15 Security zaken die ‘gratis’ zijn

waar bijna niemand gebruik van maakt

Neal Bongers

Freelance Security Architect @ SecureCraft Solutions

Team Lead IT Security Office @ Tilburg University

Security Assessments

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Gebruikte bronnen

- Centrum for Internet Security (CIS) benchmark
- Microsoft best practices
- Eigen boeren verstand

Disclaimer

Benoemde zaken komen voort uit de eerder genoemde Best Practices. Het hoeft niet zo te zijn dat dit ook de beste oplossing is bij jou of je klant.

Meningen over hoe strikt beveiliging moet worden afgedwongen verschilt per persoon en organisatie waar het op van toepassing is.

Gratis?

Alles via maximaal E3 licenties
Veel ook zonder überhaupt licenties te hebben

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Accounts & Authentication

Sign-in frequency /
Browser sessions

Global
Admins

Block Legacy
AuthN

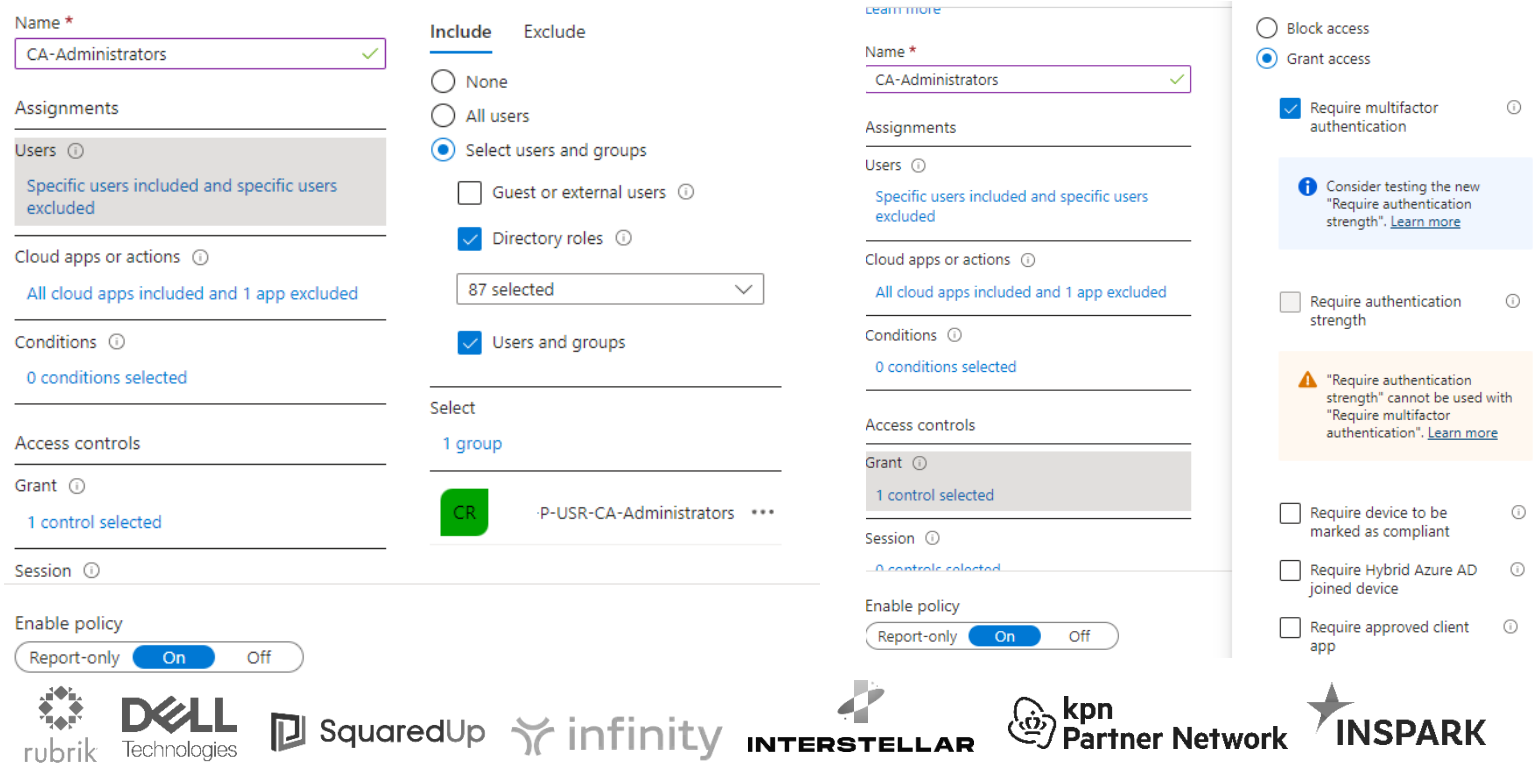
Seperate accounts

MFA & SSPR

MFA & SSPR

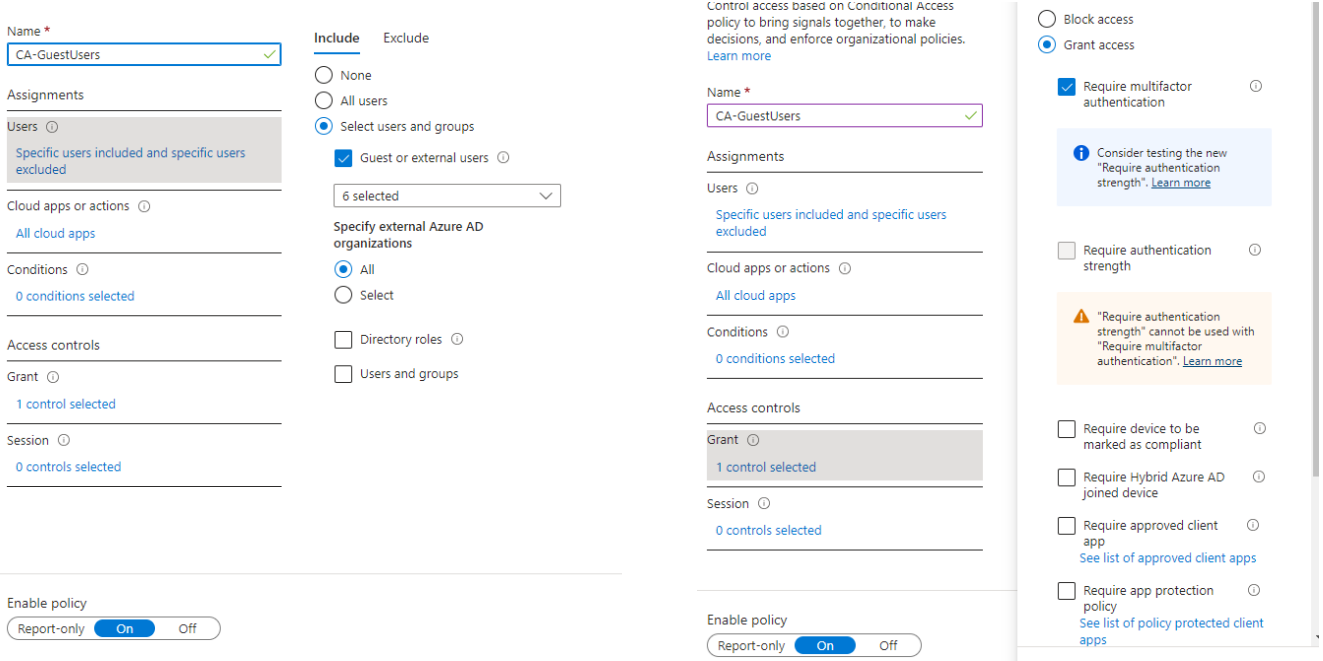
- Begin met de administrators
  - Via Conditional Access
- Uitrollen naar iedereen in je Entra ID, ook je Guests!
  - Via Conditional Access
- Gebruik nieuwe methode (ook voor SSPR)
  - Entra ID -> Protection -> Authentication methods
- Controleer wie het allemaal in gebruik heeft staan
  - Entra ID -> Protection -> Authentication methods -> Activity
- Controleer wie Capable is
  - Entra ID -> Protection -> Authentication methods -> User registration details

