Security assessment

M365 <KLANT>

VERSIE 1.0
AUTEUR Arno van Dijk

INHOUD

1. INLEIDING

1.1 ALGEMEEN

<KLANT> heeft RawWorks gevraagd om een security assessment uit te voeren op haar Microsoft 365 omgeving. Omdat dit een heel breed aspect is die ook heel gedetailleerd kan worden geanalyseerd hebben we met betrekking tot dit rapport de onderdelen hoog-over geanalyseerd. De gecontroleerde instellingen zijn gedocumenteerd, deze kunnen zowel een correcte waarde hebben of een waarde die afwijkt van het advies. Wanneer er is afgeweken van het advies, is deze in het hoofdstuk Adviezen (12) opgenomen. Deze adviezen zullen we tijdens de on-site afspraken doornemen en bespreken zodat er bepaald kan worden waarom er is afgeweken van het advies en of deze instellingen aangepast dienen te worden. Wanneer er instellingen aangepast dienen te worden zal er eerst een impact analyse moeten plaatsvinden zodat er bepaald kan worden hoe deze aanpassing doorgevoerd kan worden en of hiervoor een project voor opgestart moet worden. Uiteraard wil RawWorks graag hierbij <KLANT> in ondersteunen.

1.2 CONCLUSIE

Binnen de Cloud omgeving van <KLANT> zijn reeds diverse lagen van beveiliging ingericht. Hieronder vallen onder andere, Self Service Password reset , MFA op basis van Conditional Access en toegang beperken voor niet gemanaged devices. Daarnaast staat het standaard deelbeleid zo ingesteld dat bestaande en nieuwe gasten een verificatie code moeten ingeven bij het benaderen van de bestanden.

<KLANT> kan met betrekking tot security nog een aantal stappen maken. Dit wordt ook getoond in de secure score dit op dit moment onder de 60% zit. In het advies staat er genoemd dat er met enige regelmaat de secure score bijgehouden moet worden, zodat nieuwe aanpassingen van Microsoft geanalyseerd en doorgevoerd kunnen worden. Een aantal adviezen die genoemd worden zullen ook effect hebben op de secure score en andere zijn meer configuratie instellingen. Deze hebben betrekking tot o.a. configuratie van Intune, Conditional Access, delen van bestanden en policies, rules met betrekking tot e-mail beveiliging.

Omdat de aanpassingen effect hebben op de gebruikers ervaring is het aan te bevelen om rekening te houden met deze gebruikers ervaring. Bij gebruik van een te strak beleid m.b.t. beveiliging wordt het werken op de omgeving voor de gebruikers minder aantrekkelijk en kunnen deze de toevlucht zoeken tot 'shadow IT' oplossingen.

Om dit te voorkomen moet goed gekeken worden naar veiligheid versus gebruiksgemak en moeten de medewerkers opgeleid worden in het goed werken met de systemen.

Met betrekking tot het gebruik van het EMSe5 functionaliteiten kan <KLANT> ook stappen maken. Het advies hierin is om samen met RawWorks te kijken naar de specifieke onderdelen om zo nader te bepalen hoe het meeste uit de licentie gehaald kan worden, waarbij <KLANT> ook baat bij heeft, en hiervoor een plan/ advies voor op te stellen om het e.a. te implementeren.

1.3 VERSIEBEHEER

Versie	Status	Datum	Auteur	Opmerkingen
0.1	Concept	21-6-2023	Arno van Dijk	Initiële opzet …
1.0	Definitief	29-06-2023	Arno van Dijk	Opmerkingen n.a.v. review verwerkt.

2. AZURE AD PORTAL

<KLANT> heeft een Microsoft 365 Tenant: **<KLANT>.onmicrosoft.com**. Deze tenant heeft een hybride vorm doormiddel van AAD Connect. Er zijn ongeveer 2200 gebruikers objecten in Azure AD. Er is één domein naam gekoppeld in de tenant: **<KLANT>.nl**

2.1 LICENTIES

<KLANT> heeft de volgende licenties beschikbaar in haar tenant, hier laten we in dit rapport alleen de licenties zien de betrekking hebben op het advies. Licenties zijn gekoppeld aan Licensed based groups, met deze methode krijgt de gebruiker op basis van groep lidmaatschap automatische een licentie toegewezen. Punt van aandacht is, is dat er bij deze methode er wel gemonitord moet worden of er nog licenties beschikbaar zijn.

Licentie	Aantal	Beschikbaar	Licensed groups
Enterprise Mobility + Security E3	28	15	Licentie_office365_E1_EMS
Enterprise Mobility + Security E5	1033	8	Licentie_office365_E3_EMS_E5
Microsoft 365 Business Basic	100	23	Licentie_office365_E1 Licentie_office365_E1_EMS
Microsoft 365 E3	1030	0	Licentie_office365_E3_EMS_E5
Microsoft 365 E5	1	0	None
Microsoft 365 E5 Security	1	1	None

2.2 AAD CONNECT

Met Azure AD connect worden de on-premises gebruikers, groepen, objecten, gesynchroniseerd naar Azure AD. Hiermee kan de gebruiker met hetzelfde account inloggen op de cloud en on-premises diensten: Azure AD Connect is actief en uitgevoerd op twéé servers. Van deze twéé servers is er één actief en één heeft een staging role. Hiermee heeft <KLANT> deze dienst als High available uitgevoerd.

Server	Actief	Versie
xxx	Ja	2.2.1.0 (laatste versie)
xxx	Nee (Staging)	2.1.20 (voorlaatste versie)

De volgende instellingen zijn actief:

Instelling	Status	Advies
Password Hash Sync	Enabled	Huidige instelling behouden, deze staat correct
Seamless Single sign-on	Enabled	Huidige instelling behouden, deze staat correct

2.3 SELF SERVICE PASSWORD RESET

Met self service password reset (SSPR) kan de eindgebruikers zijn/ haar wachtwoord resetten. Tevens wordt dit wachtwoord teruggeschreven naar de on-premisse omgeving, zodat er daar met hetzelfde wachtwoord ingelogd kan worden. Opgeven gebruikers kunnen gebruik maken van de deze dienst. Bij een login dient de gebruiker zijn/ haar gegevens op te geven voor een SSPR, authenticatie methodes dienen na 180 dagen opnieuw geverifieerd te worden. Doormiddel van customization is de default aangepast.

2.3.1 PROPERTIES

Volgende instelling is actief

Instelling	Status	Advies
Self service password reset enabled	Selected (MFA_O365)	Groep heeft als leden licentie groepen, deze licentie groepen zijn statisch, deze kunnen aangepast worden naar dynamische groep.

2.3.2 AUTHENTICATION METHODS

Volgende instelling is actief

Instelling	Status	Advies
Number of methods required to reset	1	Pas deze aan naar 2 zodat er een privé mail en telefoon nodig is voor het resetten van een wachtwoord

2.3.3 REGISTRATION

Volgende instelling is actief

Instelling	Status	Advies
Require user to register when signing in	Yes	Huidige instelling behouden, deze staat correct
Number of days before…	180	Huidige instelling behouden, deze staat correct

2.3.4 NOTIFICATIONS

Volgende instelling is actief

Instelling	Status	Advies
Notify users on password resets	Yes	Huidige instelling behouden, deze staat correct

Notify all admins when other admins reset their password?	Yes	Huidige instelling behouden, deze staat correct

2.3.5 ADMINISTRATOR POLICY

Volgende instelling is actief

Instelling	Status	Advies
Is self-service password reset enabled?	Yes	Huidige instelling behouden, deze staat correct
Number of methods required to reset:	2	Huidige instelling behouden, deze staat correct

2.4 RECHTEN

In de Microsoft cloud omgeving kan er gebruik worden gemaakt van Global administrators, deze groep heeft alle rechten op alle onderdelen. Om de personen alleen toegang en rechten te geven op de onderdelen die zij moeten beheren kan er gebruik worden gemaakt van de Role Based Access Control (RBAC). Daarnaast heeft Microsoft ook de mogelijkheid om gebruik te maken van Privileged identity management (PIM) Hiermee kunnen er "tijdelijk" rechten toegekend worden aan beheerders wanneer deze nodig zijn. PIM heeft Azure AD P2 nodig, met de huidige EMSe5 licentie heeft <KLANT> de mogelijkheid om PIM in te richten.

