

# 2017

## Global Azure **BOOTCAMP**



AzureHeads

 autoexec.gr

 SQLschool.gr

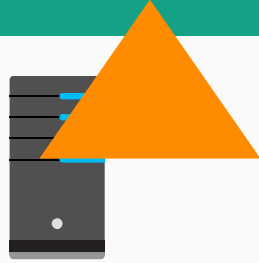


# Azure Active Directory: 5 reasons to implement it today!

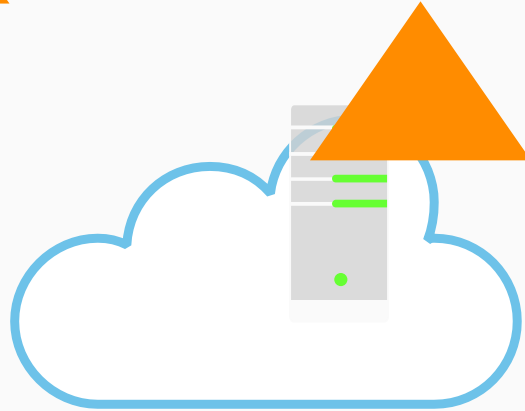
Chris Spanougakis MCT, MVP [EM]  
[chris@systemplus.gr](mailto:chris@systemplus.gr)  
<http://Spanougakis.com>  
@spanougakis  
●●●●●



