



Reportly - keep your
head in the clouds

Sapir Federovsky

About me

- Live in Tel-Aviv, Israel
- B.SC computer science
- 4+ years in the Israeli air force as a security researcher
- 1+ year @ Semperis as a security researcher

Love to write stuff for fun

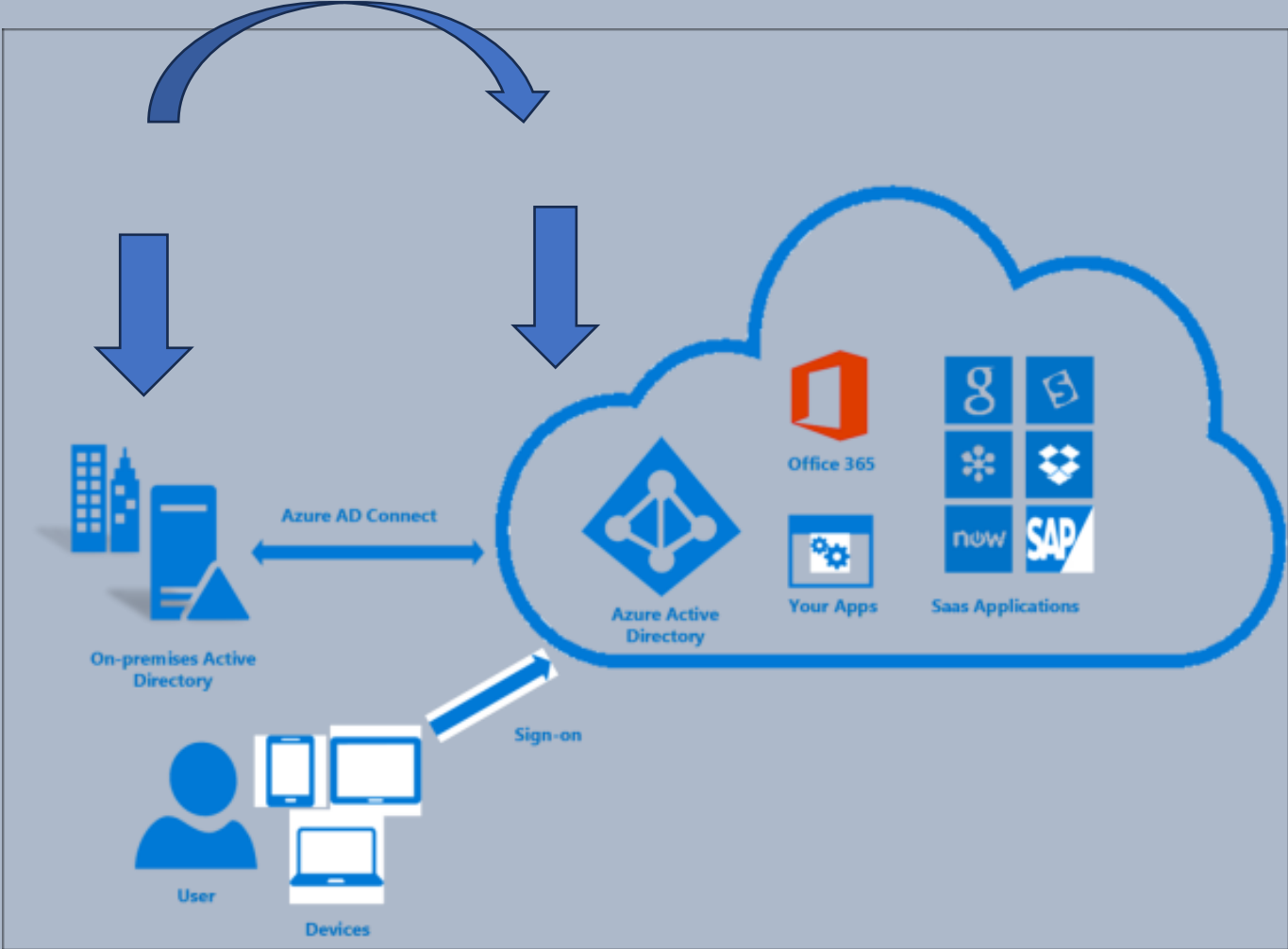
- AADInternals function
- Android Application
- NN models
- ChatGPT Plugin/Tools
- Reportly