2.4.1 GLOBAL ADMINISTRATORS

Er zijn acht personen lid van de Global administrators groep. Dit zijn gebruikersaccounts en services account. Advies in deze is om het aantal te verlagen en gebruik te maken van Role Based Access Control en PIM. De huidige services accounts hebben wellicht ook te veel rechten. Advies hierin is om te onderzoeken welke rechten deze accounts minimaal nodig hebben

Huidige instelling	Advies
Global administrators heeft 8 leden	Deze verlagen en meer gebruik maken van RBAC en PIM. Services accounts onderzoeken welke rechten deze minimaal nodig hebben

2.4.2 ROLE BASED ACCESS CONTROL

Er wordt gebruikt gemaakt van Role Bases Access Control, op deze wijze krijgen gebruikers niet te veel rechten. Dit past geheel in het advies van Microsoft, er is kort gekeken naar een aantal groepen en haar lidmaatschap. Dit zijn allemaal directe rechten

Huidige instelling	Advies
Exchange administrators	Huidige rol heeft 2 leden
Teams Administrators	Huidige rol heeft 3 leden
Global Reader	Huidige rol heeft 3 leden
Helpdesk Administrator	Huidige rol heeft 4 leden
SharePoint Administrator	Huidige rol heeft 4 leden
Password Administrator	Huidige rol heeft 1 lid

2.4.3 PRIVILEGED IDENTITY MANAGEMENT

In de omgeving van <KLANT> (lijkt) PIM niet actief te zijn, er zijn geen groepen gekoppeld. Omdat er veel met RBAC rollen en Global Administrators gewerkt wordt is het advies om gebruik te gaan maken van PIM zodat het toewijzen van de rechten gebeurt op aanvraag. Hiermee heeft <KLANT> inzicht en controle over de rechten en zullen deze naar een x periode verlopen.

2.5 COMPANY BRANDING

Met de company branding kan de default tenant login pagina aangepast worden naar een eigen template. Wanneer hier gebruik van wordt gemaakt krijgen de gebruikers een bekendere organisatie thema te zien en zal deze ook moeilijker te kopiëren zijn voor malafide logins

Instelling	Status	Advies
Company branding is aangepast	Actief	Huidige instelling behouden, deze staat correct

2.6 USER SETTINGS

De volgende user settings zijn actief in de Azure Portal

2.6.1 DEFAULT USER ROLE PERMISSIONS

Instelling	Status	Advies
Users can register applications	No	Huidige instelling behouden, deze staat correct
Restrict non-admin users from creating tenants	Yes	Huidige instelling behouden, deze staat correct
Users can create security groups	Yes	Pas deze aan naar NO als hier niet de behoefte voor is:

2.6.2 GUEST USER ACCESS

Instelling	Status	Advies
Guest user access restrictions	Guest users have limited	Huidige instelling behouden, deze staat correct

	access to properties and memberships of directory objects	

2.6.3 ADMINISTRATION PORTAL

Instelling	Status	Advies
Restrict access to Azure AD administration portal	Yes	Huidige instelling behouden, deze staat correct

2.6.4 SHOW KEEP USER SIGNED IN

Instelling	Status	Advies
Show keep user signed in	No	Huidige instelling behouden, deze staat correct

2.7 USER SETTINGS - EXTERNAL COLLABORATION SETTINGS

2.7.1 GUEST USERS ACCESS

Instelling	Status	Advies
Guest user access restrictions	Guest users have limited access to properties and memberships of directory objects	Huidige instelling behouden, deze staat correct

2.7.2 GUEST INVITE SETTINGS

Instelling	Status	Advies
Guest invite restrictions	Anyone in the organization can invite guest users including guests and non-admins (most inclusive)	Pas aan naar: Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

2.8 ENTERPRISE APPLICATIONS – CONSENT AND PERMISSIONS

2.8.1 USER CONSENT SETTING

Instelling	Status	Advies
User consent for applications	Do not allow user consent	Huidige instelling behouden, deze staat correct

3. OFFICE 365 ADMIN CENTER – ORG SETTINGS – SERVICES

In het Office 365 Admin center, zijn de volgende instellingen actief in de org settings. Org settings zijn de instellingen die geldig zijn over de hele tenant.

3.1 MICROSOFT ON THE WEB

Instelling	Status	Advies
Let users open files stored in third-party storage services in Microsoft 365 on the web	Off	Huidige instelling behouden, deze staat correct

3.1 TEAMS

De volgende instellingen zijn actief met betrekking tot Teams.
Teams wordt geactiveerd voor gebruikers met alle licenties. Gast toegang is geactiveerd.

Instelling	Status	Advies
Turn on Teams for all **users**	On	Huidige instelling behouden, deze staat correct
Allow guest access in Teams	On	Huidige instelling behouden, deze staat correct

3.2 MODERN AUTHENTICATION

Instelling	Status	Advies
Turn on modern authentication for Outlook 2013 for Windows and later	On	Huidige instelling behouden, deze staat correct
Authenticated SMTP	On	Huidige instelling behouden, deze staat correct

3.3 SHAREPOINT

De volgende instellingen zijn actief met betrekking tot het delen binnen SharePoint:
Met de huidige instelling krijgen de gebruiker die die toegang hebben tot een gedeeld bestand toegang zonder extra authenticatie.

Instelling	Status	Advies
Users can share with	New and existing guests – guests must sign in or provide a verification code	Huidige instelling behouden, deze staat correct

3.4 USER CONSENT TO APPS

Instelling	Status	Advies
Let users provide consent when apps request access to your organization's data on their behalf	Off	Huidige instelling behouden, deze staat correct

3.5 USER OWNED APPS AND SERVICES

Instelling	Status	Advies
Let users access the Office store	Off	Huidige instelling behouden, deze staat correct
Let users start trials on behalf of your organization	Off	Huidige instelling behouden, deze staat correct

4. OFFICE 365 ADMIN CENTER – ORG SETTINGS – SECURITY & PRIVACY

4.1 IDLE SESSION TIMEOUT

De volgende instellingen zijn actief met betrekking tot de Idle session time-out: Met deze instellingen worden sessies die niet actief zijn automatisch afgemeld, zo kan er worden voorkomen dat gebruikers die vanaf een niet beheerd apparaat de web portalen per ongeluk open laten staan doormiddel van een automatisch afmelding bij inactiviteit.

Instelling	Status	Advies
Turn on to set the period of inactivity for users to be signed off of Microsoft 365 web apps	Off	Pas aan naar ON

4.2 PASSWORD EXPIRATION POLICY

Instelling	Status	Advies
Set passwords to never expire	Off	Pas aan naar ON

5. SHAREPOINT ADMIN CENTER

In het SharePoint Admin Center zijn de volgende instellingen actief.

5.1 POLICIES – SHARING

De volgende instellingen zijn actief met betrekking tot delen van bestanden.

5.1.1 EXTERNAL SHARING

De huidige Sharing policy staat één niveau onder Most permissieve.

Instelling	Status	Advies
Content can be shared with	New and existing guest	Huidige instelling behouden, deze staat correct

5.1.2 MORE EXTERNAL SHARING SETTINGS

In de More external sharing settings zijn de volgende instellingen actief. Guest access verloopt niet automatisch en gebruikers hoeven niet zichzelf opnieuw te authentiseren na een x aantal dagen.

Instelling	Status	Advies
Guest must sign in using the same account to which sharing invitations are sent	On	Huidige instelling behouden, deze staat correct
Allow guest to share items they don't own	Off	Huidige instelling behouden, deze staat correct
Guest access to a site or OneDrive will expire automatically after his many days	Off	Pas aan naar ON
People who use a verification code must reauthenticate after this many days	Off	Pas aan naar ON

5.1.3 FILE AND FOLDER LINKS

Volgende instellingen met betrekking tot File and folders links zijn actief. De standaard instellingen voor het delen staat op gedefinieerde gebruikers, deze kan je aanpassen naar personen in de organisatie. Hiermee wordt het delen met externen een bewuste keuze.

Instelling	Status	Advies
Choose the type of link....	Specific people (only the	Pas aan naar Only people in your organization

	people the users specifies)	
Choose the permissions that's selected…	Edit	Pas aan naar View

5.2 POLICIES – ACCESS CONTROL

De volgende instellingen zijn actief met betrekking tot toegang controle.

5.2.1 UNMANAGED DEVICE

Met de huidige instelling hebben niet beheerde apparaten volledige toegang tot de desktop, mobiele en webapplicaties. Met deze instelling kan er bedrijfsdata benaderd en gedownload worden op niet beheerde apparaten.

Instelling	Status	Advies
Unmanaged devices	Allow limited, web-only access	Huidige instelling behouden, deze staat correct

5.2.2 IDLE SESSION SIGN-OUT

Zie ook paragraaf 4.1

5.2.3 APPS THAT DON'T USE MODERN AUTHENTICATION

Met de huidige instellingen krijgen applicaties die geen gebruik maken van Modern authenticatie geen toegang. Met de moderne authenticatie kan er meer apparaat gebaseerde restricties opgelegd worden.

Instelling	Status	Advies
Apps that don't use modern authentication	Block access	Huidige instelling behouden, deze staat correct

5.3 SETTINGS

De volgende instellingen zijn actief met betrekking tot de instellingen.

