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.

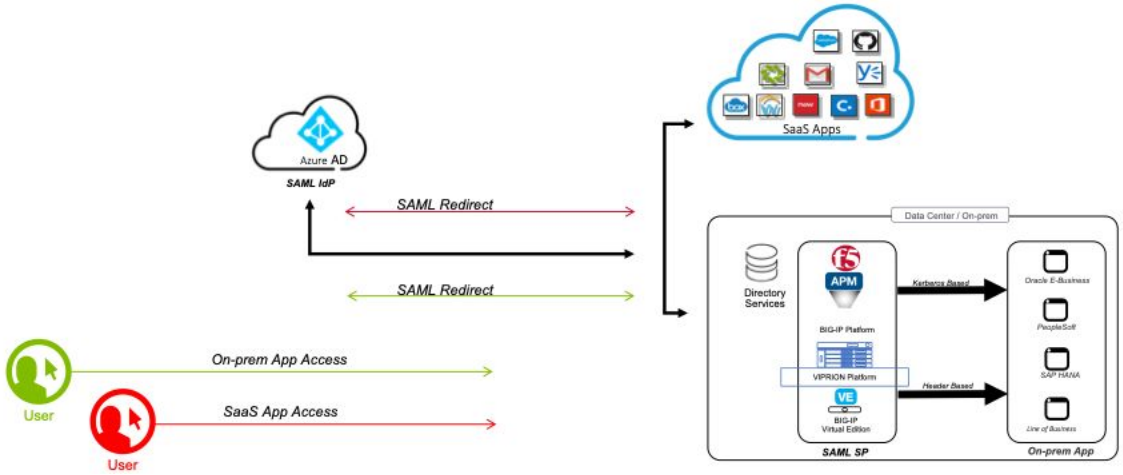


Figure 1 Secure hybrid application access

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.

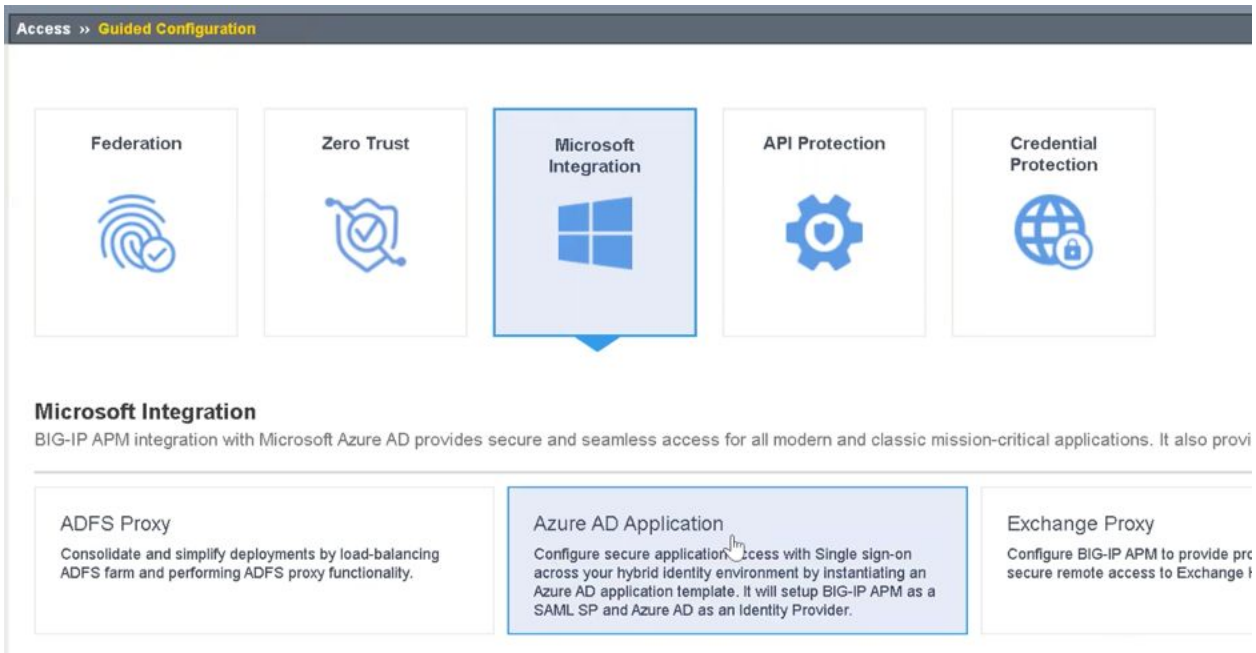
* Azure Portal - https://portal.azure.com
* BIG-IP GUI - https://bigip.funkywerx.com (aka https://10.1.1.4)

