



# **CLOUD IDENTITY WITH AZURE AD**

GLOBAL AZURE BOOTCAMP

# WHO AM I?

- Joonas Westlin
- Azure Developer @ Kompozure
- Azure MVP, MCSD, MCSE
- Active on Stack Overflow
  - Currently #4 All-time for Azure AD



@JoonasWestlin



joonasw.net

**Microsoft**  
**CERTIFIED**

Solutions Expert

Cloud Platform and  
Infrastructure

**Microsoft**  
**CERTIFIED**

Solutions Developer

App Builder

# AZURE ACTIVE DIRECTORY



- "Azure Active Directory (Azure AD) is a cloud identity service that allows developers to securely sign in users with a Microsoft work or school account."
- The login system underneath Office 365 and Azure
- Global, multi-tenant, identity and access management service
- Single Sign-On for cloud services
- If you have ever signed in to O365 or Azure, you have used Azure AD
- Quite different from on-premises Windows Server AD

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-developers-guide>

# SINGLE SIGN-ON

- Azure AD offers something known as Single Sign-On (SSO)
- Log in to Office 365
- Open another tab
- Go to Azure Portal
- **You are already logged in**
- AD offers similar system on-prem, AAD does it for cloud services



# GOOD PARTS

- Applications do not need to store passwords
- Robust, battle-proven identity system
  - 1,5 Million attacks/day (~17/sec)
- Thousands of cloud SaaS apps available
- Easy Multi-Factor Authentication
- Globally available, enterprise scale
  - Tens of Billions of authentications every day
  - Hundreds of Millions of active users every day
    - Some of these could be users of your new SaaS app!
  - 99.9% SLA





# SOME LIMITATIONS

- Integrated apps will rely on AAD to function
  - Identity is a single point of failure, by design
- Certain things like the login screen cannot be customized a lot

This is rare but possible ↓



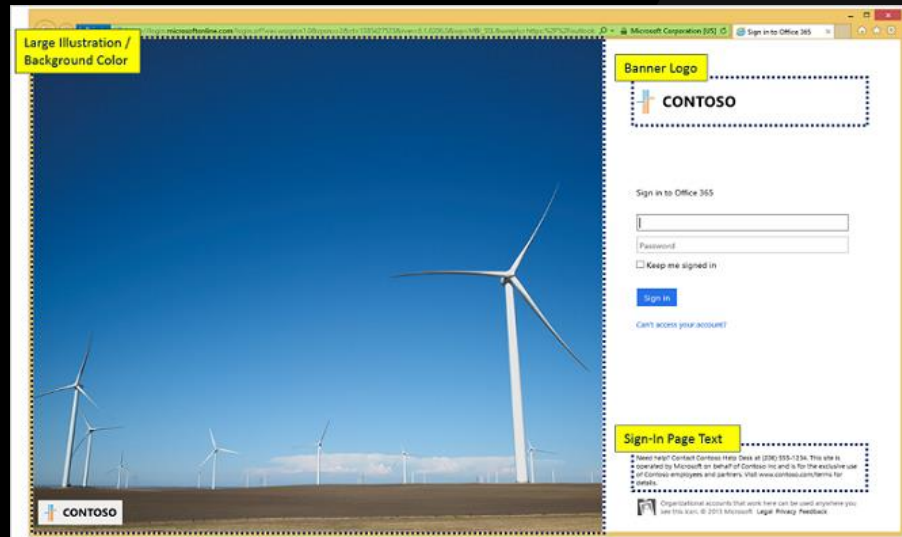
Arttu Arstila 🌤️ @nestafo

5d

A wide-spread sign-in issue in Azure AD affecting also European #Office365 clients, see health dashboard for details

**Office 365 Status** @Office365Status

We're investigating reports of access issues in the Asia Pacific region. More details will be provided shortly.