Conditional Access - Admin



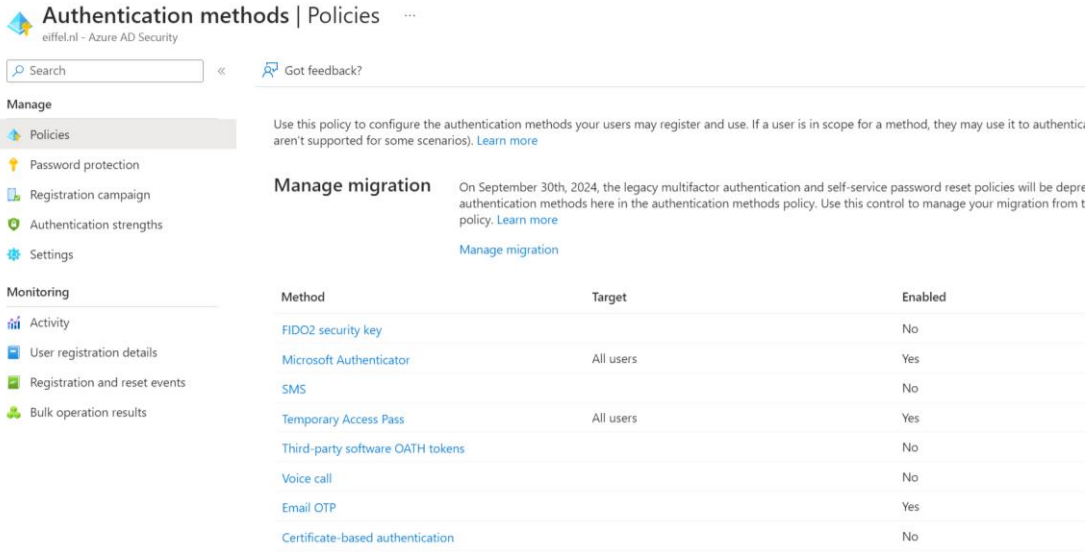
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Conditional Access - Guests



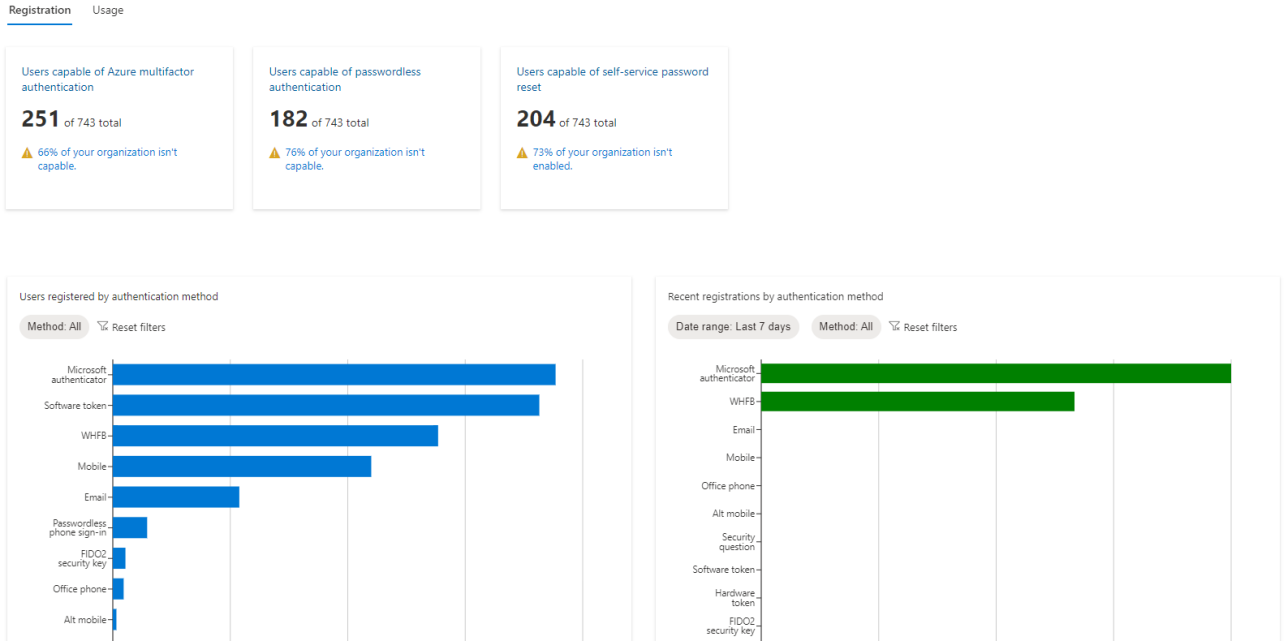
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Nieuwe methodes!



