NGINX App Protect Documentation

Matthieu Dierick

Apr 23, 2021

CONTENTS:

1	Publi	ish and protect on-prems apps with Azure AD as identity provider	1
	1.1	Class 1 - Check the Lab Architecture	2
	1.2	Class 2 - Deploy APM to protect on-prems apps	7
	1.3	Class 3 - Leverage Azure AD to protect Cloud Apps	27
	1.4	Class 4 - Enable MFA	29
	1.5	Class 5 - Clean up the lab	35

CHAPTER

ONE

PUBLISH AND PROTECT ON-PREMS APPS WITH AZURE AD AS IDENTITY PROVIDER

Warning: For any remark or mistake in this lab, please send a Teams chat to Matthieu DIERICK.

In this lab, you will learn how to connect APM to Azure AD as IDaaS. Since v15.1, you can enable APM as SAML SP and Azure AD as SAML IDP. In this lab, we will use the new **Easy Button** Guided Configuration template. This template:

- 1. Publish on-prems apps
- 2. Enable Single Sign on
- 3. Interconnect (SAML binding) APM with Azure AD tenant

Note: You will notice we will never connect to Azure AD interface. APM will use Microsoft Graph API to configure AAD tenant accordingly.



In the video below, you can see the use case. This is not the lab video, it is the public facing use case demo.

1.1 Class 1 - Check the Lab Architecture

In this class, we will protect 3 apps:

- 1. 2 internal apps
 - 1. Vanilla Application hosted in IIS
 - 2. Skyblue Application hosted in IIS
- 2. 1 cloud app hosted in Azure cloud
 - 1. Wordpress-UDF hosted in Azure cloud



Class 1 - All sections

1.1.1 Architecture of Internal Apps

Bluesky application

This application resides on-prems in IIS server. Its FQDN is https://bluesky.f5access.onmicrosoft.

 com

This application is not authenticated, meaning there is no Single Sign on required in front of this app.



Vanilla application

This application resides on-prems in IIS server. Its FQDN is https://vanilla.f5access.onmicrosoft.

 com

This application is authenticated by Kerberos. So a Signle Sign On will be required to connect to this app.



Check IIS configuration

- 1. RDP to IIS with f5access\user as user, and user as password
- 2. Click IIS manager icon in the taskbar



3. In the Connections tree, click on vanilla and Authentication

Internet Information Services (IIS) N	Manager				
← → ↓ IIS → Sites →	vanilla 🕨				
File View Help					
Connections Start Page Start Page Start Page Start Page Start Page Start Page Default Web Site Stes Default Web Site Stes Stes Start Page Start Page	Val Filter: IIS Authenticati on Modules Manageme	Compression	e Go Go C Default Document Request Filtering	Show All	Group by: Are
	Lator				

4. You can notice Anonymous Auth is Disabled and Windows Authentication is Enabled

Connections	Authentication			
	Group by: No Grouping -			
Application Pools Application Pools Sites Operault Web Site Operault Web Site Operault	Name Anonymous Authentication ASP.NET Impersonation Basic Authentication Windows Authentication	Status Disabled Disabled Disabled Enabled	Response Type HTTP 401 Challenge HTTP 401 Challenge	

Note: In the next class we will configure APM to publish, protect and SSO to internal apps.

1.1.2 Architecture of Cloud App

Note: In this use case, we don't cover only internal, sensitive or legacy applications. In a real world, customers have applications on-prems and in the public cloud.

Note: A Wordpress application is already up and running in Azure Cloud at this address https://wordpress-apm-aad.azurewebsites.net/



1. This Wordpress application is an Azure App Service.

Dashboar					
s 🗞 🗞	ordpress-apm-aad	\$			
,₽ Şearch	n (Cmd+/) «	🗹 Browse 🗌 Stop	\rightleftharpoons Swap 🖒 Restart 🛍 Delete $ $ 🖒 Refresh \downarrow Get p	ublish profile 🛛 🗘 Reset pul	olish profile 🛛 🛇 Send us your feedback
🔅 Overv	iew	Essentials			
Activit	y log	Resource group (change): WordPress-APM-AAD	URL	
Acces	s control (IAM)	Status	: Running	App Service Plan	
A		Location	: France Central	External Repository Proje	ct : https://github.com/azureappserviceoss/wordpress-azure
■ Tags		Subscription (change)	: f5-AZR_4261_SALES_EMEA_SA		
/> Diagn	ose and solve problems	Subscription ID	: 8423a9a0-4894-4fb2-97b1-2e06d7e95dec		
Securi	ty	Tags (change)	: Click here to add tags		

