



# Cyber Saiyan



800



800



2400



1700



700

<https://www.cybersaiyan.it>



# ROMHACK 2021

Saturday 25th of September



[romhack.io/cfp](https://romhack.io/cfp)

aperta fino al 28 Maggio

Entro fine Giugno: agenda & speaker  
12 Luglio: biglietti Eventbrite

Se interessati a  
sponsorizzare  
[info@cybersaiyan.it](mailto:info@cybersaiyan.it)





Organizzata in collaborazione con Hack The Box

**Si svolgerà sabato 18 Settembre, la settimana precedente**

Team illimitati

24 ore

Livello medium/hard



# Hands [off|on] MS cloud services

*Un approfondimento sulla sicurezza  
Azure AD e dintorni*

28 Aprile 2021




# Di cosa parliamo

- > Microsoft Cloud basic concepts
- > Azure AD Integration scenarios & licensing
- > Hardening Azure AD
- > Hunting



# Who? Antonio Formato

Technical Specialist Security & Compliance @ Microsoft

@anformato

<https://medium.com/@antonio.formato>



# Who? Andrea Pierini

IT Architect - Security Manager (and Security Researcher by passion)

@decoder\_it

<https://decoder.cloud>



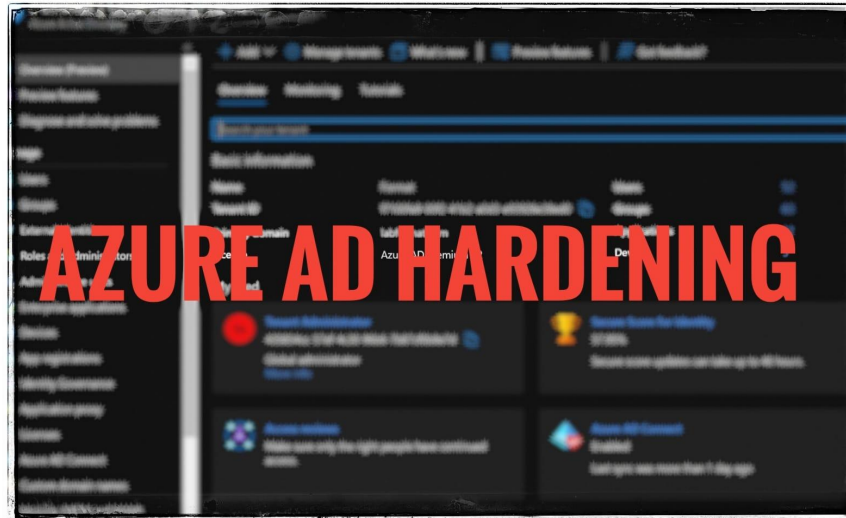
# Microsoft Cloud basic concepts





# Cloud Identity -> new challenges

- > Cloud adoption starts with **taking care of Identity** (or it should be)
- > There is **no single right way** to do cloud-based IAM and cloud security
- > Don't use on-prem mindset
- > Cloud is **not secure/insecure by default**
- > Do you have cloud workloads? Consider that **you still have responsibilities**
- > Cloud comes with **new challenges**



# Azure Active Directory - Definition

Azure Active Directory is Microsoft's **cloud-based directory** and **identity management service** that combines into a single solution

- > Core directory services
- > Application access management
- > Identity protection
- > Integration with on-prem Windows Server **Active Directory**

It's a standards-based platform that enables developers to deliver access control to their applications, based on **centralized policy and rules**

*Already using Office 365, Azure, or Dynamics CRM Online customers? You're already using Azure AD!*



# Azure Active Directory - Compare to AD

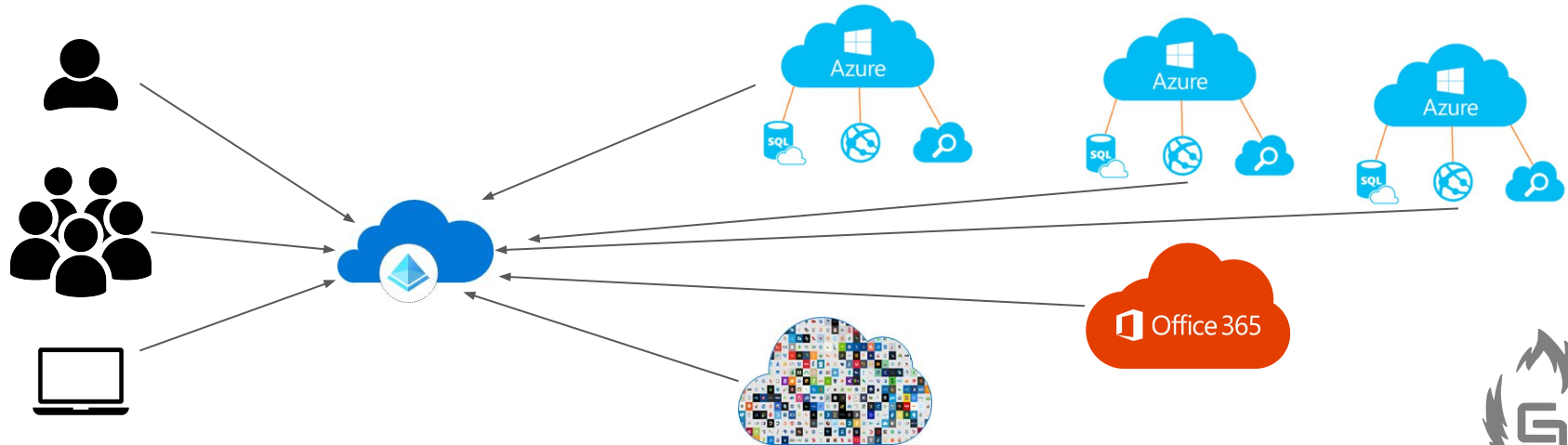
Active Directory	Azure Active Directory
Both store directory data, manage access to resources	
	Not just a domain controller in the cloud
Kerberos, NTLM	SAML, WS-Federation, OAuth and REST APIs (Graph)
	Conditional Access Policy → MFA
	Risk-based access protection
No native support for SaaS apps (federation required - AD FS)	SaaS apps supporting OAuth2, SAML, and WS-* authentication can be integrated
Domain joined Windows devices	Azure AD or Hybrid Azure AD joined devices. Modern device management

Do you want to test in lab environment? <https://go.microsoft.com/fwlink/p/?LinkID=403802>



# Azure Active Directory - Tenant Concept

- > An Azure AD tenant is a dedicated, trusted instance of Azure AD
- > Each Azure tenant has a dedicated, trusted Azure AD directory
  - > It contains users, groups and applications
  - > It performs identity and access management functions
- > One Office 365 tenant and multiple Azure Subscriptions can be associated to the org's Azure AD tenant
- > Multiple domains can be associated to an Azure AD tenant



# Azure Active Directory - Users, Groups and Azure Subscriptions

- > Azure AD **Global Administrators** have full access to all admin features and objects
- > Every Azure subscription has a **trust relationship with Azure AD** to authenticate users, services and devices
- > Multiple Azure Subscriptions can trust the same Azure AD directory, but a Subscriptions will only trust a single Azure AD directory

**Administrative roles**  
Administrative roles can be used to grant access to Azure AD and other Microsoft services. [Learn more](#)

Search by name or description  + Add filters

Role	Description
<input type="checkbox"/> Application administrator	Can create and manage all aspe
<input type="checkbox"/> Application developer	Can create application registrati
<input type="checkbox"/> Attack payload author	Can create attack payloads that
<input type="checkbox"/> Attack simulation administrator	Can create and manage all aspe
<input type="checkbox"/> Authentication administrator	Has access to view, set, and rese
<input type="checkbox"/> Authentication policy administrator	Can create and manage all aspe
<input type="checkbox"/> Azure AD joined device local administrator	Users assigned to this role are a
<input type="checkbox"/> Azure DevOps administrator	Can manage Azure DevOps org
<input type="checkbox"/> Azure Information Protection administrator	Can manage all aspects of the A

**Visual Studio Enterprise | Access control (IAM)**

Subscription

Search (Ctrl+/) + Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access **Role assignments** Roles Roles (Preview) Deny assignments Classic administrators

Number of role assignments for this subscription  / 2000

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

5 items (3 Users, 1 Service Principals, 1 Managed Identities)

<input type="checkbox"/>	Name	Type	Role	Scope
<input type="checkbox"/>	SOC [redacted]	App	Azure Sentinel Contributor	This resource
<input type="checkbox"/>	Giuseppe [redacted] giuseppe [redacted]	User	Contributor	This resource
<input type="checkbox"/>	test /subscriptions/[redacted]	Logic App	Contributor	This resource



