

WebTitan Azure AD Enterprise App

The WebTitan Azure AD Enterprise App is a built-in component of DNS Proxy. It is responsible for synchronizing Azure AD User & Groups to DNS Proxy. It regularly performs scans of the Azure sign-ins to find new sign-ins for Users. It pairs the user with the IP of the Virtual Machine that was signed into so that WebTitan Cloud can apply policies to those users.

Table of Contents

- 1. Prerequisites for the WebTitan AzureAD Enterprise App
- 2. Configure WebTitan AzureAD Enterprise App on DNS Proxy
- 3. Configure Multiple DNS Proxies with WebTitan AzureAD Enterprise App
- 4. Troubleshooting DNSProxy Deployment
- 5. Troubleshooting WebTitan AzureAD Enterprise App

Prerequisites for the WebTitan AzureAD Enterprise App

The WebTitan AzureAD Enterprise App requires access to the (Azure AD) reporting APIs to provide you with User sign-in data.

The WebTitan AzureAD Enterprise App uses OAuth to authorize access to the MS Azure APIs.

To Deploy DNSProxy and access the functionality of the WebTitan AzureAD Enterprise App the following has to be done:

- 1. License Requirements
- 2. Deploying DNSProxy
- 3. Assign roles
- 4. Register DNSProxy/WebTitan AzureAD Enterprise App as an application
- 5. Grant API permissions
- 6. Add Custom Role Assignment
- 7. Gather configuration settings

License Requirements

To access the sign-in reports for a tenant it must have an associated Azure AD Premium license. Azure AD Premium P1 (or above) license is required to access sign-in reports for any Azure AD tenant. Alternatively, if the directory type is Azure AD B2C, the sign-in reports are accessible through the API without any additional license requirement.

Deploying DNSProxy

DNSProxy is made available via an Azure App hosted by TitanHQ on its Azure Directory. This app needs to be made available on the target tenant to deploy DNSProxy.

Make DNSProxy-Distribution-Prod App available to External Organisation:

1. In the Azure portal, select Azure Active Directory from the left navigation pane.





2. Take note of your **Tenant ID** <Tenant 2 ID>

Home >		
Default Directory C Azure Active Directory	Dverview	
() Overview	☉ Switch tenant 📋 Delete tenant 🕂	Create a tenant 🔄 What's new 🛛 💀 Preview features 🛛 🛇 Got feedback?
Getting startedPreview hub	Azure Active Directory can help you enabl	e remote work for your employees and partners. Learn more
X Diagnose and solve problems	Default Directory	
Lusers	Search your tenant	
🍰 Groups	Tenant information	℅ Azure AD Connect
External IdentitiesRoles and administrators	Your role Global administrator More info	Status Not enabled
Administrative unitsEnterprise applications	License Azure AD Free Tenant ID	Last sync Sync has never run
Devices	Primary domain molloytphotmail opmicrosoft com	
Identity GovernanceApplication proxy	monoytphotman.onmicrosoft.com	

3. Open a **new tab** in your browser and enter the following **URL**:

https://login.microsoftonline.com/<Tenant Id>/oauth2/authorize?

client_id=a248315f-7d19-41c2-8acb-2619857956c9&response_type=code&redirect_uri=https%3A%2F %2Fwww.microsoft.com%2F



IMPORTANT: This will make the DNSProxy-Distribution-Prod App available to your tenant.

4. Navigate to the **resource group** you are going to **launch DNSProxy into**.



5. On the Add role assignment pane, add:

Add role assignment $~ imes$
Role (i)
Contributor i) 🗸 🗸
Assign access to ①
User, group, or service principal \checkmark
Select ①
DNSProxv-Distribution-Prod
No users, groups, or service principals f
Selected members:
DNSProxy-Distribu

Remove	
Save Discard	

a. In the Role dropdown, select Contributor.

b. In the **Assign access to** dropdown, select User, group, or service principal.

c. Select **DNSProxy-Distribution-Prod**.

d. Click Save.

Deploy DNSProxy into Resource Group of an External Organisations Tenant

IMPORTANT: You must launch DNSProxy into an existing ResourceGroup with an existing VNet & NetworkSecurityGroup.

The Subnet you launch DNSProxy into must have an NSG associated with it.

To access the UI HTTPS or HTTP ports must be open on the VNet.

As a part Port 7780 will be open on the NSG, this port is required for DNSProxy to communicate with other DNSProxies in your Azure estate.

NB: You must have the Azure CLI installed on the computer you run the DNSProxy Installer on. If you need to add the azure cli module to your powershell or bash shell please see Microsofts instructions which are available at <u>Azure CLI</u>

NB: You must have a default ssh key in your ~/.ssh folder (C:\Users<username>.ssh). If you do not have one you can generate one in powershell with the following command: "ssh-keygen -m PEM -t rsa -b 4096".

The Azure DNSProxy Installer is available for download at DNSProxy Azure Installer

When you run the Installer, it will launch a CLI where you will be asked for the following information:

- a. Your Tenant Id.
- b. The suffix for TitanHQ-DnsProxy- VM e.g. if 1 the VM name will be TitanHQ-DnsProxy-1.
- c. Name of the existing Resource Group DNSProxy will be launched into.
- d. Name of the existing VNet DNSProxy will be launched into.
- e. Name of the existing Subnet DNSProxy will be launched into.

IMPORTANT: This will launch DNSProxy into your resource group.

Assign roles

To get access to the reporting data through the API, you need to have one of the following roles assigned:

- Security Reader
- Security Administrator
- Global Administrator

Register DNSProxy/WebTitan AzureAD Enterprise App as an application

Registration is to access the reporting & management APIs. The registration gives you an **Application ID**, which is required for the authorization calls and enables the WebTitan AzureAD Enterprise App to receive tokens.

