kan automatiseren, maar telkens per device handmatig een uninstall passwoord moet gaan ingeven alvorens Symantec verwijderd kan worden.

Om dit probleem op te lossen is er onder de parent-group een uninstall folder aangemaakt, genaamd 'uninstall'. Policy inheritance is op niet actief gezet hierbij en de "require a password to uninstall the client" is afgevinkt.



Afbeelding 9: client password settings van uninstall folder

2.1.2 Domain controller

Nu er geen Symantec uninstall wachtwoord meer gevraagd gaat worden kan de volgende stap uitgevoerd worden. Deze speelt zich af op de Domain controller.

De file 'symantec_v1_DJ.csv' is een verwijzing naar één van de weggeschreven exports die 36 devices bevat. Voor elk van deze exports voer ik telkens onderstaand script uit.

move devices to another OU.ps1*

```
$destination = "OU=Enable Defender,OU=WINDOWS 10,OU=COMPUTERS,OU=SDLBE,OU=2_ACTIVE,OU=_CORP,DC=soudal,DC=be"
$computers = Import-Csv C:\Temp\Symantec_v1_DJ.csv
foreach ($computer in $computers)
{
    write-host $computer.name
    $cc=  Get-ADComputer $computer.Name | Move-ADObject -TargetPath $destination

}

```

Codefragment 1: devices verplaatsen naar een andere OU

Dit script gaat ervoor zorgen dat de devices verplaatst worden naar de OU “Enable Defender”. Op de andere OU’s binnen Active Directory Users and Computers staan policy settings ingesteld die ervoor zorgen dat Windows Defender niet automatisch actief wordt na het uninstallen van Symantec.

Dit probleem ga je niet hebben als ze in de “Enable Defender” OU zitten omdat hier andere policy settings van toepassing zijn. Dus door bovenstaand script uit te voeren, zorg je ervoor dat Defender actief komt nadat het client device geen Symantec antivirus scanner meer detecteert op het device.

2.1.3 Microsoft System Center Configuration Manager

In deze stap gaan we ervoor zorgen dat alle devices in 'symantec_v1_DJ.csv' worden toegevoegd aan de “Intune-CoMgt-Endpoint Protection-Pilot” collectie. Hiervoor moeten we onderstaand script runnen op de SCCM-server.

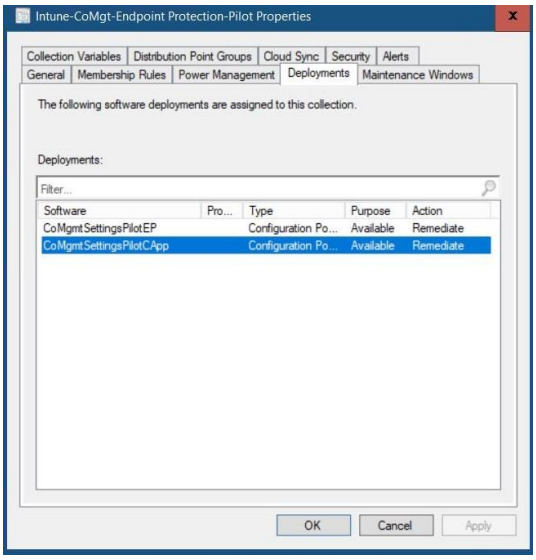
toevoegen devices.ps1

```
Get-Content "c:\Temp\Symantec_v1_DJ.csv" | foreach { Add-CMDeviceCollectionDirectMembershipRule -CollectionName "Intune-CoMgt-Endpoint Protection-Pilot"
-ResourceID (Get-CMDevice -Name $_).ResourceID }
```

Codefragment 2: devices toevoegen aan SCCM-collectie

Aan deze collectie zijn deployments gekoppeld. Deze zorgen voor de CoMgmtSettings zodat ze ook vanuit Intune kunnen beheerd worden.

Het nut hiervan is dat de devices in deze collectie nu weten dat ze hun antivirus niet via SCCM moeten verkrijgen, maar via Intune.



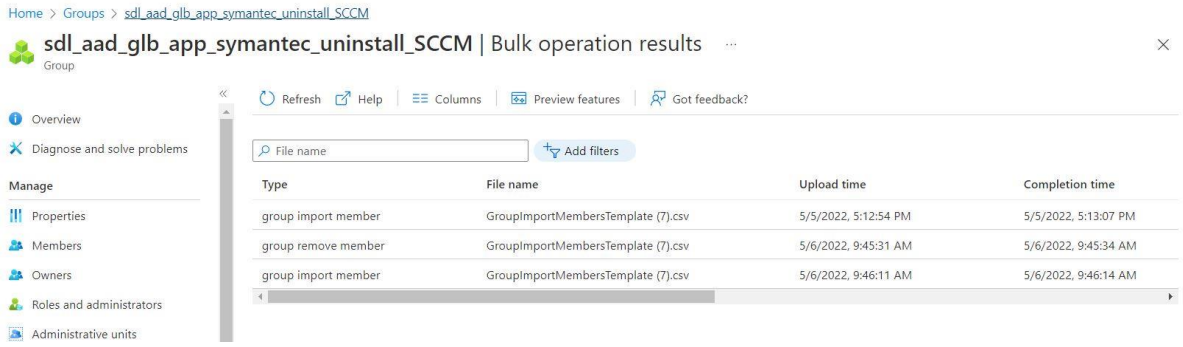
Afbeelding 10: SCCM-collectie deployments tab

2.1.4 Intune groups

Nu er geen uninstall wachtwoord meer gevraagd wordt, Defender automatisch actief gaat komen bij het verwijderen van Symantec en de CoMgmtSettings in orde zijn gebracht gaan we tot slot over naar de nodige configuratie via Intune. Dit is een service die vooral de focus legt bij het mobile device management (MDM) en het mobile application management (MAM). Via Intune gaan we de devices toevoegen aan groepen waaraan deployments gekoppeld zijn om Symantec te uninstallen en D4E actief te laten komen.

Door de devices toe te voegen aan de Intune group: "**Sdl_aad_glb_app_symantec_uninstall_SCCM"**, gaan we de Symantec uninstall effectief uitvoeren. Dit zal ervoor zorgen dat wanneer de devices online zijn, ze het uninstall request binnenkrijgen en uitvoeren.

Intune staat je om devices in bulk toe te voegen aan deze Intune groepen. Onderstaande afbeelding toont een overzicht van de uitgevoerde bulk inserts.



Afbeelding 11: overzicht bulk inserts voor het toevoegen van devices aan de Intune groep

Wanneer vorige stappen succesvol zijn uitgevoerd is het nog de bedoeling dat je ze toevoegt aan de Intune group: "**Sdl_aad_glb_endpointsecurity**". Hier komen alle devices terecht met Endpoint security activated.

Nadat de devices succesvol gemigreerd zijn, komen ze door middel van deze group ook terecht in het device inventory overzicht van D4E.

2.2 Herhaaldelijke checks migraties

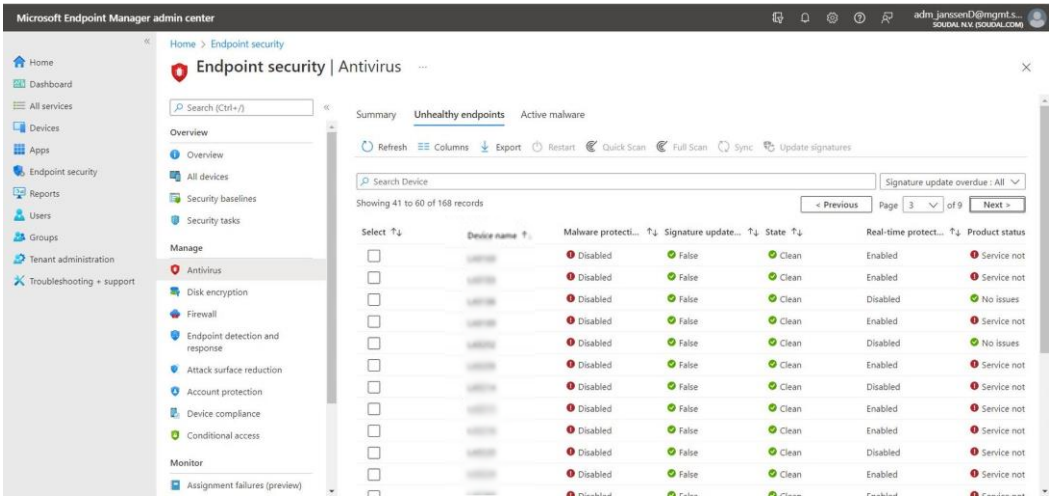
Het is belangrijk om te weten dat het device ingeschakeld moet zijn alvorens het updates binnenkrijgt en de bovenstaande stappen gaat uitvoeren.

Bijkomend kan het, voor wat voor reden dan ook, zijn dat er ergens iets misloopt. Hierdoor is het cruciaal om herhaaldelijke checks uit te voeren en de situatie zo nauw mogelijk op te volgen.

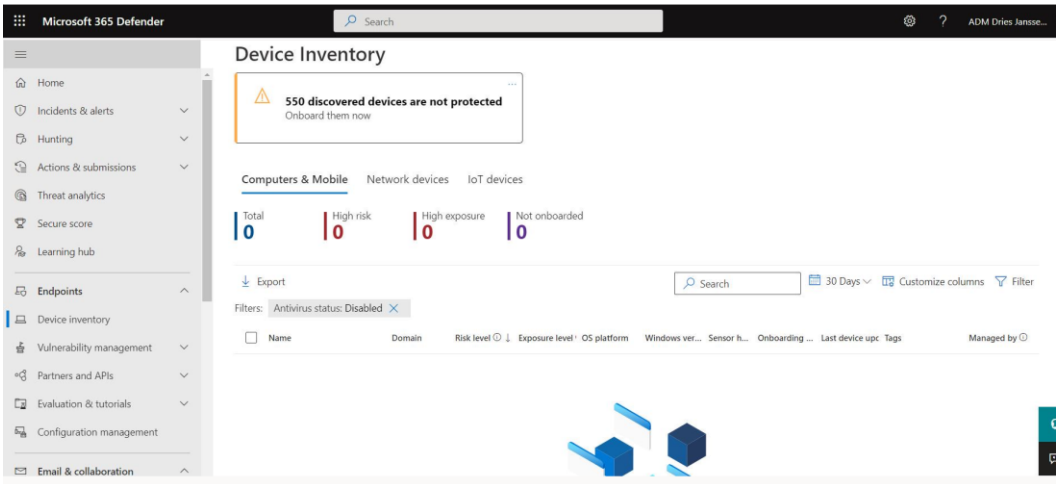
Via security.windows.com kan je aan de hand van device inventory filteren op devices die geen virusscanner hebben. Dit kan verwijzen naar een fout, waarbij er bij het automatisch actief worden van Defender iets is fout gelopen is.

