



+

○

+

+

15 Security zaken die 'gratis' zijn

waar bijna niemand gebruik
van maakt

+

○

+

○





Freelance Security Architect @ SecureCraft Solutions
Team Lead IT Security Office @ Tilburg University

Neal Bongers





Security Assessments





+ 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.



SquaredUp



infinity



INTERSTELLAR



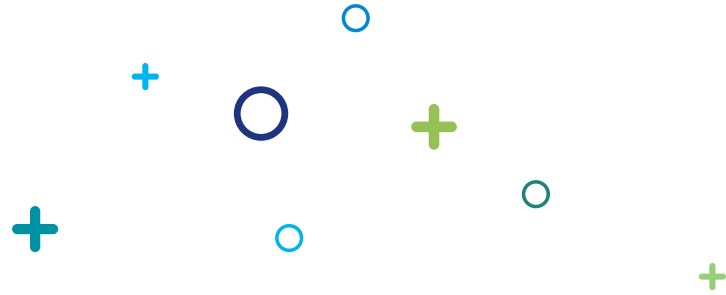
kpn
Partner Network



INSPARK



cegeka



Gratis?

Alles via maximaal E3 licenties

Veel ook zonder überhaupt licenties te hebben





Accounts & Authentication





Sign-in frequency /
Browser sessions

Global
Admins

Block Legacy
AuthN

Seperate accounts

MFA & SSPR



SquaredUp



infinity



kpn
Partner Network



INS PARK



cegeka



+ 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



SquaredUp



kpn
Partner Network



INS PARK



cegeka

Conditional Access - Admin

Name *

CA-Administrators ✓

Assignments

Users ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps included and 1 app excluded

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

Enable policy

Report-only **On** Off

Include Exclude

None

All users

Select users and groups

Guest or external users ⓘ

Directory roles ⓘ

87 selected

Users and groups

Select

1 group

CR :P-USR-CA-Administrators ...

[Learn more](#)

Name *

CA-Administrators ✓

Assignments

Users ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps included and 1 app excluded

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Enable policy

Report-only **On** Off

Block access

Grant access

Require multifactor authentication ⓘ

i Consider testing the new "Require authentication strength". [Learn more](#)

Require authentication strength ⓘ

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ



SquaredUp



kpn Partner Network



INS PARK



cegeka

Conditional Access - Guests

Name *
CA-GuestUsers ✓

Assignments

Users ⓘ
Specific users included and specific users excluded

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
1 control selected

Session ⓘ
0 controls selected

Enable policy
Report-only On Off

Include Exclude

None
 All users
 Select users and groups

Guest or external users ⓘ

6 selected

Specify external Azure AD organizations

All
 Select

Directory roles ⓘ
 Users and groups

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
CA-GuestUsers ✓

Assignments

Users ⓘ
Specific users included and specific users excluded

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
1 control selected

Session ⓘ
0 controls selected

Enable policy
Report-only On Off

Block access
 Grant access

Require multifactor authentication ⓘ

i Consider testing the new "Require authentication strength". [Learn more](#)

Require authentication strength ⓘ

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ
[See list of approved client apps](#)

Require app protection policy ⓘ
[See list of policy protected client apps](#)



SquaredUp



kpn Partner Network



Nieuwe methodes!

Authentication methods | Policies

eiffel.nl - Azure AD Security

[Got feedback?](#)

Manage

[Policies](#)

[Password protection](#)

[Registration campaign](#)

[Authentication strengths](#)

[Settings](#)

Monitoring

[Activity](#)

[User registration details](#)

[Registration and reset events](#)

[Bulk operation results](#)

Use this policy to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate (some authentication methods here in the authentication methods policy. Use this control to manage your migration from t aren't supported for some scenarios). [Learn more](#)

Manage migration

On September 30th, 2024, the legacy multifactor authentication and self-service password reset policies will be deprecated. Use this control to manage your migration from t authentication methods here in the authentication methods policy. Use this control to manage your migration from t policy. [Learn more](#)

[Manage migration](#)

Method	Target	Enabled
FIDO2 security key		No
Microsoft Authenticator	All users	Yes
SMS		No
Temporary Access Pass	All users	Yes
Third-party software OATH tokens		No
Voice call		No
Email OTP		Yes
Certificate-based authentication		No



Authentication methods: Activity

Registration Usage

Users capable of Azure multifactor authentication

251 of 743 total

▲ 66% of your organization isn't capable.