# Overview of Azure Active Directory



On-premises  
Active Directory

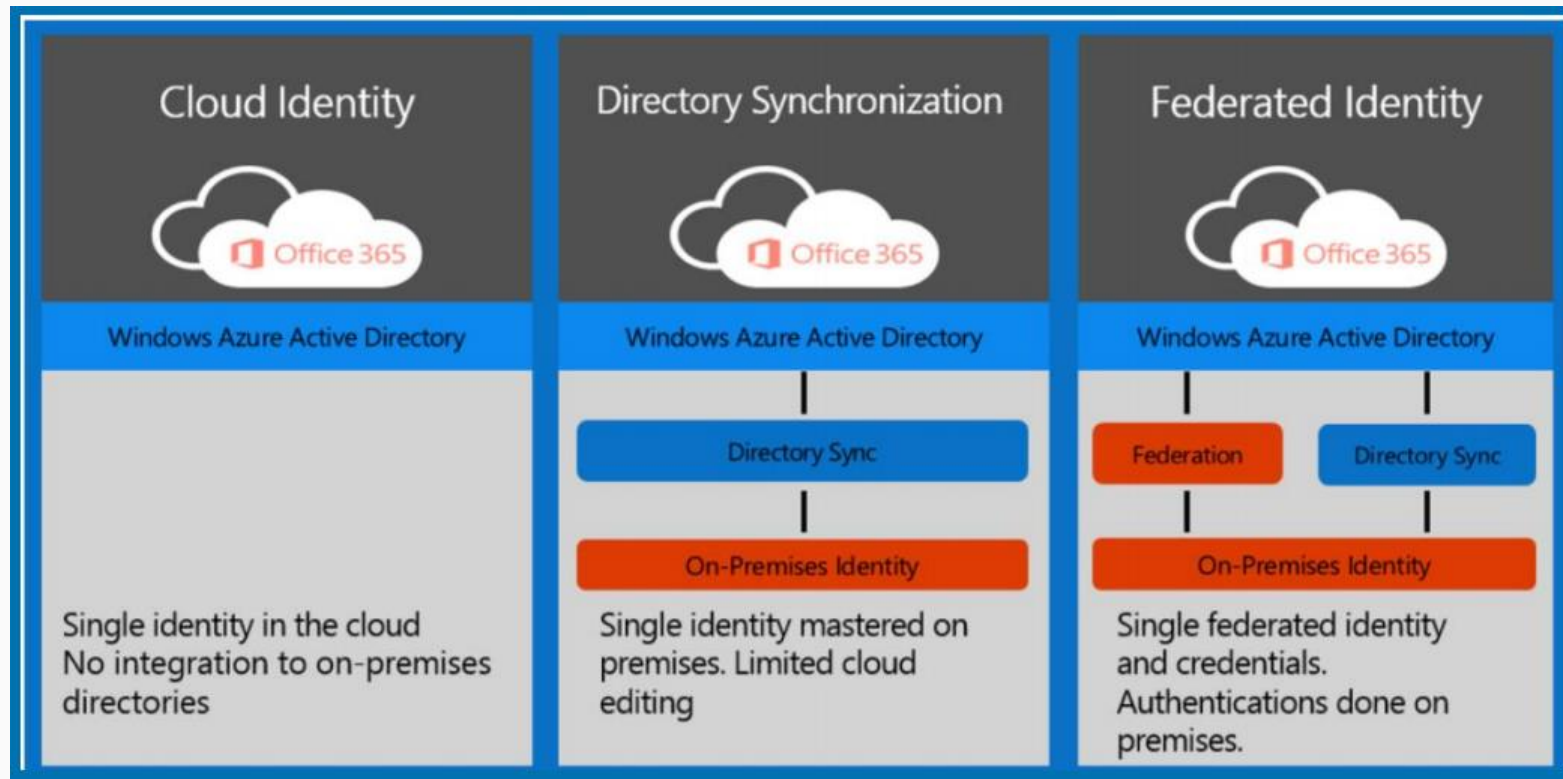


Active Directory  
on Azure VM



Azure Active  
Directory

# Σενάρια χρήσης του Azure AD

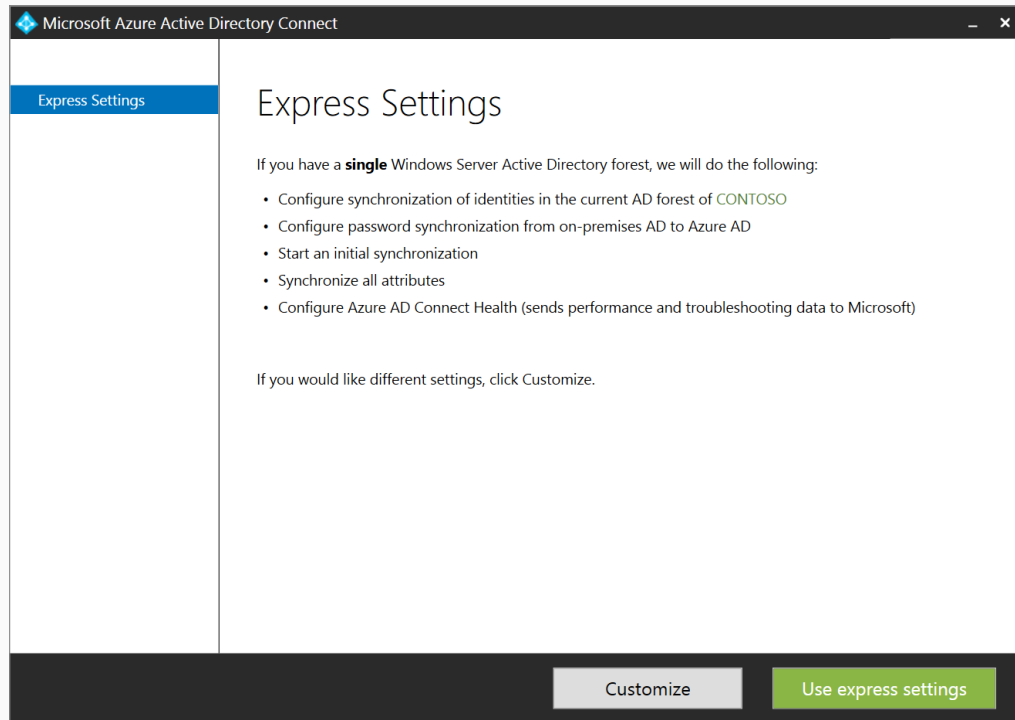


# Active Directory Synchronisation με το AADConnect

- Κατεβάζετε και εγκαθιστάτε το AADConnect σε κάποιον DC
- Πριν από τον συγχρονισμό, διορθώστε τα objects στο τοπικό σας AD με το εργαλείο IDFix, <https://www.microsoft.com/en-us/download/details.aspx?id=36832>
- Αναλυτικές πληροφορίες στο άρθρο [https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/#BKMK\\_ObjectLimits](https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/#BKMK_ObjectLimits)
- Active Directory Federation Services: Το χρειάζεστε? Ίσως όχι...

Requirement	Notes
"True" single sign-on	Domain joined computers – accessing Office 365 doesn't require users to re-enter credentials
ADFS will honor Active Directory configured login time restrictions for users.	
Integration with on-premises MFA server, or on-premises 3 <sup>rd</sup> party MFA services	ADFS has integration "hooks" if using MFA on-premises

# Azure AD Connect



- Use one tool instead of many
- Get up and running quickly (4 clicks)
- Start here, then scale up or add options
- Custom options to address more complex scenarios

Microsoft Azure Active Directory Connect

Welcome

Express Settings

Send Feedback

Show Help

# Welcome to Azure AD Connect

**Run this installation tool on the server where the synchronization service component will be installed.**

Azure Active Directory Connect integrates your on-premises and online directories.

This installation tool will:

- Guide you in selecting a solution (for example, password synchronization or single sign-on)
- Install identity synchronization and other Microsoft software components required to deploy the selected solution
- Verify the integration of your on-premises and online directories

[Learn more](#)

I agree to the [license terms](#) and [privacy notice](#).

Version 1.0.8642.0-20150617-232611  
Microsoft Internal Use Only

Continue

Microsoft Azure Active Directory Connect

Welcome

**Express Settings**

Connect to Azure AD

Connect to AD DS

Configure

## Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of **CONTOSO**