# PRICING

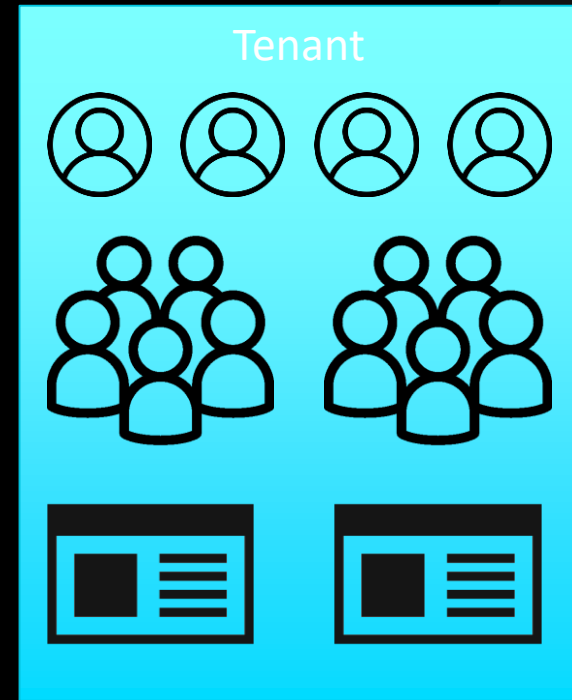
- Free = Max 500k objects, limited customizability, less features, no SLA
  - Easily good enough for testing use though
- Basic adds company branding, Self-Service Password Reset, 99.9% SLA
  - 0,844 € / user / month
- Premium P1 adds Conditional Access, better reports..
  - 5,06 € / user / month
- Premium P2 adds features like Identity Protection and Privileged Identity Management
  - 7,59 € / user / month

<https://azure.microsoft.com/en-us/pricing/details/active-directory/>

<https://docs.microsoft.com/en-us/azure/active-directory/license-users-groups>

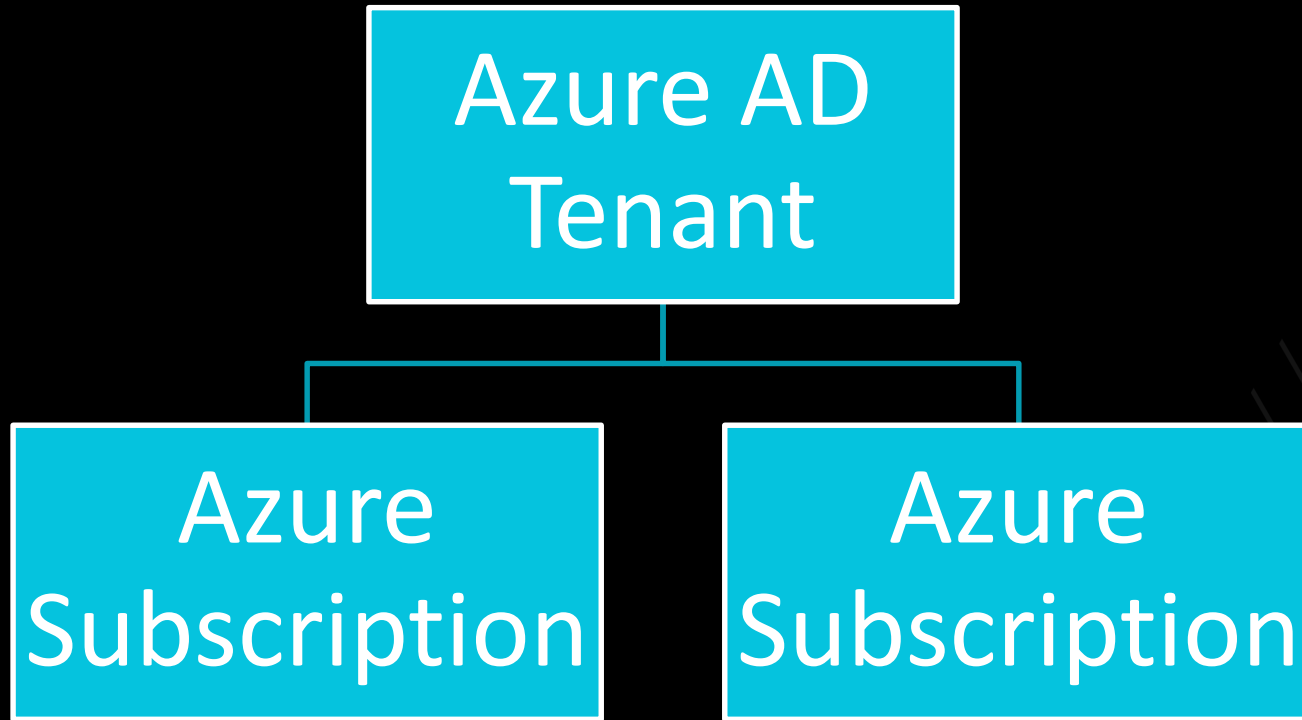
# AZURE AD “TENANTS”

- Tenant = One Azure AD “instance”
- Container for users, their passwords, groups etc.
- An organization typically has one tenant



