Apparaten en Azure AD: wie, wat en waar?

Sander Berkouwer
SCCT

WAZUG.NL
AZURE USER GROUP NL

Introductie

Sander Berkouwer

Senior consultant bij SCCT BV

MCSA, MCSE, MCT

Microsoft MVP, Veeam Vanguard

DirTeam.com

@SanderBerkouwer

WAZUG.NL
AZURE USER GROUP NL

Agenda

Identiteitskoppelingen

Koppelen van apparaten aan Azure AD en/of on-premises Active Directory Domain Services

Conditional Access

Mogelijkheden om toegang te verstrekken, of juist te verbieden

Windows Hello for Business

Hoe alles samenkomt in Windows 10 1804

Achtergrond

Een kleine introductie, zowel interessant voor IT Pro’s, ontwikkelaars als IT-leidinggevenden

Achtergrond

De traditionele IT-grenzen vervagen

Medewerkers willen en kunnen overal werken

Medewerkers kunnen hun eigen apparaten inzetten

Organisaties draaien om gegevens

Gegevens bevinden zich in applicaties

Applicaties zorgen voor informatie, inzichten, acties

De traditionele aanpak werkt niet meer

De RBAC-generator *

Actor		Action		Scope		Conditions
Device App	has	Create	on	Resource (user, app)	when	Always
User		Read		All		Elevated
Group Collection		Update Delete		Collection (AU, OU, ...)		Approved

* As conceived by Stuart Kwan, Microsoft

WAZUG.NL
AZURE USER GROUP NL

Conditional Access

Users

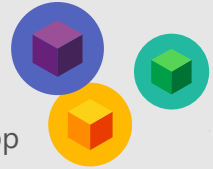
User identity
Group memberships

Devices

Azure AD joined?
Marked compliant?
Platform type
Lost/stolen?