- Configure password synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes

[Learn more about express settings](#)

If you would like different settings, click Customize.

Send Feedback

Show Help

Version 1.0.8642.0-20150617-232611  
Microsoft Internal Use Only

Customize

Use express settings



- Welcome
- Express Settings
- Connect to Azure AD**
- Connect to AD DS
- Configure

## Connect to Azure AD

Enter your Azure AD credentials: ?

USERNAME

PASSWORD

Microsoft Azure Active Directory Connect

Welcome  
Express Settings  
Connect to Azure AD  
**Connect to AD DS**  
Configure

Send Feedback  
Show Help

# Connect to AD DS

Enter the Active Directory Domain Services enterprise administrator credentials: ?

USERNAME

PASSWORD

Version 1.0.8642.0-20150617-232611  
Microsoft Internal Use Only

Previous Next

Microsoft Azure Active Directory Connect

Welcome  
Express Settings  
Connect to Azure AD  
Connect to AD DS  
**Configure**

Send Feedback  
Show Help

## Ready to configure

Once you click Install, we will do the following:

- Install the synchronization engine
- Configure AAD Connector
- Configure contoso.com Connector
- Enable Password synchronization
- Configure synchronization services on this computer

Start the synchronization process as soon as the configuration completes.

Exchange hybrid deployment [?](#)

Version 1.0.8642.0-20150617-232611  
Microsoft Internal Use Only

Previous Install

Welcome

Express Settings

Connect to Azure AD

Connect to AD DS

Configure

## Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

**The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal.**

[Learn more](#)

# Azure AD Features

- Cloud User Self Service Password Reset

• Included in all Office 365 SKUs

• Available to all users

• Available to all users

• Available to all users

• Available to all users

• Available to all users

• Available to all users

• Available to all users

• Available to all users

• Available to all users

• Available to all users

• Available to all users

• Available to all users

• Available to all users

• Available to all users


Microsoft

## Reset your password

User verification

To reset your password, begin by entering your user ID and the characters in the picture or audio below.