To configure your directory to access the Azure AD reporting API, you must sign in to the <u>Azure portal</u> with an Azure administrator account that is also a member of the **Global Administrator** directory role in your Azure AD tenant.

To register an Azure AD application:

1. In the <u>Azure portal</u>, select **Azure Active Directory** from the left navigation pane.



2. In the Azure Active Directory page, select App registrations.



3. From the App registrations page, select New registration.



4. The **Register an Application** page:

Home > TitanHQ >	
Register an applicati	on
* Name	
The user-facing display name for this a	pplication (this can be changed later).
DNSProxy	×
Supported account types	
Who can use this application or access	this API?
 Accounts in this organizational direction 	rectory only (TitanHQ only - Single tenant)
O Accounts in any organizational dir	ectory (Any Azure AD directory - Multitenant)
O Accounts in any organizational dir	ectory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Personal Microsoft accounts only	
Help me choose	
Redirect URI (optional)	
We'll return the authentication respons changed later, but a value is required f	e to this URI after successfully authenticating the user. Providing this now is optional and it can be or most authentication scenarios.
Web 🗸	e.g. https://myapp.com/auth
By proceeding, you agree to the Micro	soft Platform Policies 7
by proceeding, you agree to the Micro	
Register	

- a. In the **Name** textbox, type DNSProxy.
- b. For Supported accounts type, select Accounts in this organizational directory only.
- c. In the **Redirect URL** leave it blank.
- d. Select **Register**.

Grant API permissions

You need to grant your app the following permissions:

ΑΡΙ	Permission
Microsoft Graph	User.Read.All
Microsoft Graph	Group.Read.All
Microsoft Graph	AuditLog.Read.All
Azure Service Management	user_impersonate

1. Select API permissions then Add a permission.

₽ Search (Ctrl+/) ≪	🕐 Refresh 🛛 🗢 Got feedback	?			
 Overview Quickstart Integration assistant Manage 	Configured permissions Applications are authorized to call Al all the permissions the application ne + Add a permission	Pls when they are eeds. Learn more admin consent foi	granted permissions by users/admins as par about permissions and consent r TitanHQ	rt of the consent process. The list of configured permission	ns should include
Branding	API / Permissions name	Туре	Description	Admin consent req Status	
Authentication	✓ Microsoft Graph (1)				
📍 Certificates & secrets	User.Read	Delegated	Sign in and read user profile		
Token configuration					
API permissions	To view and manage permissions and	d user consent, try	/ Enterprise applications.		
Expose an API					
App roles Preview					
and the second se					
Owners					
 Owners Roles and administrators Preview 					
 Owners Roles and administrators Preview Manifest 					
Owners Roles and administrators Preview Manifest Support + Troubleshooting					
Convers Convers Convers Convers Converse Conve					

2. On the Request API permissions page, locate Microsoft Graph.

Request API permission	S		Х
Select an API			
Microsoft APIs APIs my organization	uses My APIs		
Commonly used Microsoft APIs			
Microsoft Graph Take advantage of the trem Access Azure AD, Excel, Inte single endpoint.	endous amount of data in Office 365, Enterprise .ne, Outlook/Exchange, OneDrive, OneNote, Sha	Mobility + Security, and Windows 10. rePoint, Planner, and more through a)
Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions	Azure Data Lake Access to storage and compute for big data analytic scenarios	
Azure DevOps Integrate with Azure DevOps and Azure DevOps server	Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	Azure Maps Create location-aware web and mobile applications using simple and secure geospatial services, APIs, and SDKs in Azure.	
Azure Rights Management Services Allow validated users to read and write protected content	Azure Service Management Programmatic access to much of the functionality available through the Azure portal	Secure, massively scalable object and data lake storage for unstructured and semi-structured data	

3. On the **Required permissions** page, select **Application Permissions**.

Request API permissions	×
< All APIs Microsoft Graph	



https://graph.microsoft.com/ Docs 🖉

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Add permissions Discard

4. Expand AuditLog checkbox AuditLog.ReadAll.

Re	quest API permissions	×
(Al	APIs	
>	AdministrativeUnit	
>	APIConnectors	
>	Application	
>	AppRoleAssignment	
>	ApprovalRequest	
~	AuditLog (1)	
(AuditLog.Read.All ① Read all audit log data	Yes
>	BitlockerKey	
>	Calendars	
>	CallRecord-PstnCalls	
>	CallRecords	
\langle	Add permissions Discard	

- a. Expand User checkbox User.Read.All
- b. Expand Group checkbox Group.Read.All
- c. Select Add permissions.
- 5. On the Request API permissions page, locate Azure Service Management.

APIs my organization	uses My APIs	
Commonly used Microsoft APIs		
Microsoft Graph		
Take advantage of the trem Access Azure AD, Excel, Int single endpoint.	endous amount of data in Office 365, Enterprise une, Outlook/Exchange, OneDrive, OneNote, Sha	Mobility + Security, and Windows 10. rePoint, Planner, and more through a
Azure Data Catalog	Azure Data Explorer	Azure Data Lake
Programmatic access to Data Catalog resources to register, annotate and search data assets	Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions	Access to storage and compute for big data analytic scenarios
Azure DevOps	Azure Key Vault	Azure Maps
Integrate with Azure DevOps and Azure DevOps server	Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	Create location-aware web and mobile applications using simple and secure geospatial services, APIs, and SDKs in Azure.
Azure Rights Management	Azure Service Management	Azure Storage
Allow validated users to read and write	Programmatic access to much of the	Secure, massively scalable object and

