

Azure Active Directory and BIG-IP APM Integration via The “Easy Button”

(Introduced with BIG-IP ver. 16.0 and AGC ver. 7.0)

Overview

The joint Microsoft and F5 solution allow classic applications incapable of supporting modern authentication and authorization to interoperate with Azure Active Directory. Even if the application is only able to support header- or Kerberos-based authentication, it can still be enabled with single sign-on (SSO) and support multi-factor authentication (MFA) through the F5 APM and Azure Active Directory combination.

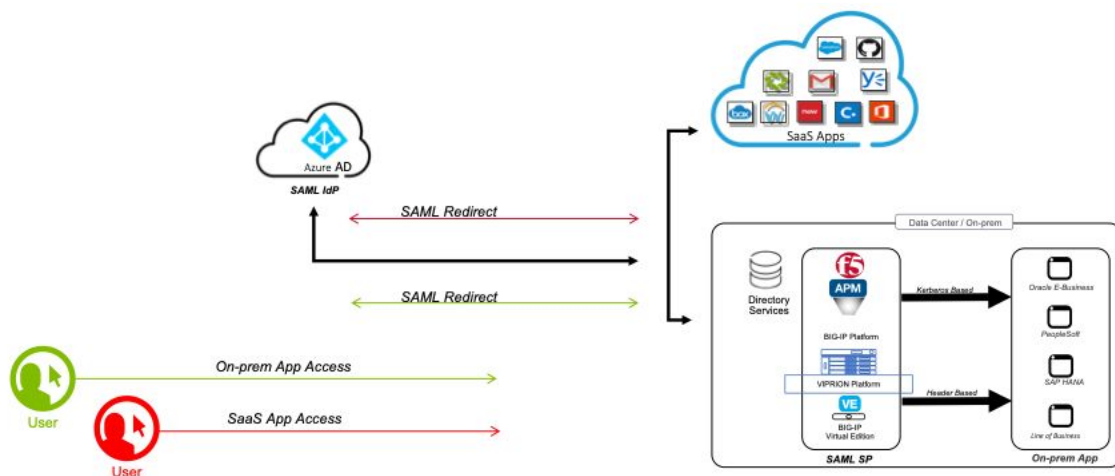


Figure 1 Secure hybrid application access

This lab/demo guide walks-through using F5’s Advanced Guided Configuration (AGC) version 7.0 to integrate Azure AD authentication with single sign-on to a “classic” on-premises application, (<https://www.funkywerx.com>) requiring header-based authentication. The associated blueprint deploys an "on-premises" environment for purposes of demonstrating the BIG-IP "Easy Button" Access Guided Configuration version 7.0.

NOTE: The following guidance references and utilizes a shared AAD demonstration tenant. However, the blueprint deployment and guidance may be used with other AAD tenants as well. The AA tenant utilized is based upon the Azure service principal credentials provided.

Access Guided Configuration 7.0 – Azure AD Easy Button

In version 16.0 of F5 BIG-IP, Access Guided Configuration v7.0 (AGC) for APM has added the ability for administrators to simply onboard and operationally manage mission-critical applications to Azure AD. The administrator no longer needs to go back and forth between Azure AD and BIG-IP as the end-to-end operation policy management has been integrated directly into the APM AGC console. This integration between BIG-IP APM and Azure AD delivers an automated “easy button” to ensure applications can quickly, easily support identity federation, SSO, and MFA. This seamless integration between BIG-IP APM and Azure AD reduces management overhead, meaning that the integration now also enhances the administrator experience.

NOTE: The following steps are completed via the deployed Jump Box.

Access Jump Server

Connect to the Jump Box server (via RDP) using the credentials provided below or the Administrator credentials located on the Jump Box 'Details' tab. From the desktop select Mozilla Firefox to complete the associated lab.

User - '**xuser**' Password - '**F5demonet**'

The Firefox desktop shortcut will open with the two tabs noted below.