2. This App Service is already bound with our demo Azure AD tenant.

Azure Active Director	ation urre Active Directory. Click here to learn more. Learn more
Active Directory Authenti These settings allow users to sign in with Ar Management mode O Client ID Issuer Url O h	ation ure Active Directory. Click here to learn more. Learn more
Active Directory Authentia These settings allow users to sign in with As Management mode O Client ID Issuer Url O	ation ure Active Directory. Click here to learn more. Learn more
Active Directory Authentia These settings allow users to sign in with A: Management mode O Client ID Issuer Url O h	ation ure Active Directory. Click here to learn more. Learn more
These settings allow users to sign in with A: Management mode ① Client ID Issuer Url ③	ure Active Directory. Click here to learn more. Learn more
Management mode ① Client ID Issuer Url ① h	
Management mode ① Client ID Issuer Url ① h	
Client ID 1 Issuer Url ① h	On Express Advanced
Issuer Url ①	1d264d-941d-4e2c-9dc6-648922d57e11
	tps://sts.windows.net/8807dced-9637-4205-a520-423077750c60/
Show Secret	
Allowed Token Audiences	
https://wordpress-apm-aad azurewebsites ne	

Warning: It is important to note this application is **not tied** to APM. APM only publishes and protects on-prems apps. All other cloud and SaaS apps are directly connected to Azure AD.

1.2 Class 2 - Deploy APM to protect on-prems apps

In this class, we will publish Vanilla and Bluesky applications hosted on-prems.

To do so, we will use Guided Configuration template Azure AD Application

Federation	Zero Trust	Microsoft Integration	API Protection	Credential Protection	
	Q.		Ø		
rosoft Integration	n th Microsoft Azure AD provide authentication.	s ecure and seamless acc	ess for all modern and classic m	ission-critical applications	. It also provides additional secu

Class 2 - All sections

1.2.1 Publish and protect Bluesky app

Let's start with Bluesky application. Reminder, Bluesky does not have any Authentication enabled.

- 1. Connect to BIG-IP HTTPS user interface from UDF as admin and password admin
- 2. In Access > Guided Configuration, select Microsoft Integration > Azure AD application

Federation	Zero Trust	Microsoft Integration	API Protection	Credential Protection	
	Q.		Ø		
osoft Integration	, 🔨	, in the second s			
osoft Integration P APM integration wi xt and adaptive MFA	n th Microsoft Azure AD provid authentication.	ies ecure and seamless acc	cess for all modern and classic	mission-critical applicatio	ns. It also provides additional secu

Configuration Properties

- 1. Click Next and start the configuration
- 2. Configure the page as below
 - 1. Configuration Name : IIS-Bluesky-<My Name> Why my name ? Because this app will be created in Azure AD tenant. And we need to differentiate all apps. Example : IIS-Bluesky-Matt
 - 2. In Azure Service Account Details, Select Copy Account Info form Existing Configuration, and select IIS-baseline, then click Copy

On Copy Account Info from Ex	isting Configuration
isting Configuration 0	
Select	~ Сору
Select	
Select	

Note: In a real world, you will set here the values from the Azure Service Application created for APM. You have to create an Azure Application so that APM gets access to Microsoft Graph API. But for **security concerns**, I can't show in this lab the application secret.

Note: The steps to create this Azure applications are below

- 1. In Azure AD, create a service application under your organization's tenant directory using App Registration.
- 2. Register the App as Azure AD only single-tenant.
- 3. Request permissions for Microsoft Graph APIs and assign the following permissions to the application:
 - 1. Application.ReadWrite.All
 - 2. Application.ReadWrite.OwnedBy
 - 3. Directory.Read.All
 - 4. Group.Read.All
 - 5. Policy.Read.All
 - 6. Policy.ReadWrite.ApplicationConfiguration
 - 7. User.Read.All
- 4. Grant admin consent for your organization's directory.
- 5. Copy the Client ID, Client Secret, and Tenant ID and add them to the Azure AD Application configuration.
- 3. Click Test Connection button -> Connection is valid

Azure Service Account Details 💌

IIS-baseline		~	Сору
anant ID fi			
8807dced-9637-42	205-a520-423077750	c60	
lient ID 6			
1ef1f16f-0472-4d3	e-9062-138030a5c4	1d	
1ef1f16f-0472-4d3	e-9062-138030a5c4	1d	
1ef1f16f-0472-4d3	e-9062-138030a5c4	1d	