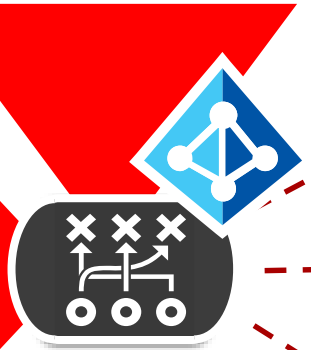
Application

Per-service
Managed client app



Other

Location (network)
Time of day
Risk profile

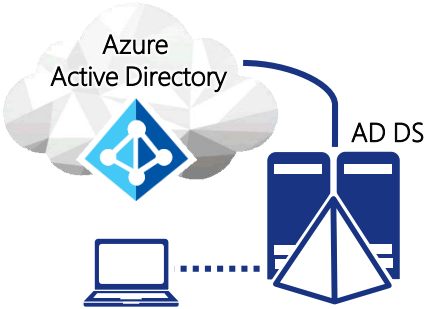


- Allow
- Block
- MFA
- Enroll
- Terms of Use

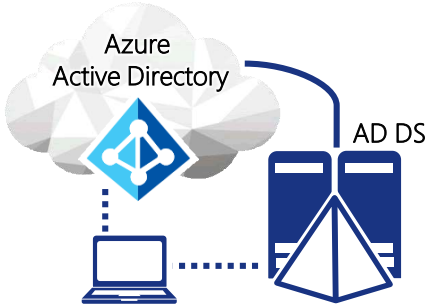
Identiteitskoppelingen

Hoe het koppelen van apparaten zorgt voor beheerbaarheid en zichtbaarheid

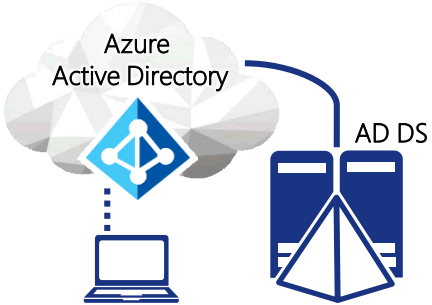
Identiteitskoppelingen



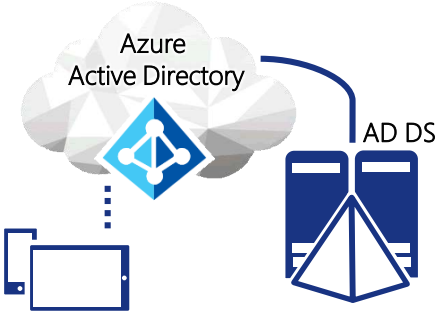
AD domain joined



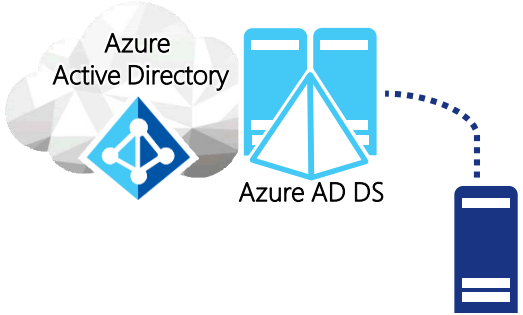
Hybrid Azure AD joined



Azure AD joined



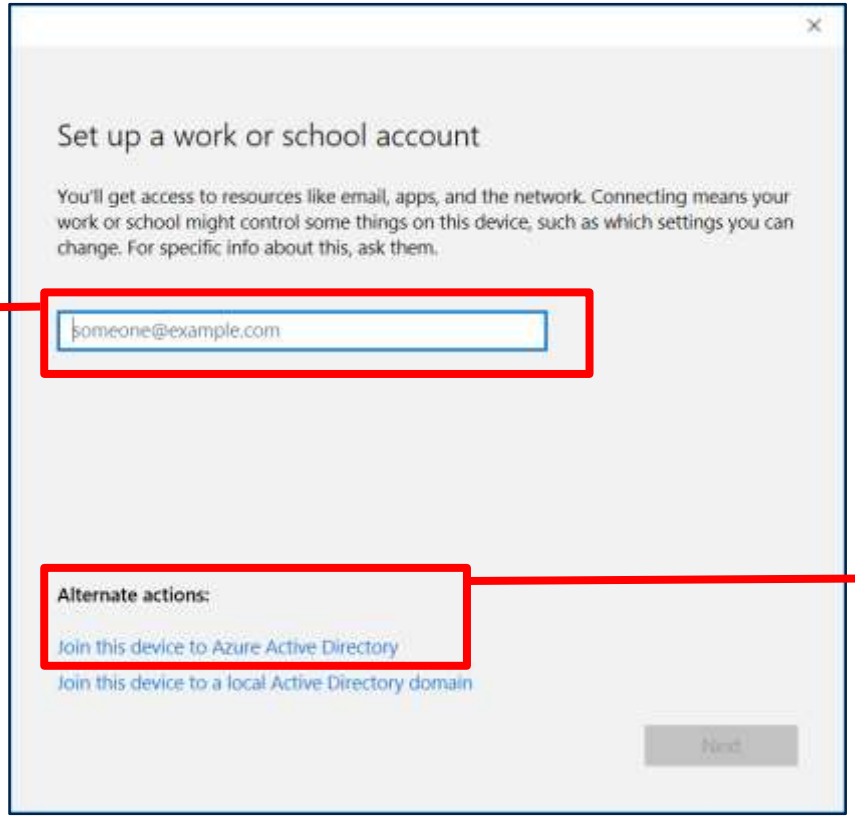
Azure AD registered



Azure AD Domain Services joined

WAZUG.NL
AZURE USER GROUP NL

Register vs. Join in Windows 10



Azure AD Register

Azure AD Join

WAZUG.NL
AZURE USER GROUP NL

Register vs. Join

Azure AD Join	Azure AD Registered
Voor zakelijke apparaten	Voor persoonlijke apparaten
Alleen mogelijk met Windows 10	Mogelijk met: • Windows • Android • iOS
Lokale beheerrechten	Lokale beheerrechten