Configure F5 BIG-IP APM

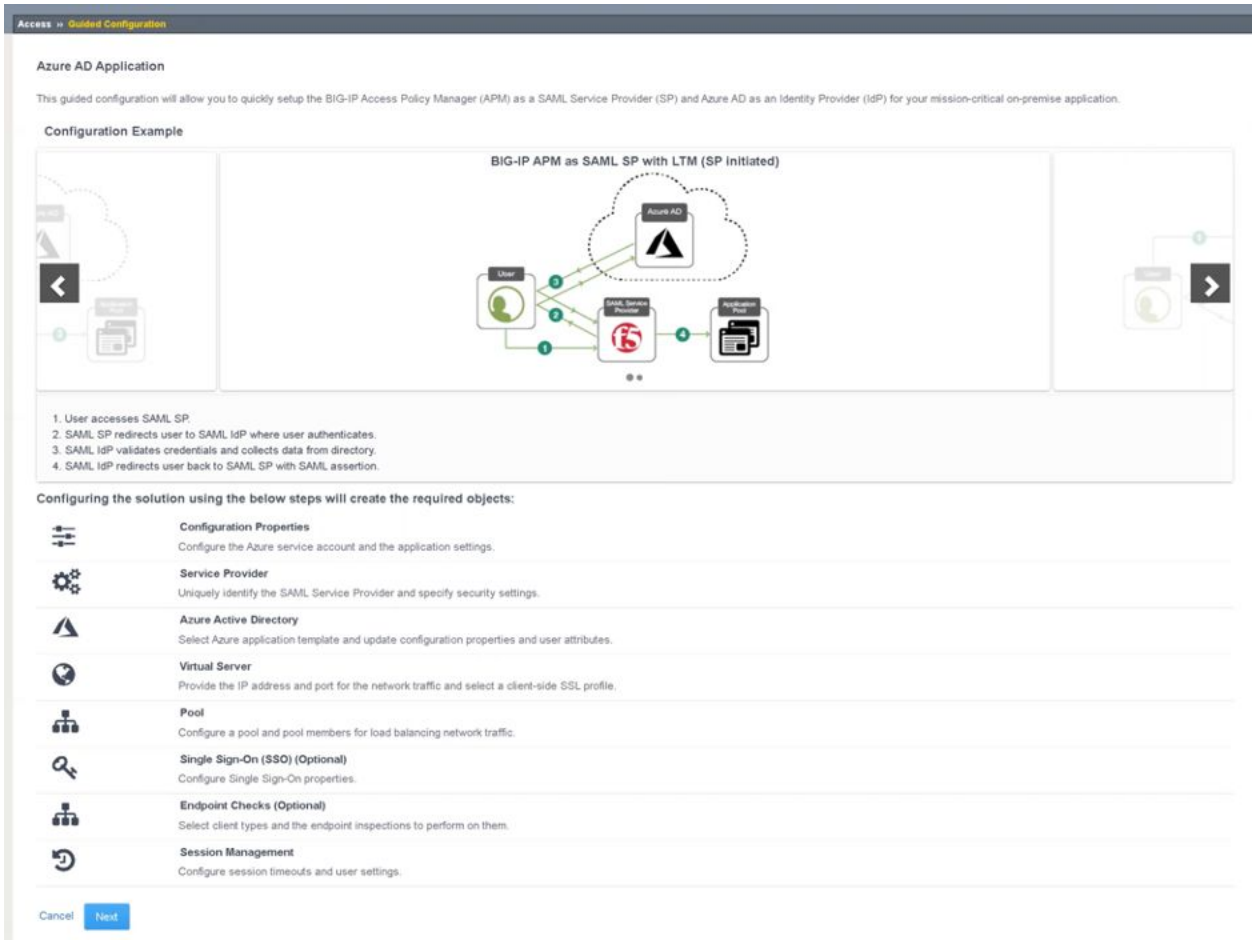
Connect to the BIG-IP using the credentials provided below.