6. Expand Permissions checkbox user_impersonate and Select Add permissions.

All APIs AJure Service Management https://management.azure.com/ Docs https://management.azure.com/ Do	
Azure Service Management https://management.azure.com/ Docs 🖓 What type of permissions does your application require? Delegated permissions Application permissions	
https://management.azure.com/ Docs 🗗 What type of permissions does your application require? Delegated permissions Application permissions	
Vhat type of permissions does your application require? Delegated permissions Application permissions	
Delegated permissions Application permissions	
Your application needs to access the API as the signed-in user. Your application runs as a background service or daemon withous signed-in user.	ut a
ielect permissions	expand all
$^{ m O}$ Start typing a reply url to filter these results	
Permission Admin consent required	
user_impersonation	

7. On the DNSProxy Application - API Permissions page, select Grant admin consent.

	🔘 Refresh 🛛 🛇 Got feedback?	?				
Overview	G Successfully granted admin con:	sent for the request	ed permissions.			
Quickstart						
Integration assistant	Configured permissions					
nage	Applications are authorized to call AF all the permissions the application ne	PIs when they are g eeds. Learn more a	granted permissions by users/admins as part of the consen bout permissions and consent	t process. The list of cor	figured permissions should i	incluc
Branding	+ Add a permission 🗸 Grant i	admin consent for	TitanHO			
Authentication		T			<u></u>	
Certificates & secrets	API / Permissions name	Туре	Description	Admin consent req	Status	
Token configuration	✓Azure Service Management (*	1)				
API permissions	user_impersonation	Delegated	Access Azure Service Management as organization use	2	🧭 Granted for TitanHQ	
Art permissions	✓ Microsoft Graph (5)					
Expose an API	AuditLog.Read.All	Application	Read all audit log data	Yes	🥝 Granted for TitanHQ	
App roles Preview	Directory.Read.All	Application	Read directory data	Yes	🧭 Granted for TitanHQ	
Owners	Group.Read.All	Application	Read all groups	Yes	Granted for TitanHQ	
		Delegated	Sign in and read user profile	-	Granted for TitanHQ	
Roles and administrators Preview	User.Read	the second se	and the second se		A CONTRACTOR CONTRACTOR	
Roles and administrators Preview Manifest	User Read All	Application	Read all users' full profiles	Var	Granted for TitanHO	

Add Custom Role Assignment

Custom roles are used to harden access of the DNSProxy application rather than using the Azure built-in permission which are currently more liberal with access rights.

O subscriptions	3	×	2
Services	Marketplace	See all	
Subscriptions	SharpCloud Subscriptions		
Event Grid Subscriptions	Barracuda WAF Add On Subscriptions		
🧟 Service Bus	officeatwork Premium Support Subscription		
(iii) Resource groups	MedStack Control Annual Subscription		
Resources	Documentation	See all	
No results were found.	Subscription decision guide - Cloud Adoption Framework		
	Create an additional Azure subscription Microsoft Docs		
	Azure subscription states Microsoft Docs		
	Subscriptions in Azure API Management Microsoft Docs		
	Resource Groups		
	No results were found.		

1. In the **Search Bar** type **subscriptions**, Select **subscriptions** from the results.



2. On the Subscriptions page, locate Access control (IAM), Select Roles, Click on + Add, and Select Add custom role.

A Development	Access control (IAM)					×
,P Search (Ctrl+/) «	🕂 Ad): Download role assignments 📰 Edit columns 🕐 Refresh 🛛 🗙 Remove 🛛 🛇 Got feedback?					
* Overview	Check access Role assignments Roles Deny assignments Classic administrators					
Activity log	A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more th					
Tags	Search by role name					
Diagnose and solve problems	Name	Type	Users	Groups	Service Principals	
Security	Cwner 🖸	BuiltinRole	1	P	0	
🗲 Events	Contributor (i)	BuiltinRole	3	0	2	
Cast Management	🗌 🐍 Reader 🛈	BuiltinRole	0	0	1	
Cost management	AcrDelete ()	BuiltinRole	0	0	0	***
Containayon	🗌 📩 ActimageSigner 🛈	BuiltinRole	0	0	0	
D Rudents	🗌 🍐 Acrouit (0)	BuiltinRole	0	0	0	***
Adviser second state	🗌 🍰 ActPush 🛈	BuiltinRole	0	0	0	
Advisor recommencations	🗌 🍰 AcrQuarantineReader 🛈	BuiltinRole	0	0	0	
Billing	AcquarantineWriter 🛈	BuiltinRole	0	0	0	
Invoices.	🗌 🍰 AgRood Platform Service Admin ())	SultinRole	0	0	0	
External services	🔲 🎂 AgFood Platform Service Contributor 🛈	BuiltinRole	0	0	0	***
Payment methods	AgFood Platform Service Reader 🛈	BuiltinRole	0	0:	0	***
^A g, Partner information	API Management Service Contributor 🛈	BuiltinRole	0	0	0	***
Settings	📄 🍰 API Management Service Operator Role 🛈	BuiltinRole	0	0	0	
Programmatic deployment	API Management Service Reader Role ().	BuiltinRole	0	0	0	***
(+) Resource groups	📄 🍰 App Configuration Data Owner ()	BuiltinRole	0	0	0	***
III Resources	🗌 🍰 App Configuration Data Reader 🔿	BuiltinRale	0	0	0	***
Preview features	🔲 🍰 Application Group Contributor 🛈	BuiltinRole	0	0	0	
Usage + quotas	Application Insights Component Contributor 🗇	BuiltinRole	0	0	0	
D Policies	🔲 🍰 Application Insights Snapshot Debugger 🛈	BuiltinRole	0	0	0	
VE Management certificates	🔲 🍰 Attestation Contributor 🛈	BuiltinRole	0	0	0	***
R My permissions	🗌 🚣 Attestation Reader ()	BuiltinRole	Ð	0	0	
E Resource providers	🗌 🍰 Automation Job Operator 🛈	BuiltinRole	0	0	0	***
Deployments	🔲 🍰 Automation Operator 🛈	BuiltinRole	0	0	0	***
III Properties	🔲 🍰 Automation Runbook Operator 🛈	BuiltinRole	0	0	0	***
A Resource locks	🔲 🍰 Autonomous Development Platform Data Contributor (Preview) ⊙	BuiltinAcle	0	٥	ō	
	Autonomous Development Platform Data Owner (Preview) 🔘	BuiltinRole	0	0	0	