# Azure Active Directory - Users, Groups and Azure Subscriptions

> Users and Groups can be **Cloud Only** or **Synchronized** from on-premises Active Directory

> Cloud Only objects can be created, managed and deleted directly from the Azure Portal or PowerShell and graph APIs

> Synchronized objects cannot be modified in the cloud since their authoritative source remains the on-premises AD

This page includes previews available for your evaluation. View previews →

Search users Add filters

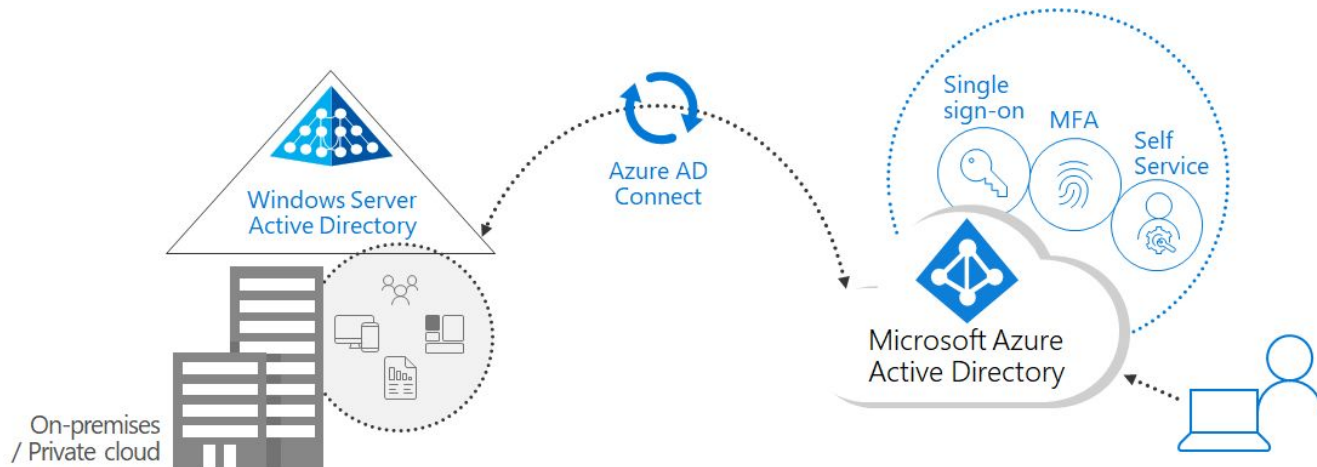
52 users found

Name	User principal name	User type	Directory synced	Identity issuer	Company name	Creation type
<input type="checkbox"/> Adele Vance	AdeleV@...	Member	No	M...	...	
<input type="checkbox"/> AD admin	admin@...	Member	No	M...	...	
<input type="checkbox"/> AD aduser1	aduser1@...	Member	Yes	M...	...	
<input type="checkbox"/> AF aformato	aformato_...it#E...T...	Guest	No	M...	...	Invitation
<input type="checkbox"/> Alex Wilber	AlexW@...	Member	No	M...	...	



# Azure Active Directory - Hybrid Identity

- > Achieved by integrating on-prem Active Directory with Azure AD using **Azure AD Connect**
- > It means you have common identity for your users for O365, Azure, 3rd party SaaS and on-prem apps
- > Single user identity for authentication and authorization to all resources, regardless of location



# Azure AD - Integration Scenarios





# Azure AD - integration scenarios

Cloud Identity



Azure Active Directory

Independent cloud identities

Synchronized Identity



Azure Active Directory

Azure AD Connect

Active Directory

Single identity, enabling single sign-on experience with Password Hash Sync or Pass-Through

Federated Identity



Azure Active Directory

Azure AD Connect

Federation

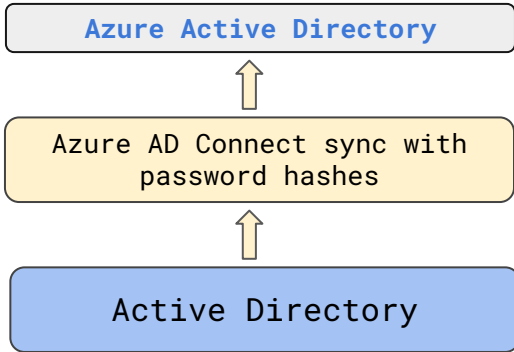
Active Directory

Single federated identity, single sign-on experience and on-premise multi-factor authentication options



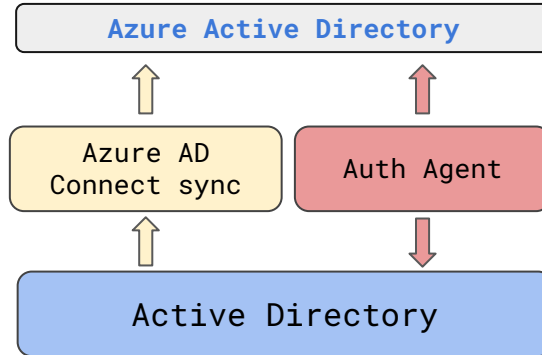
# Azure AD - hybrid authentication options

## Password-Hash Sync



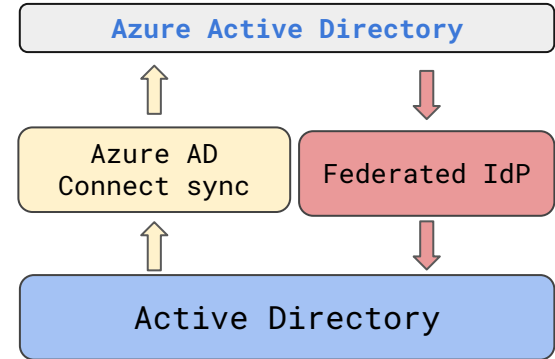
AuthN performed by Azure AD using synchronized password hashes

## Pass-Through Auth - PTA



AuthN performed by AD via authentication agent that looks for request via outbound communication