4. Click Next

Service Provider

- 1. Configure the page as below
 - 1. Host bluesky.f5access.onmicrosoft.com
 - 2. Entity ID is auto-filled https://bluesky.f5access.onmicrosoft.com/IIS-Bluesky-my name>

Service Provider

Host 0					
bluesky.f5a	ccess.onmicro	osoft.com			
Entity ID 🚯					
https://blue	sky.f5access.	onmicrosoft.	com/IIS-Bluesk	y-Matt	
Description 0					
Relay State 0					
_ ·					

Security Settings 💌

Sel	ect	, -	~	C	
Asserti	on Decryption Ce	tificate 0			
Sel	ect		~];	C	
uncel	Save Draft	Back	Save & Next		

Azure Active Directory

1. Select Azure BIG-IP APM Azure AD... template

Note: As you can notice, there are several templates available for different applications. Here, in this lab, we will publish a generic app. So we select the first template.

- 2. Click Add
- 3. In the new screen, configure as below
 - 1. Signing Key: default.key
 - 2. Signing Certificate : default.crt
 - 3. Signing Key Passphrase : F5twister\$

igning Key 🚯	
default.key	~ 2
Signing Certificate 🟮	
default.crt	~ 2
Signing Key Passphrase 0	
Signing Key Passphrase ()	
Signing Key Passphrase ① ····································	
Signing Key Passphrase ④ 	
Signing Key Passphrase ① 	· ·

4. In User And User Groups, click Add

Note: We have to assign Azure AD users/group to this app, so that they can be allowed to connect to it.

1. In the list, click Add for the user user1. If you can't find it, search for it in the search field.

/pe 🚯	Search Users 0			
User ~		Q		
		Items: 5		
			Filter by Name	
User	Email			Action
Andres Garcia				Add
coyote				Add
Jason Wilburn	J.Wilburn@f5.com			Add
M.Dierick@F5.com	Dierick			Add
user1				Add

- $2. \ Click \, {\tt Close}$
- 3. You can see user1 in the list.

er And User Groups 👻		
Add Delete		
Name	Description	Туре
user1		User

Virtual Server Properties

- 1. Configure the VS as below
 - 1. **IP** address : 10.1.10.104
 - 2. ClientSSL profile. We will get a TLS warning in the browser, but it does not matter for this lab.

Virtual Server Properties

Create New O Use Existing			
Destination Address 🚯			
10.1.10.104			
Service Port ① 443 HTTPS ~			
Enable Redirect Port			
Client SSL Profile 📵			
Create new Use Existing			
Available		Selected	
Available Filter	Ŧ	Selected Common	
Available Filter Common	Υ	Selected Common clientssl	
Available Filter Common clientssl-insecure-compatible	T 	Selected Common clientssl	
Available Filter Common clientssl-insecure-compatible clientssl-quic	T (1) (2)	Selected Common clientssl	
Available Filter Common clientssl-insecure-compatible clientssl-quic Create Profile in BIG-IP III	•	Selected Common clientssl	
Available Filter Common clientssl-insecure-compatible clientssl-quic Create Profile in BIG-IP UI	T ())	Selected Common clientssl	
Available Filter Common clientssl-insecure-compatible clientssl-quic	T () () () () () () () () () () () () ()	Selected Common Clientssl	

Pool Properties

- 1. Select Create New
- 2. In Pool Servers, select /Common/10.1.20.9 This is the IIS server.

Pool Properties				
Advanced Settings				
Select a Pool				
Create New ~				
Select an existing pool or select Create New.				
Resources Properties				
Load Balancing Method				
Round Robin ~				
Specifies the load balancing method. The default is Round Robin.				
Pool Servers				
Select servers for the pool.				
IP Address/Node name	Port		Priority Group	Action
Şelect	✓ 80	HTTP ~	0	+ ×
Select				
(/Common/10.1.20.9				

Session Management Properties

1. Nothing to change, click Save & Next

Deploy your app template

1. Click Deploy

Access » Guided Configuration					
Azure AD Application Configuration	n :IIS-Bluesky-Matt NOT DEPLOYED				
6 (E)		<u>_</u>		 	
Configuration Properties	Service Provider	Azure Active Directory	Virtual Server	Session Management	Summary
Your application is r	eady to be deployed.				
The application is correctly confi	gured, and ready to be deployed. B	eview the summary. You can click & o	n any step to make changes		
The application is concerny comi	gurea, and ready to be deproyed. In	eview the summary. For carrenore y	n any step to make changes.		
Summary					
Gammary					
Configuration Pro	operties 🕨				- Aller
Service Provider	•				GAN
	etory b				â
Azure Active Dire					ď
Ø Virtual Server ▶					540
a≞ Pool ≯					SAN .
්ට Session Manager	ment >				(All h
Cancel Save Draft	Back Deploy				

2. Behind the scene, the deployment creates an Azure Enterprise Application for Bluesky. We can see it in Azure portal (you don't have access in this lab). With this Enterprise Application, Azure knows where to redirect the user when authenticated. And this app has the certificate and key used to sign the SAML assertion.