User- ‘***admin”*** Password - ***‘F5demonet’***

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



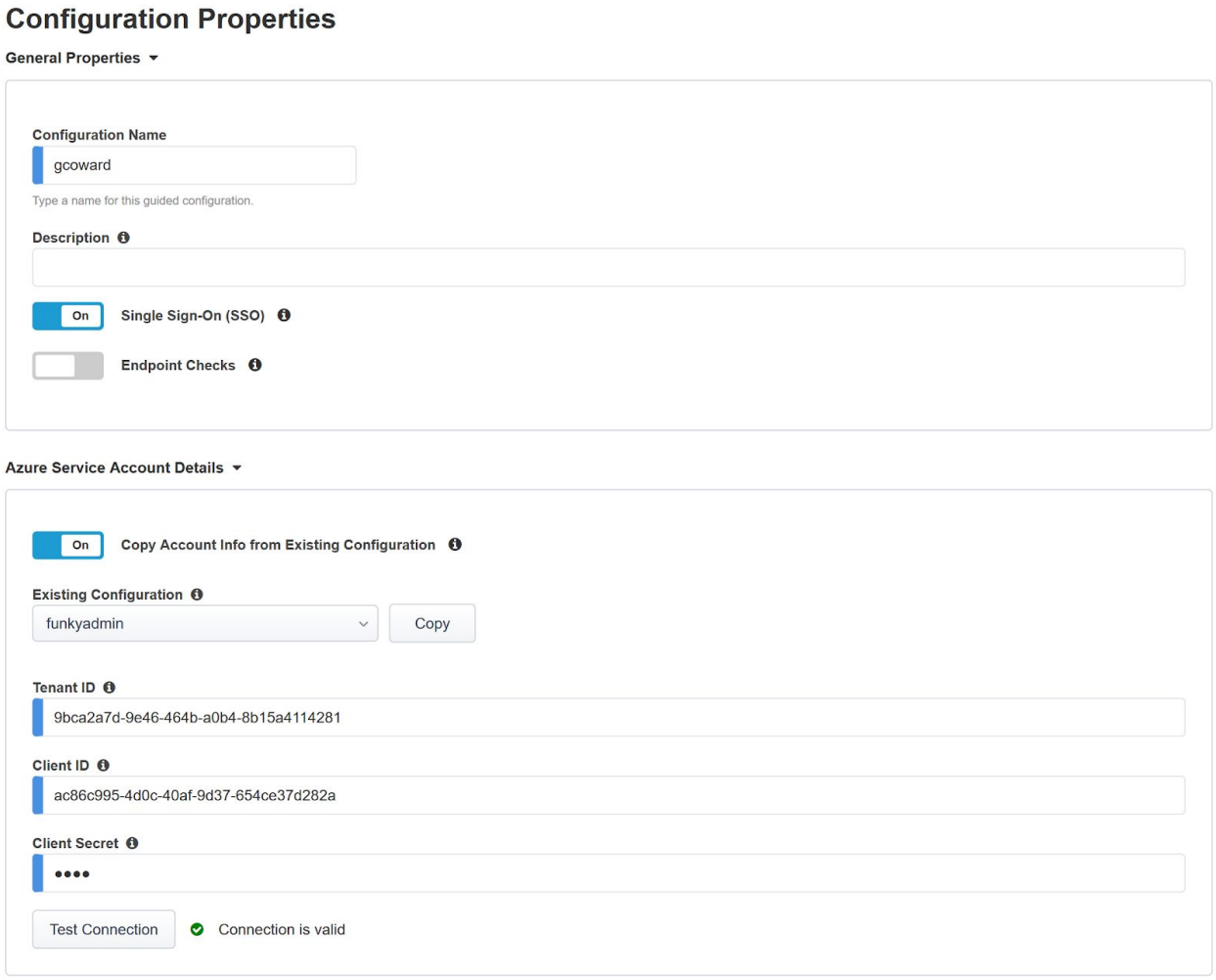
Step 2: Click **Next**.