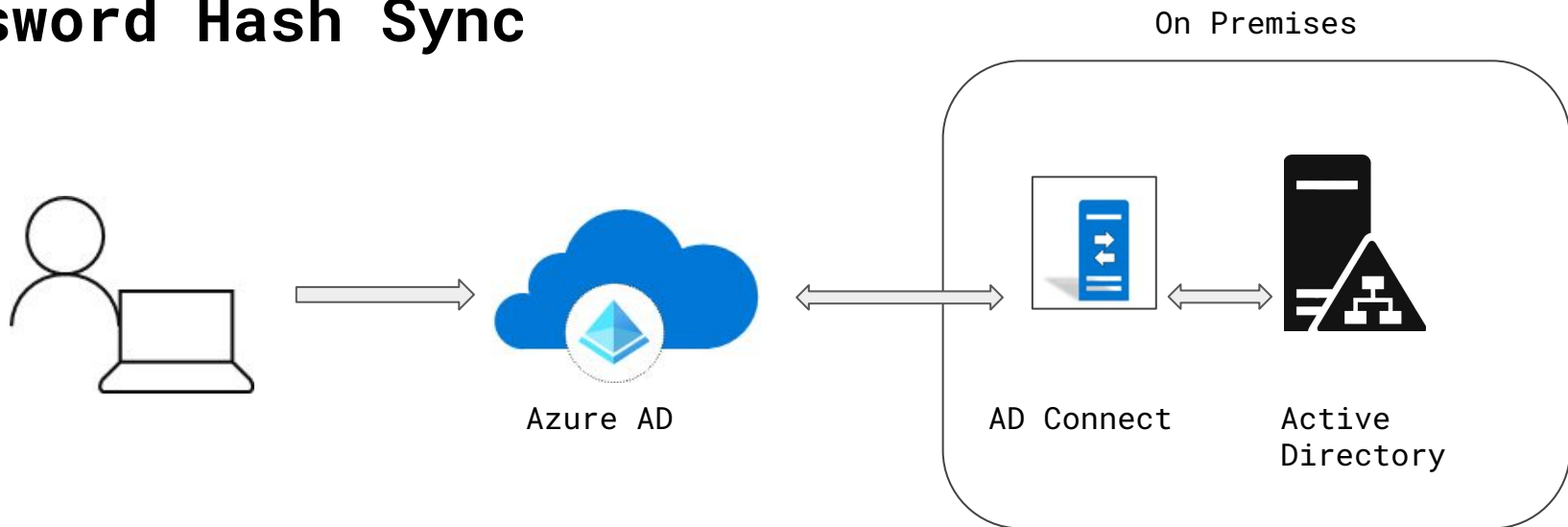
## Federated Authentication



AuthN performed by AD via federated identity provider



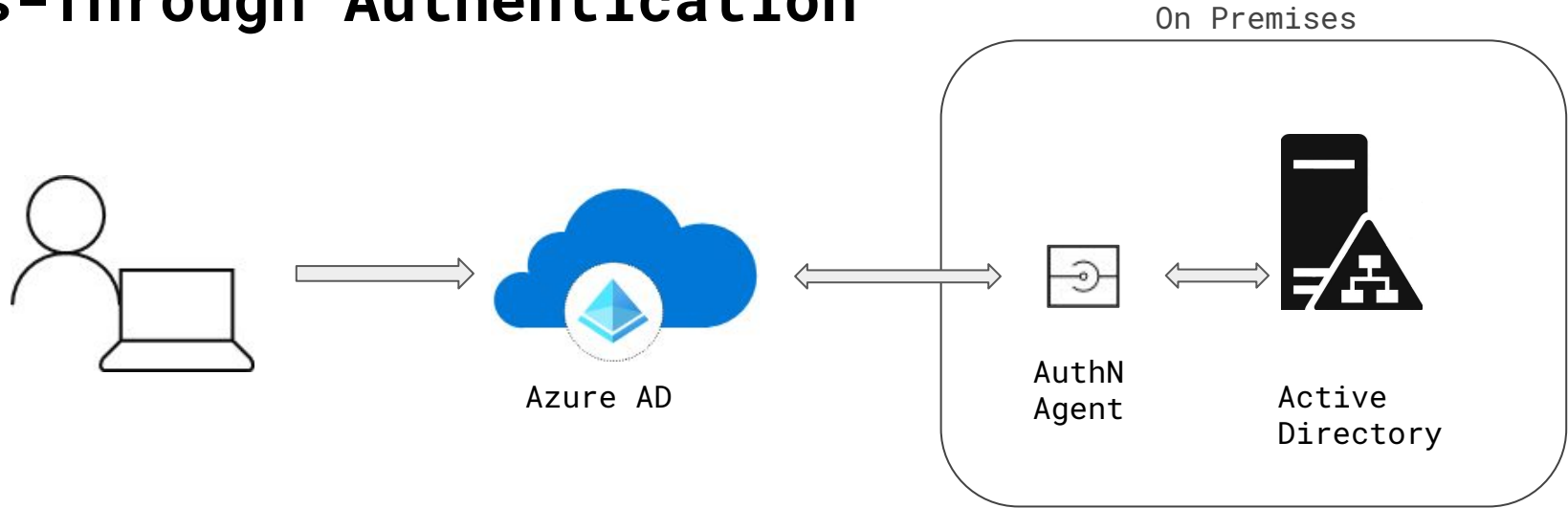
# Password Hash Sync



- > PHS doesn't sync password → Rather, it **syncs hash of the hash of user's passwords**
- > **SHA256 hash cannot be decrypted** so the plain-text version of the password is never and can never be exposed to Microsoft
- > Discover leaked credentials → Azure AD Identity Protection (it requires AAD P2)
- > Optionally, you can set up password hash synchronization as a backup if you decide to use Federation with AD FS



# Pass-Through Authentication

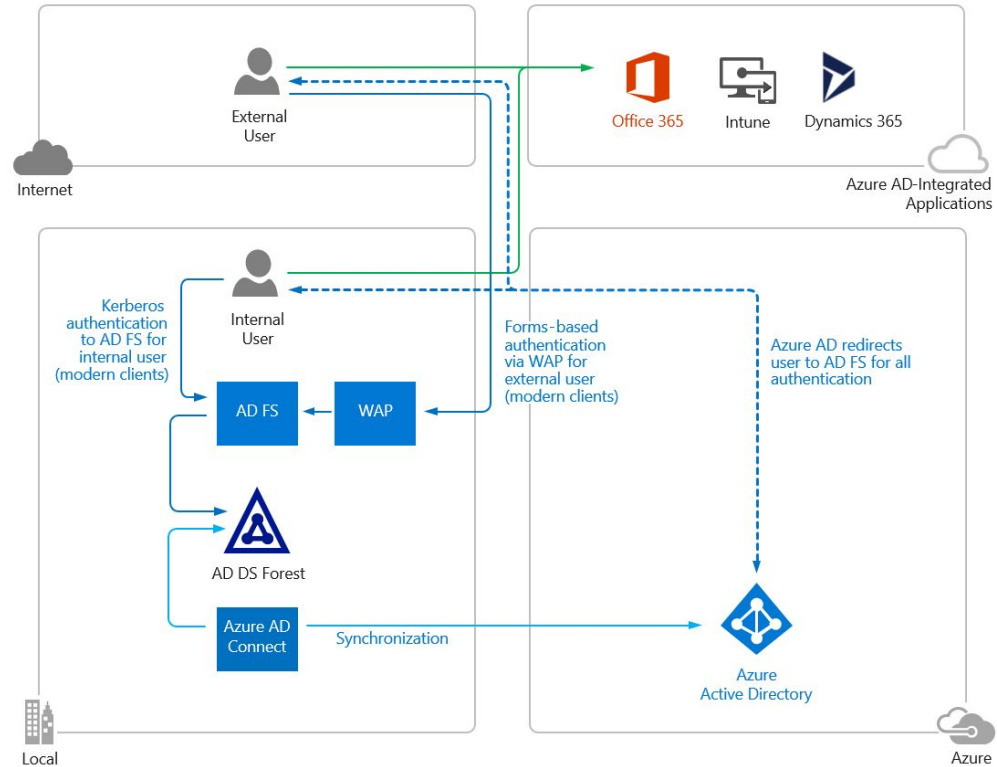


- > It provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers
- > The servers validate the users directly with your on-premises Active Directory, which ensures that the **password validation doesn't happen in the cloud**
- > The agent only makes **outbound connections** from within your network
- > The communication between an agent and Azure AD is secured using **certificate-based authentication**



# Federated Authentication

1. User **requests** access to application and is referred to Azure AD
2. User **identified** to Azure AD and **redirected** to the federated identity provider (IdP)
3. IdP **authenticates** the user, via seamless SSO when possible
4. User is **issued** a **token** and returned to Azure AD
5. Azure AD **verifies** the **token** and returns the user to the application with a resource token



Stealing AD FS Secrets, example: <https://o365blog.com/post/adfs/>

**Best Practices securing AD FS:**

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs>



# Azure AD - Licensing



# Azure AD editions and licensing

Focused on security related features

- > **Free**: MFA via Authenticator App and single sign-on across Azure
- > **P1**: MFA, Conditional Access, cloud write-back capabilities (i.e. self-service password reset), passwordless authentication
- > **P2**: identity protection, **risk-based conditional access** and **Privileged Identity Management** just-in-time administrative access



# Azure AD editions and licensing - logging

## How long does Azure AD store the data?

Report	Azure AD Free	Azure AD Premium P1	Azure AD Premium P2
Audit logs	7 days	30 days	30 days
Sign-ins	7 days	30 days	30 days
Azure AD MFA usage	30 days	30 days	30 days

You can route Azure Active Directory (Azure AD) logs to several endpoints for long term retention and data insights.

- > Archive Azure AD activity logs to an **Azure storage account**, to retain the data for a long time
- > Stream Azure AD activity logs to an **Azure event hub** for analytics, using **SIEM** tools
- > Send Azure AD activity logs to **Azure Monitor logs** to enable rich visualizations, monitoring and alerting on the connected data.