Users capable of passwordless authentication

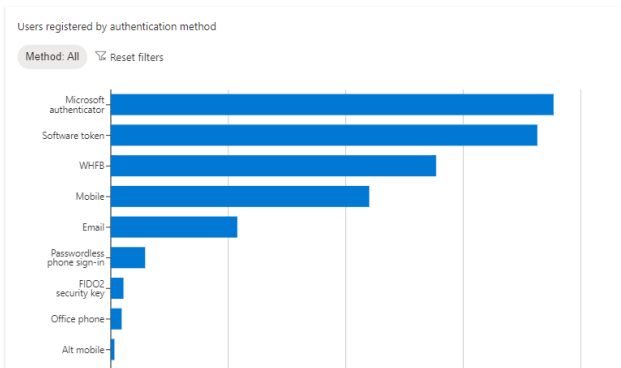
182 of 743 total

▲ 76% of your organization isn't capable.

Users capable of self-service password reset

204 of 743 total

▲ 73% of your organization isn't enabled.



SquaredUp



kpn Partner Network



Authentication methods: User registration details

Download Refresh Columns Got feedback?

Name or UPN starts with

Add filter

Multifactor authentication capable: All

Passwordless capable: All

SSPR capable: All

Methods registered: All

Reset filters

UPN ↑	Name ↓	Multifactor authen...	Passwordless Ca...	SSPR Capable	Default multifactor authent...	Methods Registered	Last Updated Time
...	...	Not Capable	Not Capable	Not Capable			6/11/23, 12:32:59 AM UTC
...	...	Capable	Capable	Capable	Microsoft Authenticator app (pl	Windows Hello for Business,Mobile phone,Micros	6/12/23, 6:58:52 AM UTC
...	...	Capable	Capable	Capable	Microsoft Authenticator app (pl	Microsoft Passwordless phone sign-in,Mobile phc	6/11/23, 12:32:59 AM UTC
...	...	Capable	Capable	Capable	Microsoft Authenticator app (pl	Windows Hello for Business,Microsoft Authentica	6/11/23, 12:32:59 AM UTC
...	...	Not Capable	Not Capable	Not Capable			6/11/23, 12:32:59 AM UTC
...	...	Not Capable	Not Capable	Not Capable			6/11/23, 12:32:59 AM UTC
...	...	Capable	Capable	Capable	Microsoft Authenticator app (pl	Email,Windows Hello for Business,Microsoft Auth	6/11/23, 12:32:59 AM UTC
...	...	Capable	Capable	Capable	Microsoft Authenticator app (pl	Windows Hello for Business,Mobile phone,Micros	6/11/23, 12:32:59 AM UTC
...	...	Not Capable	Not Capable	Not Capable			6/11/23, 12:32:59 AM UTC
...	...	Capable	Capable	Not Capable		Windows Hello for Business,FIDO2 security key	6/11/23, 12:32:59 AM UTC
...	...	Capable	Capable	Capable	Microsoft Authenticator app (pl	Windows Hello for Business,Microsoft Passworde	6/11/23, 12:32:59 AM UTC
...	...	Not Capable	Not Capable	Not Capable			6/11/23, 12:32:59 AM UTC
...	...	Capable	Capable	Not Capable		Windows Hello for Business,FIDO2 security key	6/11/23, 12:32:59 AM UTC
...	...	Not Capable	Not Capable	Not Capable			6/11/23, 12:32:59 AM UTC
...	...	Not Capable	Capable	Not Capable	Mobile phone	Windows Hello for Business,Mobile phone,Office	6/11/23, 12:32:59 AM UTC
...	...	Not Capable	Not Capable	Not Capable			6/11/23, 12:32:59 AM UTC
...	...	Not Capable	Not Capable	Not Capable			6/11/23, 12:32:59 AM UTC



SquaredUp



kpn Partner Network





+ 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



DELL
Technologies



SquaredUp



infinity



kpn
Partner Network



INSPARK



cegeka



+ 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!



SquaredUp



kpn
Partner Network



INSPARK



cegeka



+ Sign-in frequency / browser sessions

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



DELL
Technologies



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INSPARK



cegeka



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



DELL
Technologies



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INSPARK



cegeka

Stop de gebruiker!

Consent and permissions | User consent settings

Microsoft Entra ID for workforce



Save



Discard



Got feedback?

Manage

User consent settings

Admin consent settings

Permission classifications

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

- Do not allow user consent
An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- Allow user consent for apps
All users can consent for any app to access the organization's data.



With your current user settings, all users can allow applications to access your organization's data on their behalf. [Learn more about the risks](#)
Microsoft recommends allowing user consent only for verified app publishers or apps from your organization, for permissions you classify as "low impact". [Learn more](#)



SquaredUp



kpn
Partner Network



INS PARK



cegeka

Bring in Admin workflow!