Agenda

- Azure SMTP(soft) match abuse
- IR in Azure AD
- Reportly – Goal
- Reportly – Examples
- Reportly - Future features
- Questions

SMTP/Soft match



UPN
ProxyAddresses

Synchronized user

Alex Wilber User

Search

Edit properties Delete Refresh Reset password Revoke sessions Manage view Got feedback?

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Custom security attributes (preview)

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

Troubleshooting + Support

New support request

User principal name: AlexW@54824v.onmicrosoft.com

Object ID: 50065757-72fb-484e-ae49-4c3cd547186c

Identities: 54824v.onmicrosoft.com

User type: Member

Creation type

Created date time: Apr 22, 2022, 8:15 PM

Last password change date time: Jun 8, 2022, 12:27 PM

Invitation state

External user state change date ...

Assigned licenses: View

Password policies: DisablePasswordExpiration

Password profile

Preferred language

Sign in sessions valid from date ...: Jun 8, 2022, 12:27 PM

Authorization info: View

Job Information

Job title

Company name

Department

Employee ID

Employee type

Employee hire date

Employee org data

Office location

Manager

ZIP or postal code

Country or region

Business phone

Mobile phone

Email: AlexW@54824v.onmicrosoft.com

Other emails

Proxy addresses: View

Fax number

IM addresses: View

Mail nickname: AlexW

Parental controls

Age group

Consent provided for minor

Legal age group classification

Settings

Account enabled: Yes

Usage location: United States

Preferred data location

On-premises

On-premises sync enabled: Yes

On-premises last sync date time: Jun 10, 2022, 7:52 PM

On-premises distinguished name: CN=Alex Wilber,CN=Users,DC=f068-d01,DC=lab

Extension attributes

On-premises immutable ID: 5+HVHa7vuEC62lO6E5g4dg==

On-premises provisioning errors

On-premises SAM account name: AlexW

On-premises security identifier: S-1-5-21-1448646738-1848174778-616818770-1135

On-premises user principal name: AlexW@f068-d01.lab

On-premises domain name: f068-d01.lab

Proxy addresses

Alex Wilber

Proxy addresses

SMTP:AlexW@54824v.onmicrosoft.com

On-Premises attributes

Alex Wilber Properties

Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
General Address Account Profile Telephones Organization
Remote Desktop Services Profile COM+ Attribute Editor

Attributes:

Attribute	Value
lastLogon	(never)
logonCount	0
mS-DS-ConsistencyG...	\E7\E1\D5\1D\AE\EF\B8\40\BA\DA\53\
objectCategory	CN=Person,CN=Schema,CN=Configuration,[
objectClass	top; person; organizationalPerson; user
primaryGroupID	513 = (GROUP RID USERS)
proxyAddresses	SMTP:AlexW@54824v.onmicrosoft.com
pwdLastSet	6/8/2022 9:27:16 AM Coordinated Universal
sAMAccountName	AlexW
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
sn	Wilber
userAccountControl	0x10200 = (NORMAL_ACCOUNT DONT_I
userPrincipalName	AlexW@f068-d01.lab

Edit Filter

OK Cancel Apply Help





Eligible roles

Home > 54824v | Users > Users > Diego Siciliani



 **Diego Siciliani** | Assigned roles ...
User



[+ Add assignments](#) [Refresh](#) | [Got feedback?](#)