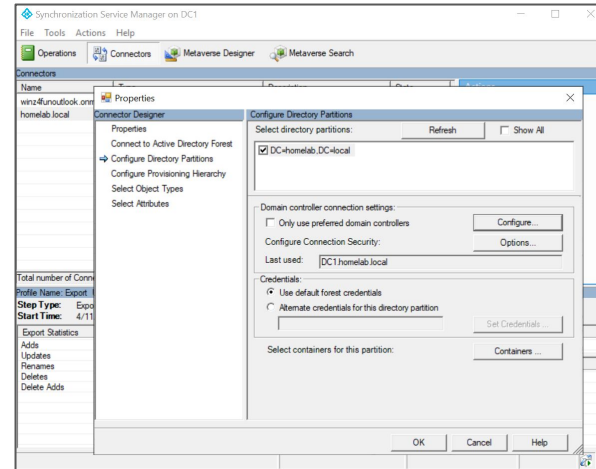
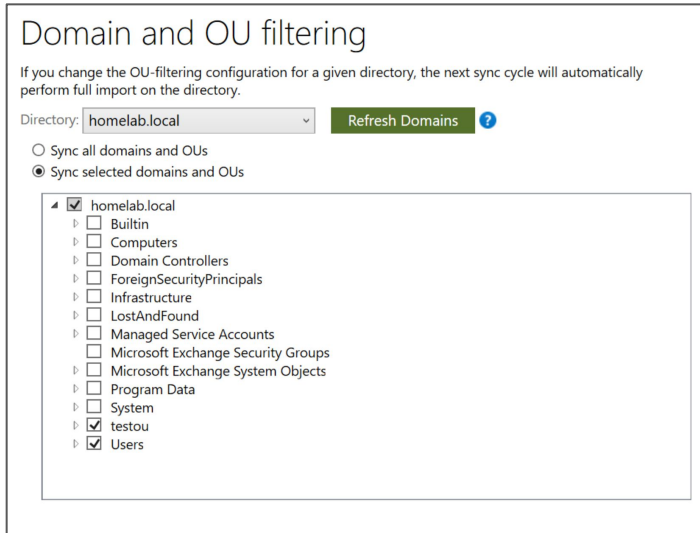
# Hardening Azure AD



# Don't replicate everything!

> Synchronize only the necessary objects/attributes (like users) and who really need to access online services or need to be managed online

> Do not sync on prem Admins (**On prem Admins != Azure Ad Admins**)



# Control Administrative Access (1 / 2)

> Reduce the number of persistent Global Admins (min.2, max <5), do you really need more?

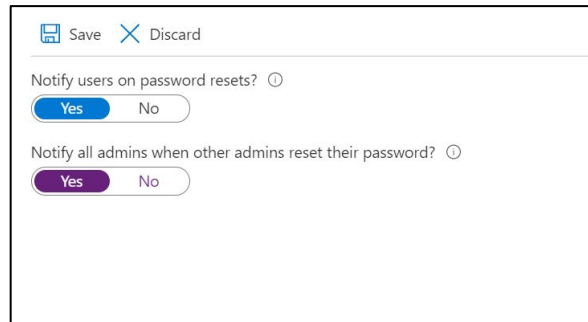
> Adopt Role Based Access Control (RBAC), create dedicated cloud only accounts for each user with specific administrative roles

Role	Description	Type
<input type="checkbox"/> Application administrator	Can create and manage all aspects of app registrations and enterprise apps.	Built-in
<input type="checkbox"/> Application developer	Can create application registrations independent of the 'Users can register applications' setting.	Built-in
<input type="checkbox"/> Attack payload author	Can create attack payloads that an administrator can initiate later.	Built-in
<input type="checkbox"/> Attack simulation administrator	Can create and manage all aspects of attack simulation campaigns.	Built-in
<input type="checkbox"/> Authentication administrator	Has access to view, set, and reset authentication method information for any non-admin user.	Built-in
<input type="checkbox"/> Authentication policy administrator	Can create and manage all aspects of authentication methods and password protection policies.	Built-in
<input type="checkbox"/> Azure AD joined device local administrator	Users assigned to this role are added to the local administrators group on Azure AD-joined devices.	Built-in
<input type="checkbox"/> Azure DevOps administrator	Can manage Azure DevOps organization policy and settings.	Built-in
<input type="checkbox"/> Azure Information Protection administrator	Can manage all aspects of the Azure Information Protection product.	Built-in
<input type="checkbox"/> B2C IEF Keyset administrator	Can manage secrets for federation and encryption in the Identity Experience Framework.	Built-in
<input type="checkbox"/> B2C IEF Policy administrator	Can create and manage trust framework policies in the Identity Experience Framework.	Built-in
<input type="checkbox"/> Billing administrator	Can perform common billing related tasks like updating payment information.	Built-in
<input type="checkbox"/> Cloud application administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	Built-in
<input type="checkbox"/> Cloud device administrator	Full access to manage devices in Azure AD.	Built-in
<input type="checkbox"/> Compliance administrator	Can read and manage compliance configuration and reports in Azure AD and Office 365.	Built-in
<input type="checkbox"/> Compliance data administrator	Can create and manage compliance content.	Built-in
<input type="checkbox"/> Conditional Access administrator	Can manage conditional access capabilities.	Built-in
<input type="checkbox"/> Customer LockBox access approver	Can approve Microsoft support requests to access customer organizational data.	Built-in
<input type="checkbox"/> Desktop Analytics administrator	Can access and manage Desktop management tools and services.	Built-in
<input type="checkbox"/> Directory readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.	Built-in



# Control Administrative Access (2 / 2)

- > If you have P1 or P2 plan, use Privileged Identity Management, it allows to implement just-in-time privileged access to Azure resources and Azure AD with approval flows
- > Use Multi Factor Authentication (needless to say...?)
- > Notify all admins when other admins reset their password



The screenshot shows a settings dialog box with a 'Save' button and a 'Discard' button. It contains two toggle switches:

- 'Notify users on password resets?' with the 'Yes' toggle selected.
- 'Notify all admins when other admins reset their password?' with the 'Yes' toggle selected.



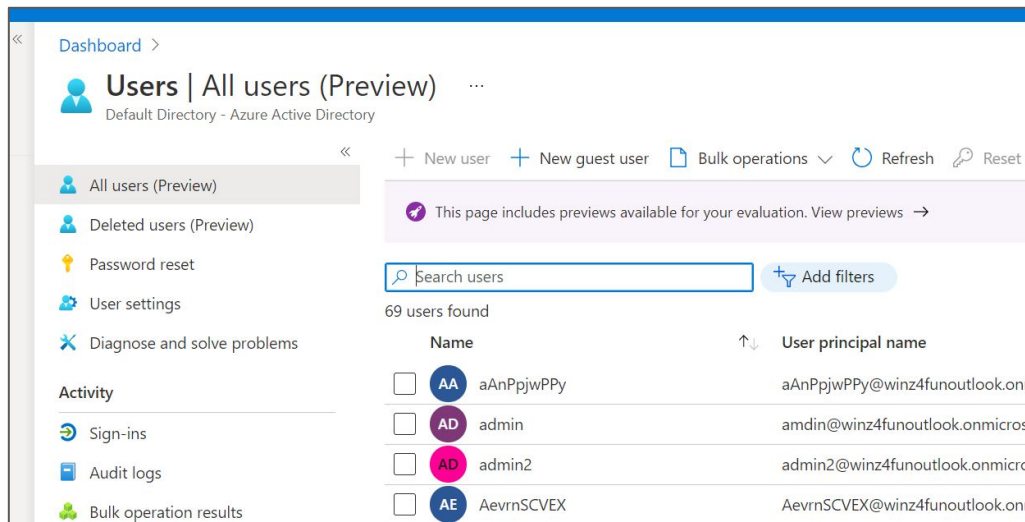
## Control / Restrict Access to non admin users

- > What are the risks in the event of credential or auth. tokens theft?
  - > What "sensitive" information can they can access?
  - > What "malicious" activities can they do?
- > Can we prevent this?



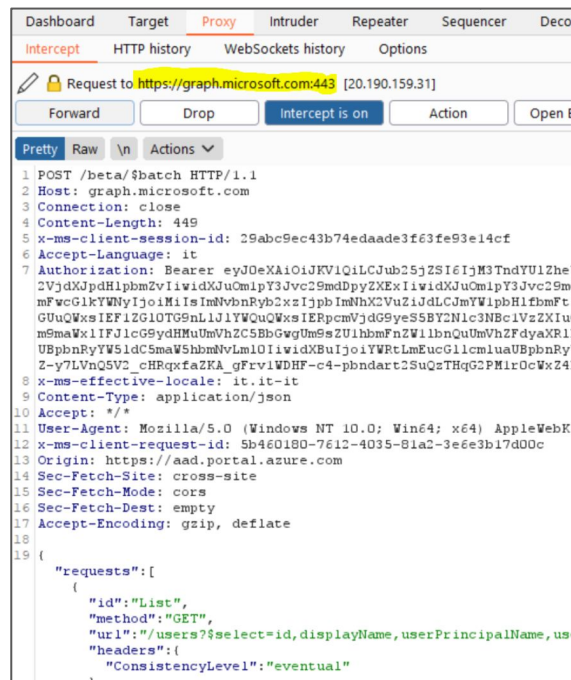
# Restrict Access to Azure Portal (1 / 2)

> By default, every Azure AD user can access the portal even without specific roles and browse the entire Azure AD including users, groups, apps...