5.3.1 ONEDRIVE – RETENTION

Met de huidige instelling worden bestanden die zijn verwijderd in OneDrive 30 dagen bewaard.

Instelling	Status	Advies
Days to retain a deleted user's OneDrive	30	Huidige instelling behouden, deze staat correct

5.3.2 ONEDRIVE – SYNC

Met de huidige instellingen kunnen gebruikers met hun privé apparaat, die niet gekoppeld is aan het domein van <KLANT> en daarmee ook niet beheerd, een OneDrive synchronisatie opstarten.

Instelling	Status	Advies
Show the Sync Button on the OneDrive website	ON	Huidige instelling behouden, deze staat correct
Allow syncing only on computers joined to specific domains	Off	Pas aan naar On

6. TEAMS ADMIN CENTER

In het Teams admin center zijn de volgende instellingen actief.

6.1 TEAMS SETTINGS

6.1.1 FILES

Met de huidige instellingen is het niet mogelijk om een integratie met Teams te maken met de onderstaande diensten. Huidige instelling is goed, wanneer een dienst niet wordt gebruikt kan deze het beste uitgezet worden.

Instelling	Status	Advies
Citrix files	Off	Huidige instelling behouden, deze staat correct
Dropbox	Off	Huidige instelling behouden, deze staat correct
Box	Off	Huidige instelling behouden, deze staat correct
Google Drive	Off	Huidige instelling behouden, deze staat correct
Egnyte	Off	Huidige instelling behouden, deze staat correct

6.2 USERS - GUEST ACCESS

6.2.1 CALLING

Met de huidige instelling kunnen gast gebruiker gebruik maken van calling functionaliteit.

Instelling	Status	Advies
Make private calls	On	Pas aan naar Off

6.2.2 MESSAGING

Met de huidige instellingen kunnen gast gebruikers een chat verwijderen en kan er gebruik worden gemaakt van Giphy's die volwassen inhoud bevatten.

Instelling	Status	Advies
Delete chat	On	Pas aan naar Off
Giphy content rating	Moderate	Pas aan naar Strict

6.3 USERS - EXTERNAL ACCESS

6.3.1 TEAMS ACCOUNTS NOT MANAGED BY AN ORGANIZATION

Met de huidige instellingen kunnen gebruikers met een privé teams account, dus niet beheerd door een organisatie, contact opnemen met de medewerkers van <KLANT>

Instelling	Status	Advies
External users with Teams accounts not managed by an organization can contact users in my organization	On	Pas aan naar Off

6.4 TEAMS APPS

Teams apps zijn niet geanalyseerd omdat het gebruikersaccount niet de rechten hiervoor heeft.

6.5 MEETINGS - MEETINGS POLICIES

6.5.1 MEETING JOIN & LOBBY

Met de huidige instellingen is het mogelijk dat anoniem gebruikers deel kunnen nemen aan een vergadering. Wanneer er geen gebruik wordt gemaakt van Live Meetings kan deze instellingen het beste aangepast worden zodat alleen uitgenodigde personen kunnen deelnemen.

Instelling	Status	Advies
Anonymous users can join a meeting	On	Pas aan naar Off
Anonymous users and dial-in callers can start a meeting	Off	Huidige instelling behouden, deze staat correct
Who can bypass the lobby	People who were invited	Pas aan naar People in my org
People dialing in can bypass the lobby	Off	Huidige instelling behouden, deze staat correct

6.6 MEETINGS – MEETING SETTINGS

6.6.1 PARTICIPANTS

Zie ook verwijzing 6.5.1

6.6.2 EMAIL INVITATION

Met de huidige instellingen wordt er gebruik gemaakt van de standaard email branding in de uitnodigingen. Om de deelnemers te laten weten dat de uitnodiging vanuit een legitieme omgeving komt kan er gebruik worden gemaakt van de branding van <KLANT>.

Instelling	Status	Advies
Logo URL	BLANK	Pas aan naar <KLANT>
Legal URL	BLANK	Pas aan naar <KLANT>
Help URL	BLANK	Pas aan naar <KLANT>
Footer	BLANK	Pas aan naar <KLANT>

6.7 MESSAGING

6.7.1 MESSAGING POLICIES

Met de huidige instellingen kan er gebruik gemaakt worden van Giphy's die volwassen inhoud bevatten.

Instelling	Status	Advies
Giphy content rating	Moderate	Pas evt. aan naar strict

7. INTUNE

In het Intune admin portaal kunnen er instellingen gemaakt worden die van toepassing zijn op apparaat beheer en beveiliging. Met deze instellingen kan er voorkomen worden dat apparaten onbedoeld compliant zijn en of worden ingeschreven. In combinatie met de Conditional Access regels kan er hiermee voorkomen worden dat Office365 bestanden lokaal op deze apparaten gebruikt kunnen worden.

7.1 COMPLIANCE POLICY SETTINGS

Met de huidige instellingen worden apparaten die geen compliance policy gekoppeld hebben, beschouwd als niet compliant. Deze instelling is goed.

Instelling	Status	Advies
Mark devices with no compliance policy assigned as:	Not Compliant	Huidige instelling behouden, deze staat correct
Compliance status validity period days	120	Pas aan naar de default 30 dagen

7.2 COMPLIANCE POLICIES

Er zijn diverse compliance policies actief, er lijken meerdere compliance policies gekoppeld te zijn aan de apparaten. Microsoft raad aan om compliance policies op user niveau te koppelen i.p.v. device niveau. Bij het koppelen op user niveau wordt toegang gecontroleerd op de gebruiker, bij het toewijzen aan apparaten kan dit problemen en inconsistentie veroorzaken.

7.3 ENROLL DEVICES – ENROLLMENT DEVICE PLATFORM RESTRICTIONS

Met de huidige instelling is het mogelijk dat gebruikers hun persoonlijke apparaten kunnen inschrijven. Op zich is dit niet een verkeerde keuze, maar er dient dan wel een compliance beleid gekoppeld zijn aan een Conditional access regel die bepaald waar de apparaten aan moeten voldoen zodat ook de privé apparaten voldoen aan het beleid.

Instelling	Status	Assigned	Advies
Android	Block personally owned	No	Er is een policy maar deze is niet gekoppeld
Windows	Block personally owned	Yes	Er is een policy deze is gekoppeld maar aan een beperkte groep
MacOS	Block personally owned	No	Er is een policy maar deze is niet gekoppeld

iOS	Block personally owned	No	Er is een policy maar deze is niet gekoppeld

7.4 APP PROTECTION POLICIES

Er zijn MAM policies aangemaakt voor iOS, maar deze niet gekoppeld. Er is geen MAM beleid voor Android. Er zijn Personal devices in gebruik in Intune. Advies is om in ieder geval voor de peronal devices MAM in te richten zodat bedrijfsdata op de privé apparaten beschermd kan worden

7.5 ENCRYPRION REPORT

Uit de encryption report blijkt dat er devices zijn waar encryptie niet actief is. Er is wel een beleid die Bitlocker vereist, maar uit de rapportage blijkt dat deze niet correct wordt doorgevoerd. Het is aan te bevelen om encryptie te forceren door het toepassen van de Bitlocker met specifieke instellingen. Op deze wijze wordt de schrijf encryptie geforceerd vanuit Intune

7.6 ENDPOINT SECURTIY

Niet alle onderdelen vanuit de EndPoint security zijn geconfigureerd of zijn gekoppeld aan een beperkte groep. Met EndPoint security wordt de beveiliging van het apparaat bepaald, deze instellingen zijn ook van toepassen op het Defender for Endpoint console. Het is aan te bevelen om deze instellingen op alle gebruikers / apparaten te forceren zodat er van een en dezelfde configuratie gebruikt gemaakt wordt.

8. MICROSOFT 365 DEFENDER

In de Microsoft Defender portal zijn de instellingen gecontroleerd

8.1 SECURE SCORE

Huidige secure score staat op 58,68%, deze kan opgehoogd worden door te kijken naar de aanbevelingen en deze waar mogelijk door te voeren en of aan te passen

8.2 EMAIL & COLLABORATION - POLICIES & RULES – THREAT POLICIES

8.2.1 ANTI-PHISING

Er is een custom policy aangemaakt: Policy 01, hierin is de impersonation en de bijbehorende acties niet actief.

Instelling	Status	Advies
Domain impersonation protection	Off	Voeg custom domain <KLANT> toe
User impersonation protection	Off	Voeg accounts toe die gevoelig zijn
Mailbox intelligence for impersonations	Off	Pas aan naar On

8.2.2 ANTI-SPAM

Er is een custom policy aangemaakt voor intakte@<KLANT>.nl, verder zijn de default policies actief.
In de connection filter zijn de volgende IP-adressen opgenomen in de IP-allow list:

- xxx.xxx.xxx.xx
- x.xxx.xx.xxx/xx
- xx.xxx.x.xxx
- xxx.xx.xxx.xxx
- xx.xxx.xx.xxx

In de outbound policy zijn geen limieten opgenomen, forwarding is gedisabeld

Instelling	Status	Advies
Automatic forwarding	Off	Huidige instelling behouden, deze staat correct

8.2.3 ANTI-MALWARE

De default policy is aangepast en is actief

8.2.4 SAFE ATTACHMENTS

Er zijn twee Safe attachments policies. De default built-in protection is de basis Built-in.