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**



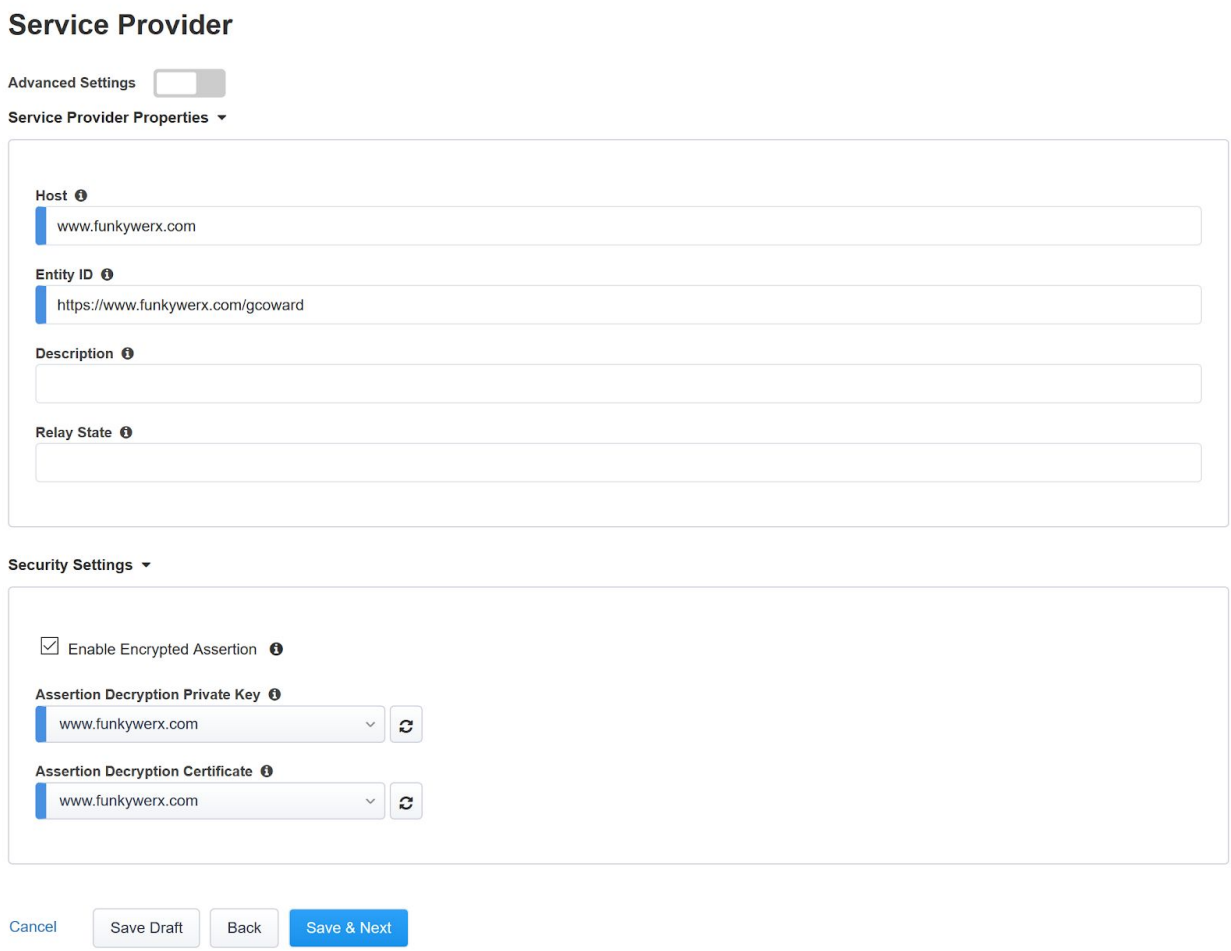
Step 4: In the **Service Provider** page, configure the following information, leave default settings and click **Save & Next**.

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

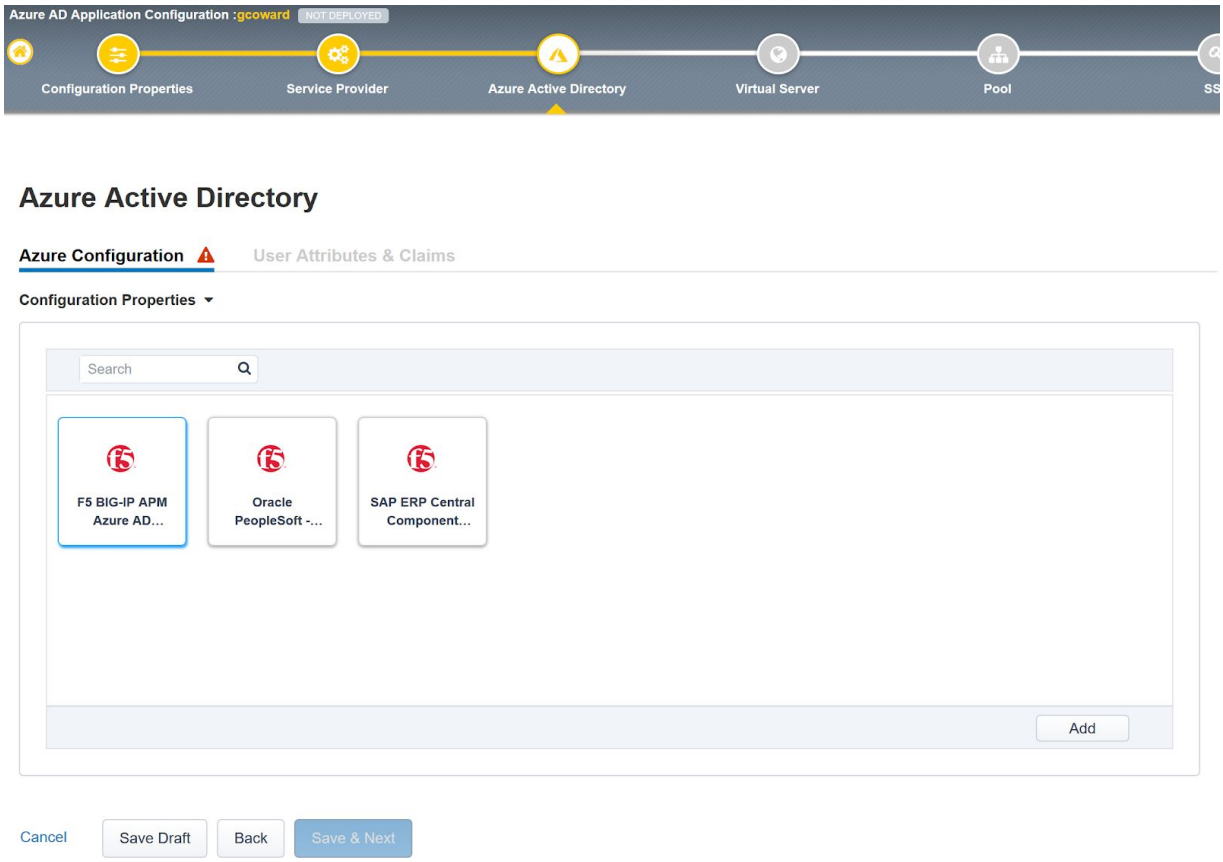
- **Assertion Decryption Key** - Select '*www.funkywerx.com*' from the drop-down
- **Assertion Decryption Certificate** - Select '*www.funkywerx.com*' from the drop-down