The screenshot shows the Azure AD Users page. The left sidebar contains navigation options: All users (Preview), Deleted users (Preview), Password reset, User settings, Diagnose and solve problems, Activity, Sign-ins, Audit logs, and Bulk operation results. The main content area shows a search bar with 'Search users' and 'Add filters' buttons. Below the search bar, it indicates '69 users found'. A table lists users with columns for Name and User principal name. The first few users are:

Name	User principal name
<input type="checkbox"/> AA aAnPpjwPPy	aAnPpjwPPy@winz4funoutlook.onm
<input type="checkbox"/> AD admin	amdin@winz4funoutlook.onmicro
<input type="checkbox"/> AD admin2	admin2@winz4funoutlook.onmicro
<input type="checkbox"/> AE AevrnSCVEX	AevrnSCVEX@winz4funoutlook.onm



The screenshot shows a proxy tool interface with the 'Proxy' tab selected. The 'Intercept' button is highlighted in yellow. Below the toolbar, a request to `https://graph.microsoft.com:443` is shown. The 'Intercept is on' button is active. The request details are displayed in a 'Pretty' view:

```
1 POST /beta/$batch HTTP/1.1
2 Host: graph.microsoft.com
3 Connection: close
4 Content-Length: 449
5 x-ms-client-session-id: 29abc9ec43b74edaade3f63fe93e14cf
6 Accept-Language: it
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJub25jZSI6IjM3TndYU1Zhe
  2VjdXJpdHlphmZvIiwidXJuOmlpY3Jvc29mdDpyZXNlIiwidXJuOmlpY3Jvc29m
  mFwcGkYWNyIjoieMIIsImNbnRyb2xzIjpbImNhX2VuZiJdLCJmYWV1pbH1ibmFt
  GUuQWxsIEF1ZG10TG9nLjU1YWQWxsIERpcmVjdg9yeS5BY2Nlc3N8c1VzZTUu
  mSmaWx1IFJlcG9ydHMUbnVhZC5BbGwgUm9sZU1hbmFnZW11bnQuUmVhZC5BbGwg
  UBpbmRyYW5ldC5maW5hbmVhZC5BbGwgUm9sZU1hbmFnZW11bnQuUmVhZC5BbGwg
  Z-y7LVnQ5V2_cHRxZaZKA_gFrviWDFH-c4-pbndart2SuQsTHqG2PM1r0cWxZ4
8 x-ms-effective-locale: it-it
9 Content-Type: application/json
10 Accept: */*
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
12 x-ms-client-request-id: 5b460180-7612-4035-81a2-3e6e3b17d00c
13 Origin: https://aad.portal.azure.com
14 Sec-Fetch-Site: cross-site
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Accept-Encoding: gzip, deflate
18
19 {
  "requests": [
    {
      "id": "List",
      "method": "GET",
      "url": "/users?$select=id,displayName,userPrincipalName,us
      "headers": {
        "ConsistencyLevel": "eventual"
      }
    }
  ]
}
```



# Restrict Access to Azure Portal ( 2 / 2 )

> Azure AD is normally exposed over the internet and in case of credential theft this could be a serious security issue.. restrict access!

Save Discard

---

Enterprise applications  
[Manage how end users launch and view their applications](#)

App registrations  
Users can register applications ⓘ  
 Yes  No

Administration portal  
Restrict access to Azure AD administration portal ⓘ  
 Yes  No

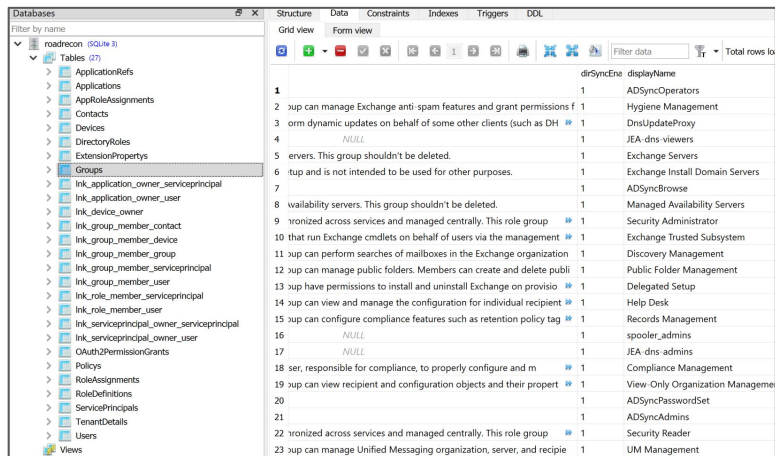


# Restrict Access to Azure Portal.. is this enough?

> NO! A standard user can still access the entire set of API's and gather a lot of informations...

> "Roadrecon" by @\_dirkjan a great tool for red teamers

<https://dirkjanm.io/introducing-roadtools-and-roadrecon-azure-ad-exploration-framework/>



dirSyncEnt	displayName
1	ADSyncOperators
2	up can manage Exchange anti-spam features and grant permissions f
3	orm dynamic updates on behalf of some other clients (such as DH
4	NULL
5	eners. This group shouldn't be deleted.
6	tup and is not intended to be used for other purposes.
7	ADSyncBrowse
8	availability servers. This group shouldn't be deleted.
9	rionized across services and managed centrally. This role group
10	that run Exchange cmdlets on behalf of users via the management
11	up can perform searches of mailboxes in the Exchange organization
12	up can manage public folders. Members can create and delete publi
13	up have permissions to install and uninstall Exchange on provisio
14	up can view and manage the configuration for individual recipient
15	up can configure compliance features such as retention policy tag
16	NULL
17	NULL
18	ser, responsible for compliance, to properly configure and m
19	up can view recipient and configuration objects and their properti
20	ADSyncPasswordSet
21	ADSyncAdmins
22	rionized across services and managed centrally. This role group
23	up can manage Unified Messaging organization, server, and recipie

```
root@kali-andrea:~# roadrecon auth -u [REDACTED]
Password:
Tokens were written to .roadtools_auth
root@kali-andrea:~# roadrecon dump
Starting data gathering phase 1 of 2 (collecting objects)
Starting data gathering phase 2 of 2 (collecting properties and relationships)
ROADrecon gather executed in 71.17 seconds and issued 3252 HTTP requests.
```





# The MSOL powershell module

> Even if “deprecated”, a standard user can access a lot of interesting `get-msol*` cmdlets

<https://docs.microsoft.com/en-us/powershell/module/msonline/get-msoluser?view=azureadps-1.0>

```
PS C:\temp> Connect-MsolService -Credential $credential
PS C:\temp> Get-MsolUser -SearchString admin
```

UserPrincipalName	DisplayName	isLicensed
-----	-----	-----
admin@winz4funoutlook.onmicrosoft.com	admin	False
admin2@winz4funoutlook.onmicrosoft.com	admin2	False

```
PS C:\temp> Get-MsolGroup
```

ObjectId	DisplayName	GroupType
-----	-----	-----
db21cc41-0168-4163-bb1f-503fd9c8d110	DnsAdmins	Security
194cc360-f7c9-4f82-b171-84a4a92b4ce5	DnsUpdateProxy	Security
0ca901e5-c2a7-42ef-98bb-eecc1dac68f4	ADSyncOperators	Security
1af5bca4-6bf9-4cd4-8b14-fd6164d9582f	JEA-dns-viewers	Security
b0edec50-7b21-4454-87a9-b399c02fccae	ADSyncAdmins	Security
3a1815a7-c9cb-4f98-896c-10a31019fbc7	ADSyncBrowse	Security
ade0beeb-04e9-4b7e-ba13-fa6462b1d2a8	ADSyncPasswordSet	Security
7c9b4e0c-d908-4e16-a01a-2197951e680a	JEA-dns-admins	Security
798414e2-68b0-40d3-a7bc-2bf9d31a386b	spooler_admins	Security

The screenshot shows a REST client interface with a request and response for a Microsoft Online Services API endpoint. The request is a POST to `/provisioningwebservice.svc` with a SOAP XML body. The response is an XML document containing user information for `admin2@winz4funoutlook.onmicrosoft.com`.

