# Hybrid Joined

|  |  |  |  |
| --- | --- | --- | --- |
| Autopilot | possible |  | Vpn needed(authenticate dc), sync time etc |
| More for Existing devices |  |  |  |
|  |  |  |  |
|  |  |  |  |

https://www.nielskok.tech/intune/windows-10-autopilot-hybrid-ad-join-vs-azure-ad-join/#:~:text=The%20main%20disadvantage%20of%20the,to%20contact%20a%20Domain%20Controller.

# AAD joined

|  |  |  |  |
| --- | --- | --- | --- |
| autopilot | possible |  | remarks |
| access to on prem | possible | https://docs.microsoft.com/en-us/microsoft-365/admin/setup/access-resources?view=o365-worldwide | See below. Modern authentication needed? |
| Group policy | Not | Intune same possible gpo needs? |  |
| Intune managed | yes |  |  |
| Sccm managed | Co management |  |  |
| Authenticate on prem | Modern authentication required |  |  |
| Laps | Not possible |  |  |
| Ad on prem | Not present |  | Group policies not |
| Ldap | Not possible |  |  |
| Tsg needed | Certificaten? |  | fas |
| Aad connect |  | Enable single sign on moet aan for on prem resources |  |
| Mor For New devices |  |  |  |
| profiles |  |  |  |

**Considerations when you join Windows devices to Azure AD**

If the Windows device that you Azure-AD joined was previously domain-joined or in a workgroup, consider the following limitations:

* When a device Azure AD joins, it creates a new user without referencing an existing profile. Profiles must be manually migrated. A user profile contains information like favorites, local files, browser settings, and Start menu settings. A best approach is to find a third-party tool to map existing files and settings to the new profile.
* If the device is using Group Policy Objects (GPO), some GPOs may not have a comparable [Configuration Service Provider](https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/how-it-pros-can-use-configuration-service-providers) (CSP) in Intune. Run the [MMAT tool](https://www.microsoft.com/download/details.aspx?id=45520) to find comparable CSPs for existing GPOs.
* Users might not be able to authenticate to applications that depend on Active Directory authentication. Evaluate the legacy app and consider updating to an app that uses modern Auth, if possible.

- <https://docs.microsoft.com/en-us/microsoft-365/admin/setup/access-resources?view=o365-worldwide>

https://oofhours.com/2020/08/06/afraid-of-windows-10-with-azure-ad-join-try-it-out-part-2/

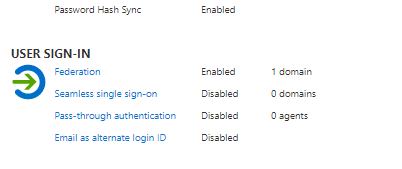
https://practical365.com/the-case-for-azure-ad-join/

# Aad connect

Upgraden!

Password hashes Synchronis is on?

Turn on single sign on



https://www.youtube.com/watch?v=dUJnIakSPkA&list=RDCMUCfmMlhX5TW8cicxHw6ExYVA&index=2

Upn wijzigen mogelijk?

federation

PS C:\Users\admin\_bh> Connect-MsolService

PS C:\Users\admin\_bh> Get-MsolDomainFederationSettings

cmdlet Get-MsolDomainFederationSettings at command pipeline position 1

Supply values for the following parameters:

DomainName: ihc.eu

ActiveLogOnUri : https://pfed.ihc.eu/adfs/services/trust/2005/usernamemixed

DefaultInteractiveAuthenticationMethod :

FederationBrandName : pfed.ihc.eu

IssuerUri : http://pfed.ihc.eu/adfs/services/trust

LogOffUri : https://pfed.ihc.eu/adfs/ls/

MetadataExchangeUri : https://pfed.ihc.eu/adfs/services/trust/mex

NextSigningCertificate : MIIC0jCCAbqgAwIBAgIQJ5ser8NxsrVH08YFqz8lljANBgkqhkiG9w0BAQsFADAlMSMwIQYDVQQDEx