Home > f5access > Enterprise application	ions
Enterprise application f5access - Azure Active Directory	ons All applications
«	$+$ New application \mid $\Xi\Xi$ Columns \mid 🐼 Preview features
Overview	Try out the new Enterprise Apps search preview! Click to enable the
 Overview 	
imes Diagnose and solve problems	Application type Applications status
Manage	Enterprise Applications V Any
All applications	First 50 shown, to search all of your applications, enter a display na
Application proxy	Name
诊 User settings	app-service-AAD
Security	IIS-baseline
Conditional Access	() IIS-Bluesky-Matt
$\widehat{igodoldsymbol{ imestyle}}$ Consent and permissions	SSO-Wordpress-Azure
Activity	

Test your deployment

- 1. RDP to Win10 machine as user and password user
- 2. Open Microsoft Edge browser icon is on the Desktop
- 3. Click on the bookmark Bluesky
- 4. You will be redirected to Azure AD login page. Login as user1@f5access.onmicrosoft.com, and for the password please ask to your instructor.

Microsoft	
Sign in	
user1@f5access.onmicrosoft.com	
Can't access your account?	
Sign-in options	
	Next





1.2.2 Publish and protect Vanilla app

Let's continue with Vanilla application. Reminder, Vanilla application as Authentication enabled with Kerberos auth. So, we will need to enable Kerberos Constrained Delegation.

- 1. Connect to BIG-IP HTTPS user interface from UDF as admin and password admin
- 2. In Access > Guided Configuration, select Microsoft Integration > Azure AD application

Note: As you can notice, we deploy one template per application

	n				
Federation	Zero Trust	Microsoft Integration	API Protection	Credential Protection	
Crosoft Integratio 3-IP APM integration wi ntext and adaptive MFA	h Microsoft Azure AD provide authentication.	secure and seamless acce	ess for all modern and classic	mission-critical application	s. It also provides additional security

Configuration Properties

- 1. Click Next and start the configuration
- 2. Configure the page as below
 - 1. Configuration Name : IIS-Vanilla-<My Name> Why my name ? Because this app will be created in Azure AD tenant. And we need to differentiate all apps.
 - 2. Enable Single Sign-on (SSO)

•	General Properties 🔻
	Configuration Name
	IIS-Vanilla-Matt
	Type a name for this guided configuration.
	Description 0
	On Single Sign-On (SSO)
	Endpoint Checks

3. In Azure Service Account Details, Select Copy Account Info form Existing Configuration, and select IIS-baseline, then click Copy

On Copy Account Info from Exi	sting Configu	ration 🚯
kisting Configuration ()		
Select	~	Сору
Soloot		
361601		

Note: In a real world, you will set here the values from the Azure Service Application created for APM. You have to create an Azure Application so that APM get access to Microsoft Graph API. But for **security concerns**, I can't show in this lab the application secret.

Note: The steps to create this Azure applications are below

- 1. In Azure AD, create a service application under your organization's tenant directory using App Registration.
- 2. Register the App as Azure AD only single-tenant.
- 3. Request permissions for Microsoft Graph APIs and assign the following permissions to the application:
 - 1. Application.ReadWrite.All
 - 2. Application.ReadWrite.OwnedBy
 - 3. Directory.Read.All
 - 4. Group.Read.All
 - 5. Policy.Read.All
 - 6. Policy.ReadWrite.ApplicationConfiguration
 - 7. User.Read.All
- 4. Grant admin consent for your organization's directory.
- 5. Copy the Client ID, Client Secret, and Tenant ID and add them to the Azure AD Application configuration.
- 4. Click Test Connection button -> Connection is valid

e Service Account D	oetails ▼		
On Copy Acc	count Info from Existing	g Configı	uration 0
xisting Configuration	0		
IIS-baseline		~	Сору
lient ID 🚯			
1ef1f16f-0472-4d3	e-9062-138030a5c41c	k	
lient Secret 0			
Test Connection	 Connection is value 	alid	