* Azure Portal - <https://portal.azure.com>

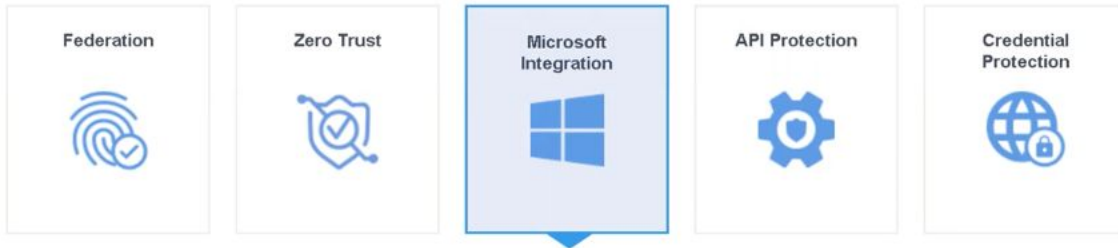
* BIG-IP GUI - <https://bigip.funkywerx.com> (aka <https://10.1.1.4>)

Configure F5 BIG-IP APM

Connect to the BIG-IP using the credentials provided below.

User- '**admin**' Password - '**F5demonet**'

Step 1: In BIG-IP click **Access > Guided Configuration > Microsoft Integration > Azure AD Application**



Microsoft Integration

BIG-IP APM integration with Microsoft Azure AD provides secure and seamless access for all modern and classic mission-critical applications. It also provides secure remote access to Exchange and Office 365.

ADFS Proxy

Consolidate and simplify deployments by load-balancing ADFS farm and performing ADFS proxy functionality.

Azure AD Application

Configure secure application access with Single sign-on across your hybrid identity environment by instantiating an Azure AD application template. It will setup BIG-IP APM as a SAML SP and Azure AD as an Identity Provider.

Exchange Proxy

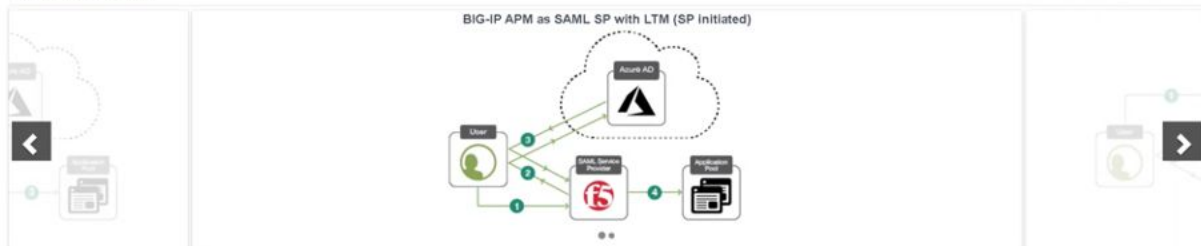
Configure BIG-IP APM to provide secure remote access to Exchange and Office 365.

Step 2: Click Next.

Azure AD Application

This guided configuration will allow you to quickly setup the BIG-IP Access Policy Manager (APM) as a SAML Service Provider (SP) and Azure AD as an Identity Provider (IdP) for your mission-critical on-premise application.

Configuration Example



1. User accesses SAML SP.
2. SAML SP redirects user to SAML IdP where user authenticates.
3. SAML IdP validates credentials and collects data from directory.
4. SAML IdP redirects user back to SAML SP with SAML assertion.

Configuring the solution using the below steps will create the required objects:



Configuration Properties

Configure the Azure service account and the application settings.



Service Provider

Uniquely identify the SAML Service Provider and specify security settings.



Azure Active Directory

Select Azure application template and update configuration properties and user attributes.



Virtual Server

Provide the IP address and port for the network traffic and select a client-side SSL profile.



Pool

Configure a pool and pool members for load balancing network traffic.



Single Sign-On (SSO) (Optional)

Configure Single Sign-On properties.



Endpoint Checks (Optional)

Select client types and the endpoint inspections to perform on them.



Session Management

Configure session timeouts and user settings.

Cancel

Next

Step 3: In the **Configuration Properties** page, configure the following information. The Azure service account you will copy the credentials from an existing AGC application, (*funkyadmin*). Leave the remaining default settings and click **Save & Next**.