8.2.5 SAFE LINKS

Naast de default is er een custom policy aangemaakt deze is actief op alle domeinen en op een aantal users. Teams en Office 365 apps worden meegenomen in de safelinks

Instelling	Status	Advies
Teams	On	Huidige instelling behouden, deze staat correct
Office 365 Apps	On	Huidige instelling behouden, deze staat correct

8.3 CLOUD APPS SETTINGS

8.3.1 APP CONNECTORS

In de settings zijn de volgende app connectors aanwezig

Instelling	Status	Advies
Microsoft 365	Connected	Huidige instelling behouden, deze staat correct
Microsoft Azure	Connected	Huidige instelling behouden, deze staat correct

8.3.2 INFORMATION PROTECTION FILES

File monitoring staat aan

Instelling	Status	Advies
Enable file monitoring	Enabled	Huidige instelling behouden, deze staat correct

8.3.3 MICROSOFT DEFENDER FOR ENDPOINT

De integratie met Defender for EndPoint staat aan:

Instelling	Status	Advies
Enforce app access	Enabled	Huidige instelling behouden, deze staat correct
Alerts	Informational	

8.3.4 MAIL SETTINGS

Mail settings zijn niet aangepast van de default, hier kan een organisatie template gebruikt worden

Instelling	Status	Advies
Enforce app access	Enabled	Huidige instelling behouden, deze staat correct

8.3.5 MICROSOFT 365 DEFENDER MAIL NOTIFICATIONS

Er zijn geen incidents, actions, threat analytics notifications aangemaakt.

Instelling	Status	Advies
Incidents	Niet geconfigureerd	Inventariseer of hier notification aangemaakt moeten worden
Actions	Niet geconfigureerd	Inventariseer of hier notification aangemaakt moeten worden
Threat analytics	Niet geconfigureerd	Inventariseer of hier notification aangemaakt moeten worden

8.3.6 ENDPOINTS

In de setting voor Endpoint zijn de volgende instellingen geanalyseerd:

Instelling	Status	Advies
Automatically resolve alerts	On	Huidige instelling behouden, deze staat correct
Tamper protection	On	Huidige instelling behouden, deze staat correct
Office 365 Threat intelligence connection	On	Huidige instelling behouden, deze staat correct
Microsoft Defender for Cloud Apps	On	Huidige instelling behouden, deze staat correct
Microsoft Intune connection	On	Huidige instelling behouden, deze staat correct
Share endpoint alerts with Microsoft compliance center	Off	Deze kan evt. aangezet worden,

9. COMPLIANCE PURVIEW

9.1 COMPLIANCE SCORE

Huidige compliance score in 75%

9.2 DATA LOSS PREVENTION

Er zijn twee policies actief:

Policy	Order	Status
DLP01 WY	0	On
Standaardbeleid voor preventie van gegevensverlies	1	Test with notifications

Uit de acitity explorer blijkt dat de standaard regel wordt gedetecteerd, deze kan niet verder dan 30 dagen terug en toont in het overzicht maar één gebruiker. De regels staat in een test modus, er wordt dus niks beperkt alleen gemonitord, hiermee wordt er geen data beschermd en kan de gebruiker deze als nog delen buiten de organisatie.

9.3 DATA LIFECYCLE MANAGEMENT

Er zijn geen retentie policies actief, er zijn twee (test) labels aangemaakt. Er zijn geen label policies aangemaakt. Hiermee wordt er geen specifieke data rententie, vanuit de Microsoft cloud oplossing, geregeld.

9.4 INFORMATION PROTECTION

De standaard labels zijn aanwezig, er zijn geen label policies en auto labeling is niet actief. Met name autolabeling is een EMS E5 functionaliteit.

10. PROTECT & SECURE (AAD)

10.1 IDENTITY PROTECION - PROTECT

De user risk policy is niet enabled, deze kan ook d.m.v. een Conditional access policy worden aangemaakt

Policy	Status	Advies
User risk policy	Disabled	Maak een CA regel aan met als Conditional User Risk policy aan dat bij een HIGH conditio MFA en Wachtwoord reset vereist is
Sign-in risk policy	Disabled	Maak een CA regel aan met als Conditional Sign-in risk High & Medium MFA vereist is
Multifactor authentication registration policy	Disabled	Zet deze regel aan om Authenticator als MFA te vereisten i.p.v. sms/ telefoon

10.2 IDENTITY PROTECTION – SETTINGS

Setting	Status	Advies
User at risk detected alerts	Één gebruiker enabled	Zet rapportage aan voor meerdere beheerders, vooral als er regels worden aangemaakt dat het account wordt geblokkeerd
Weekly digest	Enabled, 4 gebruikers	Huidige instelling behouden, deze staat correct

10.3 CONDITIONAL ACCESS

Er zijn twaalf policies actief en twee staan op report only.
De standaard SharePoint Admin center policies worden gebruikt voor het regelen van Web-only toegang voor niet beheerde apparaten

11. EMSE3 VS EMSE5

<KLANT> heeft de vraag gesteld wat de meerwaarde van EMSe5 is t.o.v. EMSe3
In onderstaande tabel worden de verschillen genoemd:

11.1 IDENTITY AND ACCESS MANAGEMENT

Met de EMSe5 Add-on kan er gebruik worden gemaakt van Riskbased conditional access. Momenteel heeft <KLANT> hier een regel voor aan staan die deze monitort. Advies is om gebruik te maken van deze mogelijkheden

Daarnaast kan er gebruik worden gemaakt van Privileged identity management (PIM) hiermee worden er rechten toegekend op aanvraag i.p.v. dat deze rechten continu beschikbaar zijn.

Identity and access management		
Simplified access management and security	✓	✓
Multi-factor authentication	✓	✓
Conditional access	✓	✓
Advanced security reporting	✓	✓
Windows Server Client Access License (CAL)[**]	✓	✓
Risk-based conditional access		✓
Privileged identity management		✓

11.2 ENDPOINT MANAGEMENT

Binnen EndPoint Management zit er geen verschil tussen de EMSe3 en EMSe5

Endpoint management		
Mobile application management	✓	✓
Advanced Microsoft 365 data protection	✓	✓
Integrated PC management	✓	✓
Integrated on-premises management	✓	✓

11.3 INFORMATION PROTECTION

Binnen de Information protection heeft de EMSe5 de mogelijkheid voor intelligent data classifaction and labeling. Hiermee hoeven eindgebruikers niet meer zelf een label toekennen, maar wordt deze automatisch toegekend. <KLANT> heeft nog geen label policies actief. Advies is om te kijken hoe Information protection geïmplementeerd kan worden binnen <KLANT> en om dan gebruik te maken van het automatisch labelen

Persistent data protection	✓	✓
Document tracking and revocation	✓	✓
Encryption key management per regulatory needs	✓	✓
Intelligent data classification and labeling		✓

11.4 IDENTITY DRIVEN SECURITY

Binnen de Identity driven security heeft de EMSe5 de mogelijkheid voor het toepassen van Defender for cloud apps en Defender for Identity. <KLANT> heeft een aantal onderdelen geactiveerd. Advies in om nader te gaan bepalen hoe er meer uit deze mogelijkheden gehaald kan worden, zodat de meerwaarde van de EMSe5 wordt benut.

Identity-driven security		
Microsoft Advanced Threat Analytics[2]	✓	✓
Microsoft Defender for Cloud Apps		✓
Microsoft Defender for Identity		✓

12. ADVIEZEN

In dit hoofdstuk zullen de adviezen verder uitgewerkt worden. Deze kunnen tijdens de on-site dagen doorgenomen en besproken worden. Hierin is een onderscheid gemaakt per portaal. Tevens wordt het gebruik van de huidige EMSe5 licentie ten op zichtte van de EMSe3 toegelicht.