5. Click Next

Service Provider

- 1. Configure the page as below
 - 1. Host vanilla.f5access.onmicrosoft.com
 - 2. Entity ID is auto-filled https://vanilla.f5access.onmicrosoft.com/IIS-Bluesky-my
 name>

Service Provider

	•
Ho	ost
	vanilla.f5access.onmicrosoft.com
En	ntity ID 🚯
	https://vanilla.f5access.onmicrosoft.com/IIS-Vanilla-Matt
De	escription 0
Re	elay State 0

Azure Active Directory

1. Select Azure BIG-IP APM Azure AD... template

Note: As you can notice, there are several templates available for different applications. Here, in this lab, we will publish a generic app. So we select the first template.

- $2. \ Click \, {\tt Add}$
- 3. In the new screen, configure as below.
 - 1. Signing Key: default.key
 - 2. Signing Certificate : default.crt
 - 3. Signing Key Passphrase: F5twister\$

SAML Signing Certificate 🝷

default.key	~ 2
gning Certificate 0	
default.crt	~ 2
gning Key Passphrase ()	
gning Key Passphrase 🕲	
gning Key Passphrase () 	~
gning Key Passphrase () 	~

4. In User And User Groups, click Add

Note: We have to assign Azure AD users/group to this app, so that they can be allowed to connect to it.

1. In the list, click Add for the user user1. If you can't find it, search for it in the search field.

class2/module2/../pictures/module2/user.png

- 2. Click Close
- 3. You can see user1 in the list.

er And User Groups 👻		
Add Delete		
□ Name	Description	Туре
user1		User

Virtual Server Properties

- 1. Configure the VS as below
 - 1. **IP** address : 10.1.10.103
 - 2. ClientSSL profile. We will get a TLS warning in the browser, but it does not matter for this lab.

Ivanced Settings			
rtual Server Create New O Use Existing			
estination Address 0			
10.1.10.103			
443 HTTPS V			
Enable Bedirect Port			
Enable Redirect Port			
Enable Redirect Port ① ient SSL Profile ① Create new ① Use Existing			
Enable Redirect Port ient SSL Profile Create new Use Existing		Salastad	
Create new Use Existing Available		Selected	
Create new Use Existing Available Filter Create new	T	Selected	
Create new Use Existing Available Filter Common alianteel incommune compatible	T	Selected Common clientssl	
Create new Use Existing Available Filter Common clientssl-insecure-compatible alianteal avia	T (1)	Selected Common clientssl	
Create new Use Existing Available Filter Common clientssl-insecure-compatible clientssl-quic	▼ () () () () () () () () () ()	Selected Common clientssl	
Create Profile in BIG-IP UI Enable Redirect Port Use Existing Common Clientssl-insecure-compatible Create Profile in BIG-IP UI	T (1) (2)	Selected Common clientssl	

Pool Properties

- 1. Select Create New
- 2. In Pool Servers, select /Common/10.1.20.9 This is the IIS server.

Pool Properties				
Advanced Settings				
Select a Pool				
Create New ~				
Select an existing pool or select Create New.				
Resources Properties				
Load Balancing Method				
Round Robin ~				
Specifies the load balancing method. The default is Round Robin.				
Pool Servers				
Select servers for the pool.				
IP Address/Node name	Port		Priority Group	Action
Şelect	✓ 80	HTTP 🗸	0	+ ×
Select				
C /Common/10.1.20.9				

Single Sign-On Settings

1. In Selected Single Sign-on Type, select Kerberos, and select Advanced Settings

Single Sign-On Settings
Advanced Settings
Selected Single Sign-On Type
Kerberos 🗸
Select the authentication type rom the
Credentials Source -
Username Source 0
session.saml.last.identity
User Realm Source 🔞

- 2. In Credentials Source, fill as below
 - 1. Username Source: session.saml.last.identity
 - 2. Delete User Realm Source value keep it empty. The domain is similar between Azure AD and on-prems AD.
- 3. In SSO Method Configuration, fill as below
 - 1. Kerberos Realm: f5access.onmicrosoft.com

- 2. Account name: host/apm-deleg.f5access.onmicrosoft.com
- 3. Account Password: F5twister\$
- 4. KDC:10.1.20.8
- 5. UPN Support : Enaled
- 6. SPN Pattern: HTTP/%s@f5access.onmicrosoft.com