-  Overview
-  Audit logs
-  Sign-in logs
-  Diagnose and solve problems

Manage

-  Custom security attributes (preview)
-  Assigned roles

Eligible assignments Active assignments Expired assignments

Role	↑↓	Principal name	Scope	↑↓	Membership	↑↓	Start time	End time
Application Developer		DiegoS@54824v.onmicrosoft.com	Directory		Direct		10/24/2022, 9:57:48 PM	Permanent

Eligible roles activation (PIM)

Microsoft Azure Search resources, services, and docs (G+)

Home > Privileged Identity Management | My roles >

My roles | Azure AD roles

Privileged Identity Management | My roles

Activate

- Azure AD roles
- Groups (Preview)
- Azure resources
- Troubleshooting + Support
 - Troubleshoot
 - New support request

Refresh Got feedback?

Eligible assignments Active assignments Expired assignments

Search by role

Role	Scope	Membership	End time
Application Developer	Directory	Direct	Permanent

Activate - Application Developer

Privileged Identity Management | Azure AD roles

Roles **Activate** Status





Custom activation start time

Duration (hours) 8

Reason (max 500 characters) *

Limitations on user synchronization(soft match)

- AAD existing user , New AD user
- UPN and Proxy address are matched
- AAD user's password is overwritten
- Original MFA remains
- **It's not possible to synchronize users from AD to high privileged Azure AD users**

<input type="checkbox"/>	Display name ↑↓	User principal name ↑↓	User type	On-premises sy...	Identities
<input type="checkbox"/>	 Patti Fernandez	PattiF@54824v.onmicrosoft.com 	Member	No	54824v.onmicrosoft.com
<input type="checkbox"/>	 Patti Fernandez	PattiF9486@54824v.onmicrosoft.com 	Member	Yes	54824v.onmicrosoft.com

Original abuse by Dirk-Jan

So about that assignment

- We created a new account
- Linked it to an existing admin
- Delegated ourselves mailbox permissions
- Flag achieved 😊



Don't worry it's fixed

- Reported to MSRC in June 2018
- Fixed mid October 2018
- Account sync not possible anymore for admin accounts



Bypass synchronization to an administrative account

1. Find Azure AD non-synced user with eligibility to high privileged role
2. Create On-Prem user with correlating ProxyAddress and UPN
3. Overwrite the user's password
4. Login as the user
5. Activate high privilege role

Azure – squid.ward.com
On-Prem – sponge.bob



The problem

Home > 54824v | Users > Users >

Lee Gu User

Search

Edit properties Delete Refresh Reset password Revoke sessions Manage view Got feedback?

Overview Monitoring Properties

Basic info

Lee Gu
LeeG@54824v.onmicrosoft.com
Member

User principal name	LeeG@54824v.onmicrosoft.com	Group member...	10
Object ID	4cca089b-4d90-467c-b3ca-327414ddea35	Applications	13
Created date time	Apr 22, 2022, 8:15 PM	Assigned roles	4
User type	Member	Assigned licens...	2
Identities	54824v.onmicrosoft.com		

My Feed

Account status
Enabled
Edit

Sign-ins
Last sign-in: May 18, 2023, 5:21 PM
See all sign-ins

B2B collaboration
Convert to external user

MFA status
Capable with 3 authentication methods.
Manage MFA authentication methods

Troubleshooting + Support
New support request

Lee Gu | Groups

User



[+ Add memberships](#) [X Remove memberships](#) [Refresh](#) [Columns](#) [Got feedback?](#)

- Overview
- Audit logs
- Sign-in logs
- Diagnose and solve problems

Manage

- Custom security attributes (preview)
- Assigned roles
- Administrative units
- Groups**
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods
- Troubleshooting + Support
- New support request

[Add filters](#)