Hybrid Azure AD Join

Azure AD Join

Voor zakelijke apparaten

Alleen met Windows 10

Interactie benodigd

- Out of the Box Experience
- PC Settings - Accounts

Hybrid Azure AD Join

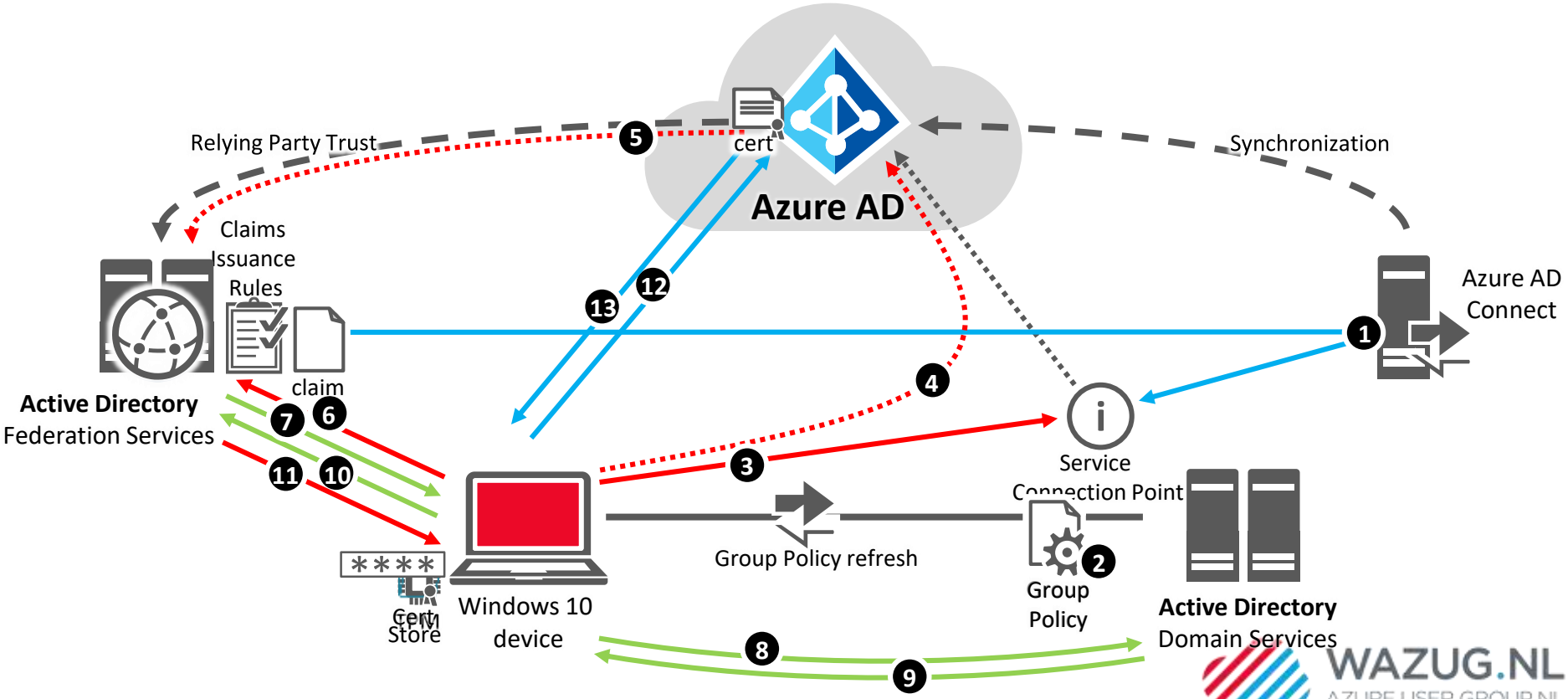
Voor zakelijke apparaten

Voor Windows 10, maar ook Windows Vista, 7, 8 en 8.1

- WorkPlace Join for legacy clients link

Geen interactie benodigd

Hybrid Azure AD Join met AD FS



Aandachtspunten Azure AD Join

Azure AD Connect

Azure AD Connect versie 1.1.486.0 of hoger benodigd

Synchronisatie van computerobjecten vindt automatisch plaats

Group Policy

Voorafgaand aan Windows 10 1607, benodigd

Windows 10, 1607, 1703, 1709 en 1804 gaan automatisch

Azure AD Instellingen

Demo

Device settings in het Azure Portal

Windows Hello for Business

Windows Hello for Business

Kijk mama, zonder wachtwoorden!