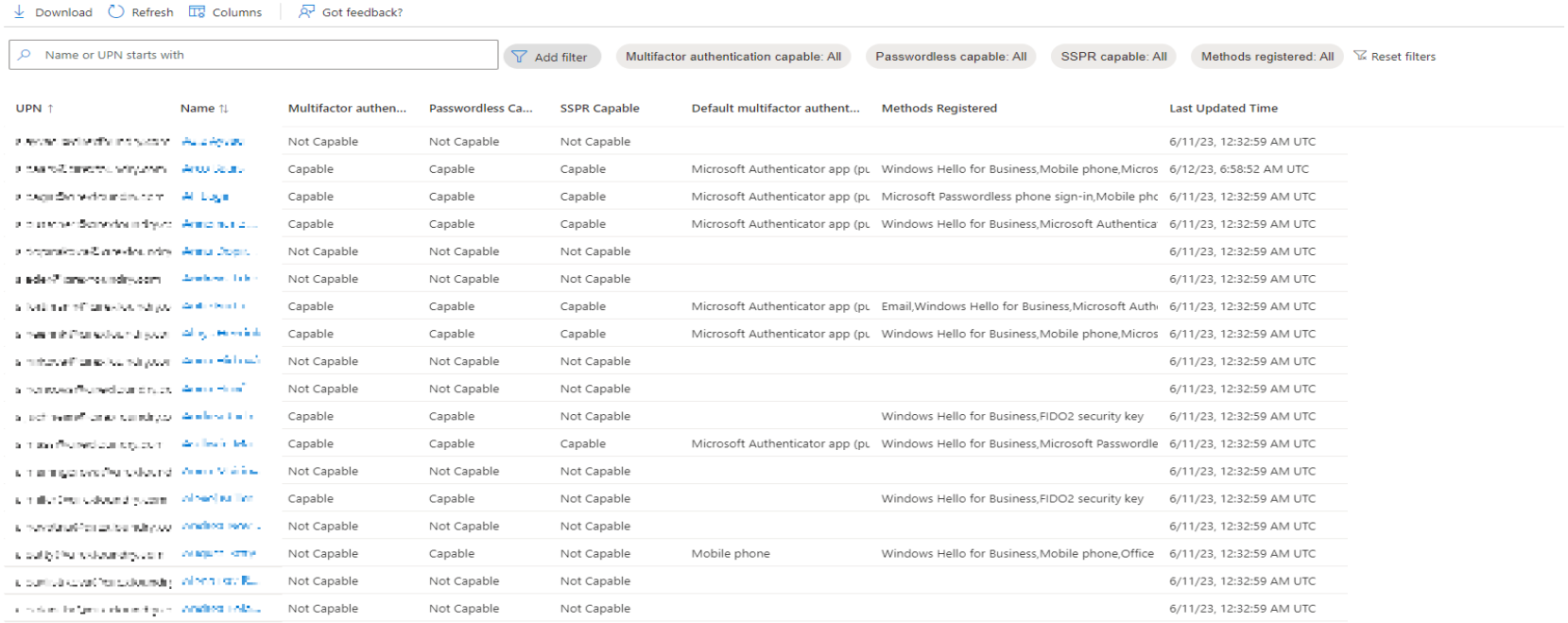
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Authentication methods: Activity



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Authentication methods: User registration details



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Separate admin accounts

- Scheiding van omgevingen
- Meer lagen van beveiliging
- Beveiliging wordt enkel in de cloud toegepast (of on-prem)
- ‘Local’ admin account in de cloud

Teveel Global Admins

- Max 4!
- Andere rollen gebruiken
- Meer controle op gebruik
- PIM gebruiken met toestemming (E5 vereist)

Blokkeer legacy AuthN

- Via Conditional Access
- Ook binnen SharePoint!