Dit overzicht is ook handig om op te volgen of devices al zichtbaar zijn in D4E.

Via Intune kan je aan de hand van "unhealthy endpoints" ook de probleemgevallen grondiger gaan bekijken en trachten op te lossen. Onderstaande afbeeldingen geven een beeld van hoe deze schermen eruit zien.



Afbeelding 12: overzicht van unhealty endpoints



Afbeelding 13: device inventory met filter op antivirus niet actief

2.3 Troubleshooting

In het gehele Symantec migratie proces kan er veel foutlopen. Dus wordt er verwacht dat wanneer er ergens iets fout loopt in dit proces, je ook de fout kan oplossen. Om dit wat makkelijker te laten verlopen, kregen we vooraf een lijst met 'known errors' en een bijpassende mogelijke oplossing.

Aangezien het troubleshooting onderdeel veel tijd in beslag nam, is het zeker het vermelden waart. Veel van onderstaande problemen zijn effectief voorgevallen en door deze troubleshooting methodes opgelost geraakt.

Troubleshoot 1: SYMANTEC UNINSTALL NIET VOLLEDIG GELUKT:

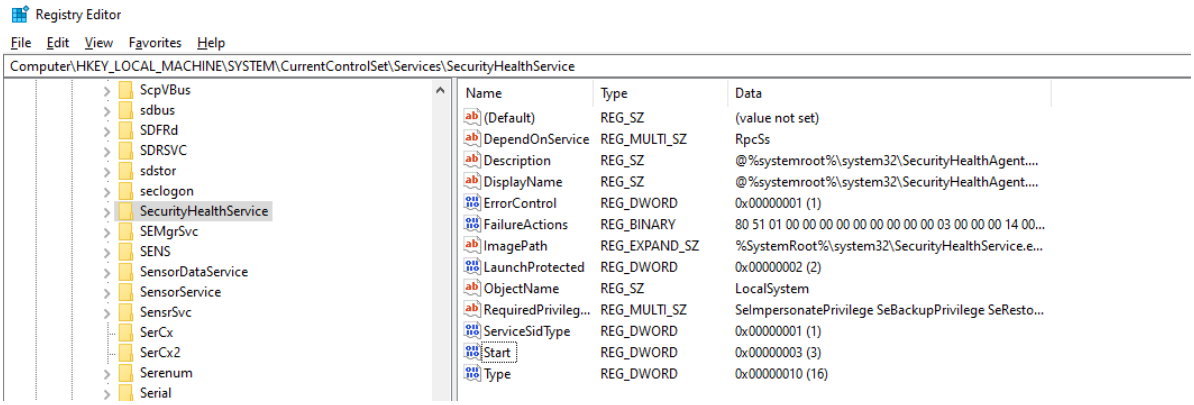
Mogelijke oplossing: kijken of Symantec nog in de Managed Apps staat. Indien wel in Discovered, maar niet in Managed moet ik de gebruiker van het toestel contacteren en vragen om zijn device te herstarten. Mocht dit niets oplossen, in de Intune group: "sdl_aad_glb_app_symantec_Force_uninstall" zetten.

Troubleshoot 2: NA VERWIJDEREN WORDT DEFENDER NIET ACTIEF:

Mogelijke oplossing: status van het toestel nakijken zoals beschreven in 'herhaaldelijke checks migraties'. Indien Malware protection niet op de client loopt is Defender niet actief.

Dit probleem kan je mogelijks verhelpen door de waarde "Start" aan te passen naar 2 (automatisch starten) in de registry editor, te vinden op volgende locatie:

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SecurityHealth Service



Afbeelding 14: registry editor Start waarde naar 2 aanpassen

Troubleshoot 3: DEFENDER STARTEN VIA CMD:

Als Defender moeite heeft om zelf online te komen kan je volgende commando's proberen in CMD:

cd %ProgramFiles%\Windows Defender
MpCmdRun.exe -signatureupdate -MMPC

Troubleshoot 4: UNINSTALL OP ON-PREM DEVICE START NIET:

Mogelijke oplossing: *"SMS Agent host" (CCMexec) op de client herstarten*

Troubleshoot 5: DEFENDER START NIET OMWILLE VAN POLICY / ERROR 577:

Uitleg problem*: The Windows Defender Antivirus Service service failed to start due to the following error: Windows cannot verify the digital signature for this file. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.*

Mogelijke oplossing*:* HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender > "DisableAntiSpyware"=dword:00000000

Troubleshoot 6: INTUNE / SCCM FORCEREN:

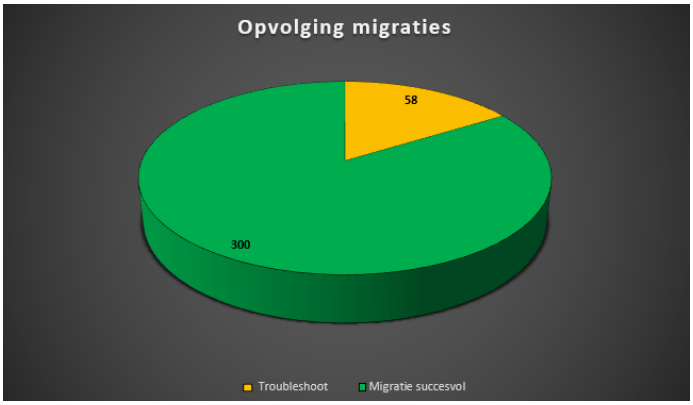
Mogelijke oplossing:

Intune -> Herstart service "Microsoft Intune management"
SCCM -> Herstart service "SMS agent host"

2.4 Opvolging resultaten

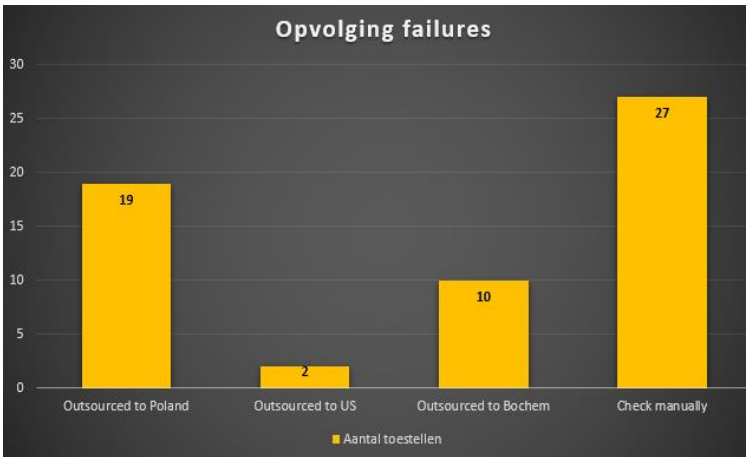
Om een volledig overzicht van het migratieproces te krijgen, is het handig dat er een gezamenlijk document wordt opgesteld. Hierbij werd mijn data gebundeld met die van de andere stagiair, Vince. Voor Soudal is dit handig zodat ze ook een single-point of overview hebben.

In totaal moesten mijn mede stagiair en ik 360 devices migreren. Zoals onderstaande grafiek aantoont zijn er hiervan 300 migraties succesvol verlopen. Voor 58 devices verliep dit proces niet foutloos.



Grafiek 1: opvolging migratiestatus Symantec

Bij het aandachtig nakijken van de overige 58 devices, zijn deze verder opgedeeld in 4 categorieën. Vermoedelijk staat er nog een outdated versie van Teamviewer op deze devices, waardoor we niet in staat waren om toegang te krijgen tot het device en het troubleshooting proces uit te voeren. Dit kwam voor bij devices van Polen, Bochem en Amerika.



Grafiek 2: opvolging failures Symantec

Na overleg met mijn mede stagiair, hebben we besloten de lokale IT-medewerkers van de desbetreffende regio's te contacteren. Hierbij werd hen gevraagd om de migratie in orde te brengen. Zoals je op bovenstaande afbeelding kan zien, zijn er op deze manier nog eens 31 van de 58 devices succesvol gemigreerd.

Door middel van regelmatige updates werden de vorderingen in de vestigingen in het buitenland genoteerd en opgevolgd.

Voor de rest zijn er nog 27 devices die manueel nagekeken moeten worden. Hiervoor is ook reeds contact opgenomen met desbetreffende eigenaars van de devices. Dit vordert mondjesmaat. Het ging hier voornamelijk ook over inactieve devices en gebruikers die niets van zich lieten horen. Deze zijn dus ook niet allemaal in orde gebracht kunnen worden.

Hier is een inventaris van gemaakt in Excel, waarbij er een overzicht gevonden kan worden van deze devices. Dit is bovendien gedeeld met een collega van op de IT-dienst met de mondelinge doorgave van het feit dat deze devices niet gebeurd zijn geweest.

Onderstaande tabel toon de opvolging van deze devices.

			Status		
Export D(	Export SCC	Intun(	Follow up	Troubleshoot	Contact stat
1	1	1	Waiting for install status	visible in D4E	1
1	1	1	Not in managed apps but still in discovered	not visible in D4E	1
1	1	1	Symantec uninstalled	not visible in D4E	1
1	1	1	Not in managed apps but still in discovered	not visible in D4E	1
1	1	1	Waiting for install status	not visible in D4E	1
1	1	1	Not in managed apps but still in discovered	not visible in D4E	1
1	1	1	Waiting for install status	not visible in D4E	1
1	1	1	Waiting for install status	not visible in D4E	1
1	1	1	Waiting for install status	visible in D4E	1
1	1	1	Symantec uninstalled	not visible in D4E	1
1	1	1	Waiting for install status	visible in D4E	1
1	1	1	Not in managed apps but still in discovered	not visible in D4E	1
1	1	1	Waiting for install status	not visible in D4E	1
1	1	1	Not in managed apps but still in discovered	visible in D4E	1
1	1	1	Waiting for install status	not visible in D4E	1
1	1	1	Uninstall failed (0x87D1041C)	visible in D4E	1
1	1	1	Waiting for install status	not visible in D4E	1
1	1	1	Waiting for install status	visible in D4E	1
1	1	1	Not in managed apps but still in discovered	not visible in D4E	1
1	1	1	Symantec uninstalled	not visible in D4E	1
1	1	1	Symantec uninstalled	not visible in D4E	1
1	1	1	Waiting for install status	not visible in D4E	1
1	1	1	Waiting for install status	not visible in D4E	1
1	1	1	Symantec uninstalled	not visible in D4E	1
1	1	1	Waiting for install status	not visible in D4E	1
1	1	1	Waiting for install status	not visible in D4E	1

Tabel 1: Overzicht opvolging 27 devices die manueel nagekeken dienen te worden

3 BITLOCKER

Bitlocker is een onderdeel van Windows, dat wordt gebruikt om data die op je Solid state drive (SSD), hard disk drive (HDD) of verwijderbare media staat, te beschermen. Dit gebeurt aan de hand van het encrypteren van deze data.