Kerb	eros Realm 🚯
f5	access.onmicrosoft.com
Acco	unt Name 🗿
h	ost/apm-deleg.f5access.onmicrosoft.com
Acco	unt Password
The pa	issword for the delegation account specified in the previous field.
Conf	rm Account Password
Re-typ	e the password for the delegation account specified in the previous field.
KDC	0
10.	1.20.8
_	
1	JPN Support
Enable	this to allow the User Principal Name to be used for SSO.
SPN	Pattern 🛈
HT	IP/%s@f5access.onmicrosoft.com
Ticke	t Lifetime 0
600	
Sond	Authorization A
Alv	

Session Management Properties

1. Nothing to change, click Save & Next

Deploy your app template

1. Click Deploy

Access	Buided Configuration						
Azure	AD Application Configuration :	IIS-Bluesky-Matt NOT DEPLOYED	_	_	_		
0	=		<u> </u>				—
С	onfiguration Properties	Service Provider	Azure Active Directory	Virtual Server	Pool	Session Management	Summary
Υοι	r application is rea	ady to be deployed.					
The a	pplication is correctly configur	red, and ready to be deployed. R	wiew the summary. You can click 🖋 o	n any step to make changes.			
Sum	mary						
÷	Configuration Prop	erties 🕨					dan .
	B. O in Drawiden A						
- 23	Service Provider	•					GP.
Δ	Azure Active Direct	tory 🕨					647
0	Virtual Comunity						\$
	Virtual Server P						T
đ	Pool ▶						(All'
5	Session Manageme	ont b					
3	ocosion Manageme						ď
Cano	Save Draft	Back Deploy					

2. Behind the scene, the deployment creates an Azure Enterprise Application for Bluesky. We can see it in Azure portal (you don't have access in this lab). With this Enterprise Application, Azure knows where to redirect you when authenticated. And this app has the certificate and key used to sign the SAML assertion.

Home $>$ f5access $>$ Enterprise application	itions	
Enterprise applicat	ions All applications	5
() Quantiew	+ New application $\mid \equiv \equiv$ Co	olumns 🐱 Preview features ♡ Got fee
Overview Overview	🕜 Try out the new Enterprise Ap	pps search preview! Click to enable the preview. $ ightarrow$
🗙 Diagnose and solve problems	Application type	Applications status Applica
Manage	Enterprise Applications V	Any V Any
All applications	First 50 shown, to search all of yo	our applications, enter a display name or the applic
Application proxy	Name	
ល User settings	app-service-AAD	/
Security	() IIS-baseline	
Conditional Access	IIS-Bluesky-Matt	
$igodoldsymbol{i$	IIS-Vanilla-Matt	
Activity	SSO-Wordpress-Azure	
→ Sign-ins		

Test your deployment

- 1. RDP to Win10 machine as user and password user
- 2. Open Microsoft Edge browser icon is on the Desktop
- 3. Click on the bookmark Vanilla
- 4. You will be redirected to Azure AD login page only if your previous session with Bluesky expired in APM. Login as user1@f5access.onmicrosoft.com, and for the password please ask to your instructor (if you are prompted). But as you already authenticated against Azure AD, you still have a session in Azure AD.

Microsoft	
Sign in	
user1@f5access.onmicrosoft.com	
Can't access your account?	
Sign-in options	
	Next

- 5. You are redirected to APM with a SAML assertion, and can access to Vanilla application.
- 6. APM did Single Sign-on with Vanilla application (Kerberos Constrained Delegation)



- 7. Click Bluesky bookmark, you can access Bluesky application as well.
- 8. Extra lab, enable Inspect mode in Edge, and follow the SAML redirections to understand the workflow.

1.3 Class 3 - Leverage Azure AD to protect Cloud Apps

In this class, we will check that user1 can access any cloud app federated with Azure AD.

1.3.1 The current config

In a real world, companies deploy applications on-prems and in public clouds. If the company uses Azure AD as IDaaS, it will federate all cloud apps with this Azure AD tenant.

This is what we prepared for you in this lab. This application is federated with our Azure AD tenant.

You have **nothing** to configure on APM side, as everything is dealed between the cloud app and Azure AD. In Azure portal, we configured Oauth for the cloud app, so that every user reaching this app will be redirected to Azure login page.



1.3.2 Test your deployment

- 1. RDP to Win10 machine as user and password user
- 2. Open Microsoft Edge browser icon is on the Desktop
- 3. Click on the bookmark Wordpress Cloud App
- 4. You will be redirected to Azure AD login page (it can take a while look at the address bar). Login as user1@f5access.onmicrosoft.com, and for the password please ask to your instructor (if prompted). You already have a session up and running in Azure AD, from previous class.
- 5. You are redirected to the cloud app in Azure cloud, and can access to Wordpress-UDF application.