Sign-in frequency / browser sessions

- Niet voor gebruikers, maar je administrators
- Global Admin bijvoorbeeld max 4 uur
- Non persistent browsersessies

Application permissions

Data management

Admin consent

External file sharing

Toegang tot data aan Apps

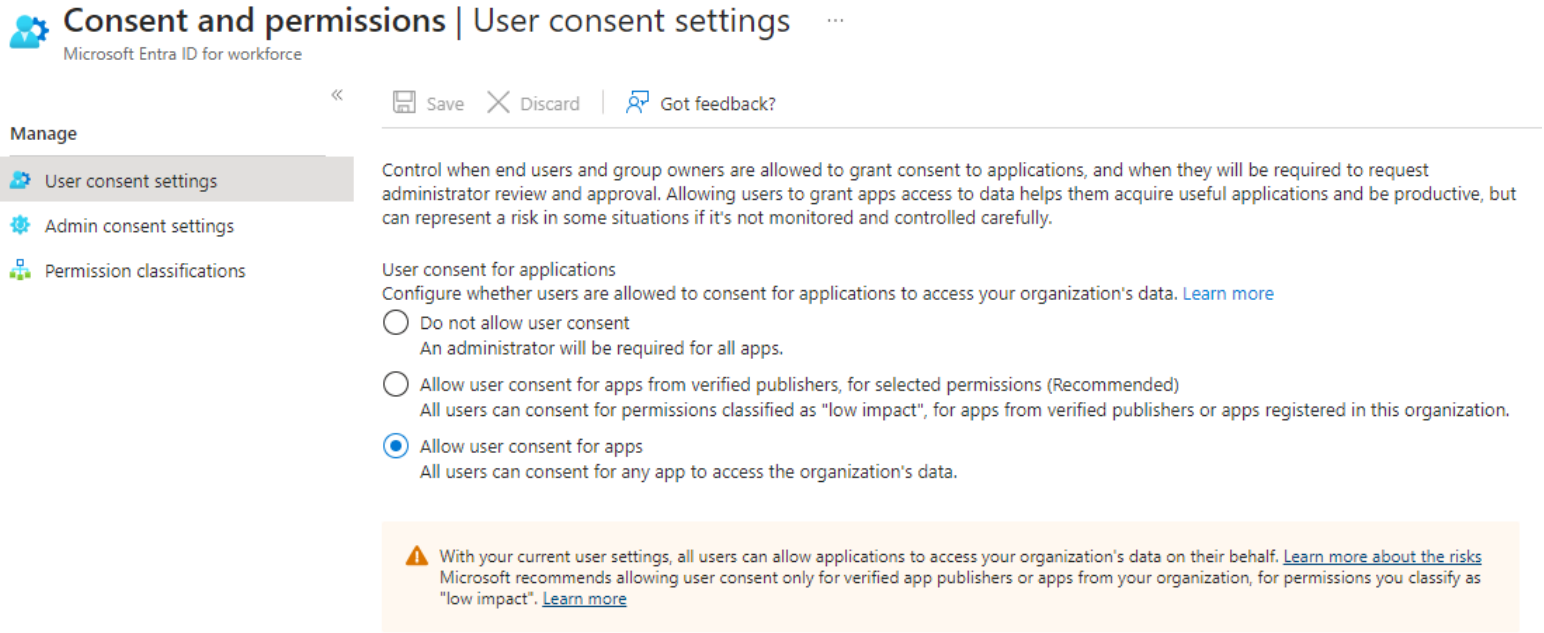
Add-ins in Office apps

Toegang aan Apps voor data en Admin consent workflow

- Meer controle
- Gebruikers doen maar wat