3. On the **Custom Role page**, Select **JSON**, and Click on **Edit**.

ne > Development >	
eate a custom role	ĺ
Got feedback?	
sics Permissions Assignable scopes ISON Review + create	
Here is your custom role in JSON format. Learn more 0*	
Download D	
<pre> properties": { "properties": { "roleName": "AlureADAgent Resource Reader", "description": "Read ResourceGroups, Virtual Machine & Network Interface Data", "assignableScopes": ["/subscriptions/], "permissions": ["microsoft.NetworkInterfaces/read", "microsoft.NetworkInterfaces/lagnosticIdentity/read", "microsoft.NetworkInterfaces/lagnosticIdentity/read", "microsoft.NetworkInterfaces/lagnosticIdentity/read", "microsoft.Compute/virtualMachines/networkInterfaces/read", "microsoft.compute/virtualMachines/networkIn</pre>	*
Review + create Previous Next	

a. Copy & paste the following JSON into the text box. b. Click on $\ensuremath{\textbf{Next}}$

{

```
"Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/instanceVi ew/read",
    "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
    }
  }
}
```

4. Select Create.

Home > Develop	Iome > Development >					
Create a cu	Create a custom role					
Got feedback?	♡ Got feedback?					
Basics Permiss	ions Assignable scopes JSON Review + create					
Basics						
Role name	AzureADAgent Resource Reader					
Role description	Read ResourceGroups, Virtual Machine & Network Interface Data					
Permissions						
Action	Microsoft.Network/networkInterfaces/read					
Action	Microsoft.Network/networkinterfaces/diagnosticidentity/read					
Action	Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/read					
Action	Microsoft.Compute/virtualMachines/read					
Action	Microsoft.Compute/virtualMachines/instanceView/read					
Action	Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read					
Action	Microsoft.Resources/subscriptions/resourceGroups/read					
Assignable Scope	s					
Scope	/subscriptions/3f51630f-4c88-4fba-b57a-5c39b5662a2f					
Create	Previous					

On the Subscriptions page, locate Access control (IAM), Select Roles, In the roles search bar type AzureADAgent Resource Reader.

IMPORTANT: It may take a few minutes for the custom role to propagate everywhere in the tenant.

Home ? Development						
A Development	Access control (IAM)					
,O Search (Ctrl+/)	n 🕂 Add 🛓 Download role assignments 💷 Edit columns 🕐 Refresh 🗙 Remove 🗢 Got feedback?					
+ Overview	· Charleman Delevationaries Refer Descentionaries Charleschericherter					
Activity log	Check access Role assignments Roles Deny assignments Classic auministrators					
Pp. Access control (IAM)	A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more of					
🗳 Tags	AzureAD Type : All					
Diagnose and solve problems	Showing 1 of 246 roles					
Security	Name	Type	Users	Groups	Service Principals	
🐓 Events	🗌 🎍 AzureADAgent Resource Reader 🔿	CustomRole	0	0	0	***
Cost Management						
Sc. Cost analysis						



5. On the Subscriptions page, locate Access control (IAM) and Select Add Role Assignment.



6. On the Add role assignment pane, add:

Role ①	
AzureADAgent Resource Reader 🛈	~
Assign access to 💿	
User, group, or service principal	~
ielect ()	
DNSProxy	
elected members:	
DNSProxy	Remove

- a. In the **Role** dropdown, select AzureADAgent Resource Reader.
- b. In the Assign access to dropdown, select User, group, or service principal.

c. Select **DNSProxy**.

d. Click Save.

Gather configuration settings

This section shows you how to get the following settings for your tenant:

- Client ID
- Client secret

Get your application's client ID

To get your application's client ID:

- 1. In the <u>Azure portal</u>, on the left navigation pane, click **Azure Active Directory**.
- 2. Select your application from the **App Registrations** page.

Ho	me >	
0	TitanHQ Overv	iew
		~
0	Overview	^
-	Getting started	
	Preview hub	
×	Diagnose and solve problems	
Ma	nage	
2	Users	
24	Groups	
0	External Identities	
2.	Roles and administrators	
a	Administrative units	
щ	Enterprise applications	
-	Devices	
(II),	App registrations	
٨	Identity Governance	
15	Application proxy	
4	Licenses	
٠	Azure AD Connect	
1	Custom domain names	
٢	Mobility (MDM and MAM)	-

3. Take note of your **Client ID**.

Home > TitanHQ >			
🔣 DNSProxy 🖈			
✓ Search (Ctrl+/) «	🔟 Delete 🜐 Endpoints 💀 Preview features		
R Overview	(\mathbf{i}) Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). $ o$		
Quickstart	↑ Essentials		
🚀 Integration assistant	Display name : DNSProxy	Supported account types	: My organization only
Manage	Application (client) ID :	Redirect URIs	: Add a Redirect URI
🚍 Branding	Directory (tenant) ID :	Application ID URI	: Add an Application ID URI
Authentication	Object ID :	Managed application in l	: DNSProxy

Get your application's client secret

To get your application's client secret:

1. Select **Certificates and Secrets** on the **API Application** page, in the **Client Secrets** section, click + **New Client Secret**.