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.

Impotant: The Entity ID must be unique.

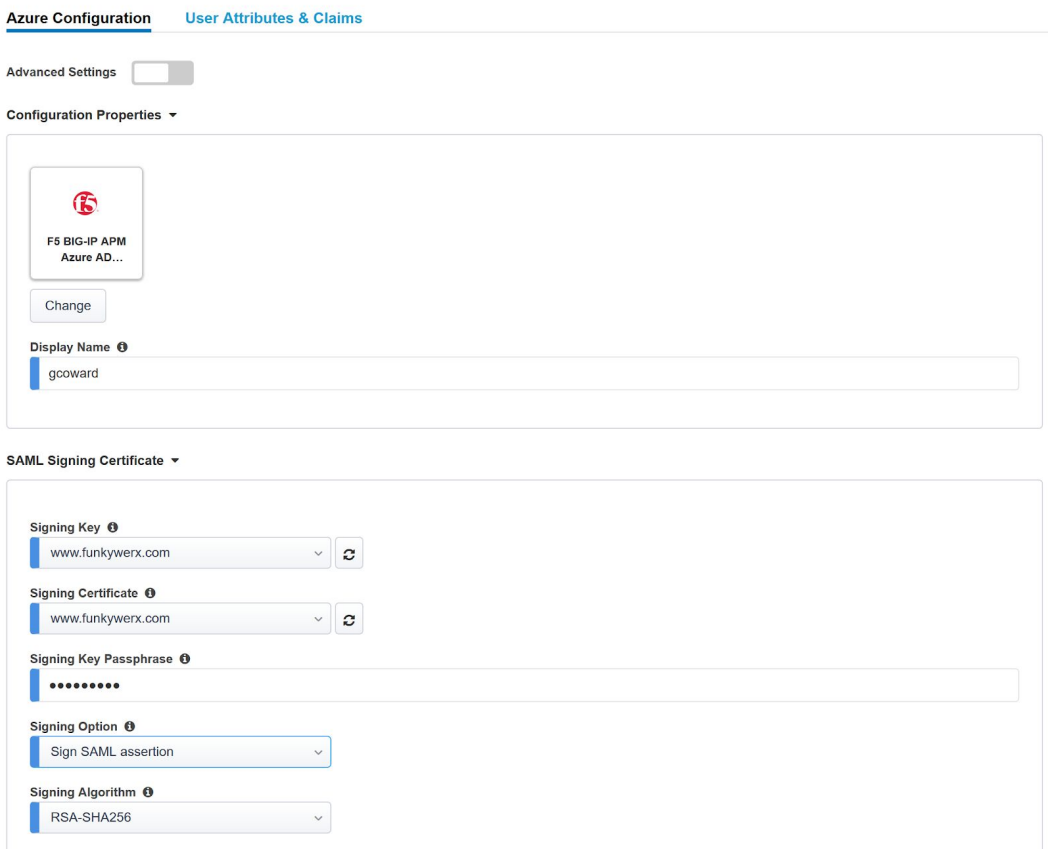


Step 5: In the **Azure Active Directory** page, double click the ***F5 BIG-IP APM Azure AD Integration*** icon.