	Name	Object Id	Group Type	Membership Type	Email	Source
<input type="checkbox"/>	54824v	f26eef7f-1198-4f76-ad78-b35197882c86	Microsoft 365	Assigned	54824v@54824v.onmicrosoft.com	Cloud
<input type="checkbox"/>	a	b56752d3-7e31-42ec-ba4c-fd1494fec10b	Microsoft 365	Assigned	a1@54824v.onmicrosoft.com	Cloud
<input type="checkbox"/>	Digital Initiative Public Relations	60b62b6e-6c48-4bea-adb8-cbb015239844	Microsoft 365	Assigned	DigitalInitiativePublicRelations@54824v.on...	Cloud
<input type="checkbox"/>	Mark 8 Project Team	846112c8-8c2b-41e9-926d-98560392224a	Microsoft 365	Assigned	Mark8ProjectTeam@54824v.onmicrosoft.c...	Cloud
<input type="checkbox"/>	Retail	5c36b7f2-f866-4a66-b094-98fe7640a077	Microsoft 365	Assigned	Retail@54824v.onmicrosoft.com	Cloud
<input type="checkbox"/>	Sales and Marketing	7f5a777a-34df-4c8f-84ea-79030efeb8f8	Microsoft 365	Assigned	SalesandMarketing@54824v.onmicrosoft.c...	Cloud
<input type="checkbox"/>	test team	9ead4ab8-81d2-4af5-b811-adfee3686e09	Microsoft 365	Assigned	testteam@54824v.onmicrosoft.com	Cloud
<input type="checkbox"/>	test4	50d9cbae-3575-4c79-953c-cb04fdb1d465	Microsoft 365	Assigned	test4@54824v.onmicrosoft.com	Cloud
<input type="checkbox"/>	testg2	8f741410-b5a8-4bb2-9ed5-999d8c745e77	Microsoft 365	Assigned	testg2190@54824v.onmicrosoft.com	Cloud
<input type="checkbox"/>	U.S. Sales	b66f196f-69c5-48a2-a3a5-1be7d83e50d0	Microsoft 365	Assigned	U.S.Sales@54824v.onmicrosoft.com	Cloud


test4 | Owners

Group

- Overview
- Diagnose and solve problems
- Manage
- Properties
- Members
- Owners**

« + Add owners ✕ Remove ↻ Refresh | ☰ Columns | 🗨️ Got feedback?

[+ Add filters](#)

Name	Type	Email	User type
<input type="checkbox"/>  Lee Gu	User	LeeG@54824v.onmicrosoft.com	Member

Home / 54824v | Users / Users / Alex Wilber | Groups / test4

test4 | Members

Group

- Overview
- Diagnose and solve problems
- Manage
- Properties
- Members**
- Owners
- Roles and administrators
- Administrative units

« + Add members ✕ Remove ↻ Refresh | 📄 Bulk operations ▾ | ☰ Columns | 🗨️ Got feedback?

Direct members All members

[+ Add filters](#)

Name	Type	Email	User type
<input type="checkbox"/>  Alex Wilber	User	AlexW@54824v.onmicrosoft.com	Member
<input type="checkbox"/>  Lee Gu	User	LeeG@54824v.onmicrosoft.com	Member

Lee Gu | Audit logs

Download Refresh Columns Got feedback?

- Overview
- Audit logs**
- Sign-in logs
- Diagnose and solve problems
- Manage
 - Custom security attributes (preview)
 - Assigned roles
 - Administrative units
 - Groups
 - Applications
 - Licenses
 - Devices
 - Azure role assignments
 - Authentication methods
- Troubleshooting + Support
 - New support request

Date: **Last 1 month** Show dates as: **Local** Service: **All** Category: **All** Activity: **All** Add filters