IMPORTANT: This lab guide utilizes a shared AAD tenant. To avoid resource conflicts the 'Configuration Name' must be unique.

- **Configuration Name:** <Enter your F5 Login name, ex: '*gcoward*'>
- **Single Sign-On (SSO):** On
- **Copy Account Info from Existing Configuration:** On
- **Existing Configuration:** funkyadmin
- Click **Copy**
- Click **Test Connection**

Configuration Properties

General Properties ▾

Configuration Name

Type a name for this guided configuration.

Description ⓘ

☒ **On** **Single Sign-On (SSO)** ⓘ

☐ **Endpoint Checks** ⓘ

Azure Service Account Details ▾

☒ **On** **Copy Account Info from Existing Configuration** ⓘ

Existing Configuration ⓘ

▾

Copy

Tenant ID ⓘ

Client ID ⓘ

Client Secret ⓘ

Test Connection

✔ Connection is valid

Step 4: In the **Service Provider** page, configure the following information, leave default settings and click **Save & Next**.

- **Host:** www.funkywerx.com
- **Enable Encrypted Assertion** - Checked

- **Assertion Decryption Key** - Select 'www.funkywerx.com' from the drop-down
- **Assertion Decryption Certificate** - Select 'www.funkywerx.com' from the drop-down

Rather than downloading an Azure signing certificate, you will provide AAD, (via a Rest API call) the above noted certificate and key. The **Entity ID** will be automatically defined utilizing the Host and Configuration Name values.

Important: The Entity ID must be unique.

Service Provider

Advanced Settings ☐

Service Provider Properties ▾

Host ⓘ	<input type="text" value="www.funkywerx.com"/>
Entity ID ⓘ	<input type="text" value="https://www.funkywerx.com/gcward"/>
Description ⓘ	<input type="text"/>
Relay State ⓘ	<input type="text"/>

Security Settings ▾

<input checked="" type="checkbox"/> Enable Encrypted Assertion ⓘ	
Assertion Decryption Private Key ⓘ	<input type="text" value="www.funkywerx.com"/>
Assertion Decryption Certificate ⓘ	<input type="text" value="www.funkywerx.com"/>

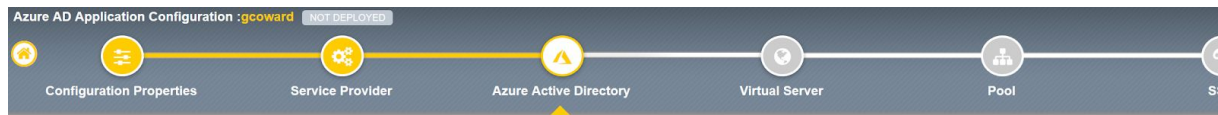
[Cancel](#)

[Save Draft](#)

[Back](#)

[Save & Next](#)


Step 5: In the **Azure Active Directory** page, double click the **F5 BIG-IP APM Azure AD Integration** icon.





Azure Active Directory


Azure Configuration  User Attributes & Claims

Configuration Properties ▾




F5 BIG-IP APM
Azure AD...


Oracle
PeopleSoft ...


SAP ERP Central
Component...

Add

Cancel

Save Draft

Back


Save & Next

Step 6: In the **Azure Active Directory** page, complete the following information to allow application access for specific Azure AD users/groups. Once completed, click the **Add** button in **User And Groups**.

- **Display Name:** Corporate Site
- **Signing Key:** [wwwfunkywerx.com](http://www.funkywerx.com)
- **Signing Certificate:** www.funkywerx.com
- **Signing Key Phrase:** F5demonet
- **Signing Option:** Sign SAML assertion
- **Signing Algorithm:** RSA-SHA256

Advanced Settings ☐

Configuration Properties ▾



F5 BIG-IP APM
Azure AD...

Change

Display Name ⓘ
 gcoward

SAML Signing Certificate ▾

Signing Key ⓘ
 www.funkywerx.com

Signing Certificate ⓘ
 www.funkywerx.com

Signing Key Passphrase ⓘ

Signing Option ⓘ
 Sign SAML assertion

Signing Algorithm ⓘ
 RSA-SHA256

Step 7: From the **User And Groups** section, select the following then click **Close**.