1.4 Class 4 - Enable MFA

Warning: You can **not** run this class without a F5 SA or F5 SME-UA lead. Please reach out to your local SA/SME-UA lead in order to activate an temporary account for you.

- 1. EMEA : Matthieu
- 2. USA : Jason or Shannon
- 3. APCJ : Shain

In this class, we will use another user account (created by SA/SME-UA), with MFA enabled for this account.

Let's say, a SA/SME created the account matt@f5access.onmicrosoft.com for me. Then he enabled the MFA for this account.

Class 4 - All sections

1.4.1 Procedure for SA/SME

Warning: Only SA and SME-UA with administrator role on this demo tenant, can create users. If you are not a SA or SME lead, move to the next section.

1. Connect to Azure Portal and select F5access tenant

2	Ŗ	¢	ŝ	?	٢	M.Dierick@F5.c F5AC	
		Dire	ctor	у+	sul	bscription	×
		Default	t subs	cript	ion fil	ter	
lback?		No subs another	criptio directo	ns in f ory.	5access	s directory - Switch t	0
		Current	directo	ry: f5a	iccess.c	onmicrosoft.com	
		Learn ab	out di	rectori	es and	subscriptions 🖻	
		Switch	direc	tory			
		Set your	defaul	t dire	ctory		
		Sign in	to you	ır last	visited	directory	\sim
		Favori	tes	All D	irector	ies	A to Z ↑↓
		D Sear	rch				
		F5 Sales F5Sales e569f29	s .onmic 9e-b09	rosoft 8-4cea	.com a-b6f0-	48fa8532d64a	
	1	F5-AAD f5emea 6b99cb	-Matt matt.o b8-995	nmicro 5a-42e	osoft.co b-884c	om I-9ed4fddc0d7f	
		f5acces f5acces 8807dc	s s.onmi ed-963	crosof 7-420	t.com 15-a520	-423077750c60	

- 2. Go to Azure Active Directory > Users
- 3. Click Create new



4. Enter the information, and click Create

Identity	
User name * ①	matt 🗸 @ f5access.onmicrosoft.com 🗸 🖺
	The domain name I need isn't shown here
Name * ①	Matthieu Dierick 🗸
First name	
Last name	
Password	
	Auto-generate password
	Let me create the password
Initial password * ①	···········
Groups and roles	
Groups	0 groups selected
Roles	User

5. Click on Multi-Factor Authentication

≡	Microsoft Azure				$\mathcal P$ Search resource	ces, service	s, and docs (0	5+ <i>/</i>)	
Но	me > f5access >								
2	Users All users (Prev fSaccess - Azure Active Directory	view)							
	*	+ New user	+ New guest user	🗋 Bulk	operations 🗸 💍 Refresh	🔎 Reset	password (Multi-Factor Authentication	🗊 Delete user
- 🚨	All users (Preview)								
-	Deleted users (Preview)	🦪 This page in	ncludes previews availa	ble for you	r evaluation. View previews $ ightarrow$				
•	Password reset				+ Add filters				
ŝ	User settings	7 users found							
*	Diagnose and solve problems	Name			User principal name	↑↓	User type		Directory synced
Act	ivity	AG And	res Garcia		andres@f5access.onmicrosoft.	com	Member		No
Э	Sign-ins	coyo	ite		coyote@f5access.onmicrosoft.	com	Member		No

6. Enable MFA for the created user

Micr	osoft		M.Dierick_F5.com#EXT	f#@f5access.onmicrosoft.com
m use Note: Befor	ulti-factor a ers service sett only users licensed to use Mi e you begin, take a look at the	uthentication ings crosoft Online Services are eligible for Multi-Factor Authenti e multi-factor auth deployment guide.	cation. Learn more about how to licent	se other users.
Vie	w: Sign-in allowed users	 Multi-Factor Auth status: Any 	bulk update	
	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS	
	Andres Garcia	andres@f5access.onmicrosoft.com	Enforced	Matthieu Dieric
	coyote	coyote@f5access.onmicrosoft.com	Disabled	matt@f5access opmicrosoft com
	Jason Wilburn	J.Wilburn@f5.com	Disabled	indition of the second second second
	M.Dierick@F5.com Dierick	M.Dierick@F5.com	Disabled	quick steps
2	Matthieu Dierick	matt@f5access.onmicrosoft.com	Disabled	Manage user settings
	user1	user1@f5access.onmicrosoft.com	Disabled	
202	20 Microsoft Legal Privacy			
	About enab	ling multi-factor auth		
	If your users do not auth: https://aka.ms	regularly sign in through the browser, you of //FASetup	can send them to this link to	register for multi-factor
		ena	ble multi-factor auth	cancel

1.4.2 Test your deployment with MFA enabled

Warning: You should have received an email or teams chat from your SA/SME to continue.