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
5/17/2023, 6:52:52 PM	Core Directory	UserManagement	Update user	Success		oktaNotSyncUser@54824v.on...	LeeG@54824v.onmicrosoft.com
5/17/2023, 6:49:23 PM	Core Directory	UserManagement	Update user	Success		oktaNotSyncUser@54824v.on...	LeeG@54824v.onmicrosoft.com
5/17/2023, 6:44:38 PM	Core Directory	UserManagement	Update user	Success		oktaNotSyncUser@54824v.on...	LeeG@54824v.onmicrosoft.com
5/17/2023, 6:41:32 PM	Core Directory	GroupManagement	Add member to group	Success		oktaNotSyncUser@54824v.on...	LeeG@54824v.onmicrosoft.com
5/17/2023, 6:41:07 PM	Core Directory	UserManagement	Add user	Success		oktaNotSyncUser@54824v.on...	LeeG@54824v.onmicrosoft.com
5/17/2023, 6:38:56 PM	Core Directory	GroupManagement	Add app role assignment to gr...	Success		okta, ca8ed294-6143-4413-95...	LeeG@54824v.onmicrosoft.com
5/17/2023, 6:38:03 PM	Core Directory	GroupManagement	Add member to group	Success		admin1@54824v.onmicrosoft.c...	LeeG@54824v.onmicrosoft.com
5/17/2023, 6:38:01 PM	Core Directory	GroupManagement	Add group	Success		testOktaNoSync	LeeG@54824v.onmicrosoft.com
5/17/2023, 6:31:23 PM	Core Directory	GroupManagement	Add app role assignment to gr...	Success		okta, 5fef2782-1b5d-4a11-84a...	LeeG@54824v.onmicrosoft.com
5/17/2023, 6:30:53 PM	Core Directory	GroupManagement	Add app role assignment to gr...	Success		okta, 027fb7b0-04cc-4939-b43...	LeeG@54824v.onmicrosoft.com
5/17/2023, 6:20:42 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/17/2023, 5:18:05 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/17/2023, 4:16:00 PM	PIM	RoleManagement	Add member to role in PIM co...	Success	aa	Global Administrator, f429596b...	Lee Gu
5/17/2023, 4:15:59 PM	PIM	RoleManagement	Add member to role in PIM req...	Success	aa	Global Administrator, f429596b...	Lee Gu
5/9/2023, 6:24:37 PM	Core Directory	ApplicationManagement	Update application	Success		dspApplication	LeeG@54824v.onmicrosoft.com
5/9/2023, 6:24:37 PM	Core Directory	ApplicationManagement	Update application – Certificat...	Success		dspApplication	LeeG@54824v.onmicrosoft.com
5/9/2023, 6:24:37 PM	Core Directory	ApplicationManagement	Update service principal	Success		dspApplication	LeeG@54824v.onmicrosoft.com
5/8/2023, 3:42:04 PM	Core Directory	GroupManagement	Add member to group	Success		LeeG@54824v.onmicrosoft.co...	LeeG@54824v.onmicrosoft.com
5/8/2023, 2:58:07 PM	Core Directory	UserManagement	Update user	Success		LeeG@54824v.onmicrosoft.com	Azure MFA StrongAuthenticati...
5/7/2023, 3:12:49 PM	Core Directory	UserManagement	Update user	Success		LeeG@54824v.onmicrosoft.com	LeeG@54824v.onmicrosoft.com
5/7/2023, 3:12:44 PM	Core Directory	UserManagement	Update user	Success		almostAdmin@54824v.onmicr...	Microsoft Office 365 Portal
5/7/2023, 3:12:44 PM	Core Directory	UserManagement	Update user	Success		almostAdmin@54824v.onmicr...	LeeG@54824v.onmicrosoft.com
5/7/2023, 3:10:25 PM	PIM	RoleManagement	Add eligible member to role in ...	Success		Application Administrator, c9d...	Lee Gu
5/7/2023, 3:10:25 PM	PIM	RoleManagement	Add eligible member to role in ...	Success		Application Administrator, c9d...	Lee Gu

Date : **Last 7 days**
 Show dates as : **Local**
 Service : **All**
 Category : **All**