**Request**

```
POST /provisioningwebservice.svc HTTP/1.1
Content-Type: application/soap+xml; charset=utf-8
Host: provisioningapi.microsoftonline.com
Content-Length: 12638
Expect: 100-continue
Accept-Encoding: gzip, deflate
Connection: close
```

**Response**

```
<?xml version='1.0' encoding='utf-8'>
<rs:rsEnvelope xmlns:rs="http://www.w3.org/2001/XMLSchema-instance" xmlns:b="BecVersion">
  <b:SecVersion>Version 16</b:SecVersion>
  <b:TenantId i:nil="true"/>
  <b:VerifiedDomain i:nil="true"/>
  <b>UserSearchDefinition xmlns:c="http://schemas.datacontract.org/2004/07/Microsoft.Online.Administration">
    <c:PageSize>500</c:PageSize>
    <c:SearchString>admin</c:SearchString>
    <c:SortDirection>Ascending</c:SortDirection>
    <c:SortField>None</c:SortField>
    <c:AccountsSku i:nil="true"/>
    <c:BlackberryUsersOnly i:nil="true"/>
    <c:City i:nil="true"/>
    <c:Country i:nil="true"/>
    <c:Department i:nil="true"/>
    <c:DomainName i:nil="true"/>
    <c:EnabledFilter i:nil="true"/>
    <c:HasErrorsOnly i:nil="true"/>
    <c:IncludedProperties i:nil="true"/>
  </b>UserSearchDefinition>
  <b:UserSearchDefinition xmlns:d="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
    <c:IndirectLicenseFilter i:nil="true"/>
    <c:LicenseReconciliationNeededOnly i:nil="true"/>
    <c:ReturnDeletedUsers i:nil="true"/>
    <c:State i:nil="true"/>
    <c:Syncronized i:nil="true"/>
    <c>Title i:nil="true"/>
    <c:UnlicensedUsersOnly i:nil="true"/>
    <c:UsageLocation i:nil="true"/>
  </b>UserSearchDefinition>
</rs:rsEnvelope>
```



# Restrict Access to MSOL powershell (1 / 2)

> As an admin run the MSOL cmdlet

```
Set-MsolCompanySettings -UsersPermissionToReadOtherUsersEnabled $false
```

```
PS C:\Users\Administrator>  
PS C:\Users\Administrator> Set-MsolCompanySettings -UsersPermissionToReadOtherUsersEnabled $false  
PS C:\Users\Administrator>
```

> This setting will prevent access to a lot of unwanted queries...

```
PS C:\temp> Connect-MsolService -Credential $credential  
PS C:\temp> Get-MsolUser -all  
Get-MsolUser : Access Denied. You do not have permissions to call this cmdlet.  
At line:1 char:1  
+ Get-MsolUser -all  
+ ~~~~~  
+ CategoryInfo          : OperationStopped: (:) [Get-MsolUser], MicrosoftOnlineException  
+ FullyQualifiedErrorId : Microsoft.Online.Administration.Automation.AccessDeniedException,Microsoft.Online.Administration.Automation.GetUser
```



# Restrict Access to MSOL powershell ( 2 / 2 )

> And “dangerous” tools too :-)

<https://dirkjanm.io/introducing-roadtools-and-roadrecon-azure-ad-exploration-framework/>

```
root@kali-andrea:~# roadrecon dump
Starting data gathering phase 1 of 2 (collecting objects)
Error 403 for URL https://graph.windows.net/96b30cb9-e66c-49f4-b89e-1d9784fa8084/users?api-version=1.61-internal
{"odata.error":{"code":"Authorization_RequestDenied","message":{"lang":"en","value":"Insufficient privileges to complete the operation."},"requestId":"f3635cb8-292b-409d-99cd-89c7ea583af8","date":"2021-04-12T17:43:11"}}
```

<https://o365blog.com/aadinternals/>

```
PS /root> Get-AADIntUsers -AccessToken $tok
Exception: /root/.local/share/powershell/Modules/AADInternals/0.4.4/ProvisioningAPI_utils.ps1:158
Line |
158 | ...           throw $Response.Envelope.Body.Fault.Reason.Text.'#text'
      | ~~~~~
      | Current user is not authorized to perform this task.
```

<https://o365blog.com/post/phishing/>

```
PS C:\andrea> .\devicelogin.ps1
Device code is: DMSQ6M3Q4
Phishing email sent, waiting for user to authenticate...
Got access token!
User has been phished!! ... dumping AD info...
Current user is not authorized to perform this task.
At C:\Program Files\WindowsPowerShell\Modules\aadinternals\0.4.4\ProvisioningAPI_utils.ps1:158 char:17
+ ...           throw $Response.Envelope.Body.Fault.Reason.Text.'#text'
+ ~~~~~
+ CategoryInfo          : OperationStopped: (Current user is...form this task.:String) [], RuntimeException
+ FullyQualifiedErrorId : Current user is not authorized to perform this task.
```



# The Azure AD Powershell Module

> The replacement of MSOL (*install-module AzureAdPreview*)

<https://docs.microsoft.com/en-us/powershell/azure/active-directory/install-adv2?view=azureadps-2.0>

```
PS C:\Users\andrea> Get-AzureADUser -SearchString "admin"
```

ObjectID	DisplayName	UserPrincipalName	UserType
75525dd8-1cc4-455e-bdda-167231fcb20f	admin	amdin@winz4funoutlook.onmicrosoft.com	Member
feec33ac-5467-4582-b273-9388e20e074b	admin2	admin2@winz4funoutlook.onmicrosoft.com	Member

The screenshot shows a network traffic analysis tool with two panes: Request and Response. The Request pane shows a raw HTTP request to https://graph.windows.net. The Response pane shows a raw HTTP response from the server, including headers like Cache-Control, Pragma, Content-Type, and Expires, and a large JSON body containing user information.

```
Request
Raw Params Headers Hex
BT
96b30cb9-e66c-49f4-b89e-1d9784fa8084/users?api-version=1.6&2filter=use
PrincipalsName%20eq%20'admin'%20or%20(stater%20eq%20'admin'%20or%20(mailNm
IDName%20eq%20'admin'%20or%20(mail20eq%20'admin'%20or%20(jobTitle%20eq%2
'admin'%20or%20(displayName%20eq%20'admin'%20or%20(startswith(displayNam
%20'admin')%20or%20(department%20eq%20'admin'%20or%20(country%20eq%20'ad
in'%20or%20city%20eq%20'admin'))))))) HTTP/1.1
Accept: application/json
Authorization: Bearer

Response
Raw Headers Hex
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 2841
Content-Type: application/json; odata=minimalmetadata; streaming=true; charset=utf-8
Expires: -1
ocp-aad-diagnostics-server-name: 678gb9004N1NXXkEjBTfoc8Pz7ys48y5w8Rkxu00UDgY=
request-id: 78961087-1147-457f-91be-9eb04f414b79
client-request-id: 6c22a5c7-78ef-426d-9161-0cd804c3c5810
x-ms-dirapi-data-contract-version: 1.6
ocp-aad-session-key:
JEWPUV280GdHRAI4_l8oHFaHoUb4LECF333vysMu2DqgYI2rm0d-sg2eW8acklkv72P61q0S80qtsBARK1CC0CQEs9s-9oInvtgPB
hRzQy-nM_N93v0a1_HmG1a1m.djI7I79WQV7NSqP4_78P3_l1zr-W7Cng4h6SAov17k
Duration: 519106
x-ms-resource-unit: 2
DataServiceVersion: 3.0;
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Strict-Transport-Security: max-age=31536000; includeSubDomains
Access-Control-Allow-Origin: *
Date: Wed, 14 Apr 2021 16:16:08 GMT
Connection: close

[{"odata.metadata": "https://graph.windows.net/96b30cb9-e66c-49f4-b89e-1d9784fa8084/$metadata#directoryO
bjects", "mail": "i", "odata.type": "Microsoft.DirectoryServices.User", "objectType": "User", "objectId": "7862
5d68-1c4-455e-bdda-167231fcb20f", "deletionTimestamp": null, "accountEnabled": true, "ageGroup": null, "ass
ignedLicenses": [], "assignedPlans": [], "city": null, "companyName": null, "consentProvideForTine": null, "cou
```



# Restrict access to Azure AD Powershell Module

> The “*UsersPermissionToReadOtherUsersEnabled*” set to *\$false* will also limit access to Azure Ad cmdlets

```
PS C:\temp> Connect-AzureAD -Credential $credential

Account                               Environment TenantId                               TenantDomain                               AccountTyp
-----                               -
test1@winz4funoutlook.onmicrosoft.com AzureCloud 96b30cb9-e66c-49f4-b89e-1d9784fa8084 winz4funoutlook.onmicrosoft.com User

PS C:\temp> Get-AzureADuser
Get-AzureADuser : Error occurred while executing GetUsers
Code: Authorization_RequestDenied
Message: Insufficient privileges to complete the operation.
RequestId: 12179f46-d11a-4f14-a77a-6d93dd6bb8ea
DateTimeStamp: Sun, 21 Mar 2021 16:10:14 GMT
HttpStatusCode: Forbidden
HttpStatusDescription: Forbidden
HttpResponseStatus: Completed
At line:1 char:1
+ Get-AzureADuser
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Get-AzureADuser], ApiException
+ FullyQualifiedErrorId : Microsoft.Open.AzureAD16.Client.ApiException,Microsoft.Open.AzureAD16.PowerShell.GetUser
```