In geval van verlies of diefstal van je device, wil je niet dat iemand met kwaadwillige intenties toegang krijgt tot je data. Mocht deze data niet geëncrypteerd zijn, dan kan je op diverse manieren deze data uitlezen via een andere computer. Voor een bedrijf met een omvang zoals Soudal is dit een reëel gevaar. Om dit te voorkomen maakt Soudal onder meer gebruik van de implementatie van de Bitlocker om hun bedrijfsdata veilig te stellen.

Voor de encryptie bij Bitlocker wordt er gebruik gemaakt van de Advanced Encryption Standard (AES). Dit is een bekende vorm van encryptie en wordt vandaag de dag nog veel gebruikt.

Bij aanvang van de stage, werd er gebruik gemaakt van de Bitlocker met encryptiemethode AES-128. Er werd de opdracht gegeven om deze AES-128 niet meer als standaard te gebruiken, maar om de encryptiemethode op de devices aan te passen naar AES-256.

Dit is belangrijk aangezien er binnenkort nieuwe Intune policies komen. Dit zijn strengere voorwaarden waaraan devices moeten voldoen om compliant te zijn. Dit wil zeggen, voldoen aan opgelegde vereisten zoals geconfigureerd in Intune om toegang te krijgen tot bepaalde bedrijfsdata. Ter voorbereiding op deze nieuwe policies diende de encryptiemethode aangepast te worden.

3.1 Aanpak

De scope van deze migratie beperkt zich tot alle Azure AD joined devices. Dit zijn de bedrijfstoestellen die een werknemer mee naar huis kan nemen. Dit staat gelijk aan ongeveer 1520 devices waarop de wijziging van Bitlocker moet worden aangebracht.

Ook hier worden stappen doorlopen en kan je dit hele proces opdelen in 4 grote onderdelen.

In stap 1 gaan we ervoor zorgen dat de AES-128 encryptiemethode gaat decrypteren.

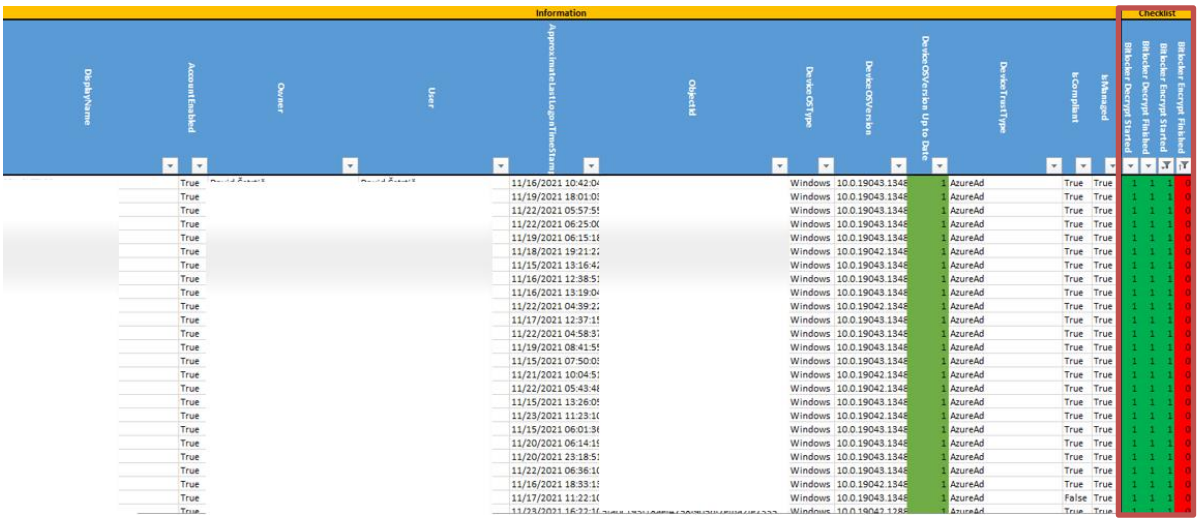
In stap 2 gaan de devices volledig gedecrypteerd zijn.

In stap 3 worden deze devices vervolgens in een groep gestoken waar ze hun AES-256 encryptie gaan verkrijgen.

Tot slot is er de 4de stap waarbij er een controle gedaan gaat worden op recovery keys die aangemaakt worden in het encryptieproces via de nieuwe encryptiemethode.

Dit alles verloopt via de Intune omgeving, waarbij script in de achtergrond runnen op het client device.

De opvolging van Bitlocker status van al deze devices, werd ook hier bijgehouden aan de hand van een gezamenlijke Excel-file met de andere stagiair.



Tabel 2: overzicht opvolging Bitlocker status

De rode kader op bovenstaande afbeelding toont de checklist. Dit gaat over de opvolging van de 4 stappen die doornomen dienen te worden. Bij het voltooien van een stap, komt er een '1' te staan, bij de nog te voltooien stappen staat een '0'.

3.1.1 Bitlocker decryptie (start)

Bij de eerste stap gaan we via Intune de devices toevoegen aan de groep 'SDL_aad_GLB_app_DecryptBitlocker'. Aan deze groep is een applicatie verbonden die een detection script en een decrypt script bevat.

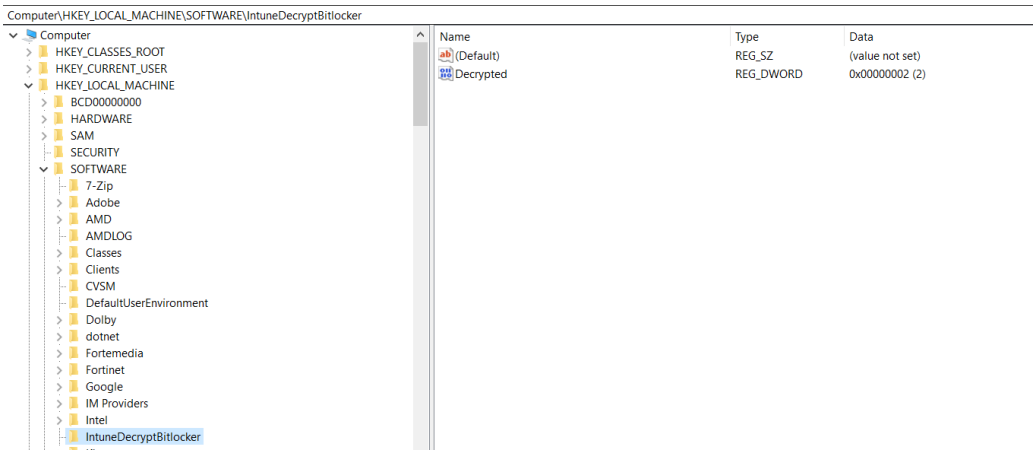
Devices toevoegen aan deze groep gaat ook hier weer gebeuren in bulk operaties. Dit heeft te maken met beveiligingsredenen. Bij het decrypteren gaat de encryptie op de schijven wegvallen, waardoor je een device krijgt zonder Bitlocker. Vandaar dat het toevoegen van devices aan deze groep per 100 devices gebeurde in het begin en geleidelijk is opgetrokken tot 250 per keer om niet heel je omgeving in één keer zonder Bitlocker te zetten.

Het is ook niet best-practice om dit op een vrijdag te doen, aangezien je device mogelijks een heel weekend zonder encryptie kan zitten. Vandaar dat dit telkens aan het begin van de week werd gedaan.

3.1.2 Bitlocker decryptie (voltooid)

Het doel van het detection script is om te controleren of het decrypt script succesvol uitgevoerd is. Dit gaat gebeuren aan de hand van het nakijken van een registry waarde die in het decrypt script wordt aangepast.

Zo gaat, wanneer een schijf volledig gedecrypteerd is, het decrypt script een registry waarde aanpassen. De locatie 'HKLM\Software\IntuneDecryptBitlocker' gaat worden aangemaakt en een attribuut 'Decrypted' gaat de waarde 2 krijgen.



Afbeelding 15: Registry Editor overzicht

Wanneer de waarde 'Decrypted' gelijk is aan 2, dan zal het detection script de naam van het device wegschrijven naar een CSV-bestand. Dit wordt bijgehouden op een share beschikbaar via het netwerk.

3.1.3 Bitlocker encryptie (start)

Alle devices die volledig gedecrypteerd zijn, worden momenteel weggeschreven naar het CSV-bestand. Zo krijg je een overzicht welke devices klaar zijn met het decryptie proces en kunnen doorgaan naar de volgende stap, het encrypteren.

Deze file dien je regelmatig te controleren op nieuwe devices die weggeschreven worden naar het CSV-bestand. Voor elks van deze devices ga je onderstaande handelingen uitvoeren.

In deze stap wordt het device verwijderd uit de decryptie groep en toegevoegd aan de encryptie groep, genaamd 'sdl_aad_glb_Intune2.0_Bitlocker'.

Het is niet de bedoeling dat dit één per één gaat gebeuren aangezien dit veel tijd in beslag zou nemen. Hierdoor heb ik besloten het mezelf zo makkelijk mogelijk te maken en heb ik een script geschreven in powershell dat mij helpt deze stappen uit te voeren.

Onderstaand script gaat de decryptie groep verwijderen en de encryptie groep toekennen aan alle devices die in de array '$DeviceDN' zijn geplaatst.