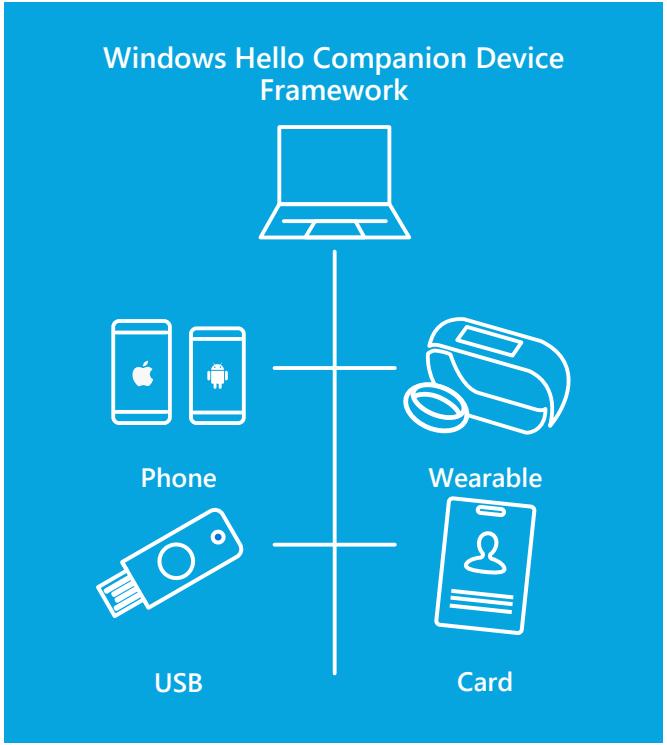
Password-less, strong authentication,

Standaard met multi-factor authentication

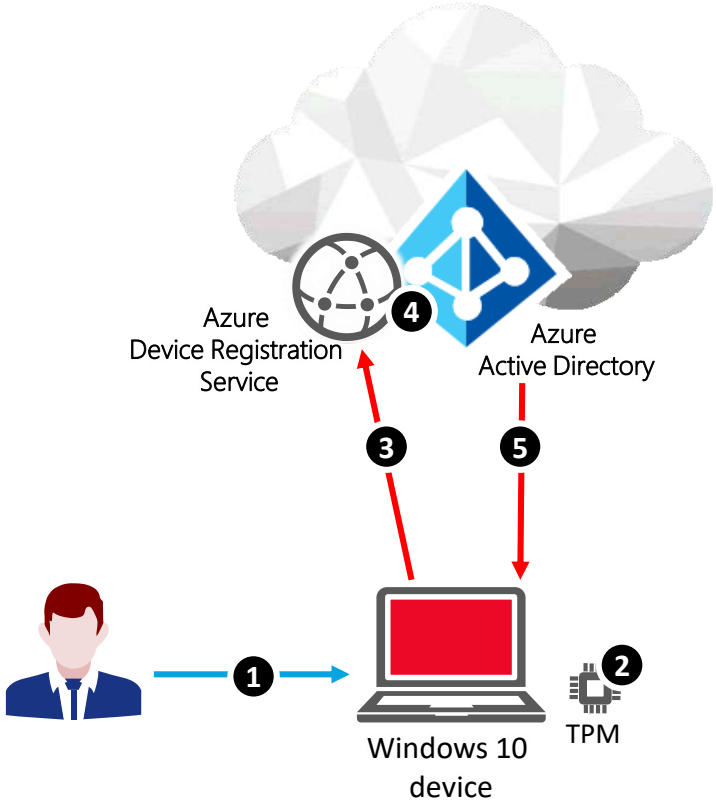
Beschikbaar op Windows 10

Beveiliging

Aanmeldgegevens worden beschermd door hardware



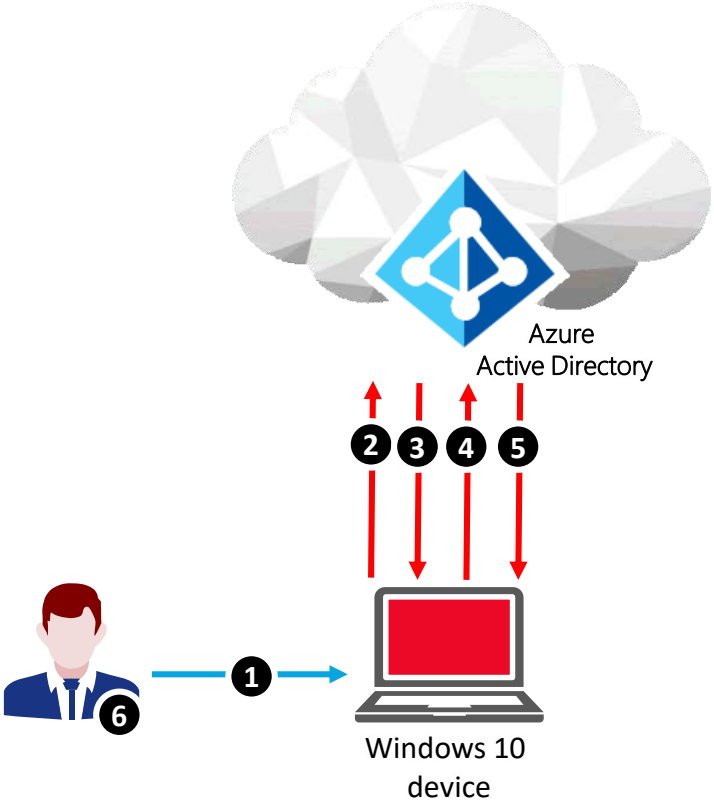
Windows Hello registratie



1. Persoon meldt aan met wachtwoord en MFA en registreert biometrische aanmeldmethode.
2. Windows genereert een Windows Hello for Business sleutel in TPM, beschermd met biometrische aanmeldmethode en *attestation blob*.
3. Windows stuurt publieke sleutel van HfB certificaat, attestation blob en AIK certificaat naar Azure DRS.
4. Azure DRS verifieert de HfB sleutel met de attestation blob en registreert sleutel met useraccount.
5. Azure retourneert de sleutel ID.

WAZUG.NL
AZURE USER GROUP NL

Aanmelden met Windows Hello



1. Persoon meldt aan met biometrische optie.
2. Windows stuurt ‘Hello’.
3. Azure AD stuurt ‘nonce’.
4. Windows stuurt ondertekende ‘nonce’ met Windows Hello sleutel.
5. Azure AD stuurt PRT, ID token en versleutelde sessiesleutel, gekoppeld aan TPM.
6. Persoon heft Single Sign-On toegang tot cloud en on-premises applicaties.

WAZUG.NL
AZURE USER GROUP NL

Aanbevelingen

Zet Intune in

Azure AD Join en Intune samen verschaffen beheerzekerheid

Zonder Intune ontstaat *device drift*

Standaard limieten

Azure AD Join is standaard gelimiteerd tot 20 apparaten

Intune's limiet is 15 apparaten, maar standaard ingesteld op 5.

Let op lokale beheerrechten

Afsluitend

Afsluitend

Identiteitskoppelingen

Cloudapplicaties én functionaliteit on-premises, met één aanmelding

Toegangscontrole met Conditional Access en Identity Protection

Single Sign-On toegang tot cloudapplicaties

Windows Hello for Business

Gemakkelijker wordt multi-factor authenticatie niet…

Bedankt!