- **Type:** User Group
- **Classic Application Users:** Add

User And User Groups ▾

Type ⓘ
 User Group

Items: 1
 Filter by Name...

Group	Description	Action
Classic Application Users		Add

Close

Add Delete

<input type="checkbox"/>	Name	Description	Type
<input type="checkbox"/>	Classic Application Users		User Group

Step 8: In the **Azure Active Directory** page, **User Attribute and Claims** tab click **Add** button.

Azure Active Directory

Azure Configuration **User Attributes & Claims**

Required Claims ▾

Claim Name	Value
Unique User Identifier (Name ID)	user.userprincipalname
Identity	user.onpremisesamaccountname

Additional Claims ▾

Claim Name	Value
------------	-------

Add

Step 9: You will need to add an additional claim, (EMPLID) to enable SSO to the backend classic application. In the **Azure Active Directory** page, **User Attribute and Claims** tab, Additional Claims section, complete the following information, click **Done** and then click **Save & Next** at the bottom of the page.

- **Name:** EMPLID
- **Source Attribute:** user.employeeid

Additional Claims ▾

Name ⓘ

EMPLID

Namespace ⓘ

Source Attribute ⓘ

user.employeeid

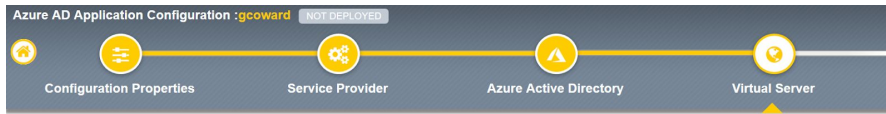
Cancel Done

Claim Name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail

Step 10: In the **Virtual Server Properties** page, configure the following information, leave default settings and click **Save & Next**.

- **Destination Address:** 10.1.20.10
- **Service Port:** 443 HTTPS (default)
- **Enable Redirect Port:** Checked (default)

- **Redirect Port:** 80 HTTP (default)
- **Client SSL Profile:** Create new
- **Client SSL Certificate:** www.funkywerx.com
- **Associated Private Key:** www.funkywerx.com



Virtual Server Properties

Advanced Settings ☐

Virtual Server

☒ Create New ☐ Use Existing

Destination Address ⓘ

10.1.20.10

Service Port ⓘ

443

HTTPS ▾

☒ Enable Redirect Port ⓘ

Redirect Port ⓘ

80

HTTP ▾

Client SSL Profile ⓘ

☒ Create new ☐ Use Existing

Client SSL Certificate ⓘ

www.funkywerx.com ▾



Associated Private Key ⓘ

www.funkywerx.com ▾



[Cancel](#)

[Save Draft](#)

[Back](#)

[Save & Next](#)

Step 11: In the **Pool Properties** page, configure the following information, leave default settings and click **Save & Next**.

- **Advanced Settings:** On
- **Select a Pool:** Create new
- **Health Monitors:** /Common/http
- **Load Balancing Method:** Least Connections (member)
- **IP Address/Node name:** /Common/10.1.10.7
- **Port:** 80 HTTP

Access » **Guided Configuration**

Azure AD Application Configuration : **geoword** View properties

Configuration Properties Service Provider Azure Active Directory Virtual Server Pool SSO

Single Sign-On Settings

Selected Single Sign-On Type
HTTP header-based ▾

Select the authentication type from the list.

SSO Headers ⓘ

Header Operation	Header Name	Header Value	Delimiter	Action
insert ▾	EMPLID	%(session.saml.last.attr.EMPLID)		+ x
insert ▾	NAME	/r/g/ws/2005/identity/claims/givenname)		+ x

Cancel Save Draft Back Save & Next

Step 13: In the **Session Management Properties** page, leave default settings and click **Save & Next**.