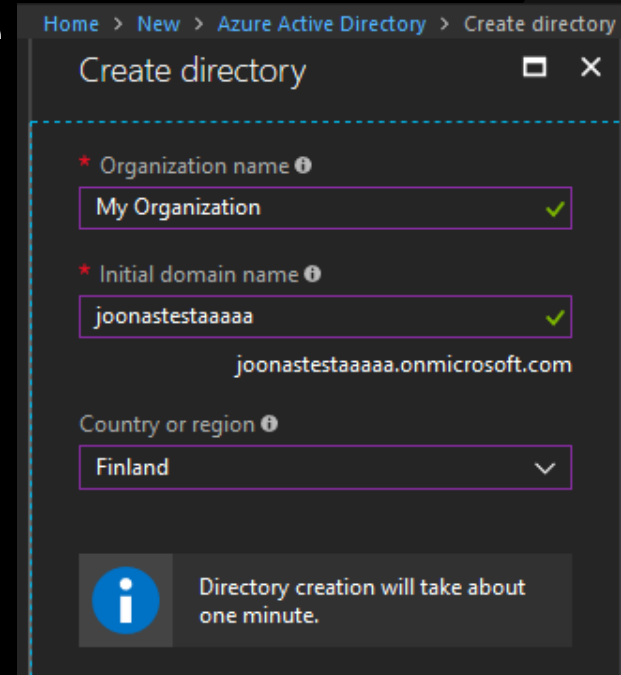


# TENANTS AND AZURE SUBSCRIPTIONS



# CREATING TENANTS

- You already have one if you have Office 365, Azure or Dynamics CRM!
- More tenants can be created from the Portal
- Initial domain name: something.**onmicrosoft.com**
- You can add domain names later
- Country affects datacenter used, cannot be changed later



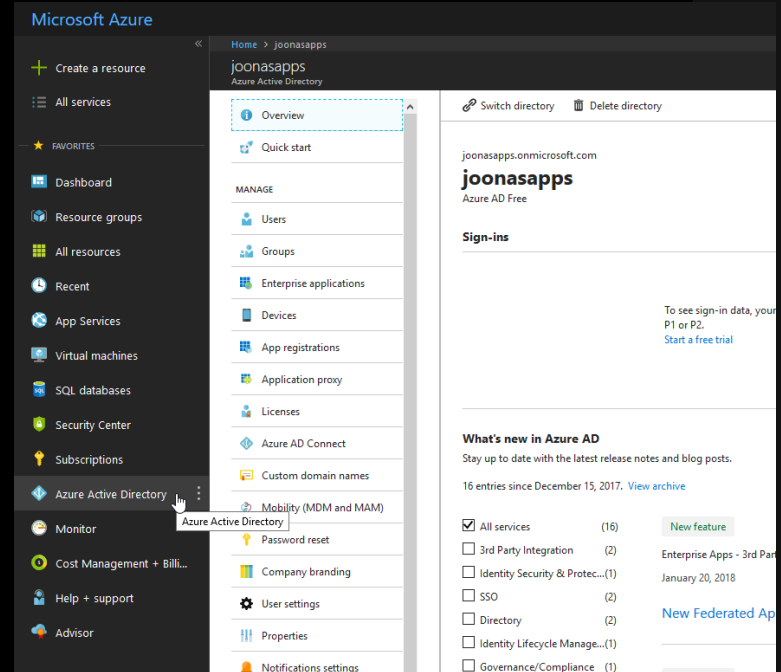
The screenshot shows the 'Create directory' form in the Azure Active Directory portal. The breadcrumb navigation at the top reads 'Home > New > Azure Active Directory > Create directory'. The form title is 'Create directory'. It contains three main input fields, each with a red asterisk and an information icon:

- Organization name:** The text 'My Organization' is entered, followed by a green checkmark.
- Initial domain name:** The text 'joonastestaaaaa' is entered, followed by a green checkmark. Below this field, the full domain 'joonastestaaaaa.onmicrosoft.com' is displayed.
- Country or region:** A dropdown menu is open, showing 'Finland' as the selected option.

At the bottom of the form, there is an information icon and a message: 'Directory creation will take about one minute.'