\* User ID:

  
Example: user@contoso.onmicrosoft.com or user@contoso.com

Enter the characters in the picture or the words in the audio.

[Next](#) [Cancel](#)



# Configuring Multi-Factor Authentication Settings

The screenshot shows a web browser window displaying the Azure Multi-Factor Authentication management console. The browser's address bar shows the URL <https://phonefactor.net/traffactory>. The page title is "Azure Multi-Factor Authentication".

The main content area is titled "Welcome" and includes a "Contact Support" link. Below the welcome message, there are three main sections:

- VIEW A REPORT**: View usage of all users of Multi-Factor Authentication within an organization. Account ID: POHI-WH3-KFA33.
- CONFIGURE**: Configure Multi-Factor Authentication settings such as caching, voice messages and notifications received by users.
- DOWNLOADS**: Download the Multi-Factor Authentication Server.

The left sidebar contains a navigation menu with the following categories and items:

- USER ADMINISTRATION**
  - Block/Unblock Users
  - One-Time Bypass
- VIEW A REPORT**
  - Usage
  - Server Status
  - Blocked User History
  - Bypassed User History
  - Fraud Alert
  - Queued
- CONFIGURE**
  - Settings
  - Caching
  - Voice Messages
  - Notifications
- DOWNLOADS**
  - Server
  - SDK

# Configuring Advanced Multi-Factor Authentication Settings

- Fraud Alert
- One-Time Bypass
- Custom Voice Messages
- Trusted IPs
- App Passwords

# Azure AD Authenticator App (NEW!)



For added security, we need to further verify your account

How do you want us to verify your account?



chris@systemplus.gr  
Use mobile app to verify my account



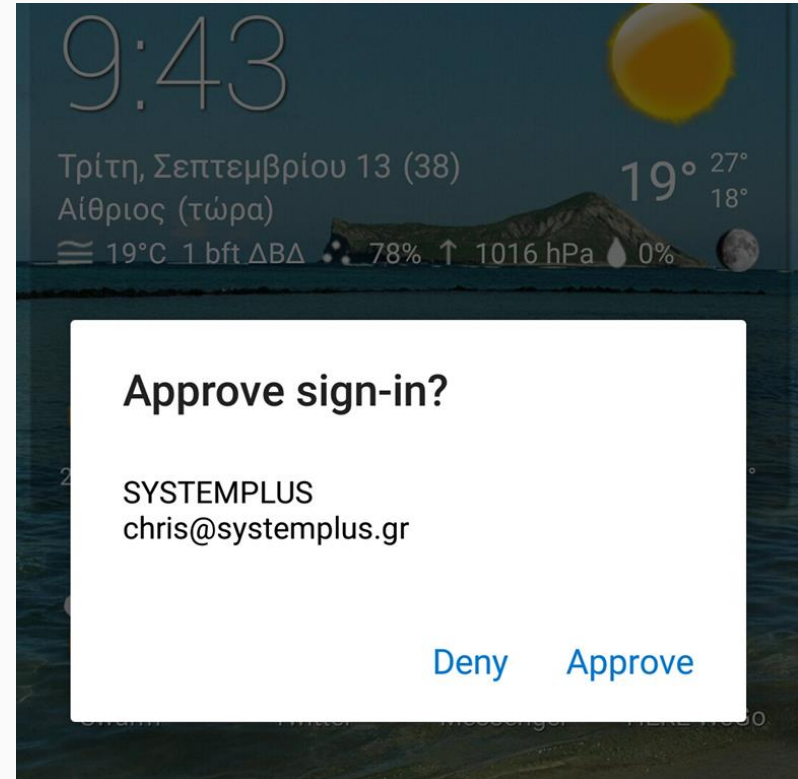
We've sent a notification to your mobile device. Please respond to continue.