Consent and permissions | Admin consent settings

Microsoft Entra ID for workforce

<< Save Discard

Manage

User consent settings

Admin consent settings

Permission classifications

Admin consent requests

Users can request admin consent to apps they are unable to consent to

Yes No

Who can review admin consent requests

Reviewer type	Reviewers
Users	2 users selected.
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests

Yes No

Selected users will receive request expiration reminders

Yes No

Consent request expires after (days)

-----○----- 30



+ External file sharing

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



SquaredUp



infinity



kpn
Partner Network



INS PARK



cegeka

External file sharing

Dashboard

Teams

Manage teams

Teams settings

Teams policies

Team templates

Templates policies

Teams update policies

Teams upgrade settings

Files

Select the file storage and sharing options that you want to be available in the Files tab.

Citrix files

Off

DropBox

Off

Box

Off

Google Drive

Off

Egnyte

On



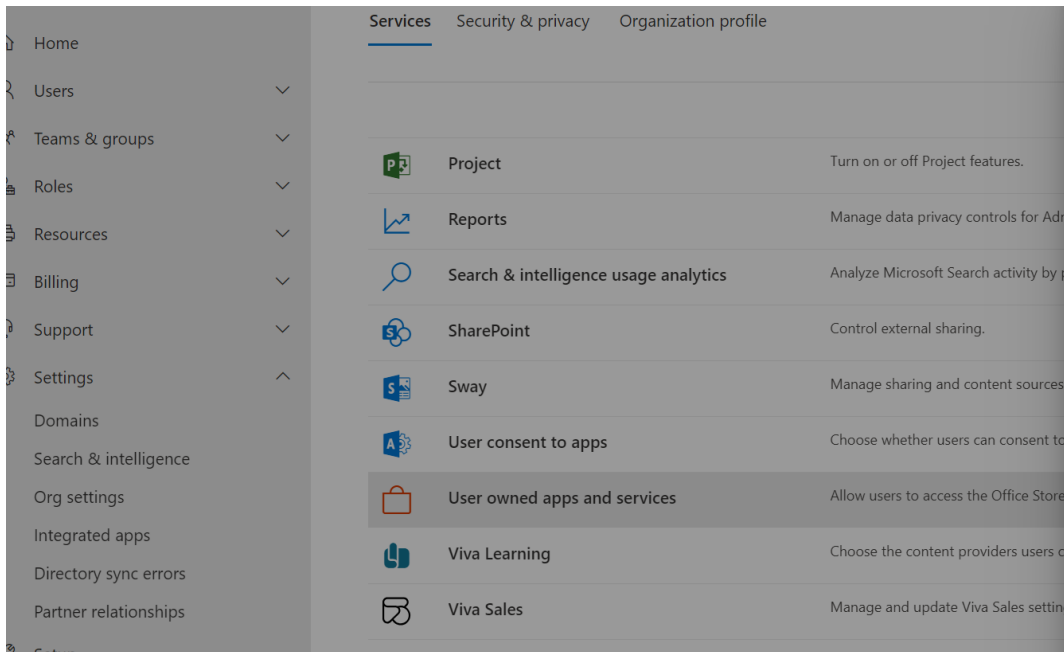


+ Add-ins in Office apps

- 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 auto-claim-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.



Add-ins in Office apps

Home > User roles

User roles

User roles allow users to manage end-user permissions, and create role assignment policies. Role assignment policies define the level of access that users have to manage their own Exchange mailboxes and distribution groups that they own. [Learn more](#)

[+ New role assignment policy](#) [Delete](#) [Refresh](#)

Name	Description
<input checked="" type="checkbox"/> Default Role Assignment Policy	This policy grants end users the permission to set Outlook on the web and perform other self-administrated tasks.



Default Role Assignment Policy

MyProfileInformation ⓘ

MyDisplayName

MyName

Distribution groups

MyDistributionGroups ⓘ

Distribution group memberships

MyDistributionGroupMemberships ⓘ

Other roles

My Custom Apps ⓘ

My Marketplace Apps ⓘ

My ReadWriteMailbox Apps ⓘ

MyBaseOptions ⓘ





Email security

Exchange Online





Spam policies

Welke domeinen
wel, en welke niet?

SPF, DKIM,
DMARC

Email forwarding



DELL
Technologies



SquaredUp



infinity



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



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INS PARK



cegeka



+ 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!





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



SquaredUp



infinity



kpn
Partner Network



INS PARK



cegeka



+ 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.





Please evaluate this session in the App.

THANK YOU

Are there any questions?