# Restrict access to Azure AD Powershell Module

> There's more! You can even restrict access to Az AD only to specific users

```
PS C:\Users\andrea> $appId = "1b730954-1685-4b74-9bfd-dac224a7b894" #azure ad graph
PS C:\Users\andrea> $sp = Get-AzureADServicePrincipal -Filter "appId eq '$appId'"
PS C:\Users\andrea> get-AzureADServiceAppRoleAssignment -ObjectId $sp.ObjectId
```

ObjectId	ResourceDisplayName	PrincipalDisplayName
2F1SdcQcXkW92hZyMfyyD-pmcPSPFlhMrt4o5k13VFM	Azure Active Directory PowerShell	admin
jMz8VB8nwUKmHtIJ_3jo_aXISST8QJPK-qm0oyT-N4	Azure Active Directory PowerShell	user 1.

```
PS C:\Users\andrea> $secpass=ConvertTo-SecureString [REDACTED] -AsPlainText -Force
PS C:\Users\andrea> $credential = New-Object System.Management.Automation.PsCredential("test1@winz4funoutlook.onmicrosoft.com", $secpass)
PS C:\Users\andrea> Connect-Azuread -Credential $credential
Connect-Azuread : One or more errors occurred.: AADSTS50105: The signed in user '{EmailHidden}' is not assigned to a role for the application
'1b730954-1685-4b74-9bfd-dac224a7b894' (Azure Active Directory PowerShell).
Trace ID: 77cd3242-d051-4019-9fde-d6fbebff4700
Correlation ID: 65baa5d7-9ff1-48a9-9c7c-fe6dcfe3bb4f
```

> Restrict access to Microsoft Graph module too  
`$appid="14d82eec-204b-4c2f-b7e8-296a70dab67e"`







# Disable Legacy Authentication

> Legacy Authentication refers to all protocols that use the unsecure Basic Authentication mechanism and if you don't block legacy authentication your MFA strategy won't be effective as expected. Use Modern Authentication! (OAuth 2.0/ADAL)

> Monitor users/application who are using legacy/insecure authentication

Date	Request ID	User	Application	Status
4/16/2021, 1:30:54 PM	06ec0673-aab9-4e27-ab58-71e95715400	[REDACTED]	Office 365 Exchange Online	Success
4/16/2021, 1:25:51 PM	6e70bc1d-77b5-4456-a27d-fd51f94	[REDACTED]	Office 365 Exchange Online	Success

**Basic info** | Location | Device info | Authentication Details | Conditional Access | Report-only | Additional Details

Date: 4/16/2021, 1:30:54 PM  
Request ID: 06ec0673-aab9-4e27-ab58-71e95715400  
Correlation ID: c3d991b2-9be8-498d-8197-2d743bbababa  
Authentication requirement: Single-factor authentication  
Status: Success

User: [REDACTED]  
Username: [REDACTED]  
User type: Member  
User ID: ccca22b-aacc-421c-a194-727ac024b1e9  
Sign-in identifier: [REDACTED]  
Application: Office 365 Exchange Online  
Application ID: 00000002-0000-0ff1-ce00-000000000000  
Resource: Office 365 Exchange Online  
Resource ID: 00000002-0000-0ff1-ce00-000000000000  
Resource tenant ID: 38039e65-fc02-4526-9984-f6c3c47d51d3  
Home tenant ID: 38039e65-fc02-4526-9984-f6c3c47d51d3  
Client app: Outlook Anywhere (RPC over HTTP)

**Client app**

- Exchange Online PowerShell
- Exchange Web Services
- IMAP
- MAPI Over HTTP
- Offline Address Book
- Other clients
- Outlook Anywhere (RPC over HTTP)
- POP
- Reporting Web Services
- SMTP
- Universal Outlook

**Apply**

If you have P1 or P2 licenses, block with **Conditional Access Policies**  
*Test with "report-only" before*





# Disable Legacy Auth. Service Side: Exchange Online

> Monitor email app usage



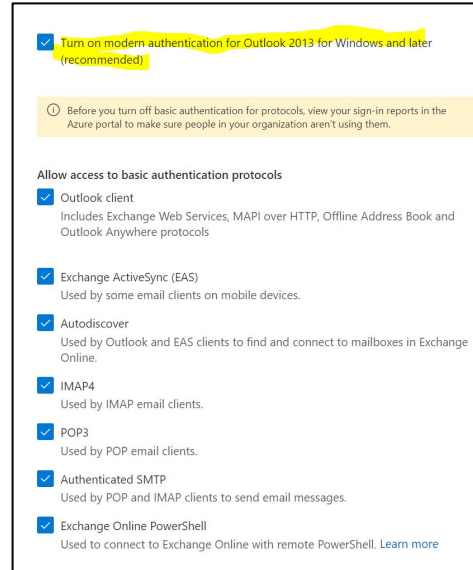
# Disable Legacy Auth. Service Side: Exchange Online

> The easiest way: disable protocols which by default use legacy authentication like Pop3, Imap, etc

```
Get-CASMailbox -Filter {ImapEnabled -eq "true" -or PopEnabled -eq "true" }  
| Set-CASMailbox -ImapEnabled $false -PopEnabled $false
```

> You can then re-enable these protocols for some specific user(s)

> Exch.Online "Authentication Policies" permit you to manage Modern auth. and selectively disable/enable Basic auth. for certain protocols



## Disable Legacy Auth. Service Side: Exchange Online

> You can even more fine grain these settings by allowing / disallowing basic authentication protocols for specific users using the authentication policies with Exchange powershell cmdlets:

```
New-AuthenticationPolicy -Name "Allow Basic Authentication for POP3"
```

```
Set-AuthenticationPolicy -Identity "Allow Basic Authentication for POP3"  
-AllowBasicAuthPop
```

```
Set-user -Identity mypop3user@mydomain -AuthenticationPolicy "Allow Basic  
Authentication for Pop3"
```



# Applications, consents and permissions

> Change the default settings!  
Require "Admin" consent

Dashboard > Enterprise applications >

## Consent and permissions | User consent settings

Manage

- User consent settings
- Permission classifications

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data. [Learn more about consent and permissions](#)

Save Discard

Manage

User consent settings

Permission classifications

User consent for applications

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

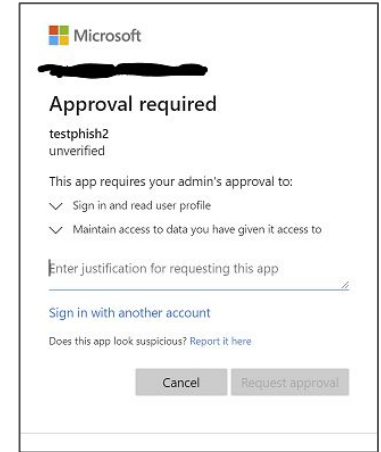
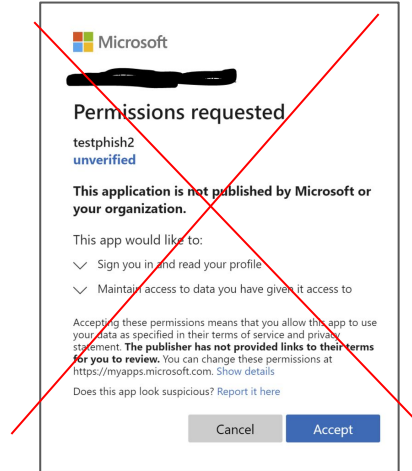
- Do not allow user consent  
An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions (Recommended)  
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this 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](#)

Group owner consent for apps accessing data

Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. [Learn more](#)

- Do not allow group owner consent  
Group owners cannot allow applications to access data for the groups they own.
- Allow group owner consent for selected group owners  
Only selected group owners can allow applications to access data for the groups they own.
- Allow group owner consent for all group owners  
All group owners can allow applications to access data for the groups they own.