Don't ask again for 14 days

[Use a different verification option](#)

[Sign out and sign in with a different account](#)

[More information](#)





# Azure AD per app MFA

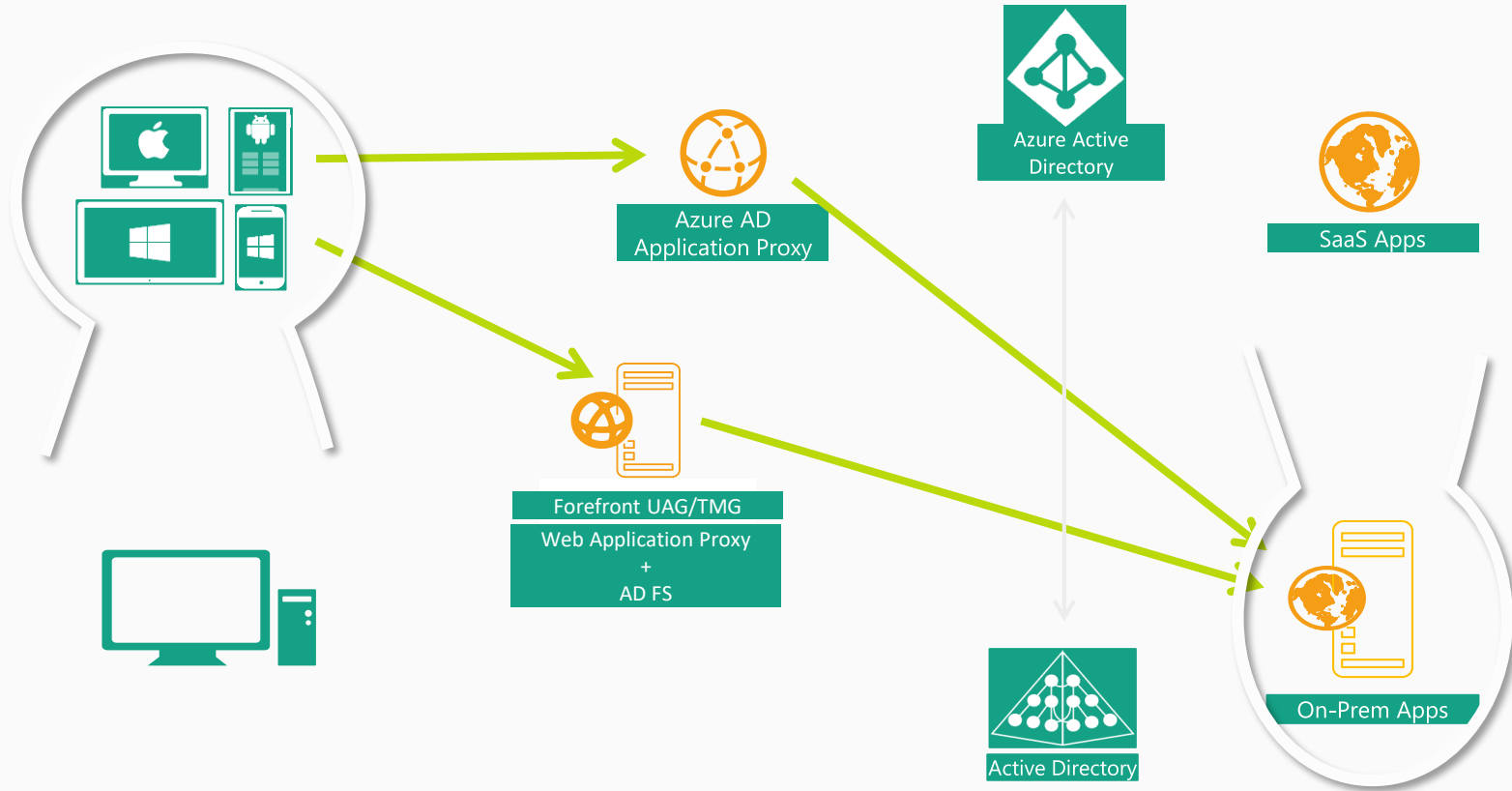
The screenshot displays the Microsoft Azure portal interface for configuring Dynamics CRM Online. The top navigation bar includes the Microsoft Azure logo, a dropdown arrow, a link to "Check out the new portal", and the user's email address "chris@systemplus.gr". The left-hand navigation pane lists various applications, with "Dynamics CRM O..." selected. The main content area is titled "dynamics crm online" and has two tabs: "DASHBOARD" and "CONFIGURE".