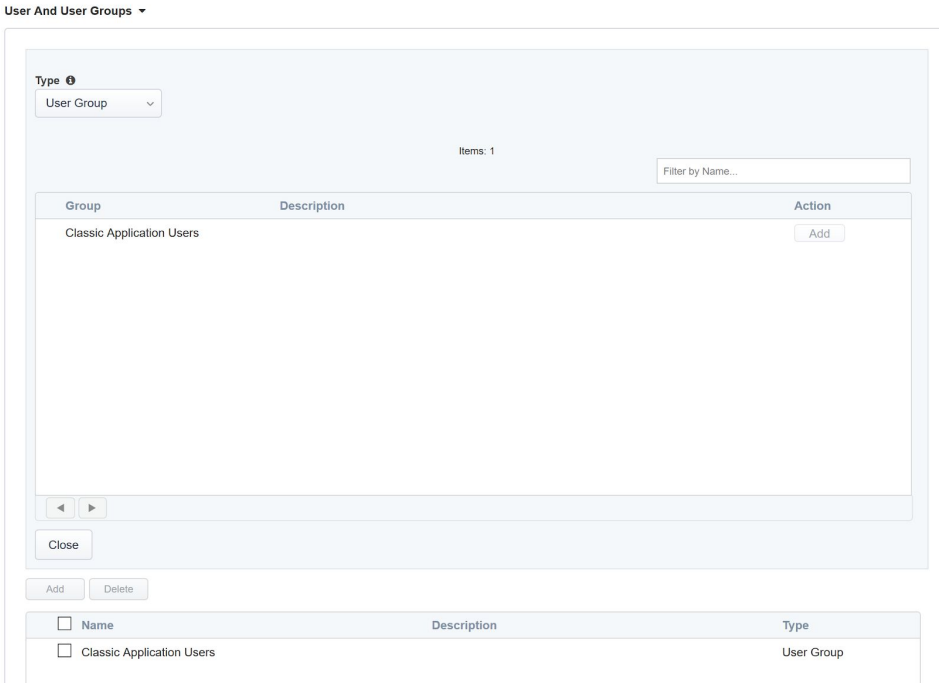
Step 6: In the **Azure Active Directory** page, complete the following information to allow application access for specific Azure AD users/groups. Once completed, click the ***Add*** button in **User And Groups**.

- **Display Name:** Corporate Site
- **Signing Key:** wwwfunkywerx.com
- **Signing Certificate:** www.funkywerx.com
- **Signing Key Passphrase:** F5demonet
- **Signing Option:** Sign SAML assertion
- **Signing Algorithm:** RSA-SHA256

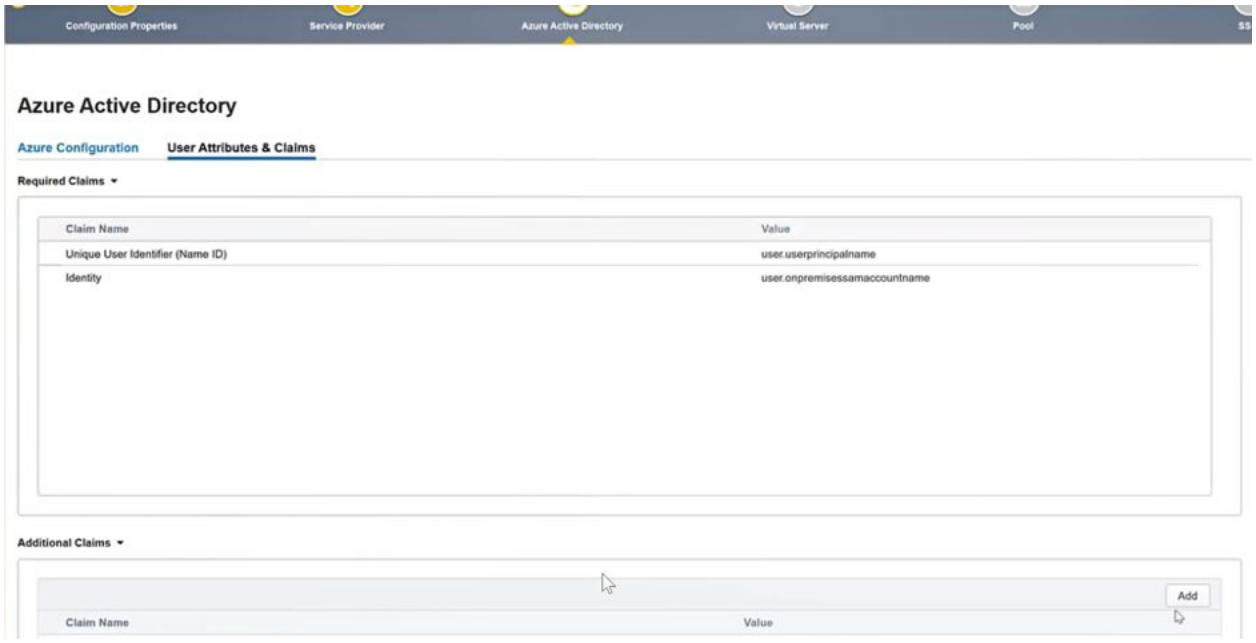


Step 7: From the **User And Groups** section, select the following then click **Close**.