Session Management Properties

Advanced Settings ☐

Timeout Settings ▾

Inactivity Timeout ⓘ
900

Access Policy Timeout ⓘ
300

Maximum Session Timeout ⓘ
604800

Minimum Authentication Failure Delay ⓘ
2

Maximum Authentication Failure Delay ⓘ
5

Max Concurrent Users ⓘ
0

Max Sessions Per User ⓘ
0

Max In Progress Sessions Per Client IP ⓘ
128

☐ Restrict to Single Client IP ⓘ

☐ Use HTTP Status 503 for Error Pages ⓘ

Cancel Save Draft Back Save & Next

Step 14: In the **Your application is ready to be deployed** page, click **Deploy**.

Access > Azure Configuration

Azure AD Application Configuration **new**

1 Configuration Properties

2 Service Provider

3 Azure Active Directory

4 Virtual Server

5 Pool

6 SSO

7 Session Management

8 Summary

Configuration saved successfully

Your application is ready to be deployed.

The application is correctly configured, and ready to be deployed. Review the summary. You can click on any step to make changes.

Summary

Configuration Properties

Description

SSOEnabled

Endpoint ChecksDisabled

Session ManagementDisabled

Tenant ID74297fa3-6d58-4521-bc8e-d3d8b0591926

Client ID20e03a16-df56-4bb0-916b-803030303030

Service Provider

Azure Active Directory

Virtual Server

Pool

SSO

Session Management

Cancel

Save Draft

Back

Deploy

This deployment process takes approximately 10-15 seconds to complete. Once completed select **FINISH**.

Azure AD Application Configuration :goward **DEPLOYED**

1 Configuration Properties

2 Service Provider

3 Azure Active Directory

4 Virtual Server

5 Pool

6 SSO

Your application is deployed.

Your application is deployed. Review the summary. To make changes to the configuration, click on any step.

Quick

Test

View

Objects

Summary

Configuration Properties

Service Provider

Azure Active Directory

Virtual Server

Pool

SSO

Session Management

Cancel

Save Draft

Back

Finish

Undeploy

The application has now been deployed.

Configurations

Import

Filter Configuration

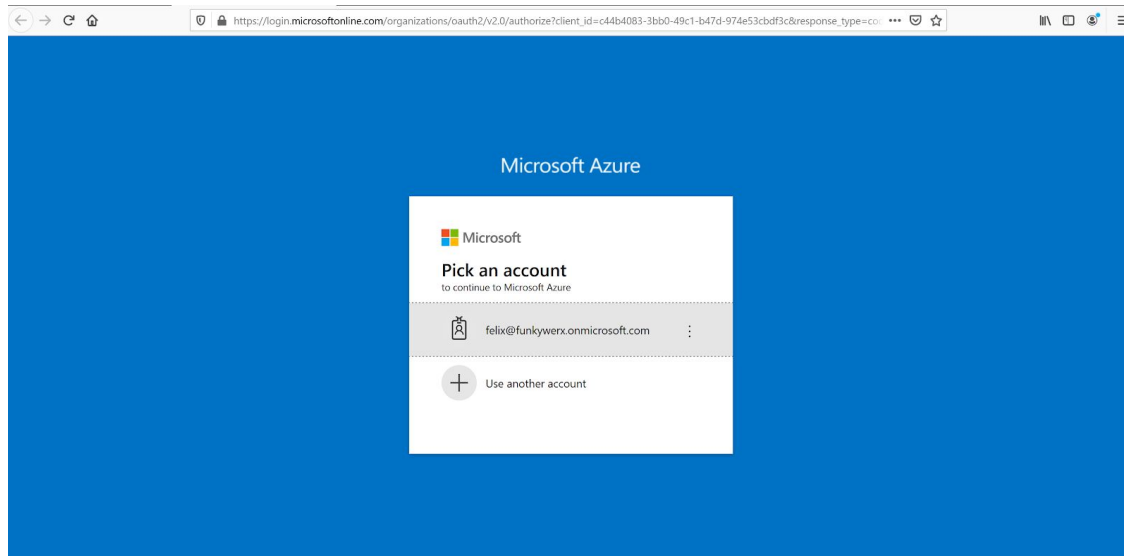
Status	Name	Type	
NOT DEPLOYED	funkyadmin	Azure AD Application	
DEPLOYED	goward	Azure AD Application	

Verify the Application Deployment

With the application now deployed, verify a successful application deployment.