The "properties" section shows the application name set to "Dynamics CRM Online".

The "multi-factor authentication and location based access rules" section contains the following settings:

- ENABLE ACCESS RULES:** A toggle switch is currently set to "ON".
- APPLY TO:** A dropdown menu is set to "ALL USERS". There is an "EXCEPT" checkbox which is currently unchecked.
- RULES:** A list of three radio button options:
  - Require multi-factor authentication
  - Require multi-factor authentication when not at work
  - Block access when not at workA link below the rules states: "Click here to define/edit your work network location".

# Azure AD Application Proxy



# Benefits



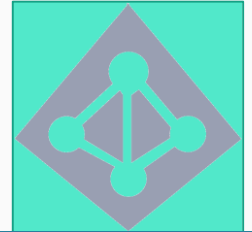
On-Premises  
Applications

## Remote Access as a Service

Easily publish your on-prem applications to users outside the corporate network

## Extend Azure AD to on-prem

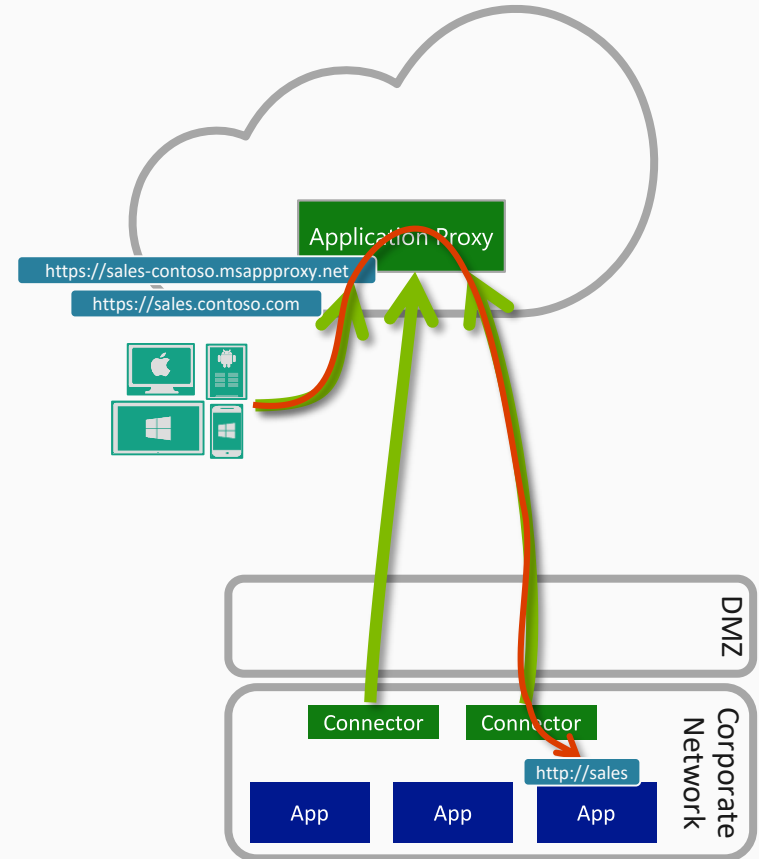
Utilize Azure AD as a central management point for all your apps