Home > TitanHQ > DNSProxy P DNSProxy Certific	ates & secrets 👒			
Search (Ctrl+/)	Sot feedback?			
 Overview Quickstart 	Add a client secret			
Manage	Expires			
BrandingAuthentication	In 2 years			
Certificates & secrets Token configuration	Add Cancel	1.4		
 API permissions Expose an API 				
App roles Preview	Client secrets A secret string that the application	n uses to prove its identity when r	requesting a token. Also can be	referred to as application password.
 Roles and administrators Preview Manifest 	+ New client secret			
Support + Troubleshooting	Description	Expires	Value	ID
 Troubleshooting New support request 	NO CIERT SECIEIS Have been creat	eu for uns application.		

- 2. On the **Add a client secret** page, add:
- a. In the $\ensuremath{\textbf{Description}}$ textbox, type <code>DNSProxy Secret</code>.

b. As **Expires**, select **Never**.

c. Click Save.

d. Copy the key value.

3. Take note of your **client secret**.

Home > TitanHQ > DNSProxy					
🛉 DNSProxy Certific	ates & secrets 🛛 🖈				
♀ Search (Ctrl+/) «	♡ Got feedback?				
R Overview	Copy the new client secret value. You we	on't be able to retrieve it after you perform another o	peration or leave this bla	de.	
📣 Quickstart					
🚀 Integration assistant	Credentials enable confidential applications scheme). For a higher level of assurance, we	to identify themselves to the authentication servic recommend using a certificate (instead of a client	ce when receiving toke it secret) as a credential	ns at a web addressable location (using	an HTTPS
Manage					
🔜 Branding	Certificates				
Authentication	Certificates can be used as secrets to prove t	the application's identity when requesting a toker	n. Also can be referred t	o as public keys.	
📍 Certificates & secrets					
III Token configuration	Thumbprint	Start date	Expires	ID	
➔ API permissions			1.000		
🙆 Expose an API	No certificates have been added for this app	lication.			
🎎 App roles Preview					
0wners	Client secrets				
👔 Roles and administrators Preview	cheffe secrets				
Manifest	A secret string that the application uses to p	rove its identity when requesting a token. Also ca	in be referred to as app	lication password.	



1. On your DNSProxy locate **Active Directory** and Click on **Add**.

Configuration Logs Troubleshooting	
Network Cloud Credentials Active Directory Time	Change Password Updates Shutdown/Restart
Active Directory Servers	

2. On the Add Active Directory modal Select Azure Active Directory from the dropdown menu.

2 Edit Active Directory Domain (Azure)		
Type:	Azure Active Directory	
Domain:	domain	
Azure Tenant Id:	-	
Azure Client Id:		
Azure Client Secret:		
Azure Subscription Id:		
Enable periodic import:		
Import frequency:	10 minutes 💌	
		-
	Save Cancel	

3. On the Active Directory Servers table Select Azure AD tickbox and Click on Import Users.

	Z					Logged In: admin Lo Version: (Build) License: 10 WTC IP: 99.79.28.22
nfiguration Logs Tro work Cloud Credentials	ublieshooting Active Directory Time Change Password	Jpdates ShubdowrvRestart				
Active Directory Serve	a la					
Туре	Berver	Base Entry (DN)	Last Import	Imported users -	Imported groups	Options
Anze AD	Azure	AzureAD	03 February 2021, 6:19:54	244	295	18
Synchronization Statu	a Catharr	Last Boothe	unization Date Time	Last Symphocication Info	Last Sunchronization F	Tele
WTC IP Address	Customer	Last Bynchr	unization Date Time	Last Synchronization Info	Last Synchronization Ex	Tot
						Sync Users

4. On the **Synchronization Status table** Click on **Import Users**.

Configuration Logs Troubleshooting ietwork Cloud Credentials Active Directory Time Change Password Updates Shutdown/Restart Active Directory Servers Server Base Entry (DN) Last Import Imported users Imported groups 7 Type Berrer Base Entry (DN) Last Import Imported users Imported groups Active AD Active AD 0.3 February 2021, 0.19.54 244 225 Synchronization Status WTC /P Address Customer Last Synchronization Date Time Last Synchronization Infe Last Synchronization Error 0.3 February 2021, 15.20.24 237 User(s), 167 Onup(s), 150 Onup(s),			d Underter Dividing Destart	Troubleshooting	
Active Directory Servers Base Entry (3N) Last sepont Important users Imported groups 7 ype Base Entry (3N) Last sepont Important users Imported groups Acure AD Acure AD Acure AD 83 February 2021, 6.19 54 244 235 Synchronization Status Exet Synchronization Infe Last Synchronization Infe Last Synchronization Infe Last Synchronization Error 03 February 2021, 15 20 24 237 User(a), 167 Oscop(a) Signetronized) 03 February 2021, 15 20 24 237 User(a), 167 Oscop(a) Signetronized)				Asthe Directory Tone Change Barrier	onfiguration Logs The
Active Directory Servers Type Server Base Entry (DN) Last Import Imported groups Active AD Active AD Active AD 03 February 2021, 6 19 54 244 235			o opoares onuciowronesian	Howe bready Time Charge Passwo	TWORK CIOLO CROOPHDans
C Type Server Base Entry (DN) Last Import Important users Import users A zure AD A zure AD A zure AD A zure AD B February 2021, 6:19:54 244 235 Import Users Import Users Synchronization Status WTC (P Address Customer Last Synchronization Date Time Last Synchronization Infla Last Synchronization I				I ANN THE	Acove Directory Serve
Addread Addread B3 February 2021, 5, 19 54 244 235 Synchronization Status WTC /P Address Last Synchronization Date Time Lest Synchronization Infla Lest Synchronization Error 03 February 2021, 15 20 24 237 User(a), 167 Group(a) Signetronized 237 User(a), 167 Group(a) Signetronized	Imported groups Option	st import imported user	Base Entry (DN)	Server	🖬 Туре
03 Hebruary 2021, 15,25,29 231 User(p), 157 Windpp), alpromitiveed	hronization Info Last Synchronization Error	n Dete Time Lest Synchronization Info	Last Synchri	Customer	Synchronization Statu WTC IP Address
🖉 Success.	(), 167 Group(s) Synchronized	120.24 237 User(s), 167 Group(s) Synch	03 February 2		Success.