Date	Service	Category	Activity
6/14/2023, 10:42:55 AM	Core Directory	Agreement	Update
6/13/2023, 10:41:31 PM	Core Directory	Agreement	Update
6/13/2023, 10:40:58 AM	Core Directory	Agreement	Update
6/12/2023, 10:40:10 PM	Core Directory	Agreement	Update
6/12/2023, 9:04:01 PM	Core Directory	ApplicationManagement	Update
6/12/2023, 9:04:00 PM	Core Directory	ApplicationManagement	Update
6/12/2023, 9:04:00 PM	Core Directory	ApplicationManagement	Update
6/12/2023, 10:39:57 AM	Core Directory	Agreement	Update
6/11/2023, 10:37:37 PM	Core Directory	Agreement	Update
6/11/2023, 10:36:30 AM	Core Directory	Agreement	Update
6/10/2023, 10:35:22 PM	Core Directory	Agreement	Update
6/10/2023, 7:47:30 PM	Core Directory	GroupManagement	Add m
6/10/2023, 7:47:27 PM	Core Directory	GroupManagement	Add m
6/10/2023, 7:43:44 PM	Core Directory	UserManagement	Update
6/10/2023, 7:43:44 PM	Core Directory	UserManagement	Chang
6/10/2023, 7:43:44 PM	Core Directory	UserManagement	Update
6/10/2023, 7:43:44 PM	Core Directory	UserManagement	Chang
6/10/2023, 7:41:52 PM	Core Directory	UserManagement	Add us
6/10/2023, 7:41:52 PM	Core Directory	UserManagement	Add us
6/10/2023, 7:17:29 PM	Core Directory	GroupManagement	Add m

Activity	Target(s)	Modified Properties
Activity		
Date	6/12/2023, 9:04 PM	
Activity Type	Update service principal	
Correlation ID	51d089bf-1660-4836-b3a5-208b0d907fa6	
Category	ApplicationManagement	
Status	success	
Status reason		
User Agent		
Initiated by (actor)		
Type	Application	
Display Name	Microsoft Intune	
App ID		
Service principal ID	8b9f58ad-6e1f-4f48-938f-f44bfd2b89be	
Service principal name		
Additional Details		
AppId	0000000a-0000-0000-c000-000000000000	

Audit Log Details

Activity Target(s) Modified Properties

Target

Type ServicePrincipal

Id 8b9f58ad-6e1f-4f48-938f-f44bfd2b89be

Display Name Microsoft Intune

User Principal Name

Audit Log Details



Activity Target(s) Modified Properties

Target	Property Name	Old Value	New Value
Microsoft ...	Included Updat...		""
Microsoft ...	TargetId.Service...		"https://fef.msua09.manage.microsoft.com;https://fef.msuc06.manage.microsoft.com;https://fef.amsuin01.manage.microsoft.com;0000000a-0000-0000-c000-000000000000/manage-beta.microsoft.com;0000000a-0000-0000-c000-000000000000/manage.microsoft.com;0000000a-0000-0000-c000-000000000000;https://fef.msua01.manage.microsoft.com;https://fef.msua02.manage.microsoft.com;https://fef.msua04.manage.microsoft.com;https://fef.msua05.manage.microsoft.com;https://fef.amsua0502.manage.microsoft.com;https://fef.msua06.manage.microsoft.com;https://fef.amsua0602.manage.microsoft.com;https://fef.msuc01.manage.microsoft.com;https://fef.msuc02.manage.microsoft.com;https://fef.msuc03.manage.microsoft.com;https://fef.msuc05.manage.microsoft.com;https://fef.msub01.manage.microsoft.com;https://FEF.amsub0102.manage.microsoft.com;https://fef.msub02.manage.microsoft.com;https://fef.msub03.manage.microsoft.com;https://fef.msub05.manage.microsoft.com;https://fef.msua07.manage.microsoft.com;https://fef.bmsub01.manage-beta.microsoft.com;https://fef.bmsua01.manage-beta.microsoft.com;https://fef.shmsua01.manage-selfhost.microsoft.com;https://manage-selfhost.microsoft.com;https://manage.microsoft.com"



Lee Gu | Audit logs

Download Refresh Columns Got feedback?