- Aanvragen erg simpel

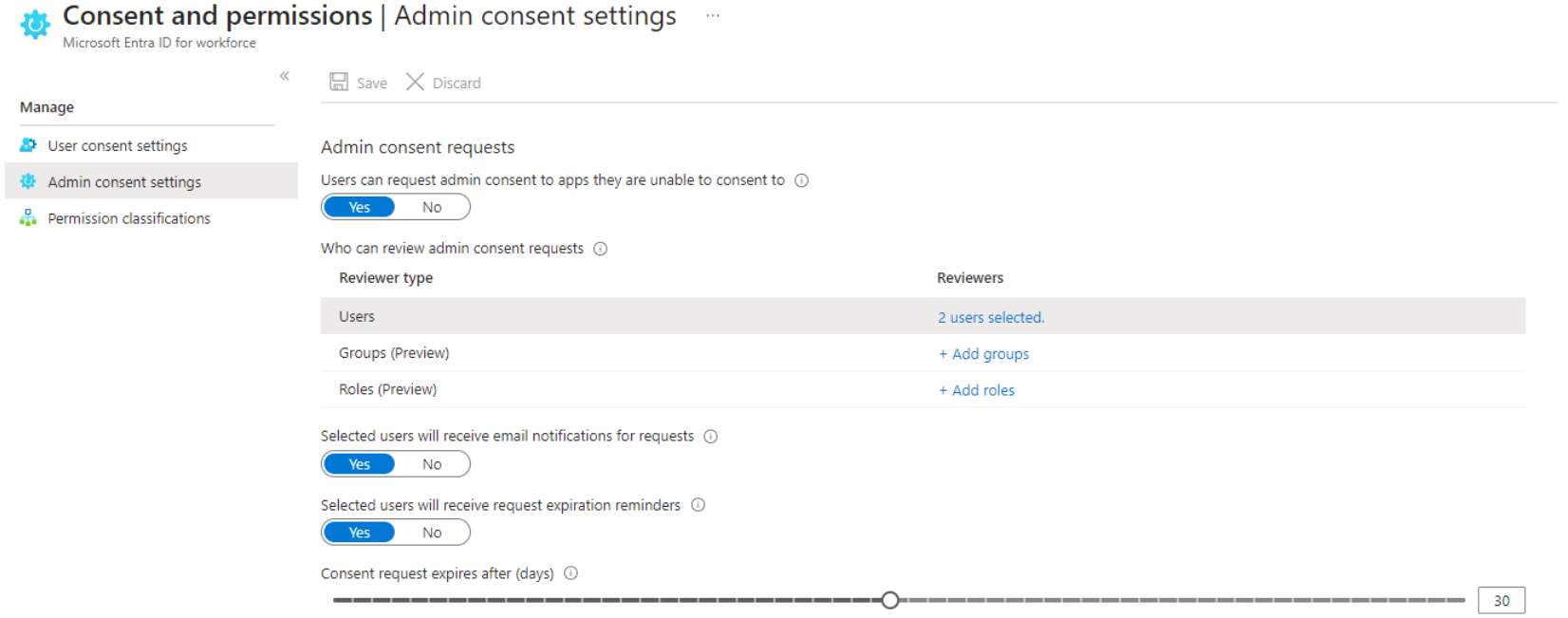
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Stop de gebruiker!



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Bring in Admin workflow!

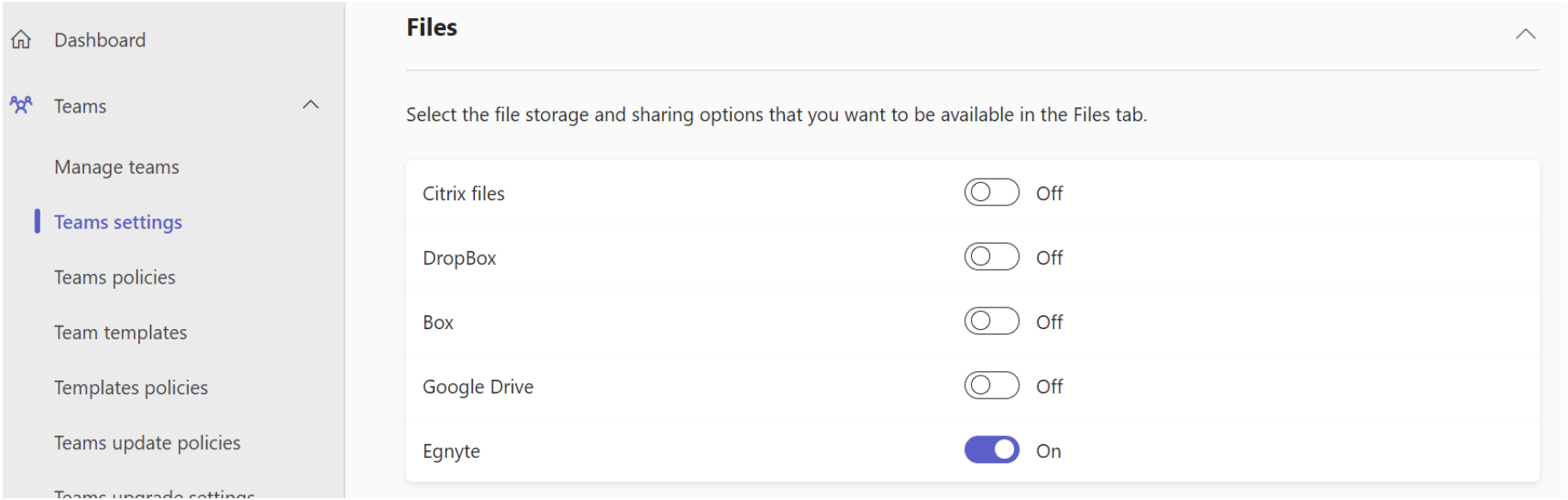


rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

External file sharing

- Teams (en daarmee SharePoint)
- Third party cloud services
- Staat aan by default!