Primary DNSProxy Basic Setup

 On your DNSProxy locate Network->DNS Settings a. Enter your WebTitan Cloud IP in the text area and Click Add b. Click Add in the WebTitan Cloud DNS Servers section and Enter your WTC IP into the modal box.

						Logged In: admin Logout Version: 2.06 (Build 19612) License: - WTC IP: -
Configuration Logs Troubleshooting Network Cloud Credentials Active Directory Synchroniz	ation Devices Time Change Password	Updates Shutdown/Restart				
Network Configuration	IAL SERVERS STATIC ROUTES					0
WebTitan Cloud IP:						Save
WebTitan Cloud DNS Servers:	IP Address					Options
						Add
	Domain		Action	DNS Server(s)	Last Modified	Options
Exceptions:	No domains rerouted					
						Add
Success: WebTitan Cloud DNS Servers updated						

2. Locate the Cloud Credentials tab, enter the credentials of Customer Account from your WTC & Click Save

		Logged In: admin Logout Version: 2.06 (Build 19612) License: - WTC IP:
Configuration Logs Troubleshooting		
Network Cloud Credentials Active Directory Synchronization Devic	es Time Change Password Updates Shutdown/Restart	
Cloud Credentials		0
WebTitan Cloud Email address: Password:		Save
Success: WTC account updated		

3. On your DNSProxy locate Active Directory and Click on Add.

Configuration Logs Troubleshooting	
Network Cloud Credentials Active Directory Time	Change Password Updates Shutdown/Restart
Active Directory Servers	

4. On the Add Active Directory modal Select Active Directory from the dropdown menu.

	main (10.1.0.100) ×
Туре:	Active Directory Server 💌
Domain:	
IP Address/DNS Name:	
Search Base	
Server login user:	
Server login password:	
Enable periodic import:	0
Import frequency:	24 hours 💌

5. On the **Add Active Directory** modal Select **Azure Active Directory** from the dropdown menu.

Туре:	Azure Active Directory 🔻
Domain:	
Azure Tenant Id:	
Azure Client Id:	
Azure Client Secret:	
Azure Subscription Id:	
Enable periodic import:	
Import frequency:	24 hours 💌

Secondary DNSProxy Basic Setup

 On your DNSProxy locate Network->DNS Settings a. Enter your WebTitan Cloud IP in the text area and Click Add b. Click Add in the WebTitan Cloud DNS Servers section and Enter your WTC IP into the modal box.

						Logged In: admin Logout Version: 2.06 (Build 19612) License: - WTC IP: -
Configuration Logs Troubleshooting						
Network Cloud Credentials Active Directory Synchroniza	tion Devices Time Change Password L	Jpdates Shutdown/Restart				
Network Configuration						0
IP CONFIGURATION HOSTNAM DNS SETTINGS ERMINA	AL SERVERS STATIC ROUTES					
WebTitan Cloud IP:						Save
WebTitan Cloud DNS Servers:	IP Address					Options S
						Add
	Domain		 Action 	DNS Server(s)	Last Modified	Options
Exceptions:	No domains rerouted					
						Add
Success: WebTitan Cloud DNS Servers updated						

2. Locate the Cloud Credentials tab, enter the credentials of Customer Account from your WTC & Click Save

		Logged In: admin Logout Version: 2.06 (Build 19612) License: - WTC IP:
Configuration Logs Troubleshooting		
Network Cloud Credentials Active Directory Synchronization Devices	Time Change Password Updates Shutdown/Restart	
Cloud Credentials		0
WebTitan Cloud Email address: Password:		Save
Success: WTC account updated		

Secondary DNSProxy Synchronization Setup

1. On your DNSProxy locate **Synchronization** and Click on **Set Secondary**.

	TAN 5 proxy						Logged In: admin Logout Version: 2.06 (Build 19612) License: - WTC IP:
Configuration Logs	Troubleshor	oting					
Network Cloud Credentia	als Active Di	rectory Synchroniza	ation Devices Time Change	Password Updates Shutdown/Restart			
Synchronization							0
	P						Set Secondary
List of DNS Proxy instance	tances synchi	ronized:	Primary				Secondary
List of DNS Proxy instance	tances synch	ronized: Client Id	Client Secret	Last Synchronization Date Time	Last Synchronization Status	Last Synchronization Log	Options
List of DNS Proxy Instance	tances synch figured.	ronized: Client Id	Client Secret	Last Synchronization DateTime	Last Synchronization Status	Last Synchronization Log	Options

2. Take Note of the Credentials Displayed for entry onto the Primary DNSProxy

Primary DNSProxy Synchronization Setup

1. Locate the **Synchronization** tab, enter the credentials for **Secondary DNSProxy** & Click **Save**.

Add DNSProxy Instance			×			
Instance IP: Client ID: Client Secret:	1	Save Cancel				
						Logged In: admin Logout Version: 2.06 (Build 19612) License: - WTC IP:
Configuration Logs Troubleshooting Network Cloud Credentials Active Director	ry Synchronization	Devices Time Change Password L	Jpdates Shutdown/Restart			
Synchronization						0
DNS Proxy Instance Type:		Primary				Set Secondary
List of DNS Proxy instances synchroniz	zed:					
Instance IP Clie	ent ld	Client Secret	Last Synchronization DateTime	Last Synchronization Status	Last Synchronization Log	Options
1						28
Success: DNSProxy instance addec	d					Push Add