pBREZTIFNpZ25pbmcgLSBwZmVkLmloYy5ldTAeFw0yMTA5MTIxOTU1MjZaFw0yNDA4MDYxOTU1MjZa

MCUxIzAhBgNVBAMTGkFERlMgU2lnbmluZyAtIHBmZWQuaWhjLmV1MIIBIjANBgkqhkiG9w0BAQEFAA

OCAQ8AMIIBCgKCAQEAuuK7n+fmLV6PT9egLUcVEK/KhJYt6yWudomNNOz/VPSbljk08AOLaUladsMo

zgtt8EU42/rZU4zh27REwyL/D3ihSpw9xGX4xEXgvDWzvkWu1RLer1XfRmS44HLOh18Yo0xHLAHIUA

KlxKWq39OyJDelARZ5Xk+AHKRcw75b3HTKP65r3Kqm29Pc9Ie6ERBoccyWkgV1XkbrYC3BQV2wwPp7

z77vv5JJJYlSX8ULVFWnALbq0HVNxbN/3p2VvJdhRB2/rs9ERj6rl6gX04yOQTFty2G6ErjIuX490m

vYkQ8HlJCNFQ6CqsDdFGrGWUbJYzZeZbsPcuKBb244oCWL1wIDAQABMA0GCSqGSIb3DQEBCwUAA4IB

AQBuSHdiDFQMVfkuRKSJoQucga+m/0bakYlMUwAN78bSe0CZGTfkN2gD/R7QKgpNw6UsnNs0TEDWFe

RYENbAaK18ECA2I4ufff4IILYAmb/orwq9zd1YkBVlL6eBogYunU0fXZ9AS9WhBFUnGhPSk7xbllpB

81ouJWk2YdLQ9yUB6nz8gLoonSn+z52wNpp8zvvWZoCoYO8ooKc+rSRyqx/i42OA/bV0yC96cjPVr2

/a/SxM+Chsht071YfJrLIYxcyK8f3mbby8jDO8oEvawIs6MntMwboiukV5d2aN6yTIBqR/wXkhYTuK

ulGaetPzHjaG70N6V7Zed/a8lpL0pN3M

OpenIdConnectDiscoveryEndpoint :

PassiveLogOnUri : https://pfed.ihc.eu/adfs/ls/

SigningCertificate : MIIC0jCCAbqgAwIBAgIQcdE68hEzSppDmlSAZeq8NTANBgkqhkiG9w0BAQsFADAlMSMwIQYDVQQDEx

pBREZTIFNpZ25pbmcgLSBwZmVkLmloYy5ldTAeFw0xODExMDgxNTUxMDdaFw0yMTEwMDIxNTUxMDda

MCUxIzAhBgNVBAMTGkFERlMgU2lnbmluZyAtIHBmZWQuaWhjLmV1MIIBIjANBgkqhkiG9w0BAQEFAA

OCAQ8AMIIBCgKCAQEAlb1TEfxiwWT8xczOOQpf9cQVW9LPgwsl0njoGUBuxl3dgzTo98WLK6Fk6e+h

LU9JzxhH1o3L5OrNpV9MazRPY7SMXkclQ203Q8V0ackxIeEYoXYFQi/KXnTieyBl+6RVNRc0uve/LB

Vx3NSnTY7W/j8i140VgoXNV8SFYrQ8Iy6aiBkYT8HY0py7wQFvAGR5F1v3G90PiJC9PjgzIv/OwrP8

G/Bm/nePwOfXZusZtacAiASgWy42q8xtycIwLcN8QX+oH1hNaNseJPy5DGH1VoMuMY/FXxUyOQgeBy

/Ti/q1JwXeq2UAgfQTre1qPe60Gcgx7W1D1+7frnBC6Ra3iwIDAQABMA0GCSqGSIb3DQEBCwUAA4IB

AQBdzlzD6T1mcAzo89bDr9oxFvOjGOIUaja6jwZDnXTp3Ao+z24N9P/iVaRK+e0OWKHSusz9q1/uXA

kMeSkZlh7WyqZgaIAFnH0uc6G234uR+O4YMgEdxVd+K3/mI7NcaQ02HV4gHRpNgdr09XR0aL+XxoMa

psecuTd7vCg+b7paDwNJTtx5aR6vo/ftCTbGdnc/aQ5yBAePSZih9sFQ8piIVgYYkD2Z+MCSkogwea

O9qGOILZ9ni5FRnZwTVIXDHxCFSLi0GqnP1ktw0+xaCPA+7n7dgwq8qWlqSV6hx0f7FnYBxsLeHrfw

LZsECTuHope+OVrvYPJ0FIQkc1HBznJV

SupportsMfa :

# Ad

Domain functional Level: 2012

Forest functional level: 2012

# Gpo

168 stuks

Endpoint windows 10: 32