- 1. Close any opened browser and re-open Microsoft Edge
- 2. Connect to Bluesky. Don't try with Vanilla as your MFA test account does not exist in on-prem AAD. Thus, the SSo will not work. You can add this user in ADDS if you are confident with AD.
- 3. If you are not prompted at Azure AD login page, open an incognito window. It means you still have Azure AD cookies from previous session with ``user1``account.
- 4. At prompt, login with your MFA account. In my case, matt@f5access.onmicrosoft.com and the password provided by your SA/SME
- 5. You will be asked to enroll and select an MFA method

Microsoft
matt@f5access.onmicrosoft.com
More information required
Your organization needs more information to keep your account secure
Use a different account
Learn more
Next

- 6. Click Next
- 7. You have the choice to use the Microsoft Authenticator mobile app, or use SMS. Make your choice and follow the step to enroll your device (or phone number)

Keep your account secure Your organization requires you to set up the following methods of proving who you are.	
Microsoft Authenticator Start by getting the app On your phone, install the Microsoft Authenticator app. Download now After you install the Microsoft Authenticator app on your device, choose "Next". I want to use a different authenticator app	xt
I want to set up a different method	

8. I select the mobile app, scan the QR code, and approve the push notification on my mobile phone.

9. I click Next and Done



- 10. Azure AD asks you to change your password set by your SA/SME.
- 11. When done, and redirected to Bluesky, you can notice it does not work. The user has to be assigned with the Bluesky app.



12. In the BIG-IP, edit the ISS-Bluesky-<my name> template, and in Azure Active Directory step, add your account.

Гуре 🛈	Search Users 0			
User ~			Q	
		Items: 6		
			Filter by Name	
User	Email			Action
Andres Garcia				Add
coyote				Add
Jason Wilburn	J.Wilburn@f5.com			Add
M.Dierick@F5.com	m Dierick			Add
Matthieu Dierick				Add
user1				Add

13. Click Save and Next and Deploy

Azure AD Application Configuration :IIS-Bluesky-Matt PENDING Configuration Properties Service Provider Azure Active Directory Virt Configuration has pending changes to deploy. Do you want to deploy now? Deploy	cess » Guided Configuration			
Configuration Properties Service Provider Azure Active Directory Virt Configuration has pending changes to deploy. Do you want to deploy now? Deploy	ure AD Application Configuration	on :IIS-Bluesky-Matt	iG	
Configuration has pending changes to deploy. Do you want to deploy now? Deploy	Configuration Properties	Service Provider	Azure Active Directory	Virtual S
	Configuration has pending	changes to deploy. Do	you want to deploy now?	Deploy
Virtual Server Properties	Virtual Server F	Properties		

14. Make a new test, approve the push notification or enter the OTP received by SMS.

Note: This lab is not **Azure AD Conditional Access**. This is just **user MFA**. Conditional Access is similar but it is tied to a policy (group, location, app ...). In this lab, matt will be prompted for MFA whatever the apps he connects to.

1.5 Class 5 - Clean up the lab

Warning: In order to keep the Azure AD tenant clean, it is important you delete your application in Guided Configuration, when your demo is finished.

1. In Guided Configuration menu, click on the Undeploy icon, then OK

Federation	Zero Trust	Microsoft Integration	API Protect	tion	Credentia Protection	1
	Ø.		Ø			
nfigurations						
nport				Filter Configurati	ons by Name	
Status	Name 🔺	Туре				
DEPLOYED	IIS-baseline	Azure Al	O Application	0	O 🕹 ሰ	
	IIS-bluesky-matt	Azure Al	O Application	0	0 🕹 🖞	

2. When finished, click on Delete icon

Federation	Zero Trust	Microsoft Integration	API Protection	Cr Pr	edential otection
	Q.		Ø	¢	
figurations					
port			Filter Co	nfigurations by N	lame
	Name 🔺	Туре			
Status		Azure AD	Application	ο Φ	🚣 🔟 🔒
DEPLOYED	IIS-baseline				

Note: Thanks a lot, you cleaned up your config on both sides (APM and AAD). FYI, all old deployments will be

deleted automatically in Azure AD.