- Overview
- Audit logs**
- Sign-in logs
- Diagnose and solve problems
- Manage
 - Custom security attributes (preview)
 - Assigned roles
 - Administrative units
 - Groups
 - Applications
 - Licenses
 - Devices
 - Azure role assignments
 - Authentication methods
- Troubleshooting + Support
 - New support request

5/4/2023, 1:36:58 PM	Core Directory	UserManagement	Update user	Failure	Microsoft.Online.DirectoryServi...	testOktaSapir@54824v.onmicr...	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:36:11 PM	Core Directory	UserManagement	Add user	Success		testOktaSapir@54824v.onmicr...	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:33:43 PM	Core Directory	UserManagement	Add app role assignment grant...	Success		okta, sapirf_semperis.com#EXT...	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:26:24 PM	Core Directory	UserManagement	Add app role assignment grant...	Success		okta, LeeG@54824v.onmicroso...	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:25:43 PM	Core Directory	UserManagement	Add app role assignment grant...	Success		okta, AlexW@54824v.onmicros...	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:20:58 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:20:57 PM	Core Directory	ApplicationManagement	Update application	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:20:57 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:20:57 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:50 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:50 PM	Core Directory	ApplicationManagement	Update application	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:50 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:50 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:48 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:48 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:48 PM	Core Directory	ApplicationManagement	Add service principal credentials	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:47 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:46 PM	Core Directory	ApplicationManagement	Add policy to service principal	Success		okta, 1835123d-7245-4006-83...	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:46 PM	Core Directory	ApplicationManagement	Update service principal	Success		okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 1:11:46 PM	Core Directory	Policy	Add policy	Success		ClaimIssuancePolicy	LeeG@54824v.onmicrosoft.com
5/4/2023, 11:39:34 AM	Core Directory	ApplicationManagement	Update service principal	Success		Okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 11:39:33 AM	Core Directory	ApplicationManagement	Update application	Success		Okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 11:39:33 AM	Core Directory	ApplicationManagement	Update service principal	Success		Okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 11:39:33 AM	Core Directory	ApplicationManagement	Update service principal	Success		Okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 11:39:31 AM	Core Directory	ApplicationManagement	Update service principal	Success		Okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 11:39:31 AM	Core Directory	ApplicationManagement	Update service principal	Success		Okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 11:39:31 AM	Core Directory	ApplicationManagement	Add service principal credentials	Success		Okta	LeeG@54824v.onmicrosoft.com
5/4/2023, 11:39:31 AM	Core Directory	ApplicationManagement	Update service principal	Success		Okta	LeeG@54824v.onmicrosoft.com

The problem

- There is no convenient way to understand what a user has done over time
- A lot of information can be missed in the form of "scrolling logs"
- The information about the user is scattered
- Authentication logs and user activity logs are on different pages

All these reasons are only a small part of the description of the difficulty of investigating and responding to an incident quickly and effectively

Reportly



Example – normal report

What have we learned from the example report?

- User-friendly interface
- Provide a concise and easily interpretable overview of suspicious user
- Creating a user **timeline** to paint a more coherent picture
- Highlighting more **suspicious events** tied to the user for further investigation