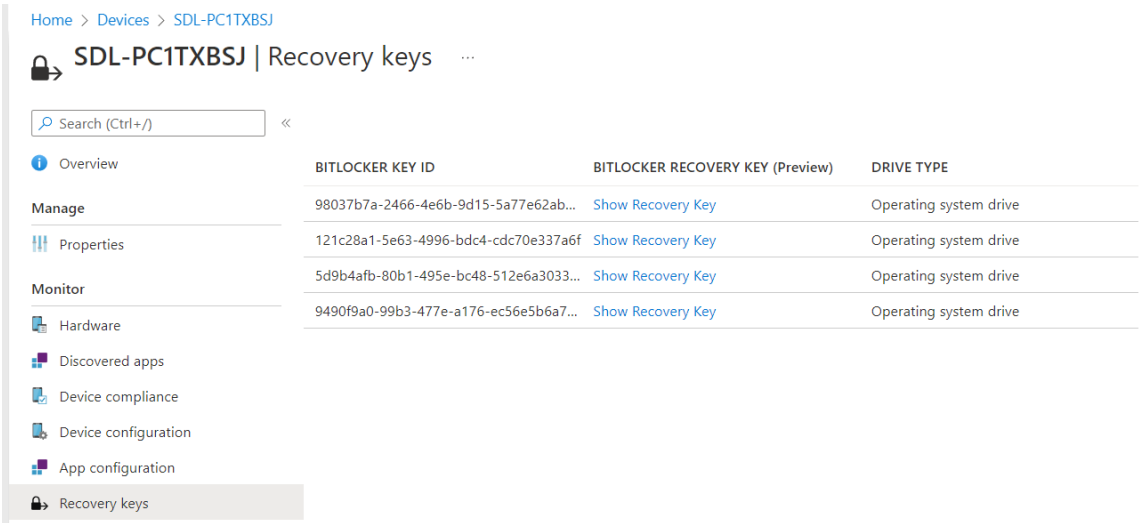
Remove_Add-groups.ps1

```powershell
#Credential Information
Import-Module AzureAD
$cred = Get-Credential -Username ADM_JanssenD@soudal.com -Message "Enter password:"
Connect-AzureAD -Credential $cred

#Variables
$DecryptGroup = Get-AzureADGroup -SearchString "SDL_aad_GLB_app_DecryptBitlocker"
$IntuneBitlockerGroup = Get-AzureADGroup -Filter "DisplayName eq 'sdl_aad_glb_Intune2.0_Bitlocker'"
$DeviceDN = ("SDL-PF14QXX6", "SDL-PC18F3ZJ", "SDL-S4PG5490", "SDL-H4Z25R2", "SDL-PF1DUA61", "SDL-PC1TXBSL", "SDL-PF3CYY6L", "SDL-R913VF0Z", "USELTAC-LA1648")

#Convert displayname to deviceobjectIDs

foreach($Device in $DeviceDN)
{
    $DeviceID = Get-AzureADDevice -SearchString $Device

    #Remove device from BitlockDecrypt
    Write-Host -ForegroundColor Red "Remove $($Device) from Bitlocker Decrypt group"

    try {

         Remove-AzureADGroupMember -ObjectId $DecryptGroup.ObjectId -Memberid $DeviceID.ObjectId
    }

    catch {

        Write-Warning $Error[0]
        write-host "`n"

    }

    #Add device to intune2.0Bitlocker
    Write-Host -ForegroundColor Green "Add $($Device) to Bitlocker Encrypt group"


    try{

    Add-AzureADGroupMember -ObjectId $IntuneBitlockerGroup.ObjectId -RefObjectId $DeviceID.ObjectId

    }

    catch{

        Write-Warning $Error[0]
        write-host "`n"

    }
}
```

Codefragment 3: remove and Add groups script

3.1.4 Bitlocker encryptie (voltooid)

Tot slot moet er nagekeken worden of de encryptie gelukt is. Dit kan je ofwel handmatig doen via Teamviewer of via Intune. De meest efficiënte methode is via Intune. Hierbij ga je naar het overzicht van alle devices en controleer je of het device recovery keys heeft aangemaakt. Mocht dit zo zijn, dan is de encryptie gelukt en heeft het device vanaf nu de AES-256 encryptie.



Afbeelding 16: overzicht recovery keys

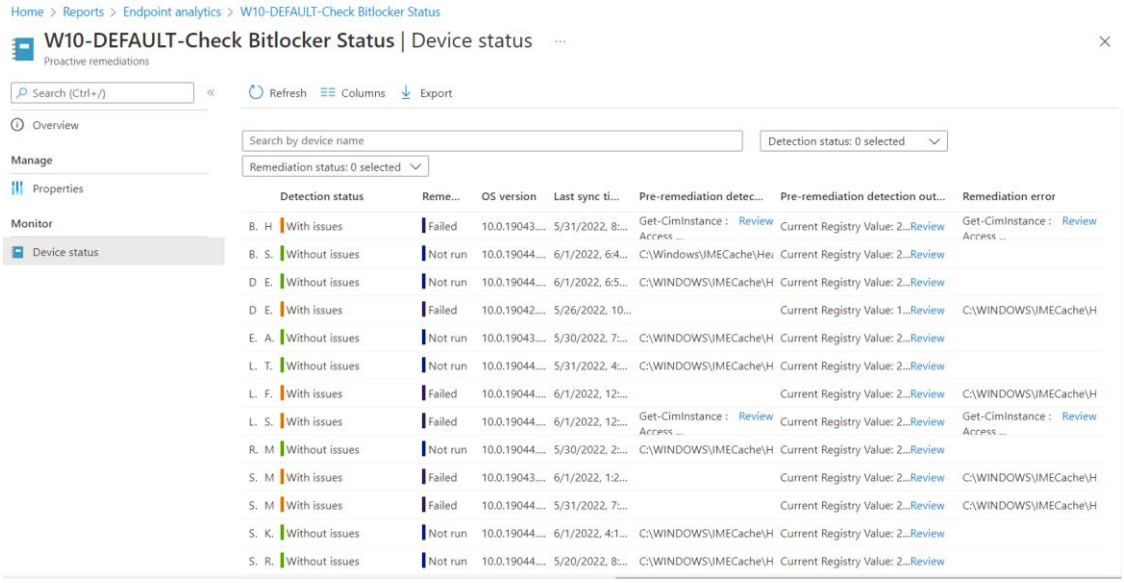
3.2 Troubleshooting

Tijdens het Bitlocker proces verliep ook hier niet alles vlekkeloos. Er doken regelmatig problemen en errors op die het gehele proces hebben vertraagd. Onderstaand kan je de meest voorkomende problemen terugvinden.

De coronapandemie heeft er onder meer voor gezorgd dat telewerken de nieuwe standaard werd voor jobs waarbij dit mogelijk is.

De link met telewerken en de Bitlocker opdracht is dat devices verbonden moeten zijn met het Soudal netwerk. Dit is niet altijd het geval voor mensen die van thuis uit werken aangezien de meeste geen verbinding maken met de VPN. Dit is belangrijk aangezien de share waarop het detection script de gedecrypteerde devices plaatst enkel beschikbaar is via het Soudal netwerk.

Via een Proactive remediation script krijg je hiervoor een beter overzicht voor aan error-handling te doen. Op onderstaande foto kan je een overzicht terugvinden van wat dit script toont. Via de laatste 3 kolommen kan je de status terugvinden van het 'decrypted' attribuut en eventuele error meldingen waarop het device vastloopt tijdens het decrypteren.

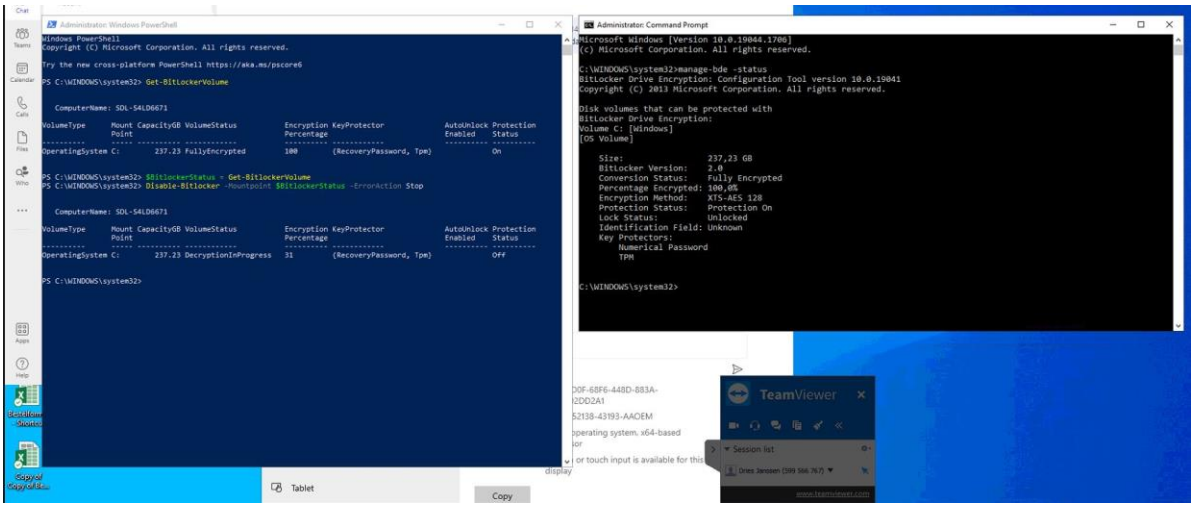


Afbeelding 17: overzicht Proactive remediation script output.

Een registry value van '1' betekent 'in progress', dit kan betekenen dat er ergens iets is fout gelopen is. Een mogelijke oplossing hiervoor is om het toestel over te nemen via Teamviewer en de waarde handmatig naar 0 te zetten. Hierdoor gaat opnieuw het detection en decryptie script getriggerd worden.

"BitLocker Drive Encryption cannot be turned off on the operating system drive until the auto unlock feature has been disabled for the fixed data drives and removable data drives associated with this computer."

Als dit het probleem niet verhielp was er ook nog altijd de methode om via powershell zelf de decryptie uit te voeren. In onderstaande afbeelding kan je hiervan een voorbeeld terugvinden.



Afbeelding 18: manueel decrypteren

In de gezamenlijke Excel-file stonden ook nog heel wat devices dat niet meer gebruikt werden. Om deze eruit te filteren heb ik een script geschreven voor de last-logon time na te kijken van alle devices in de lijst. Deze devices kregen dan vervolgens een rode kleur in de lijst. Waardoor het doelgericht focussen op de actieve devices die opvolging nodig hebben overzichtelijker werd.

Filter_inactive-devices.ps1

```
#Connect with Soudal AAD tenant
Connect-AzureAD

#All bitlocker devices with status decrypt started
$deviceList = ("USELTAC-LA1616", "SDL-R90VV2QS", "SDL-PF2PB9P4", "SDL-PF1QR4B4", "SDL-S4LE3762", "SDL-9TTGQM2", "SDL-PF1QR4AP", "SDL-PF2C9LYD", "SDL-FILLEDBYOEM", "SDL-R911TY08", "Facturas", "SDL-PF2DA

#Inactivity settings
$LastLogonDate = (Get-Date).AddDays(-120)

Write-Host -ForegroundColor Yellow 'Loading Results...'

$table = foreach ($device in $deviceList){

    $deviceID = Get-AzureADDevice -SearchString $device
    Get-AzureADDevice -SearchString $device | where ApproximateLastLogonTimeStamp -LT $LastLogonDate  | select DisplayName,DeviceTrustType,ApproximateLastLogonTimeStamp, ProfileType, AccountEnabled
}

$table | Format-Table
Write-Host -ForegroundColor Yellow "$($table.Count)  Results found."
```

Codefragment 4: last-logon time check

Bitlocker maakt gebruik van een Trusted Platform Module (TPM) chip. Dit is een geïntegreerde hardware beveiliging die voor de encryptie zorgt. Deze TPM-chip werkt samen met de secure boot optie in UEFI. Dit gaat ervoor zorgen dat enkel legitieme processen toegang krijgen tot deze TPM-chip.

Het gebeurde dat de TPM-optie niet enabled was via UEFI, waardoor Bitlocker ook niet ging werken en foutmeldingen gaf. Voor dit probleem op te lossen moest je de gebruiker met zijn device even laten langskomen zodat je handmatig naar BIOS kon gaan om dit te enablen.