12.1 EMSE5

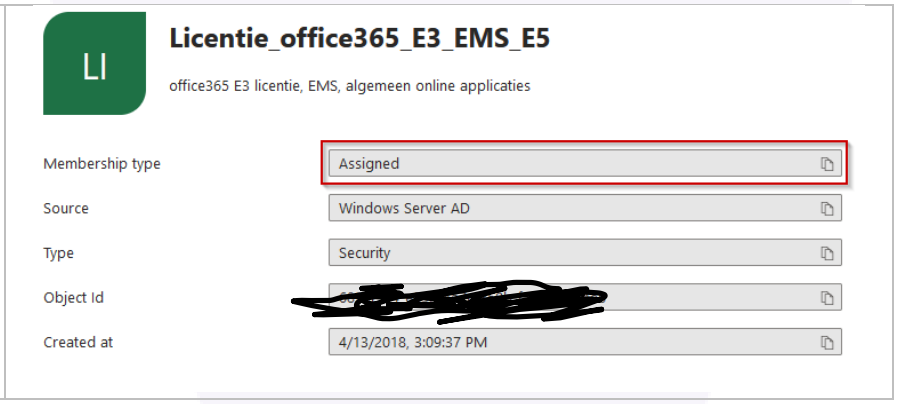
Vanuit de licentie mogelijkheden van EMSe5 wordt niet alles optimaal benut. <KLANT> heeft al wel een aantal zaken voor deel geconfigureerd. Advies hierin is om samen met <KLANT> te kijken of onderstaande functionaliteiten beter benut kunnen worden en te bepalen wat een inrichtingsplan hiervoor zou kunnen zijn. Een aantal onderdelen van de opsomming die hieronder is genoemd zijn ook separaat benoemd, maar globaal zijn er de volgende hoofd activiteiten die betrekking hebben tot het optimaal benutten van de EMSe5 licentie.

- Privileged Identity Management (PIM)
- Riskbased conditional access
- Inrichting Information Protection en AutoLabeling
- Defender for Cloud apps
- Defender for Identity

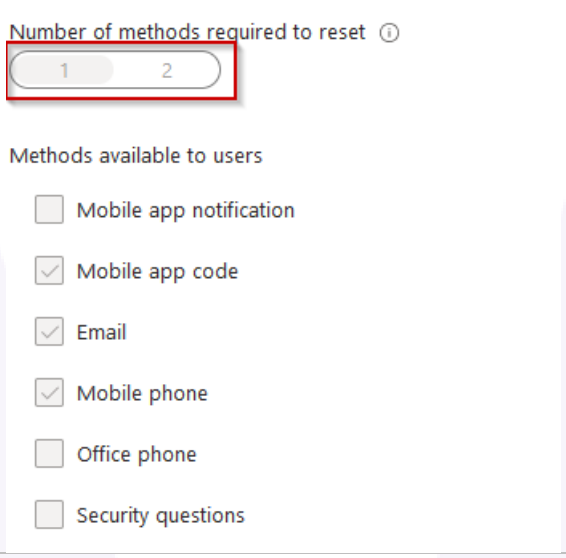
12.2 ADVIEZEN MET BETREKKING TOT HET AZURE PORTAAL

Volgende instellingen wijken af van het advies en kunnen aangepast worden:

12.2.1 SSPR GROEPLIDMAATSCHAP

Advies: Pas instelling groep lidmaatschap aan naar dynamische lidmaatschap op basis van de licentie.	

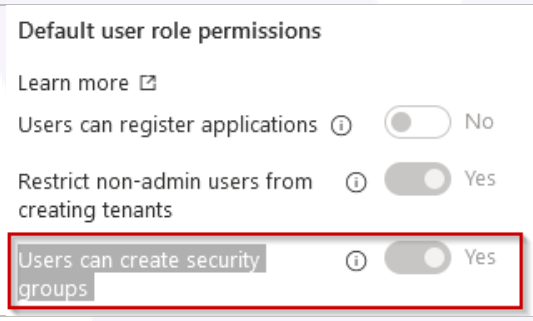
12.2.2 SSPR AUTHENTICATION METHODS

Advies: Pas instelling aan naar 2 zodat de eindgebruikers minimaal 2 methodes moeten opgeven	

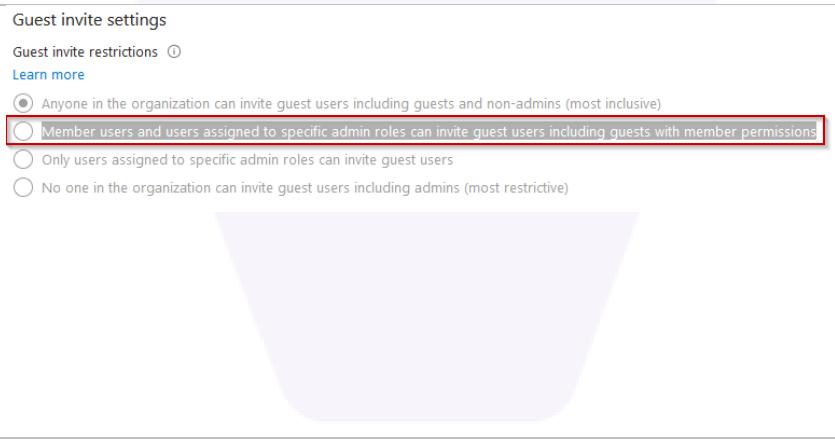
12.2.3 VERLAGEN AANTAL GLOBAL ADMINISTRATORS & PIM

Verminder het aantal global administrator leden en inventariseer de minimale rechten voor de service accounts. Maak gebruik van PIM in combinatie met RBAC rollen.

12.2.4 USER SETTINGS CREATE SECURITY GROEPS

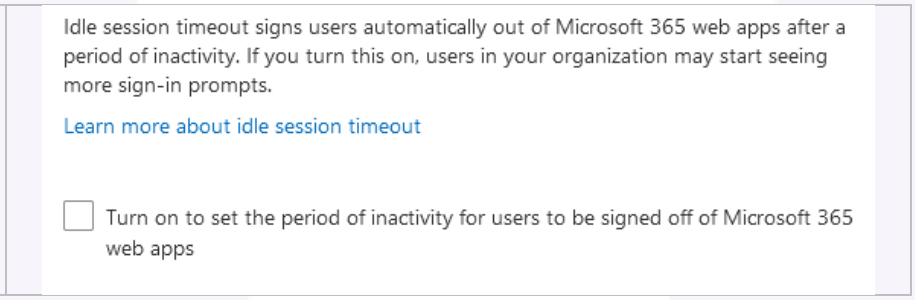
Advies: Pas instelling eventueel aan naar NO als hier geen behoefte aan is.	

12.2.5 GUEST INVITE SETTINGS

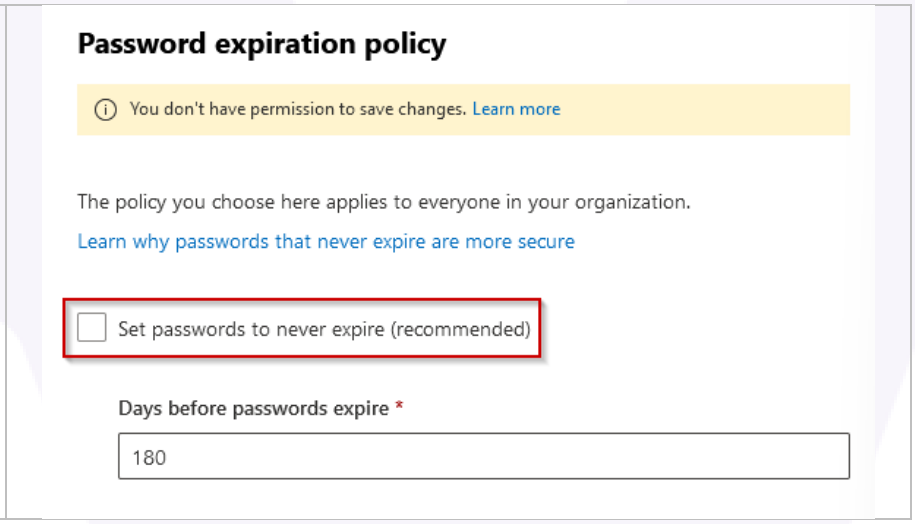
Advies: Pas instelling aan naar Member users and users assigned to specific admin roles can invite guest users including guests with member permissions	

12.3 ADVIES M.B.T. OFFICE 365 ADMIN CENTER – ORG SETTING

12.3.1 IDLE SESSION TIME OUT

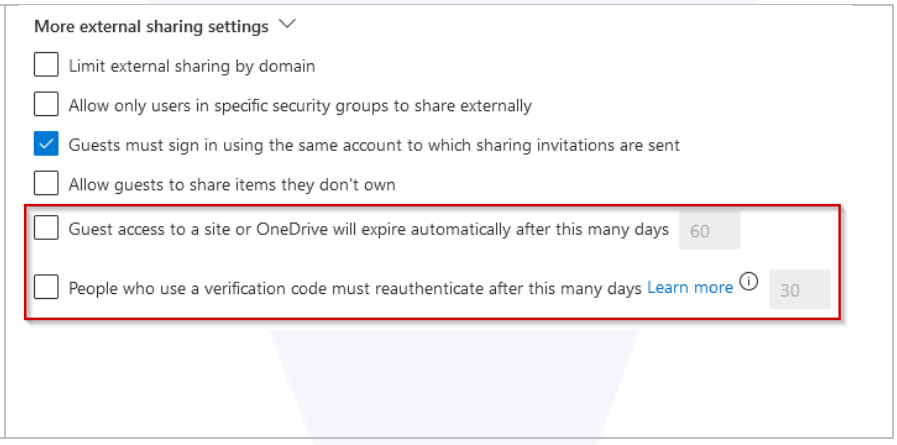
Advies: Zet deze setting aan en specifieer een time out periode voor de Office 365 Web apps	