2. On the Active Directory Servers table Select Azure AD tick box and Click on Import Users.

ork Cloud Cre	ogs Troubleshooting dentials Active Directory Syncl	hronization Devices Time Change Pa	ssword Updates	Shutdown/Restart				
Active Directo	ry Servers							
🗹 Туре	Server		Base Entry (DN)	Last Import		Imported users	Imported groups	Opti
Active Direc	ory 10.1.0.1	00	DC=copperf,DC=local			0	0	I
Azure AD	Azure		AzureAD			0	0	1
ynchronizati	on Status		Last Sunshani	ntion Data Time	Lost Sunshrani	antion lafe		
TC ID Addresse		Customer	Last Synchroni.	auon Date nine	Last Synchronia		Last Synchronization Error	
VTC IP Address								(
WTC IP Address								SUDE

3. On the Synchronization Status table Click on Import Users.

							Logged In: admin Log Version: 2.06 (Build 196 License: - WTC IP:
Configuration Logs Troubleshooting							
atwork Cloud Credentials Active Directory	Synchronization Devices Time Change Pa	assword Updates	Shutdown/Restart				
Active Directory Servers							6
Туре	Server •	Base Entry (DN)	Last Import		Imported users	Imported groups	Options
Active Directory	10.1.0.100	DC=copperf,DC=local	30 March 2021, 10:21:49		124	17	2 ×
Azure AD	Azure	AzureAD	30 March 2021, 10:22:13		297	243	28
Synchronization Status							
WTC IP Address	Customer	Last Synchroni	zation DateTime	Last Synchroni	ration Info	Last Synchronization Error	
		30 March 2021,	10:23:53	416 User(s), 192	Group(s) Synchronized		
Success.							Sync Users

4. Locate the **Synchronization** tab and Click on **Push**.

Configuration Logs Troubleshooting Network Cloud Credentials Active Directory Synchronization Devices Time Change Password Updates Shutdown/Restart Synchronization DNS Proxy Instance Type: Primary Set Secondar List of DNS Proxy instances synchronization Client Id Client Secret Use The request to push data to DNSProxy instance(s) was made successfully. Push Add		AN					Logged In: admin Logo Version: 2.06 (Build 1961 License: qwerty WTC IP:
Synchronization Primary Set Secondary DNS Proxy Instance Type: Primary Set Secondary List of DNS Proxy instances synchronized: Instance IP Client Id Client Secret Last Synchronization Date Time Last Synchronization Log Options 1 2021-03-30 09:24:33 200 Synchronization was made successfully. Image: Client Id Client Id Client Id Add	Configuration Logs	Troubleshooting Active Directory Synchron	nization Devices Time Change Password	Updates Shutdown/Restart			
DNS Proxy Instance Type: Primary Set Secondary List of DNS Proxy instances synchronized: List of DNS Proxy instances synchronized: Image: Client Idd Client Secret Last Synchronization Date Time Last Synchronization Log Option: Instance IP Client Idd Client Secret Last Synchronization Date Time Last Synchronization Log Option: Image: Client Idd Client Secret Last Synchronization 2021-03-30 092433 200 Synchronization was made successfully. Image: Client Secret Image: Client Idd DNSProxy instance(s) was made successfully. Image: Client Secret Image: Client Secret Image: Client Secret	Synchronization			•			6
List of DNS Proxy instances synchronized: Instance IP Client Id Client Secret Last Synchronization Date Time Last Synchronization Status Last Synchronization Log Option 1 2021-03-30 09:24:33 200 Synchronization was made successfully.	DNS Proxy Instance Typ	e:	Primary				Set Secondary
Instance IP Client Id Client Secret Last Synchronization Date Time Last Synchronization Status Last Synchronization Log Option 1 2021-03-30 09:24:33 200 Synchronization was made successfully. Add	List of DNS Proxy instan	ices synchronized:					
1 2021-03-30 09:24:33 200 Synchronization was made successfully. Image: Contract to push data to DNSProxy instance(s) was made successfully. Push Add	Instance IP	Client Id	Client Secret	Last Synchronization DateTime	Last Synchronization Status	Last Synchronization Log	Options
The request to push data to DNSProxy instance(s) was made successfully.		1		2021-03-30 09:24:33	200	Synchronization was made successfully	2 X

Configure Azure VNet to use DNSProxy

1. Navigate to the **DNSProxy VM** and take note of its **Private IP Address**.

Virtual machine	\$			
P §earch (Ctrl+/) ≪	🖋 Connect ▷ Start 🤇	Restart 🔲 Stop 😥 Capture 💼 Delete 🖒 Refresh 🔲 Open in mobile		
📮 Overview 🧕	▲ A Essentials			
Activity log	Resource group (change) : apr	n-azure-ad-agent	Operating system	: Linux (freebsd 11.2)
Access control (IAM)	Status : Rur	aning	Size	: Standard DS1 v2 (1 vcpus, 3.5 GiB memo
A +	Location : We	st Europe	Public IP address	: 20.71.182.217
lags	Subscription (change) : Dev	velopment (sean's CC)	Virtual network/subr	net : aadds-vnet/aadds-subnet-01
Diagnose and solve problems	Subscription ID : 3f5	1630f-4c88-4fba-b57a-5c39b5662a2f	DNS name	: Configure
Settings	Tags (change) : Clic	ik here to add tags		
2 Networking	Description - Manifestori	Combiliaire (7) - Decomposidations - Tetraiaire		
Ø Connect	monitoring	Capabilities (7) Recommendations Tutonais		
8 Disks	Virtual machine		Setworking	
Size	Computer name	dnsproxy-az.example.com	Public IP addre	20.71.182.217
·	Operating system	Linux (freebsd 11.2)	Public IP addre	ess (IPv6) -
C Security	Publisher		Private IP addr	ess (10.101.1.6)
Advisor recommendations	Offer		Private IP addr	ess (IPv6) -
Extensions	Plan		Virtual network	
🐔 Continuous delivery	VM generation	V1	DNS name	Configure
Availability + scaling	Agent status	Ready	The second second	
	Agent version	9.9.9.9	Size	
	Host group	None	Size	Standard DS1 v2
🗞 Identity	Host		vCPUs	1
Properties	Provimity placement are	-	RAM	3.5 GiB