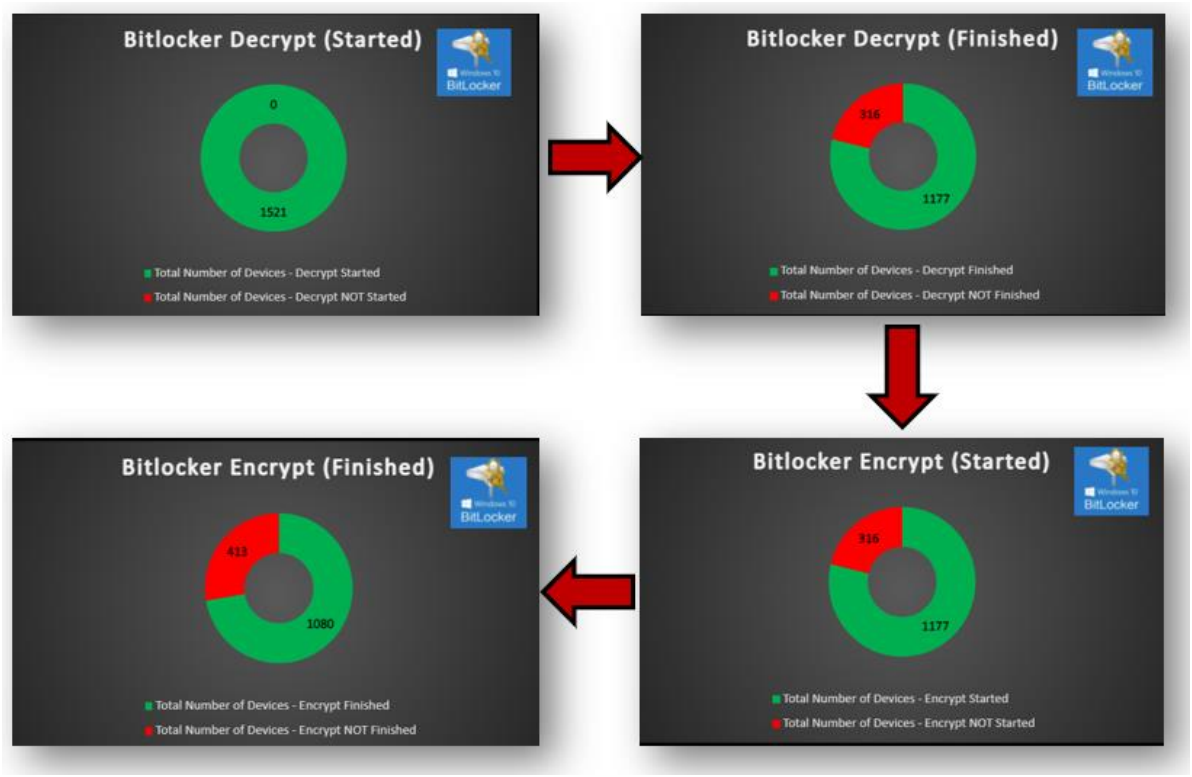
Soms gaf een lokale Group Policy Object (GPO) op het device een conflict waardoor AES-256 encryptie niet standaard

3.3 Opvolging resultaten

Zoals reeds aangekaart gebeurde het Bitlocker proces in 4 grote stappen. De opvolging van elke individuele stap werd ook telkens bijgehouden. Zo kan je op onderstaande afbeelding zien dat alle 1521 devices werden toegevoegd aan de nodige groep om het decryptie proces in gang te zetten. Dit proces verliep niet foutloos zoals bij het topic troubleshooting besproken. Hierdoor zijn er uiteindelijk 1177 devices volledig gedecrypteerd geraakt. Bij de overige 316 devices liep ergens iets fout waardoor er handmatig telkens iets nagekeken diende te worden, wat dit proces enorm lang liet duren.

Alle devices die succesvol gedecrypteerd zijn, werden succesvol toegevoegd aan de encryptie groep en daarna verwijderd uit de decryptie groep.

Voor 1080 van de 1170 devices werd er succesvol een recovery key aangemaakt. Dit betekent dat de encryptie succesvol is toegepast op deze devices. Dat wilt ook zeggen dat op 90 devices dit niet vlekkeloos verliep. Mogelijke problemen die hiervoor gezorgd hebben is het niet hebben van een TPM-chip, volledig gedecrypteerde schijven, maar nog steeds een 'Decrypted' waarde van 1 hebben.



Afbeelding 19: Bitlocker opvolging resultaten

4 WINDOWS UPDATES

In dit onderdeel kan je meer informatie terugvinden over de Windows updates. In een omgeving zoals Soudal gebeuren deze aan de hand van update policies waarbij je alle client devices op eenzelfde feature update versie van Windows zet.

Hier durfde regelmatig wel eens iets fout te gaan. Mijn taak bij dit onderdeel is voornamelijk de devices updaten die voor wat voor reden dan ook, blijven vasthangen op een vorige feature update en waar mogelijk, ook uitzoeken waarom deze update policies niet uitgevoerd werden, om dit in de toekomst te voorkomen.

4.1 Windows feature update policy Soudal

Om een beter beeld te krijgen van de verschillende feature update versies, biedt onderstaande tabel ondersteuning.

De feature updates voor Windows 10 komen 2 keer per jaar uit. Deze bevatten de laatste nieuwe Windows-versie met verbeterde functies, beveiligingsverbeteringen en meer.

Momenteel hanteert Soudal de versies 20H2, 21H1 en 21H2 voor Windows 10 clients. Client toestellen die één van deze versies hebben, worden aanzien als compliant. Wanneer er een device niet voldoet aan één van deze versies, gaat het in Intune ook aangegeven worden als niet compliant.

Compliant devices W10

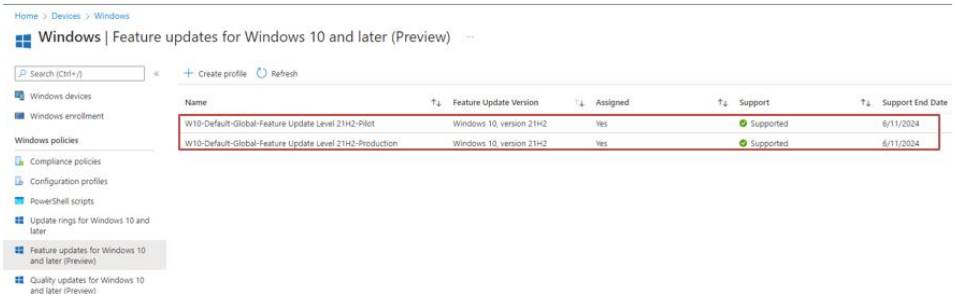
Name	Codename	Release date	Version	Editions	Build number
Windows 10 version 1507	Threshold[5][f]	2015-07-29	NT 10.0[g][h]		10240
Windows 10 version 1511	Threshold 2	2015-11-10	1511		10586
Windows 10 version 1607	Redstone 1	2016-08-02	1607		14393
Windows 10 version 1703	Redstone 2[8]	2017-04-05	1703		15063
Windows 10 version 1709	Redstone 3[9]	2017-10-17	1709	• Windows 10 Home • Windows 10 Pro • Windows 10 Education • Windows 10 Enterprise • Windows 10 Pro for Workstations[i] • Windows 10 Pro Education[j]	16299
Windows 10 version 1803	Redstone 4	2018-04-30	1803		17134
Windows 10 version 1809	Redstone 5[10]	2018-11-13	1809		17763
Windows 10 version 1903	19H1[11]	2019-05-21	1903		18362
Windows 10 version 1909	Vanadium[12][13]	2019-11-12	1909	• Windows 10 S[k] • Windows 10 Enterprise LTSC[l]	18363
Windows 10 version 2004	Vibranium[12][14][n]	2020-05-27	2004		19041
Windows 10 version 20H2		2020-10-20	20H2		19042
Windows 10 version 21H1		2021-05-18	21H1		19043
Windows 10 version 21H2		2021-11-16	21H2		19044
Windows 11 version 21H2	Sun Valley[o]	2021-10-05		• Windows 11 Home • Windows 11 Pro • Windows 11 Pro for Workstations • Windows 11 Pro Education	22000
				• Windows 11 Education • Windows 11 Enterprise	

Tabel 3: overzicht Windows 10 versions

Vanuit Intune kan je deze settings configureren en bepalen welke feature-update versies er gehandhaafd dienen te worden.

In onderstaande configuratie is er nog een onderscheid gemaakt tussen Autopilot devices (pre-configured toestellen bij implementeren in productie) en de toestellen die al reeds actief zijn in de productieomgeving.

Hier zie je dat ondanks 20H2 en 21H1 nog compliant versies zijn, deze niet meer uitgerold worden. Ondertussen staat de policy actief om 21H2 uit te rollen op de Windows 10 devices.



Afbeelding 20: overzicht feature updates for Win-10

4.2 Realisatie Windows Updates

Aangezien er verwacht werd de niet compliant toestellen compliant te maken betreffende Windows updates, heb ik hier opzoekwerk verricht over wat mogelijke oorzaken kunnen zijn, waar je de logs hiervoor kan opzoeken en wat je best kan doen om de Windows updates door te laten komen.

Na het opzoekwerk, heb ik dit voor mezelf uitgeschreven in een soort van stappenplan met troubleshoot methodes. Bij het troubleshooten van devices hanteerde ik vervolgens deze uitgeschreven stappen.

Stap 1:

Bij het gebruik van Teamviewer, altijd eerst device name nakijken om er zeker van te zijn of je op het juiste device bezig bent. Vervolgens ook kijken of ze verbonden zijn met het Soudal netwerk of gebruik maken van de Forticlient indien ze van thuis uit werken.

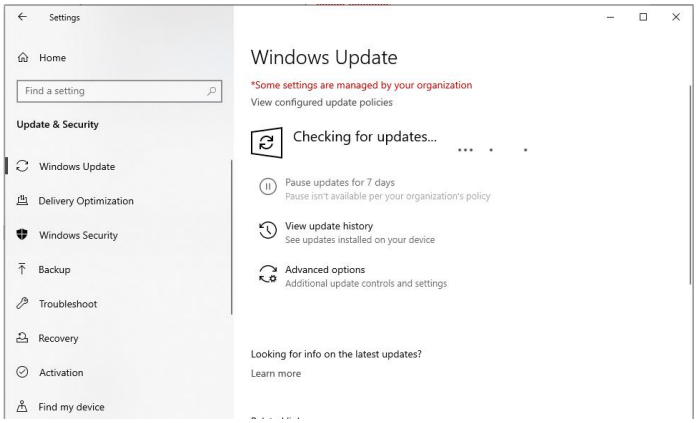
Afbeelding 21: output Winver commando

Stap 2:

Vervolgens run ik telkens het commando 'Winver'. Dit laat de Windows versie zien die actief is op het device, alsook de exacte OS Build version.