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



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



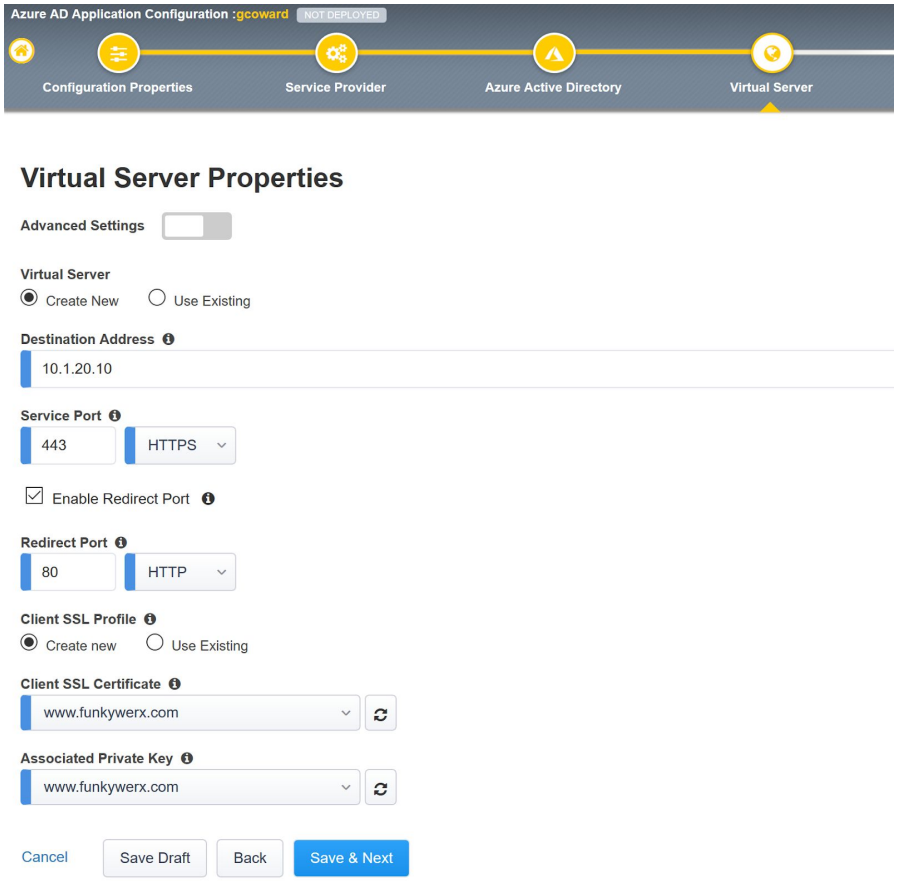
Step 9: You will need to add an additional claim, (EMPLID) to enable SSO to the backend classic application. In the **Azure Active Directory** page, **User Attribute and Claims** tab, Additional Claims section, complete the following information, click **Done** and then click **Save & Next** at the bottom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