12.3.2 PASSWORD EXPIRATION POLICY

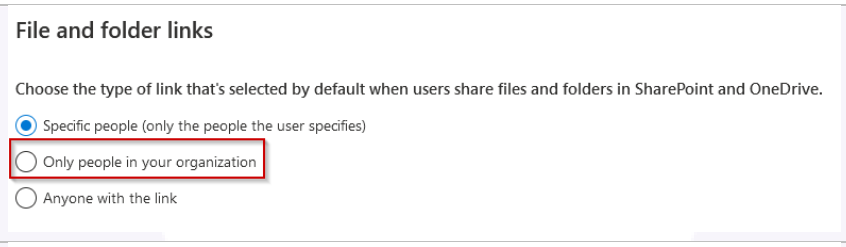
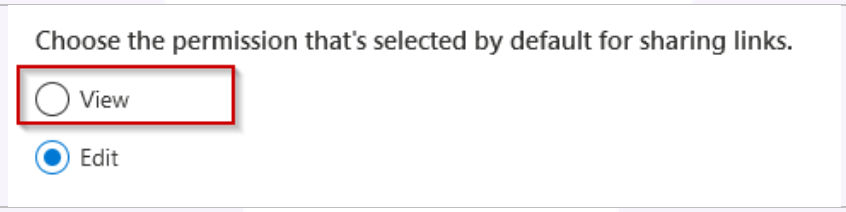
Advies: Zet deze setting aan	

12.4 ADVIES M.B.T. SHAREPOINT ADMIN CENTER

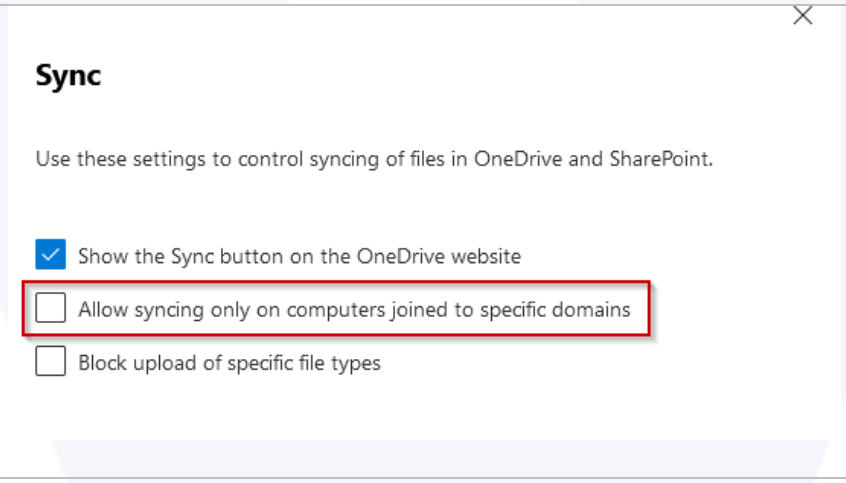
12.4.1 MORE EXTERNAL SHARING SETTINGS

Advies: Pas instelling aan zodat gast toegang automatisch verloopt na een x aantal dagen en dat personen na x aantal dagen opnieuw moeten authentiseren	

12.4.2 FILES AND FOLDERS LINKS

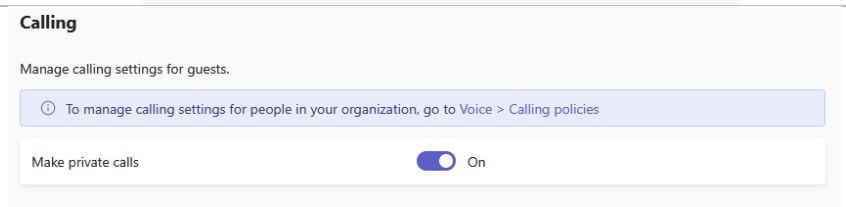
Advies: Pas instelling aan de standaard optie voor delen op interne gebruikers staat	
Pas instelling aan naar View, zodat er niet standaard gewijzigd kan worden.	

12.4.3 ONEDRIVE SYNC

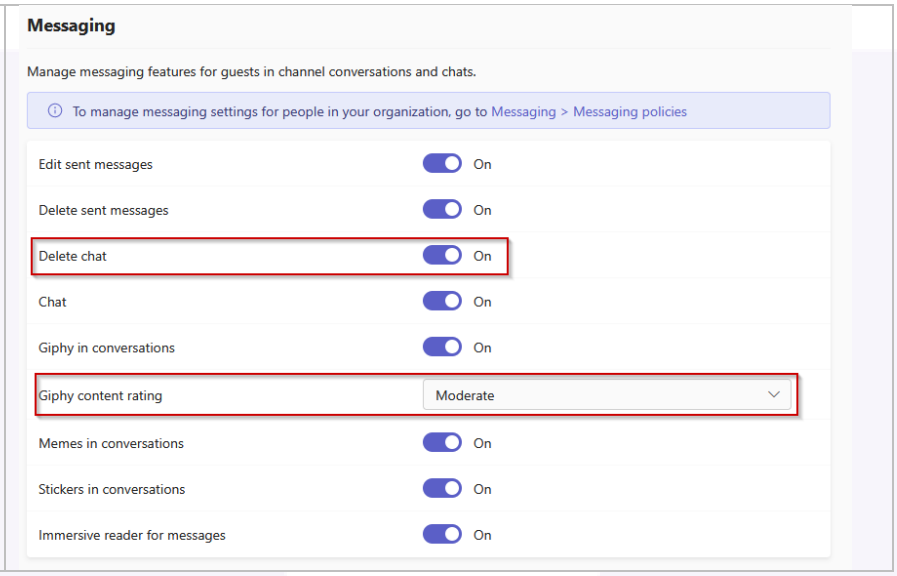
Advies: Pas instelling aan zodat alleen pc's die verbonden zijn aan het interne of Azure AD domein kunnen synchroniseren. Hiermee krijgen niet beheerde apparaten geen toegang.	

12.5 ADVIES M.B.T. TEAMS ADMIN CENTER

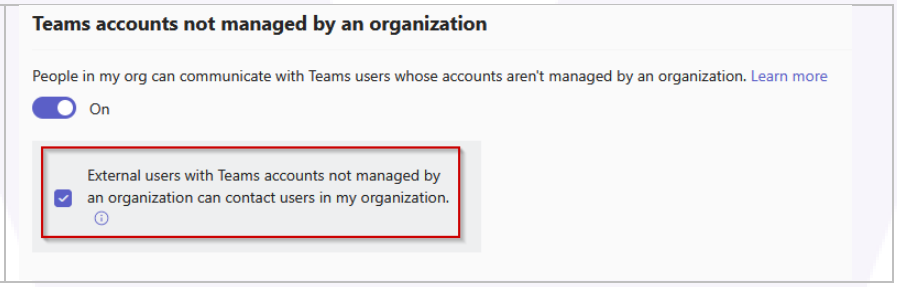
12.5.1 GUEST ACCESS CALLING

Pas instelling aan zodat er gast gebruikers geen private calls kunnen maken	

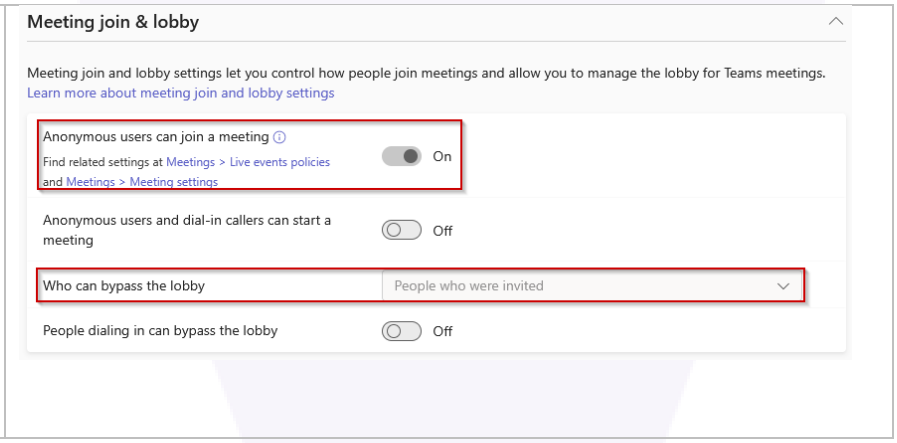
12.5.2 GUEST ACCESS MESSAGING

Pas instelling aan zodat gast gebruikers geen chats kunnen verwijderen en geen volwassen inhoud in giphy kunnen gebruiken	