Stap 3:

Bij Settings onder categorie "Update & Security" handmatig checken naar updates. Het kan zijn dat deze updates niet automatisch uitvoeren op sommige toestellen of dat er in deze stap errors tevoorschijn komen.



Afbeelding 22: zoeken naar Windows Updates

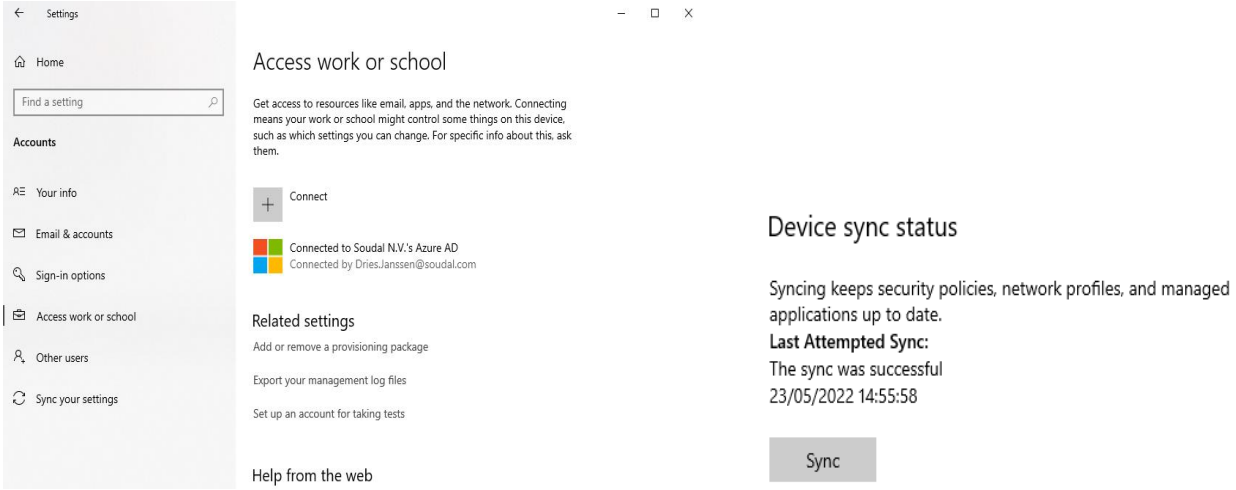
Stap 4:

Bij Settings onder categorie "Accounts" gaan naar Access Work or school. Hier kijken of je verbonden bent met de organisatie Soudal. Afhankelijk of het toestel domain joined is of Azure AD joined gaat de output zoals te zien op onderstaande foto variëren.

Mocht dit niet zo zijn, moet je hier Connecteren en aanloggen met je Soudal gegevens.

Vanuit hier voer ik ook altijd handmatig een Sync uit zodat je device terug up-to-date is met de settings en policies van Soudal. Normaal gezien runt deze Sync ook elke x-aantal minuten.

Error meldingen in deze fase kan je verder oplossen via het cmd commando dsregcmd.exe /status (/debug, /leave, /join)

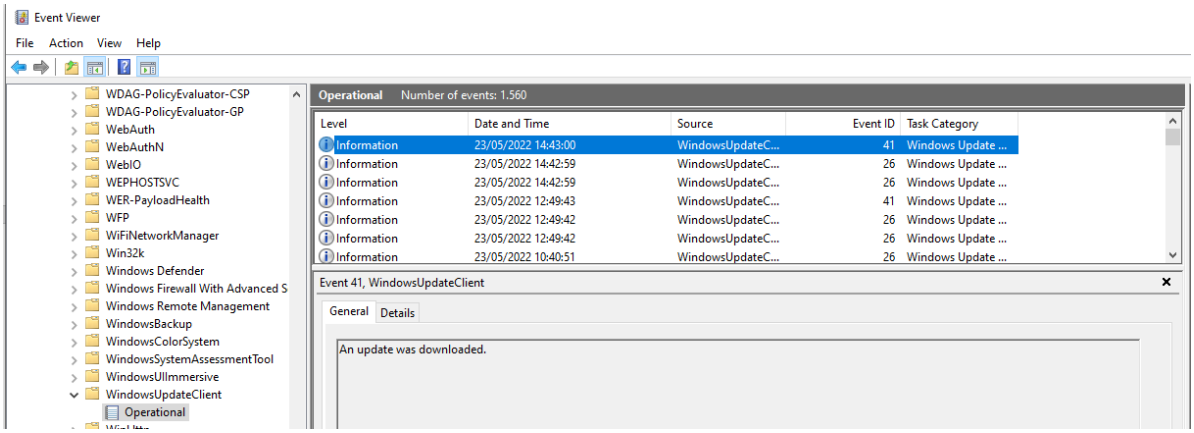


Afbeelding 23:Windows settings "Acces work or school" + Device Sync status

Stap 5:

In deze stap ga ik controleren of er in Eventviewer error logs binnenkomen op Windows updates. Onderstaande foto toont een voorbeeld van mijn device, waar de updates wel binnenkomen.

Errors die zich in deze stap kenbaar maken, worden meestal opgelost door te googelen op de specifieke error log, dit aan de hand van EventID.

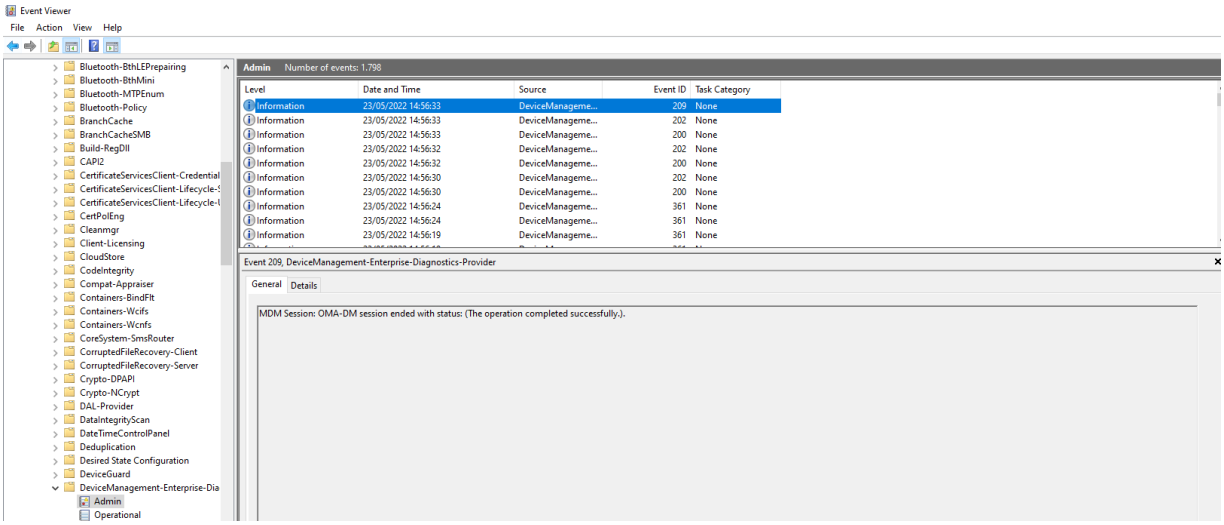


Afbeelding 24: Event Viewer WindowsUpdateClient

Stap 6:

Het ligt niet altijd aan de Windows updates zelf die niet willen uitvoeren. Soms kan het ook gewoon zijn dat er problemen zijn met Mobile device management (MDM), dus de manier van device management door SCCM of Intune.

Ook hier telt het principe van EventID code googelen bij het controleren van deze logs. Een voorbeeld log kan je onderstaand vinden.



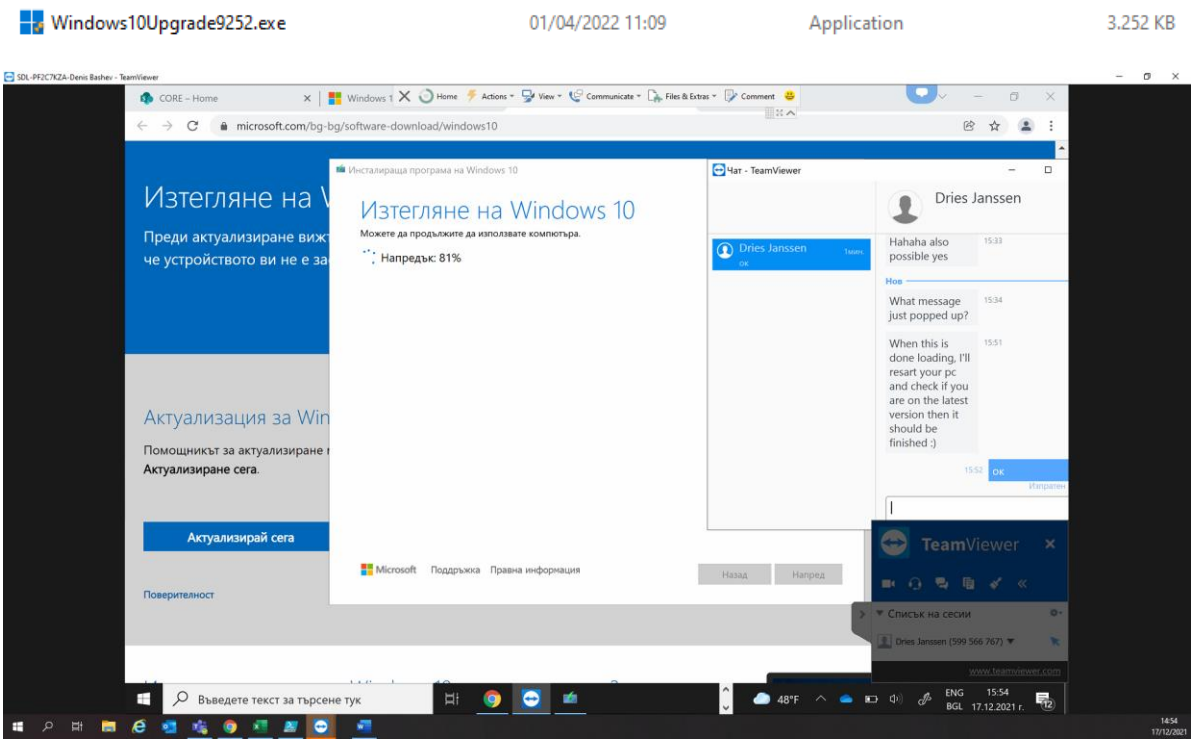
Afbeelding 25: Event Viewer DeviceManagement

Stap 7:

Tot slot komen we bij de laatste stap. Indien vorige stappen geen duidelijke oplossingsmethode hebben, heb ik gebruik gemaakt van de Windows Update Assistant tool.