Azure Active  
Directory

# How it works

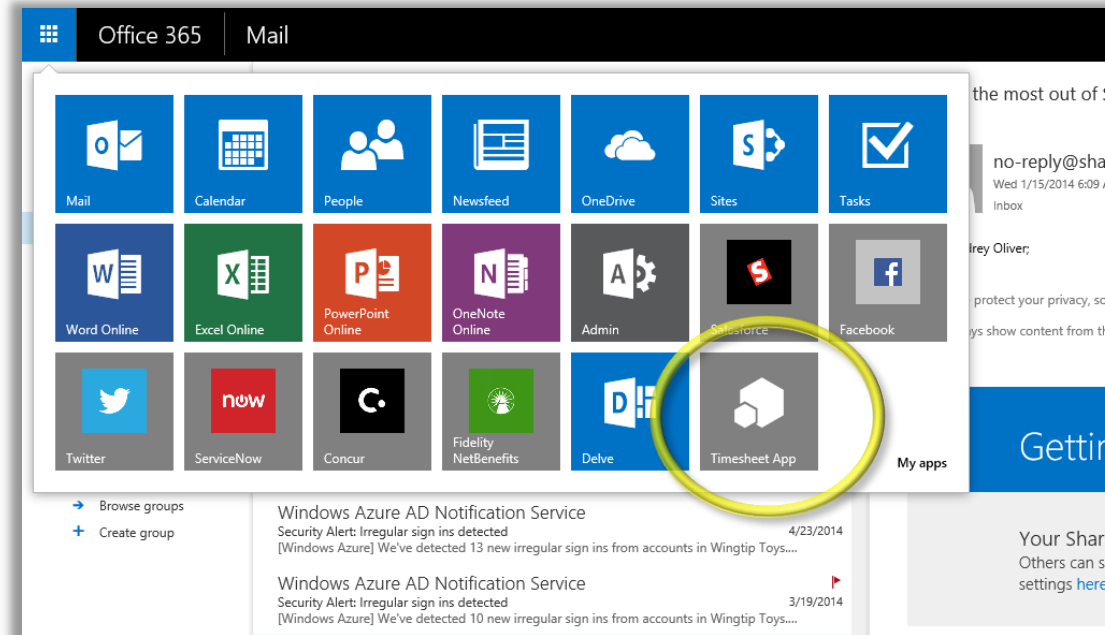
- Connectors are deployed on your network
- Multiple connectors can be deployed for redundancy and scale
- The connector auto connects to the cloud service
- User connects to the cloud service that routes their traffic to the resources via the connectors



# Works better with Office365

- Seamless single-sign-on from all Office 365 apps
- Add on-prem apps Office365 App Launcher.

- Same identity and security infrastructure for your on-prem apps and Office365



# Azure AD Identity Protection

**SYSTEMPLUS**  
Azure Active Directory - PREVIEW

Classic portal

The Azure AD management experience is in preview. [Learn more](#)

Search (Ctrl+F)

**MANAGE**

- Overview
- Quick start
- Users and groups
- Enterprise applications
- App registrations
- Azure AD Connect
- Domain names
- Password reset
- Company branding
- User settings
- Properties

**ACTIVITY**

- Sign-ins
- Audit logs

**Recommended**

- Sync with Windows Server AD**  
Sync users and groups from your on-premises directory to your Azure AD
- Self-service password reset**  
Enable your users to reset their forgotten passwords
- Company branding**  
Customize the text and graphics your users see when they sign in to your Azure AD

**Users and groups**

DU AD DA HE IT AD AD AD AD

**Enterprise applications**  
USERS SIGN INS

Date	Users Sign Ins
Aug 14	0
Aug 21	25
Aug 28	45
Sep 4	75
Sep 11	15

**Azure AD Connect**

Sync not enabled

**App registrations**

1

**Quick tasks**

- Add a user
- Add a group
- Find a user
- Find a group
- Find an enterprise app

**Other capabilities**

- Identity Protection
- Privileged Identity Management
- Cloud App Discovery

**What's new**

- Microsoft Authenticator: Updates to our hit app!
- 23 more apps now work with #AzureAD
- APIs for Microsoft Identity Protection are now available!