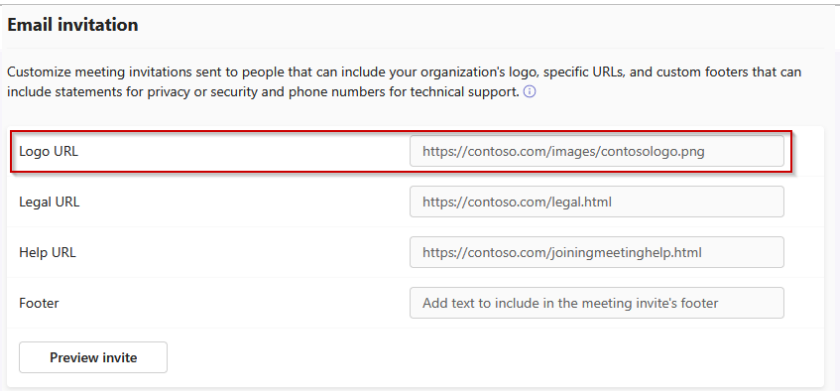
12.5.3 USERS – EXTERNAL ACCESS

Pas instelling aan externe gebruikers die niet vanuit een organisatie komen berichten kunnen sturen naar medewerkers	

12.5.4 MEETING JOIN & LOBBY

Pas instelling aan zodat anonieme gebruikers niet kunnen deelnemen aan een meeting en dat alleen gebruikers in de organisatie de lobby kunnen verlaten	

12.5.5 EMAIL INVITATION

Pas instelling aan zodat de email uitnodiging voor Teams wordt aangepast naar het bedrijf branding	

12.5.6 MESSAGING POLICIES

Pas instelling evt. aan van moderate naar strict	

12.6 ADVIEZEN M.B.T. INTUNE PORTAAL

12.6.1 COMPLIANCE STATUS VALIDITY PERIOD

Pas instelling naar de default van 30 dagen	

12.6.2 COMPLIANCE POLICIES

Advies is om de huidige compliance policies door te lopen en maar één actieve compliance per device te hebben. Maak gebruik van de Microsoft Defender for EndPoint machine score. De compliance policy moeten gekoppeld worden op gebruikers i.p.v. apparaten.

12.6.3 BLOCK PERSONAL DEVICES

In de Intune portaal zijn er wel regels aangemaakt, maar deze zijn niet gekoppeld of aan een beperkte groep. Advies is om persoonlijke apparaten te beperken.

12.6.4 APP PROTECTION POLICIES

Er zijn geen App Protection policies actief, er worden zowel corperate als personal owned apparaten gebruikt advies is om voor de personal owned devices een MAM beleid in te richten.

12.6.5 ENCRYPTION REPORT

Huidige encryption report doorlopen en beleid aanpassen dat Bitlocker vereist is. Advies is om hiervoor een separate policy aan te maken in de endpoint security center.

12.6.6 ENDPOINT SECURITY

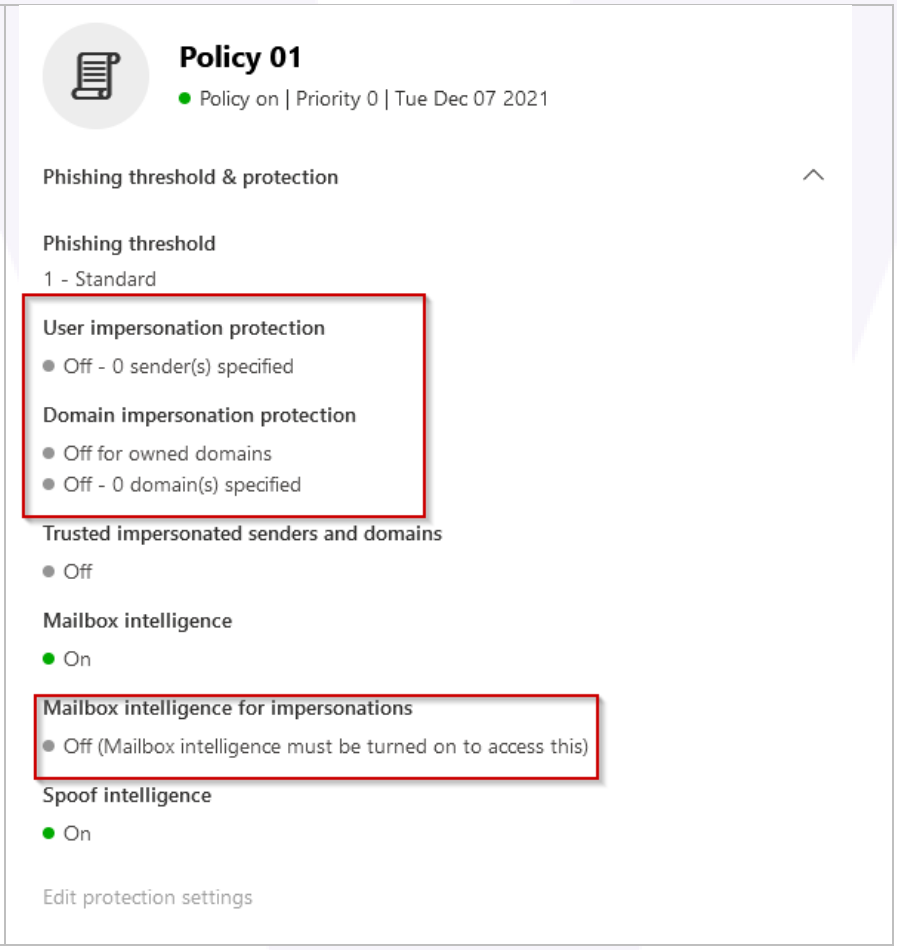
Maak meer policies aan binnen EndPoint security zoals ASR, Bitlocker, Antivirus, met betrekking tot de policies kan RawWorks <KLANT> voorzien van advies vanuit de Baseline

12.7 ADVIEZEN M.B.T. DEFENDER PORTAL

12.7.1 SECURE SCORE

Doorloop met regelmaat de secure score portal en doorloop de adviezen.

12.7.2 ANTI-PHISING

Pas instelling aan zodat er gebruik wordt gemaakt van impersonation	

12.7.3 ANTI-SPAM

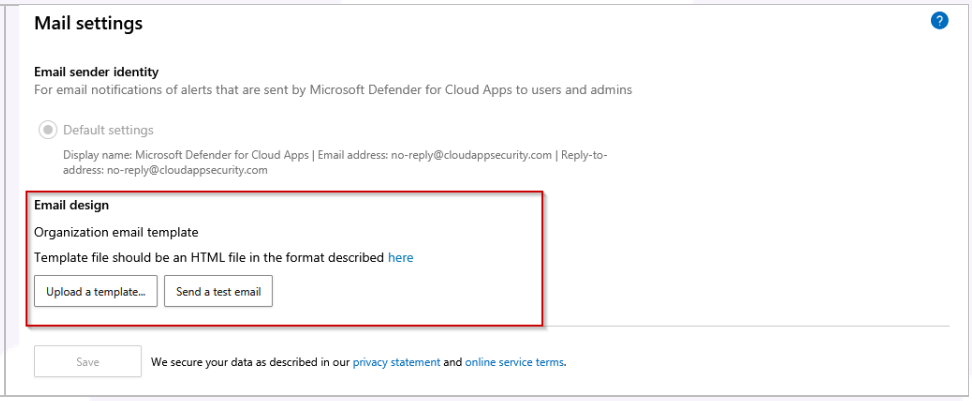
Doorloop de custom en default policy en pas deze aan naar wensen van <KLANT>. Hierin kan de bulk treshhold aangepast worden en evt. bepaalde websites en url redirects aangepast worden.
Controleer de IP allow list in de connection filter en specifieer evt. in de outbound policy een berichten limiet.

12.7.4 SAFE ATTACHMENTS

Policies kunnen aangepast worden van Monitor naar evt. block of dynamic, deze kan op een beperkte groep worden gezet om te kijken of dit een gewenste instelling is.