2. Navigate to the VNet page, in the left-hand navigation pane locate DNS Servers & Click on it.



3. On the DNS Server page, Select custom and Add the Private IP of the DNSProxy.

Home > Resource gro	ups > apm-azure-ad-agent > aadds-vnet
😑 aadds-vn	et DNS servers
Virtual network	
🔎 Search (Ctrl+/)	"
Overview	Virtual machines within this virtual network must be restarted to utilize the updated DNS server settings.
Activity log	
Access control (IAM	DNS servers ①
🛷 Tags	Default (Azure-provided)
Diagnose and solve	problems
Settings	IP Address
Address space	10.101.1.6
${\mathscr S}$ Connected devices	Add DNS server
 Subnets 	
ODoS protection	
🛖 Firewall	
Security	



IMPORTANT: You must restart the DNSProxy immediately after this step.

IMPORTANT: All VM must be restarted for them to use the DNSProxy for processing DNS request, they will keep using the oldDNS settings till restarted.

1. On DNSProxy Navigate to Configuration->Network->DNS Settings

					Logged In: admin Logout Version: 2.06 (Build 19984) License: 1234 WTC IP: 52.211.117.97
Configuration Logs Troubleshooting					
Network Cloud Credentials Active Directory Synchroniz	ation Devices Time Change Password Updates Shutdown/	Restart			
Network Configuration					0
IP CONFIGURATION HOSTNAME DNS SETTINGS TERMIN	IAL SERVERS STATIC ROUTES				
WebTitan Cloud IP:	52.211.117.97				Save
	IP Address				Options
WebTitan Cloud DNS Servers:	52.211.117.97				08
					Add
	Domain	Action	DNS Server(s)	Last Modified	Options
Exceptions:	No domains rerouted				
					Add

2. On the Redirect Pane click on Add

	X
T.	
Redirect	•
	l Refrect

The following list is by no means exhaustive:

core.windows.net
internal.cloudapp.net
prd.aadg.trafficmanager.net
prd.ags.akadns.net
prd.ags.msidentity.com
prd.ags.trafficmanager.net
privatelink.msidentity.com

These domains have been observed as windows azure related lookups that generate a lot of noise in the history on WTC.

Error: The access token is from the wrong issuer

az account get-access-token needs to be applied in Azure Cloud Shell

The access token is from the wrong issuer 'https://sts.windows.net/642f1773-84ee-4a58-81b8-1b2c13bdaa93/'. It must match the tenant 'https://sts.windows.net/896d169b-ffab-4391-8348-fc1b4644dfdd/' associated with this subscription. Please use the authority (URL) 'https://login.windows.net/896d169b-ffab-4391-8348-fc1b4644dfdd' to get the token. Note, if the subscription is transferred to another tenant there is no impact to the services, but information about new tenant could take time to propagate

Error: The subscription is not registered to use namespace

The Resource provider for the mentioned namespace needs to be made available to your tenant.

```
StatusCode: 409
ReasonPhrase: Conflict
ErrorCode: MissingSubscriptionRegistration
ErrorMessage: The subscription is not registered to use namespace 'Microsoft.Network'. See https://aka.ms/rps-
not-found for how to register subscriptions.
Additional details:
    Code: MissingSubscriptionRegistration
    Message: The subscription is not registered to use namespace 'Microsoft.Network'. See https://aka.ms/rps-
not-found for how to register.
```

Navigate to **Resource providers**, search for the missing namespace, **highlight** it and click on **register**

ome > Subscriptions > Pay-As-You- Subscription > Pay-As-You-Go Subscription	Go Resource providers	×
Search (Ctrl+/) Kesource groups Resources	Kefresh Kefresh Microsoft.network	×
 Preview features Usage + quotas 	Provider	Status
 Policies Management certificates My permissions 	Microsoft.Network	🕄 NotRegistered
š≡ Resource providers		
 Deployments Properties Resource locks 		
Support + troubleshooting		

Troubleshooting WebTitan AzureAD Enterprise App

This section lists the common error messages you may run into while accessing activity reports using the Microsoft Graph API and steps for their resolution.

Error: Tenant is not B2C or tenant doesn't have premium license

Accessing sign-in reports requires an Azure Active Directory premium 1 (P1) license. If you see this error message while accessing sign-ins, make sure that your tenant is licensed with an Azure AD P1 license.

Error: Application missing AAD 'Read directory data' permission

Follow the steps in the [Prerequisites to access the WebTitan AzureAD Enterprise App] to ensure your application is running with the right set of permissions.

Error: Application missing Microsoft Graph API 'Read all audit log data' permission

Follow the steps in the [Prerequisites to access the WebTitan AzureAD Enterprise App] to ensure your application is running with the right set of permissions.

Error: Access token validation failure. Invalid audience.

Follow the steps in the Prerequisites to access the WebTitan AzureAD Enterprise App to ensure your application is running with the right set of permissions.