# Azure AD Identity Protection

The screenshot shows the Azure AD Identity Protection console for configuring a User risk remediation policy. The interface is divided into three main sections: a left-hand navigation pane, a central configuration area, and a right-hand control selection area.

**Navigation Pane (Left):**

- Search (Ctrl+/)
- GENERAL
  - Overview
  - Getting started
- INVESTIGATE
  - Users flagged for risk
  - Risk events
  - Vulnerabilities
- CONFIGURE
  - Multi-factor authentication regis...
  - User risk policy**
  - Sign-in risk policy
- SETTINGS
  - Alerts
  - Weekly Digest

**Policy Configuration (Center):**

- Policy name:** User risk remediation policy
- Assignments:**
  - Users: All users
  - Conditions: User risk
- Controls:** Access (Selected)
- Review:** Estimated impact: Number of users impacted
- Enforce Policy:** On (Selected), Off

**Control Selection (Right):**

Select the controls to be enforced.

- Block access
- Allow access
- Require multi-factor authentication
- Require Azure MFA registration
- Require password change

# Azure AD Identity Protection


Cloud optimize your business

Microsoft Azure  
**Your account is at risk**

We've detected suspicious activity on your account.

To help you—and only you—get back into feduser3@fabtoso.com, we need to verify your identity.


[Next](#)

© 2016 Microsoft. [Terms of use](#) [Privacy & Cookies](#) 

Cloud optimize your business

Microsoft Azure  
For added security, we need to further verify your account.

How do you want us to verify your account?

 **chris@systemplus.gr** \*\*\*  
Text me at -X XXXXXXXXXX

We've sent you a text message with a verification code.

[Sign in](#)

[Use a different verification option](#)  
[Sign out and sign in with a different account](#)  
[More information](#)

Cloud optimize your business

Microsoft Azure  
**Update your password**

Since someone else may have access to your account, you need to choose a new password. Don't use the same password that you use for other sites.  
[View details](#)

[Update password and sign in](#)




# Azure AD PIM

The screenshot displays the Azure AD PIM User Administrator interface, split into two panes. The left pane shows a list of users under the 'USER ADMINISTRATOR' group, with columns for 'USER', 'PERMISSION', and 'EXPIRATION'. The right pane shows configuration settings for 'Activations', 'Notifications', 'Incident/Request Ticket', and 'Multi-Factor Authentication'.

**User Administrator**  
PREVIEW

+ Add user | Filter | Refresh | Group | Review | Export | Settings

Search

USER	PERMISSION	EXPIRATION
USER ADMINISTRATOR		
 Admin2 admin2@systemplus.gr	Eligible	-

**Activations**  
Maximum Activation duration (hours) ⓘ  
24

**Notifications**  
Send email notifying admins of activation ⓘ  
Enable | Disable

**Incident/Request Ticket**  
Require Incident/Request ticket number during activation ⓘ  
Enable | Disable

**Multi-Factor Authentication**  
Require Azure Multi-Factor Authentication for activation ⓘ  
Enable | Disable

# Resources

- <http://systemplus.gr/trainingvideos.html>
- <http://mcse.gr/>
- <http://Spanougakis.com>
- <http://azureschool.net>
- <https://techcommunity.microsoft.com/t5/Azure-Active-Directory/bd-p/Azure-Active-Directory>
- @Spanougakis
- <https://blogs.technet.microsoft.com/enterprisemobility/?product=azure-active-directory>

Ερωτήσεις - Απαντήσεις



<https://aka.ms/cc9cf1>

Thank You