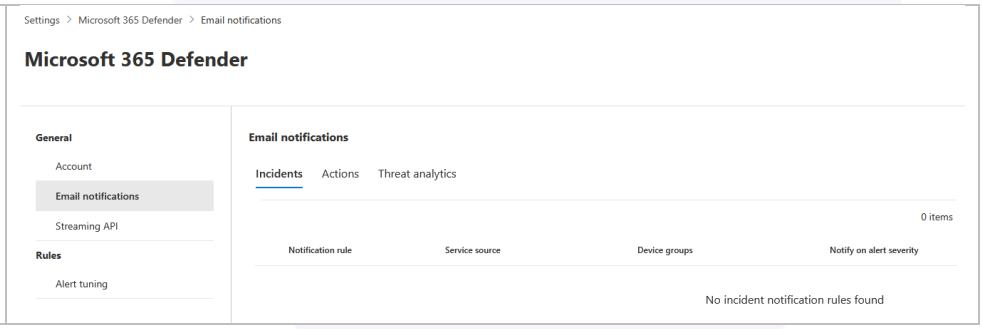
12.7.5 CLOUD APPS - MAIL SETTING

De default template kan aangepast worden naar een organisatie template

Pas instelling aan zodat er gebruik wordt gemaakt van impersonatio n	

12.7.1 SETTINGS - MICROSOFT 365 DEFENDER MAIL NOTIFICATIONS

Er zijn geen notifications aangemaakt, inventariseer of er notifications aangemaakt moeten worden

Pas evt. de notifications naar wens aan	

12.8 ADVIEZEN M.B.T. COMPLIANCE PORTAL

12.8.1 COMPLIANCE SCORE

Doorloop met regelmaat de compliance score portal en doorloop de adviezen.

12.8.2 DLP POLICIES

De standaard policy staat aan in test modus, hierdoor wordt deze alleen gelogd. Maak evt. DLP policy aan:

Maak evt. DLP policies aan	**Standaardbeleid voor preventie van gegevensverlies** **Status** Test with notifications **Description** Met standaardbeleid voor preventie van gegevensverlies worden documenten beveiligd die gevoelige gegevens bevatten, zoals nummers van creditcards en betaalpassen, burgerservicenummers, enzovoort. Beleid wordt gemaakt via het M365-beheercentrum. **Admin units (preview)** None **Locations** Exchange email - All accounts SharePoint sites OneDrive accounts - All accounts **Policy settings** Regel: kleine hoeveelheid gevoelige gegevens gedetecteerd

12.8.3 DATA LIFECYCLE MANAGEMENT

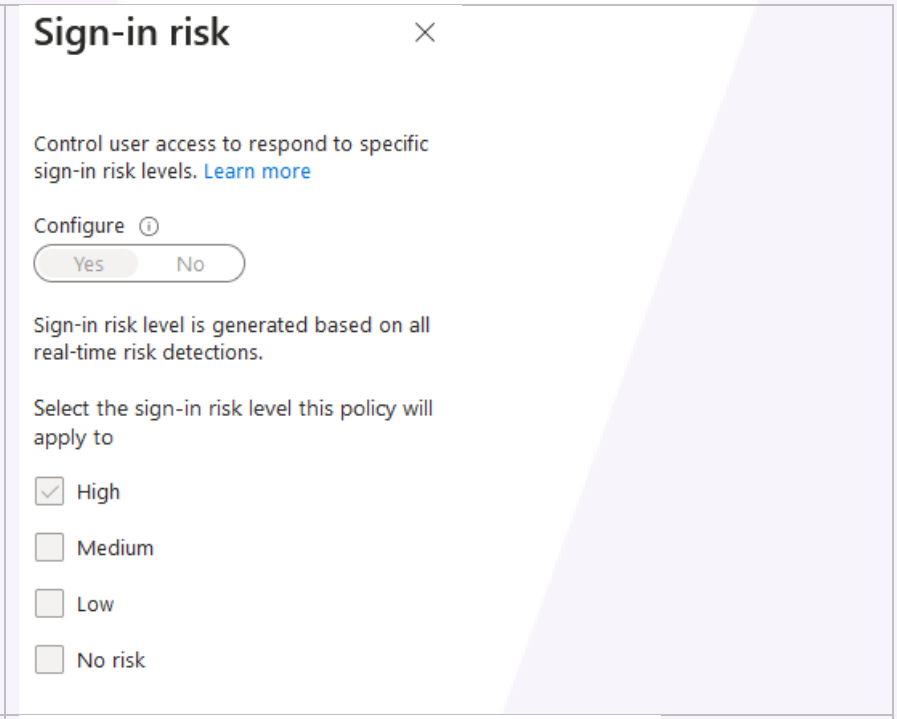
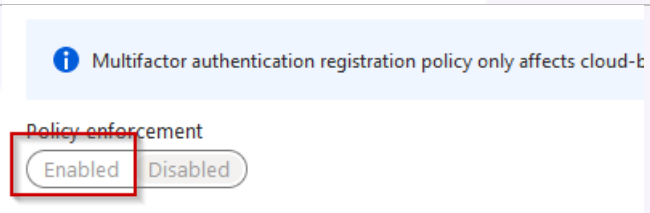
Maak evt. Data lifecycle (Retentie) policies aan om gegevens te bewaren voor een x periode

12.8.4 INFORMATION PROTECTION

Richt information protection in met labels en policies. Met de huidige licentie kan er gebruik worden gemaakt van auto-labeling

12.9 ADVIEZEN M.B.T. PROTECT & SECURE (AAD)

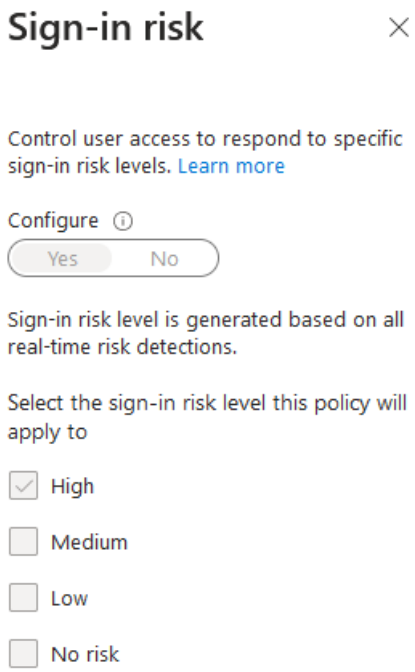
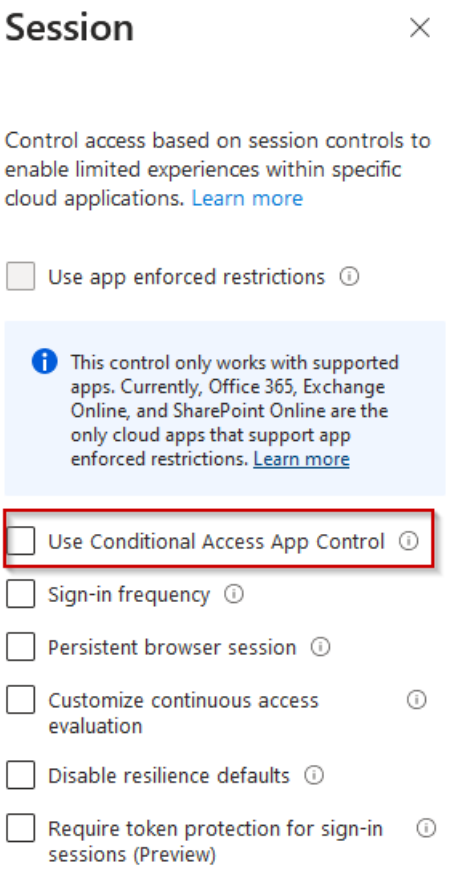
12.9.1 PROTECT

Maak een CA regel voor User Risk en een CA Sign In risk	
Zet de MFA registration policy aan om SMS en telefoon MFA te blokkeren.	

12.9.2 CONDITIONAL ACCESS

Doorloop de huidige conditional access policy en inventariseer of er correct gebruikt wordt gemaakt van MFA ook voor Guest users.
Inventariseer of non-compliant apparaten worden geblokkeerd,

Zet Block legacy authentication aan, maak gebruik van de rapportage om te achterhalen of legacy auth nog wordt gebuikt	

Maak Sign-in en User Risk policies aan	
Maak evt., gebruik van de CA App control in combinatie met de Cloud Apps	 https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

12.10 POWERSHELL COMMANDO'S

12.10.1 SHAREPOINT ONLINE – PREVENT USERS FROM DOWNLOADING MALICIOUS FILES

Controleer instelling of gebruikers malafide bestanden van SharePoint Online downloaden. Onderstaande commando kan gebruikt worden om te voorkomen dat malafide bestanden gedownload kunnen worden.

Huidige instelling	Advies
	NOT LISED

12.10.2 EXCHANGE ONLINE – ADMINAUDITLOGCONFIG

Controleer of de audit log bestanden bijgehouden.

Huidige instelling	Advies
	NOT LISTED

12.10.3 DISABLE SIGN-IN SHARED MAILBOXES

Huidige instelling	Adv(NOT LISEies
	NOT LISTED

12.11 EXCHANGE INBOUND RULE

Er kan een inbound rule aangemaakt worden die externe berichten voorziet van een TAG