Aan de hand van deze tool kan je zelf het Windows 10 device bijwerken met de versie die je wilt.

Telkens wanneer ik gebruik maakte van deze tool, heb ik de versie 21H2 op het device gezet. Dit gebeurde door onderstaande programma te runnen op het Windows 10 device. Dan telkens de install wizard te doorlopen.

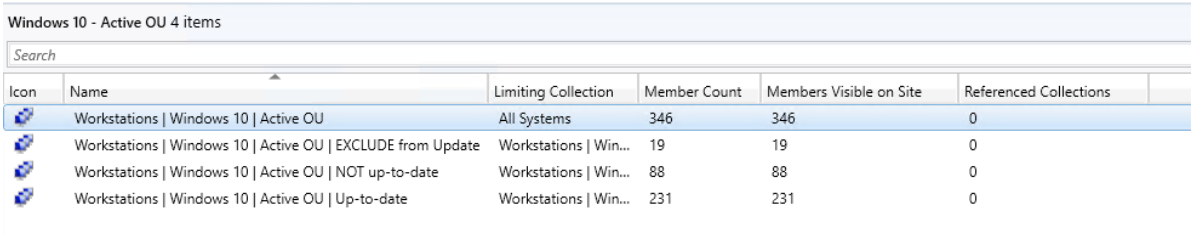


Afbeelding 26: updates uitvoeren aan de hand van Update Assistant

4.2.1 Specifieke troubleshoot SCCM devices

Voor de laatste 2 weken kregen we nog een extra taak in kader van Windows updates. Dit heeft betrekking op devices waarvan het Mobile Device Management gebeurd via SCCM, maar Windows updates verkregen gaan worden door Intune.

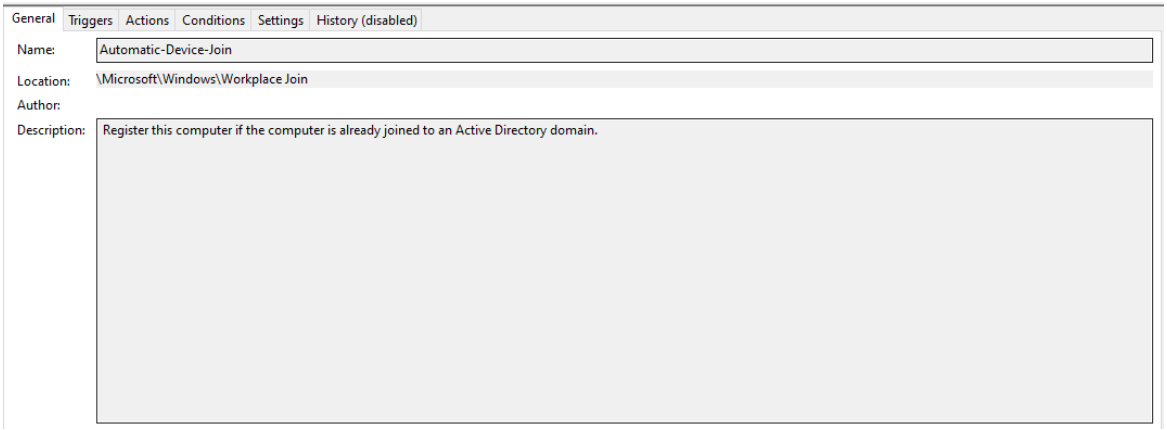
Onderstaande afbeelding toont de verschillende collecties in SCCM waar deze devices inzitten. Zo kan je zien dat er 346 devices zijn die SCCM managed zijn, maar hun Windows updates via Intune verkrijgen. Hiervan zijn er 231 die zonder enige moeite deze updates verwerken. 88 devices hebben problemen met deze updates te verwerken.



Afbeelding 27: overzicht SCCM devices die via Intune Windows updates verkrijgen

Ik heb gemerkt dat de meeste van de 88 devices, inactief zijn. Bij sommige toestellen kwam het ook voor dat ze nog niet deel uitmaakte van de AAD-omgeving. Voor deze devices werd er handmatig via Task scheduler de Task 'Automatic-Device-Join' op enabled gezet en vervolgens het commando **dsregcmd.exe -debug /join** uitgevoerd. Hiermee zorg je ervoor dat ze ook Azure AD joined gaan worden en hun updates via Intune kunnen verkrijgen aangezien dit een vereiste is om via Intune gemanaged te kunnen worden.

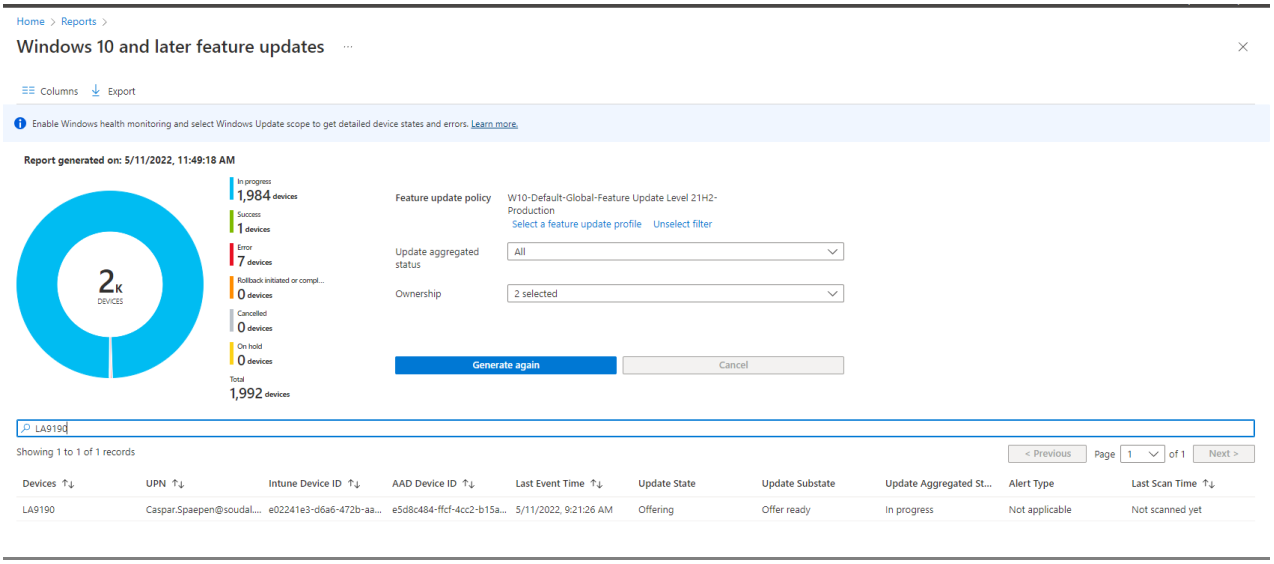
Onderstaande afbeelding toont de Automatic-Device-Join task.



Afbeelding 28: Scheduled Task voor Automatic-Device Join

Via Intune is het ook mogelijk om een report te genereren over de uitrol van de Feature Updates. In dit geval voor versie 21H2.

Hier kan je de namen van de devices opzoeken en kijken naar de status van de updates. Onderstaande afbeelding toont een Update State van 'offering', dit betekent dat de Windows update aangeboden wordt aan het device.



Afbeelding 29: Rapport van Windows 10 feature updates

5 HELPDESK TAKEN

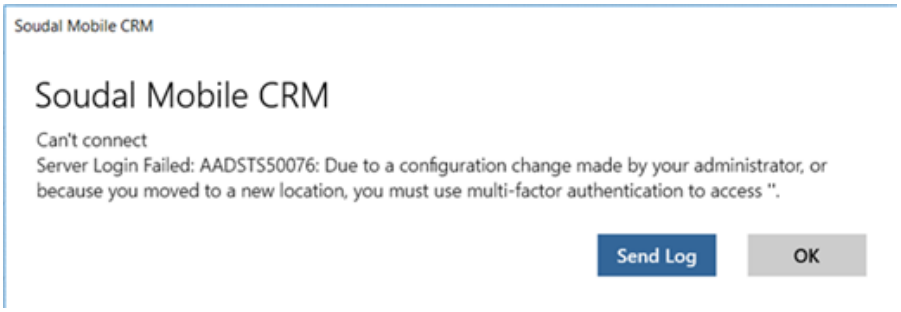
Aangezien ik bij de opdrachten off-boarding, bitlocker en Symantec migraties in aanraking kom met eindgebruikers, gebeurde het ook wel eens dat deze eindgebruikers hun IT-problemen en storingen bij mij kwamen melden in plaats van bij de helpdesk medewerkers.

Deze problemen variëren zich sterk, maar zijn meestal niet al te moeilijk om te verhelpen. Indien ik er zelf niet uitkwam heb ik ofwel de persoon doorverwezen naar helpdesk of zelf even geïnformeerd hoe je dit probleem kan verhelpen.

Onderstaand vindt u een opsomming van de meest voorkomende vragen en taken die hierbij werden opgelost:

5.1 Probleem met Resco na MFA-setup:

Nadat je Multi-factor authentication (MFA) hebt ingesteld voor je Soudal account kan het voorvallen dat je onderstaande error krijgt bij het openen van Resco voor de eerste keer.



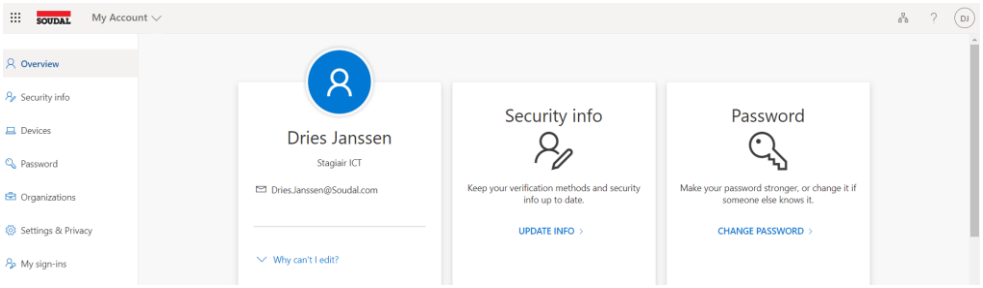
Afbeelding 30: Resco foutmelding

Om dit probleem op te lossen moet je Resco Mobile CRM openen en naar Setup gaan. Vervolgens dient User Mode aangepast te worden naar O2Auth en de bijkomende invulvelden zoals URL en passwoord ingevuld te worden. Eens dit gedaan is voeg je een Sync uit en komt er een login prompt waar de gebruiker zich moet aanmelden met zijn Soudal account.

Eens de login succesvol is, gaat Resco zichzelf synchroniseren en daarna zou het probleem verholpen moeten zijn.

5.2 Wachtwoord reset:

Wegens veiligheidsredenen moeten alle medewerkers van Soudal hun wachtwoord verplicht om de 3 maanden wijzigen. Dit proces heb ik meermaals begeleid.