Step 15: Access the Azure portal by either selecting the appropriate browser tab or navigating to <https://portal.azure.com>. Login to the portal as the tenant administrator using the credentials listed below.

User - '**felix@funkywerx.onmicrosoft.com**' Password - '**F5demonet**'



Step 16: Navigate to Azure Active Directory → Enterprise Applications

Upon successful deployment, you will see your application listed. Since this is a shared tenant, you may see other lab-generated applications in addition to your own.

Home > Funky Werx > Enterprise applications

Enterprise applications | All applications

Funky Werx - Azure Active Directory

+ New application | Columns | Preview features | Got feedback?

Try out the new Enterprise Apps search preview! Click to enable the preview. →

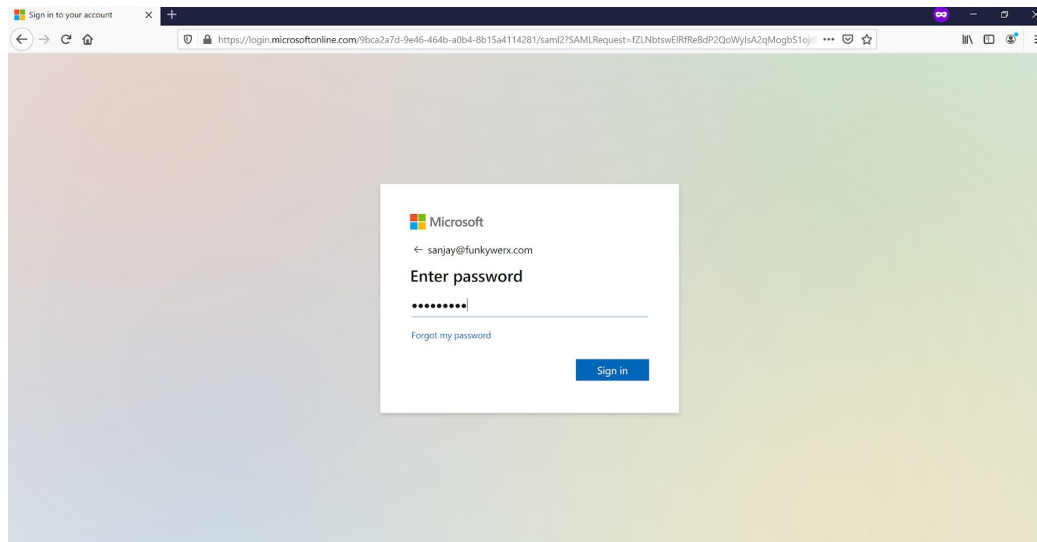
Application type: Enterprise Applications | Applications status: Any | Application visibility: Any | Apply | Reset

First 50 shown, to search all of your applications, enter a display name or the application ID.