External file sharing

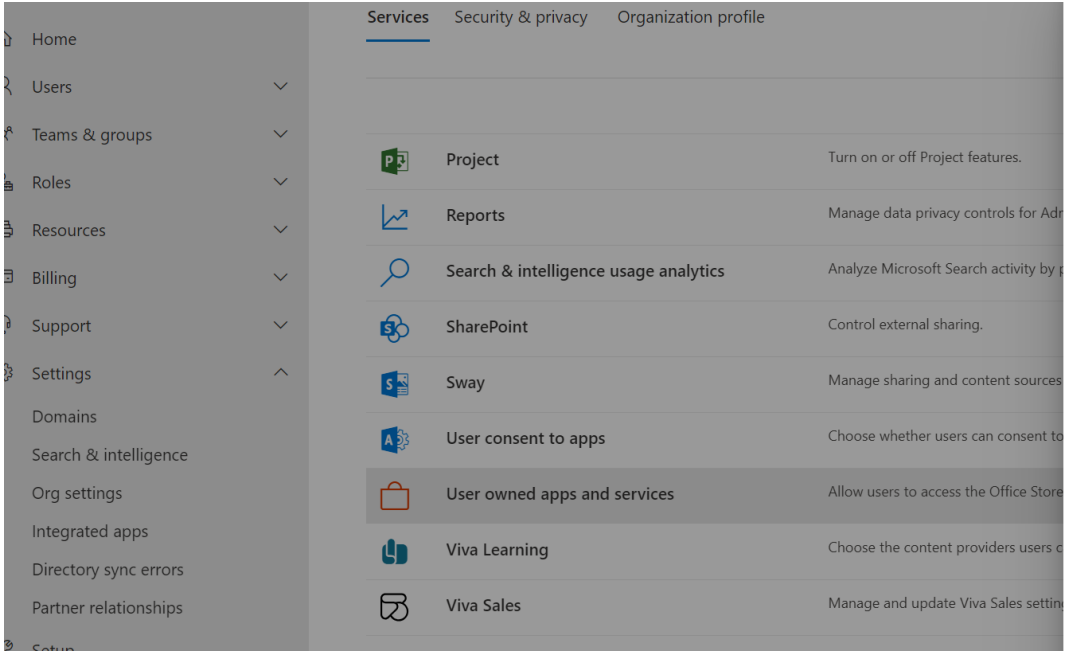


rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Add-ins in Office apps

- Geen inzicht in welke gebruikt worden
- Geen zicht op gebruik van data
- Veel malafide gewoon beschikbaar
- Blokkeer in Outlook, Word, Excel, PowerPoint
  - Outlook in nieuwe admin center!

Add-ins in Office apps



User owned apps and services

Choose whether users in your organization can access the Office Store and create Microsoft 365 trial accounts.

☐ Let users access the Office Store

Allow people in your organization to access the Office Store using their work account. The Office Store provides access to apps that aren't curated or managed by Microsoft.

☐ Let users start trials on behalf of your organization

Allow people in your organization to start trial subscriptions for apps and services that support trials. Admins manage licenses for these trials in the same way as other licenses in your organization. Only admins can upgrade these trials to paid subscriptions, so they won't affect your billing.