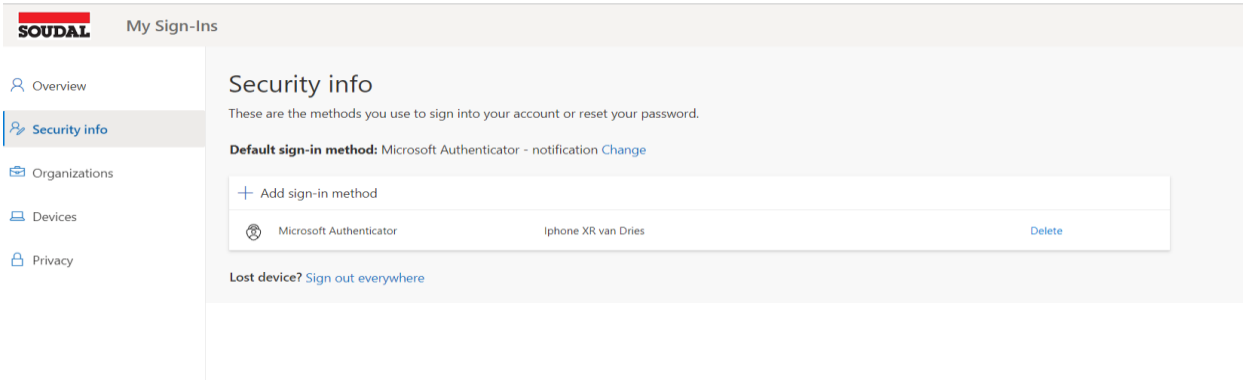
Afbeelding 31: myaccount.microsoft.com overview

Via myaccount.microsoft.com kan je het wachtwoord wijzigen. Door dit te doen log je automatisch uit bij de huidige Office365 sessies die nog openstaan. Hierbij dien je vervolgens opnieuw in te loggen met het nieuwe wachtwoord.

5.3 MFA configureren:

Het gebruiken van MFA is een vereiste bij Soudal. De eindgebruiker is vrij in de keuze hiervoor. Dit kan ofwel via de Microsoft Authenticator app of via een code die je verkrijgt per SMS.

Dit proces heb ik ook ondersteund bij diverse medewerkers. Via aka.ms/mfasetup kom je op het nodige scherm terecht om dit in te stellen.



Afbeelding 32: aka.ms/mfasetup instellen van MFA-methode

5.4 Accounts unlocken:

Wanneer een gebruiker meermaals zijn wachtwoord foutief ingeeft, kan het zijn dat zijn account tijdelijk geblokkeerd gaat worden. Dit probleem kan verholpen worden door de gebruiker te zoeken in AD en handmatig te gaan unlocken. Eventuele wachtwoord resets kunnen hier ook uitgevoerd worden als de gebruiker zijn wachtwoord vergeten is.

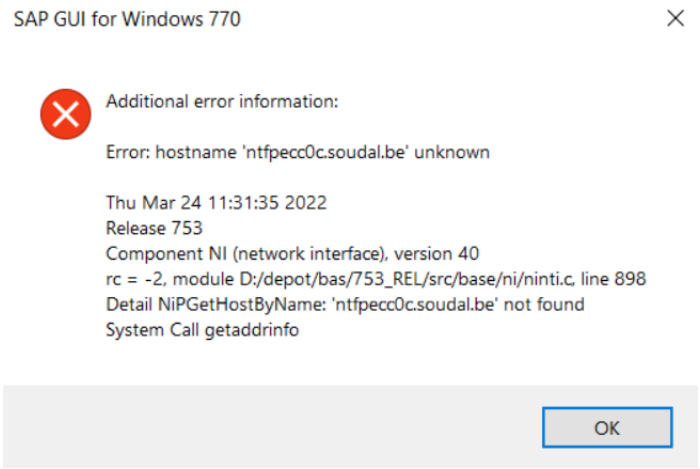
5.5 Verbinden met de Forticlient:

De Forticlient VPN wordt gebruikt wanneer iemand van thuis uit met het Soudal netwerk wilt verbinden. Dit is handig als je toegang wilt krijgen tot resources die enkel via het netwerk ter beschikking worden gesteld.

Het verbinden hiernaar kan soms lastig zijn bij mensen die niet al te technisch zijn aangelegd. Hierover geef ik dan info over de handelingen die voltooid dienen te worden.

5.6 System Analysis Program Development (SAP) error:

SAP is kortweg software voor het managen van bedrijfsprocessen. Hier heb ik meermaals te maken gekregen met medewerkers die onderstaande error kregen. Aangezien ik geen achterliggende kennis heb van SAP, heb ik dit nagevraagd bij een helpdesk medewerker.



Afbeelding 33: foutmelding in SAP

Door naar %AppData% te gaan, zie je de folder SAP staan. Als je deze folder opent en doorgaat naar de folder ‘common’ dien je daar 2 xml-files te overschrijven. Namelijk de SAPUILandscapeGlobal.xml en SAPUILandscape.xml.

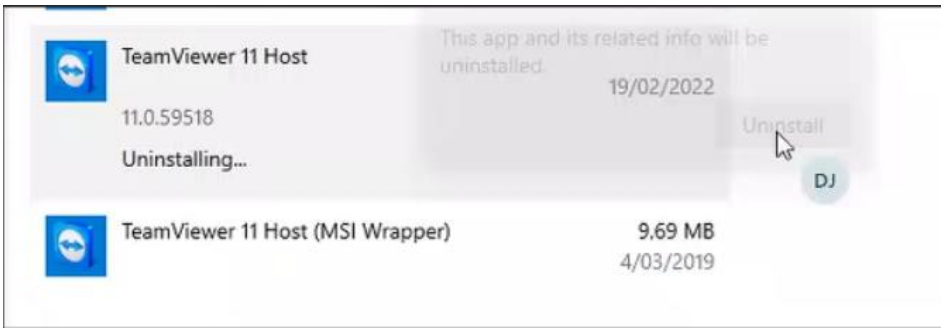
5.7 Teamviewer versie verwijderen:

Er is een periode geweest dat Teamviewer bij enkele personen elke ochtend opnieuw geïnstalleerd werd bij het opstarten van het device.

Dit had te maken met het feit dat er 2 versies van Teamviewer op het device stonden en via Intune ook nog eens de laatste nieuwe versie van Teamviewer gepushed werd.

Door het handmatig verwijderen van de 2 versies die op het toestel stonden was het probleem opgelost. Intune kon zo ook succesvol de laatste nieuwe versie automatisch installeren op het device.

Onderstaande afbeelding toont een voorbeeld waarbij er 2 versies van Teamviewer aanwezig zijn op het device.



Afbeelding 34: Meerdere versies van Teamviewer

6 BRONVERMELDING

Catrinescu, V. (2021, juli 15). *Microsoft Azure Fundamentals*. Retrieved from pluralsight: https://www.pluralsight.com/

Download Windows 10. (2022). Retrieved from Microsoft: https://www.microsoft.com/nl-nl/software-download/windows10

Hallez, A. (2022, februari 14). *Wat is offboarding?* Retrieved from Liantis: https://blog.liantis.be/nl/personeelsbeleid/wat-is-offboarding

Huculak, M. (2022). *The difference between Windows 10 'feature updates' and 'quality updates*. Retrieved from windowscentral: https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

Jones, T. (2018, september 20). *INTUNE CLIENT-SIDE LOGS IN WINDOWS 10*. Retrieved from smsagent.blog: https://smsagent.blog/2018/09/20/intune-client-side-logs-in-windows-10/

Kumar, J. (2021, maart 30). *Windows 10 Feature Update Intune Report | Endpoint Manager*. Retrieved from howtomanagedevices: https://howtomanagedevices.com/intune/5280/windows-10-feature-update-intune-report-endpoint-manager/

List of Microsoft Windows versions. (2022). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/List_of_Microsoft_Windows_versions

Manage BitLocker policy for Windows devices with Intune. (2022, maart 1). Retrieved from Microsoft: https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

Sclater, H. (2021, juli 1). *Exchange hybrid – fixing shared mailboxes that were created as user mailboxes*. Retrieved from cloudrun: https://cloudrun.co.uk/office365/exchange-hybrid-fixing-shared-mailboxes-that-were-created-as-user-mailboxes/

Surksum, K. v. (2021, april 7). *Designing and configuring compliance policies*. Retrieved from vansurksum: https://www.vansurksum.com/2021/04/07/designing-and-configuring-compliance-policies-for-your-windows-modern-workplace-using-microsoft-endpoint-manager/

Woude, P. v. (2020, januari 27). *Working with (custom) detection rules for Win32 apps*. Retrieved from petervanderwoude: https://www.petervanderwoude.nl/post/working-with-custom-detection-rules-for-win32-apps/

7 BESLUIT

Om een antwoord te geven op de vraag: "Is het gelukt bedrijfsdata beter te beveiligen door het toepassen van bedrijfpolicies?", is het antwoord ja. In aantocht van de nieuwe Intune policies die ervoor zorgen dat de toegang tot bedrijfsdata verstrengt gaat worden, is ervoor gezorgd dat bij implementatie hiervan, de devices voldoen aan de Bitlocker voorwaarden en aan de minimum Windows Operating System voorwaardes.

Naast het implementeren van Bitlocker en Windows Updates om compliant te zijn met de nieuwe voorwaardes, dienden er ook nog andere processen uitgevoerd te worden. Zo is er ook voor de migratie van antivirus gezorgd voor alle Co-managed devices van Symantec naar Windows Defender + Defender for Endpoint. Dit was preventief aangezien de licenties voor Symantec gaan verlopen in juni. Om niet zonder virusscanner te komen is hierbij de switch reeds gemaakt.

Als bijkomende opdracht werd er ook nog gezorgd voor het off-boarden van ex-medewerkers. Hierbij werden licenties vrijgemaakt om vervolgens door te geven aan nieuwe werknemers. Dit proces is correct verlopen en er werden voldoende licenties vrijgemaakt. Ook werd hier de off-boarding site opgeschoond waardoor hier nieuwe data op geplaatst kon worden.

Voor Bitlocker is 72% van alle devices succesvol geëncrypteerd met de encryptiemethode AES-256. Dit proces heeft vertraging opgelopen door de diverse problemen die eerder werden verklaart.

De Symantec migraties die in de scope van de opdracht lagen zijn voor 85% voltooid. 9% werd doorverwezen naar de IT-dienst van de betrokken buitenlandse vestigingen. Deze kunnen als klaar beschouwt worden. De overige 6% zijn wellicht devices die onlangs defect zijn geraakt, gebruikers die niet hebben gereageerd enzovoort.

Aan deze percentages zal nog verder gesleuteld worden tijdens mijn vakantiewerk bij Soudal.