# MANAGING AZURE AD

- Can use [portal.azure.com](https://portal.azure.com)
- Find **Azure Active Directory** from the left or from under **All services**
- Pro-tip: Use <https://aad.portal.azure.com>
- PowerShell:  
<https://docs.microsoft.com/en-us/powershell/azure/active-directory/install-adv2?view=azureadps-2.0>
- AAD Graph Explorer (advanced stuff):  
<https://graphexplorer.azurewebsites.net/>

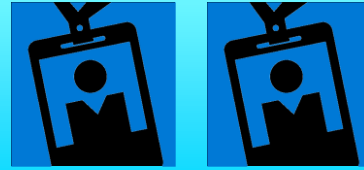


# USER TYPES IN A TENANT

Cloud-only Users



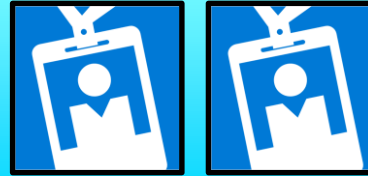
Partner Accounts



Microsoft Accounts



On-prem Accounts



# AZURE AD CONNECT

- Software installed on a machine in on-prem domain
- Synchronize on-prem AD accounts and groups to AAD
- Same account for intranet and cloud services -> *Hybrid Identity*
- Optional Password Sync
  - Allows users to sign in directly to AAD
  - If not using, authentication done against on-prem DC

# AZURE RBAC

- Give access rights in Azure with Role-Based Access Control (RBAC)
- **Access Control (IAM)** tab on:
  - Subscription
  - Or Resource Group
  - Or resource (like an SQL Database)
- Some available roles:
  - *Owner* = Do anything
  - *Contributor* = Read/write, cannot give access
  - *Reader* = Read-only

# MULTI-FACTOR AUTHENTICATION

- Very easy to set up, 99.9 % SLA
- Two-step verification with:
  - Phone calls
  - Text messages
- Multi-factor authentication with:
  - Azure Authenticator app, codes or push to confirm
- Different pricing models
  - 1.181 € / user / month
  - 1.181 € / 10 authentications
  - Special volume pricing for Enterprise Agreement customers

# GROUPS IN AZURE AD

- Groups can be used for various purposes
- Apps can check if user is in a group, base authorization on that
  - Apps can also define roles that can be assigned to users
  - Roles can be assigned to groups too
- Groups can also be members in groups = groupception
  - Membership is transitive
    - User A member of group 2, which is member of group 1 -> user is member of both groups
- Groups can be synced from on-prem AD





**DEMO**

AAD MANAGEMENT AND USER CREATION

# SAAS APPLICATION INTEGRATION

- Office 365
- Dropbox for Business
- Salesforce
- DocuSign
- Box
- Google Apps
- And *thousands* more..

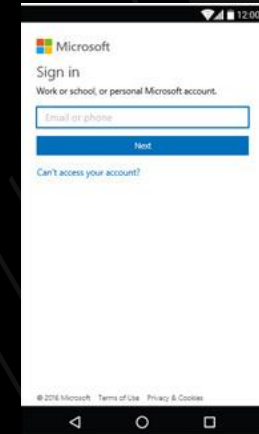
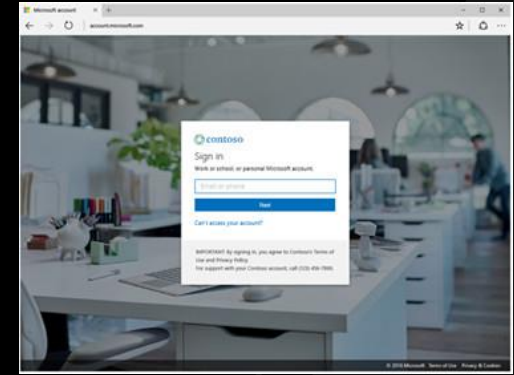


# REGISTERING YOUR APPS

- Applications developed by your organization can be registered to AAD
- By default *single tenant*, i.e. used only by your organization
- Can also make *multi-tenant* apps, can be used by any organization
  - SaaS applications
  - Users can use their own organizational accounts
  - *The other organization is responsible for things like password management*

# SUPPORTED APP TYPES

- Back-end Web applications
- Front-end Single Page Applications
- Mobile Applications
  - Android, iOS, Windows Phone
- Native Applications on Windows, Mac or Linux





# DEMO

WEB APP USING AZURE AD  
[WESTL.IN/AADDEMO](https://westl.in/aaddemo)

# SUMMARY

- Azure AD offers a superb highly available single sign-on system for applications using it
- Your organization can get access to thousands of existing applications
- Millions of possible users for your SaaS apps
- Rich user and access management features
- On-prem AD sync allows hybrid identity

# LINKS

- Documentation: <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-what-is>
- Developer guide: <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-developers-guide>
- Code samples: <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-code-samples>
- My posts on AAD: <https://joonasw.net/tag/azure-ad>



# THANKS!

QUESTIONS?



@JoonasWestlin



joonasw.net