Application administrator Privileges escalation

Application administrator **can't** grant admin consent to an application

Configured permissions

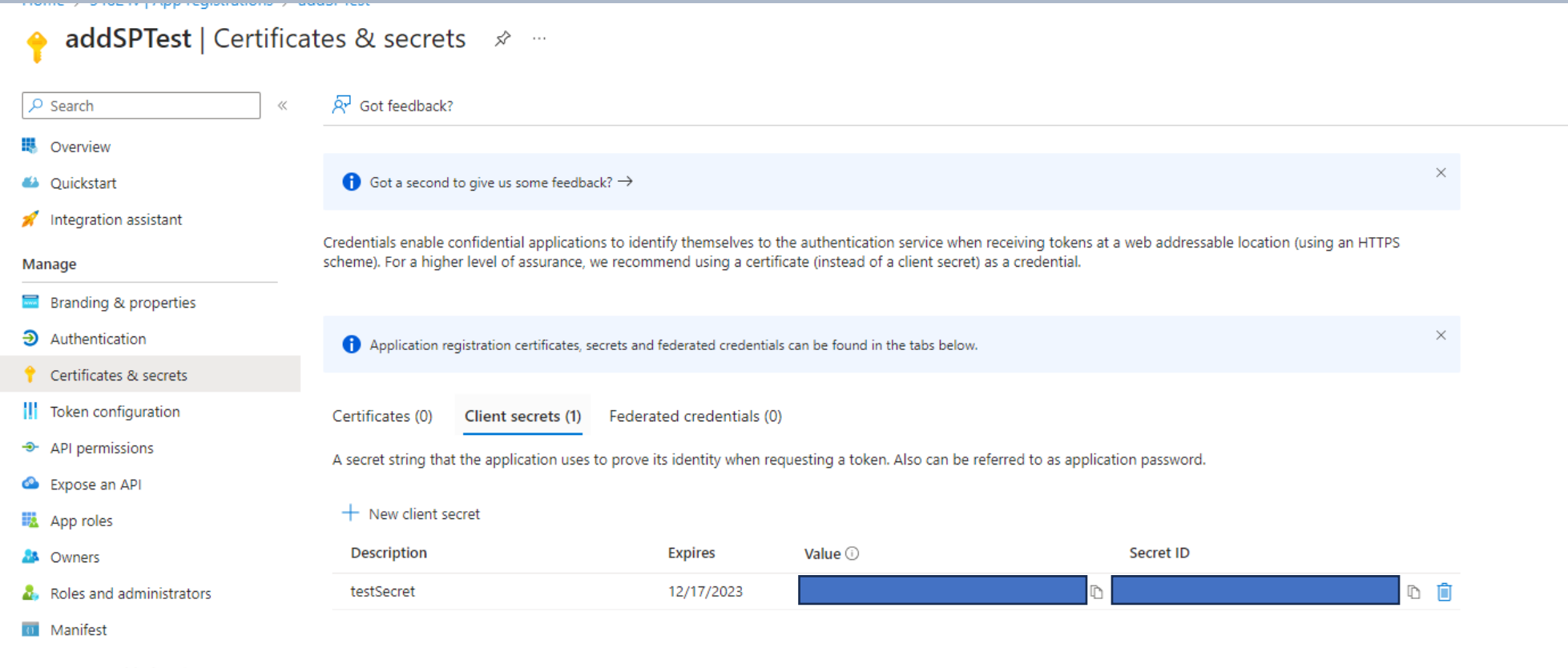
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+](#) Add a permission [✓](#) Grant admin consent for 54824v

API / Permissions name	Type	Description	Admin consent requ...	Status	
Microsoft Graph (4)					...
AdministrativeUnit.Read.All	Application	Read all administrative units	Yes	 Not granted for 54824v	...
AppRoleAssignment.ReadWrite.All	Application	Manage app permission grants and app role assignments	Yes	 Granted for 54824v	...
AttackSimulation.ReadWrite.All	Application	Read, create, and update all attack simulation data of an o...	Yes	 Granted for 54824v	...
AuditLog.Read.All	Application	Read all audit log data	Yes	 Granted for 54824v	...

Application administrator Privileges escalation

Application administrator **can** add a secret to an existing application (And by doing that, using the application – already consented - permissions)



Example – privileges escalation report + BF

Example – eligible sync abuse report

1. Find Azure AD non-synced user with eligibility to high privileged role
2. Create On-Prem user with correlating ProxyAddress and UPN
3. Overwrite the user's password
4. Login as the user
5. Activate high privilege role

Future features

- Highlighting more suspicious events
- More information about the user
- A more convenient way to authenticate when using the tool
- Improving the visual interface
- Support for additional events

Reportly will be available here:

<https://github.com/sap8899/reportly>



Questions