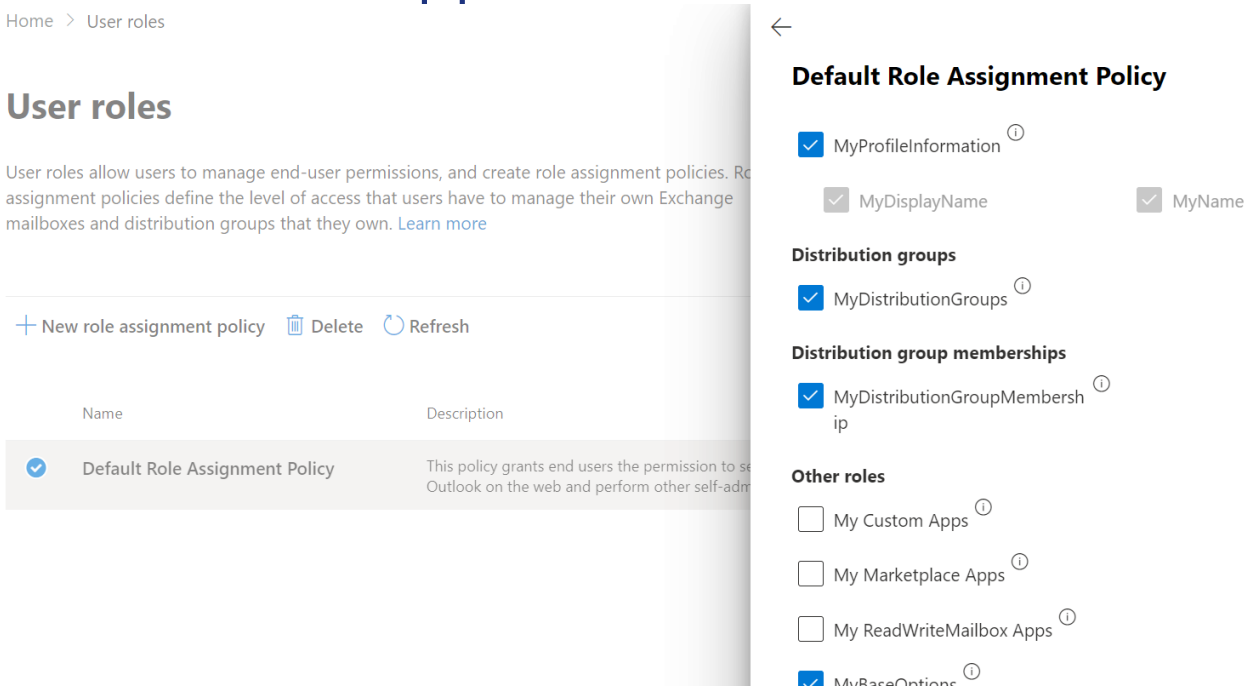
☐ Let users auto-claim licenses the first time they sign in

Allow users to automatically claim a product license the first time they sign in to an app. To use this setting, select it here and then create an auto-claim policy.

In the autoclaim-policy, you'll set which app a person uses to claim a license, and which product the license will come from. To create an auto-claim policy, go to Billing > Licenses - Auto-claim policy.

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Add-ins in Office apps



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Email security

Exchange Online

Spam policies

SPF, DKIM, DMARC

Welke domeinen wel, en welke niet?

Email forwarding

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Spam policies

- Niet ingesteld
- Niet voldoende ingesteld
- Geen notificatie

Email forwarding

- Veel gebruikte methode door hackers
- Geautomatiseerde doorsturen
- Handmatig doorsturen kan nog wel

SPF, DKIM, DMARC

- Vaak alleen SPF
- Vaak alleen op de emaildomeinen
- SPF en DKIM makkelijk in te stellen
- Voor DMARC aanvullende tool nodig
  - Dmarcian en Valimail

Sender Policy Framework

DomainKeys Identified Mail

Domain-based Message Authentication, Reporting & Conformance

Welke domeinen wel, en welke niet?

- Alle domeinen die in je bezit zijn!

Het feit dat jij niet via die domeinen mailt,
betekent niet dat een ander dat niet doet!

Echter zit jij met de reputatieschade!

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Storage

Mobile Device Management

Mobile Devices

OneDrive op unmanaged devices

External storage in OotW

OneDrive op unmanaged devices

- Toegestaan by default
- Data valt in zwart gat
- Data kan achterblijven
- Data kan niet gewist worden op afstand

- Grootste risico is de gebruiker

External storage in OotW

- Outlook on the Web
- Opslag van bijlages
- Staat aan by default

Mobile Devices

- Hebben geen wachtwoorden
- Mogen wachtwoorden hergebruiken
- Mogen jailbroken of rooted zijn
- Hebben geen sterke wachtwoorden
- Etc.
- Etc.
- Etc.
- Etc.
- Etc.
- Etc.
- Etc.
- Etc.
- Etc.
- Etc.
- Etc.
- Etc.

Please evaluate this session in the App.

THANK YOU

Are there any questions?