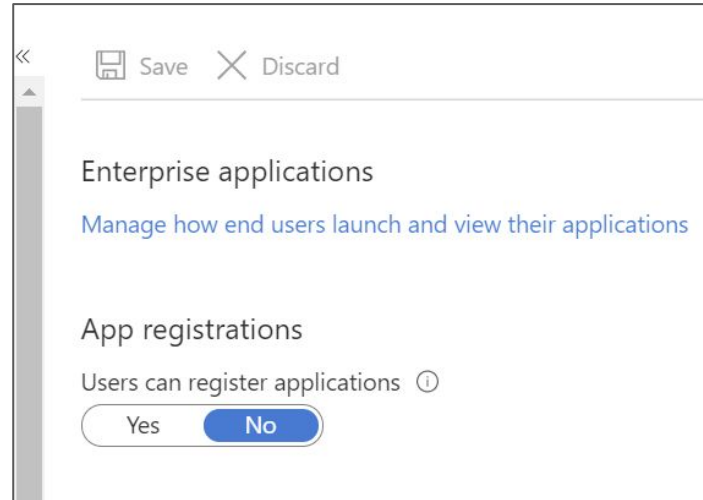


This will block phishing attempts using "malicious" apps and OAuth2, bypassing MFA



# Applications, consents and permissions basics

> Change the default settings! Standard users should not be allowed to publish their application



## Conclusions...

“MFA” all the things! (cit)

*Più facile a dirsi che a farsi (ndr)*

read more here

<https://decoder.cloud/2021/04/06/hands-off-my-ms-cloud-services/>



# Hunting



## A different approach

- > Cloud has **new challenges**
- > Don't try to use/extend the on-prem logic only, **use cloud capabilities and software**
- > **Adapt** your defense strategy
- > **Integrate** on-prem and cloud information





**Cloud Services**

**IaaS**  
Azure (VM)  
Other services

**PaaS**  
DNS, DB etc  
Other services

**SaaS**  
Office365  
Exchange

**Endpoint**  
Defender for  
Endpoint

**Azure Sentinel (SIEM)**

**Microsoft 365 Security**

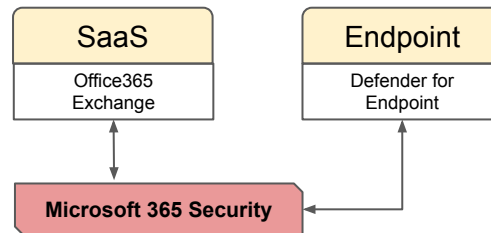


**On-Prem Security Architecture**  
SIEM + Ticketing + whatever



- > **Existing** queries and alerts
- > **Extend** with your own queries and **adapt** to your scenario

<https://github.com/gmellini/Microsoft-Defender-Security-Center-Hunting-Queries>



✓	Nome incidente
∨	'Donoff' malware was detected on one endpoint
	'Donoff' malware was prevented
∨	Impossible travel activity involving one user
	Impossible travel activity <a href="#">↗</a>

### Anomalies Hunting - Attempted lateral movement via WMI + PowerShell + Cobalt Strike

■■■ High ● Risolto

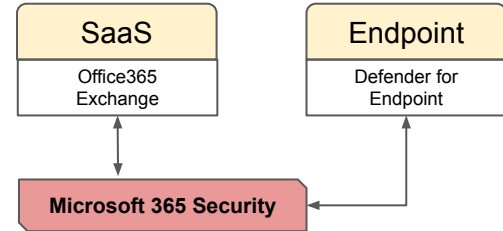
---

Descrizione avviso

Check  
<https://github.com/gmellini/Microsoft-Defender-Security-Center-Hunting-Queries#detection-opportunity-5-attempted-lateral-movement-via-wmi--powershell--cobalt-strike>

and for details  
<https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/>





- > Integrate **Threat Intel** feeds in the cloud to have the same detection capabilities on-prem & on-cloud
- > Use Cyber Saiyan Info Sharing feed  
<https://github.com/CyberSaiyanIT/InfoSharing/>
- > How-to integrate Minemeld with Defender ATP  
<https://medium.com/@antonio.formato/microsoft-defender-atp-minemeld-bring-your-own-threat-intelligence-feeds-c56033203aa7>

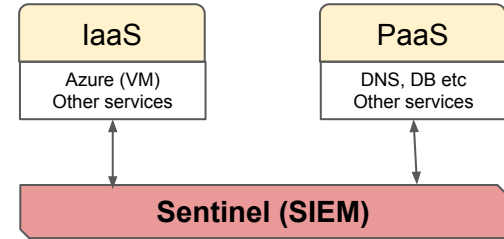


> Configure Azure Subscriptions to log into Log Analytics

> Activate Data Connectors for

> Azure Activities logs (VM creation, resource allocation, access management etc)

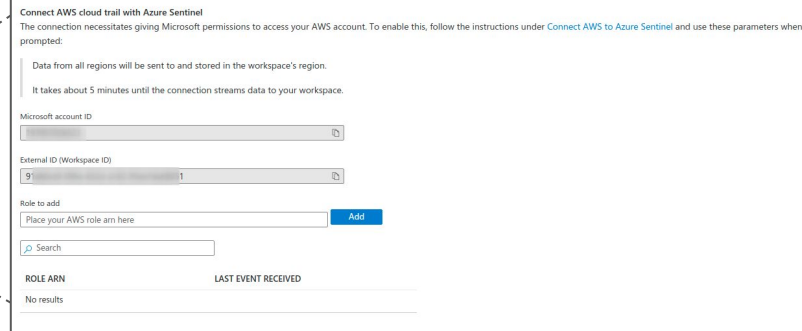
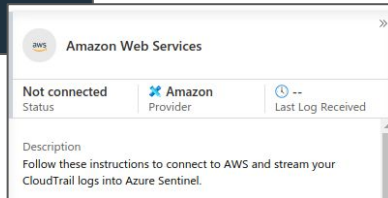
> Services and resources in MS cloud / other clouds / on prem services



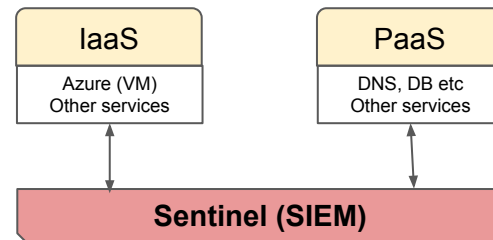
## AWS CloudTrail

Monitoraggio attività dell'utente e utilizzo di API

Inizia a usare AWS CloudTrail



- > Use predefined queries
- > And **make your own**
- > Azure AD Service Principal



<https://medium.com/@antonio.formato/azure-sentinel-monitoring-azure-active-directory-service-principal-dfe00bdcdb>

- > Example: PaaS DNS → zone/record actions

```
1 AzureActivity
2 | where OperationNameValue contains "Microsoft.Network/dnsZones/"
```

Results Chart Columns Add bookmark Display time (UTC+00:00)

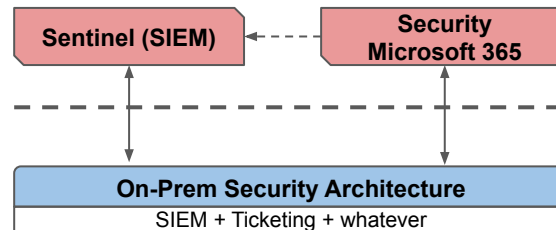
Completed. Showing results from the last 7 days.

TimeGenerated [UTC]	CallerIpAddress	CategoryValue	Correlation
		id /subscriptions/.../resource	
		location global	
		<b>name test.lol</b>	
		properties {"maxNumberOfRecordSets":10000,"maxNumberOfRecordsPerRe	
		tags {}	
		<b>type Microsoft.Network/dnszones</b>	
	serviceRequestId 033988b5-5f9b-4bd9-906b-3b588dbf7cc1		
	statusCode Created		



> Keep your on-prem solution **central**

> **Integrate** alerts via API



Security Events Overview

Alert Time	Incident	Severity	TicketID	Details
2023-10-27 10:00:00	[MALWARE - ATP - Anomalous activity originated from onboarded device(s) alert on 2023-10-27 10:00:00 via MS cloud ATP Defender	HIGH	1	<a href="#">View</a>
2023-10-27 10:00:00	[MALWARE - ATP - Connection to suspicious IP address alert on 2023-10-27 10:00:00 via MS cloud ATP Defender	HIGH	5	<a href="#">View</a>
2023-10-27 10:00:00	[MALWARE - ATP - MineMeld - doc-0k-5s-docs.googleusercontent.com alert on 2023-10-27 10:00:00 via MS cloud ATP Defender	HIGH	1	<a href="#">View</a>

> Use cloud telemetry to check for vulns/policy violations etc and **enhance security capabilities**



**Any  
question?**