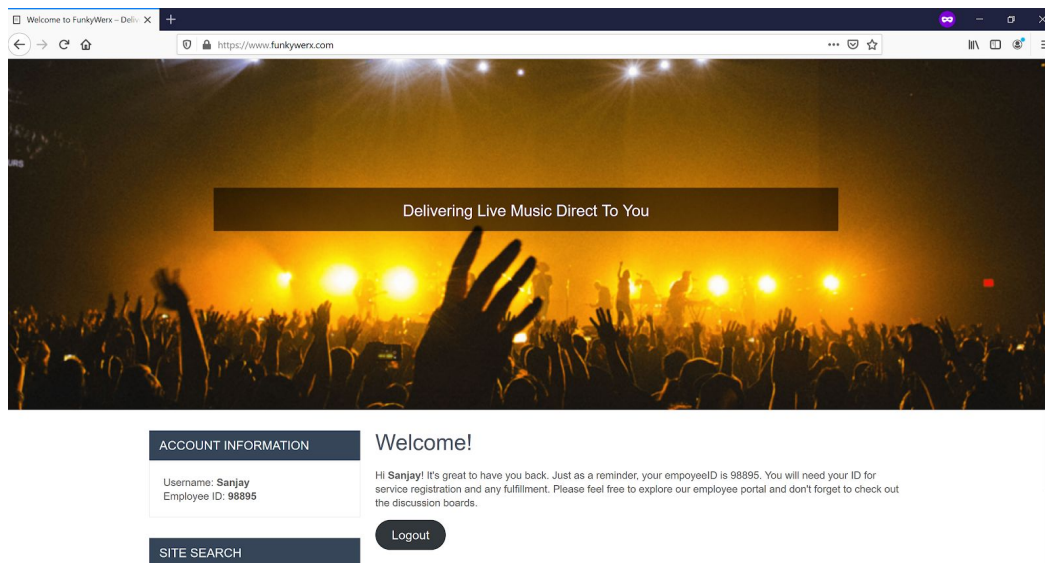
Name	Homepage URL	Object ID	Application ID
amareedu	https://www.f5.com/	d7d03ba1-f07-43a8-be5a-93ab09eba05f	49f8719b-2b7a-46bd-8d6c-eaf4219a7376
funkywerx_sp		18583be0-4579-4135-9046-b0bf16ea661a	ac86c995-4d0c-40af-9d37-654ce37d282a
gcoward	https://www.f5.com/	b326cbf8-14a4-4425-bda9-6be9a789b3fd	0829f6f8-345b-40b4-84b8-c738adff5527
nmoshiri	https://www.f5.com/	a9e5de10-93da-46e6-81b1-8fd482bd4fae	6f8ee809-9d61-43d0-b929-c71b38688762

Step 17: From the Jump Box open a new firefox browser private window session by right-clicking the Firefox icon and selecting 'New *Private Window*'. From the browser navigate to the application, (<https://www.funkywerx.com>). Login to the application using the below user credentials.

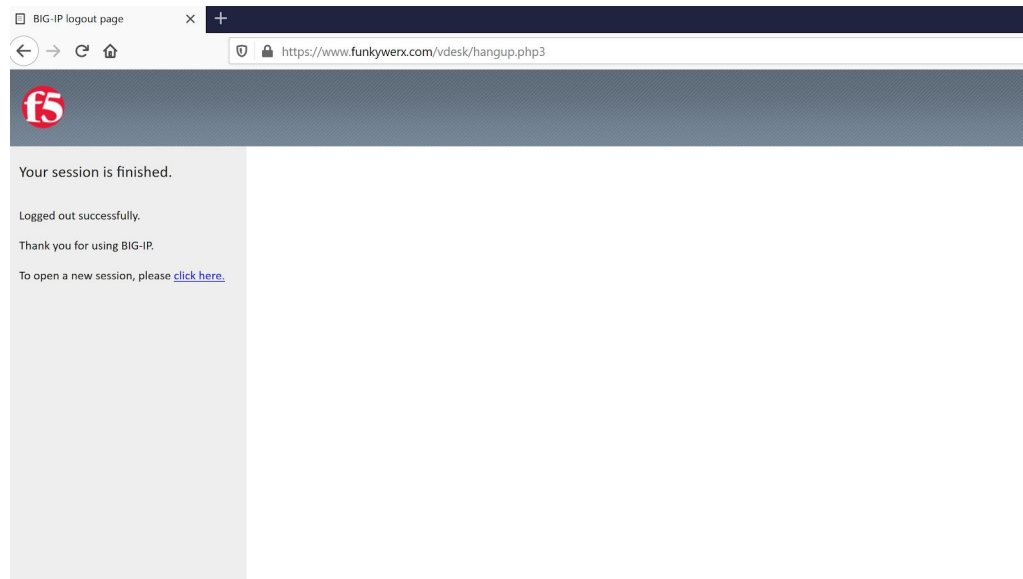
User - '**sanjay@funkywerx.com**' Password - '**F5demonet**'



Upon Successful login, you will be redirected to the backend application's homepage. Note, the user's logon information, (name & employeeID) will be correctly displayed.



Step 18: Select 'Logout' to test SLO, (Single LogOut) functionality. The user will be signed out of both Azure AD and BIG-IP APM.



Step 19: To complete the lab and clean up shared tenant resources, undeploy the application deployment. From the BIG-IP AGC main page, click on the 'undeploy' icon, (see highlighted below).