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

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

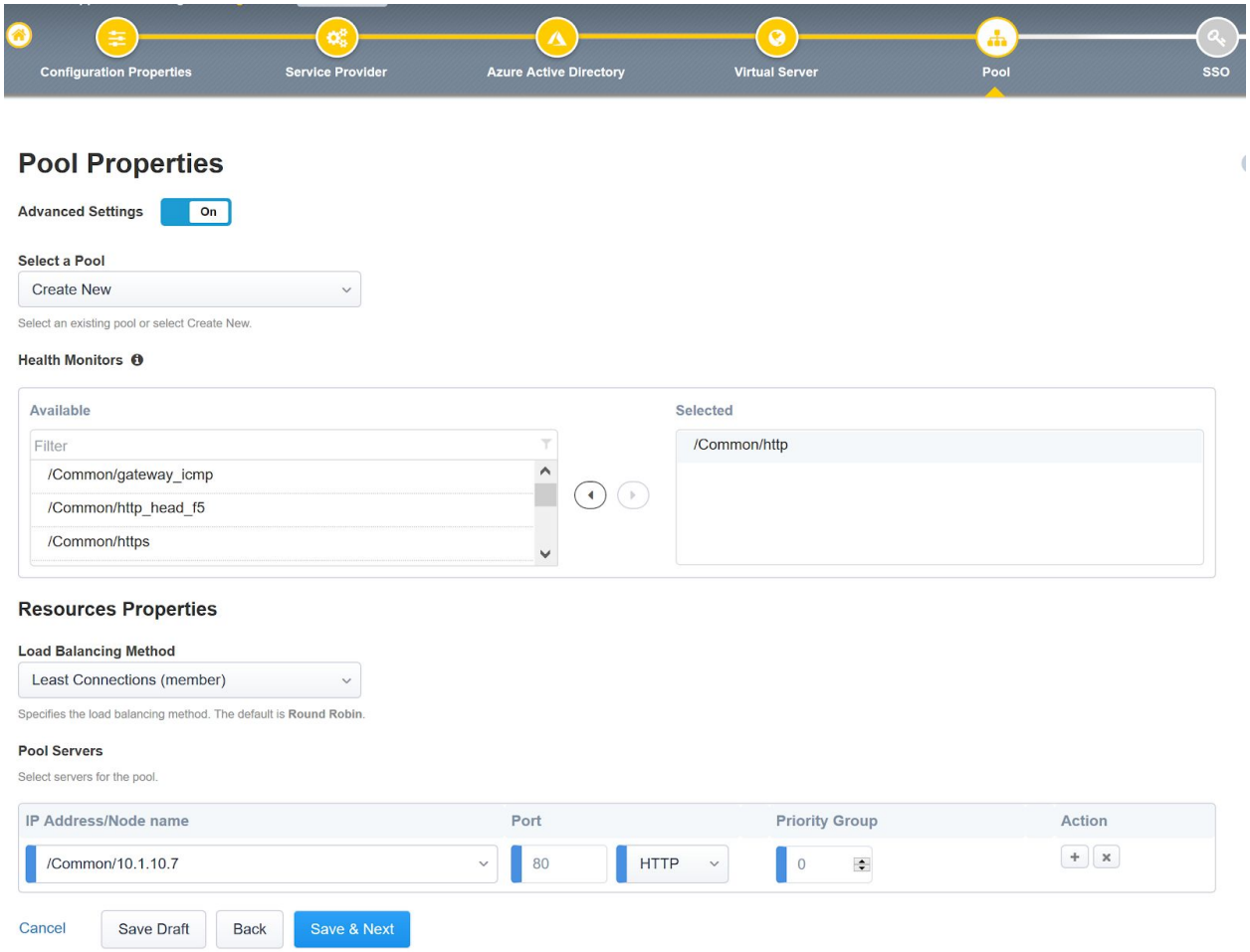
- **Destination Address:** 10.1.20.10
- **Service Port:** 443 HTTPS (default)
- **Enable Redirect Port:** Checked (default)

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



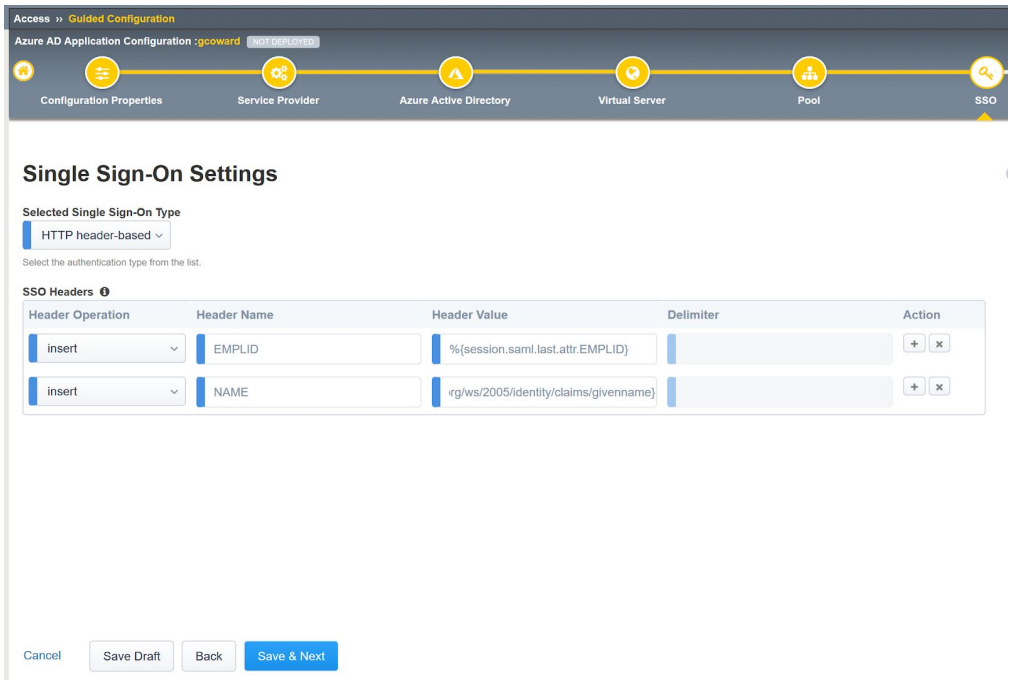
Step 11: In the **Pool Properties** page, configure the following information, leave default settings and click **Save & Next**.

- **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

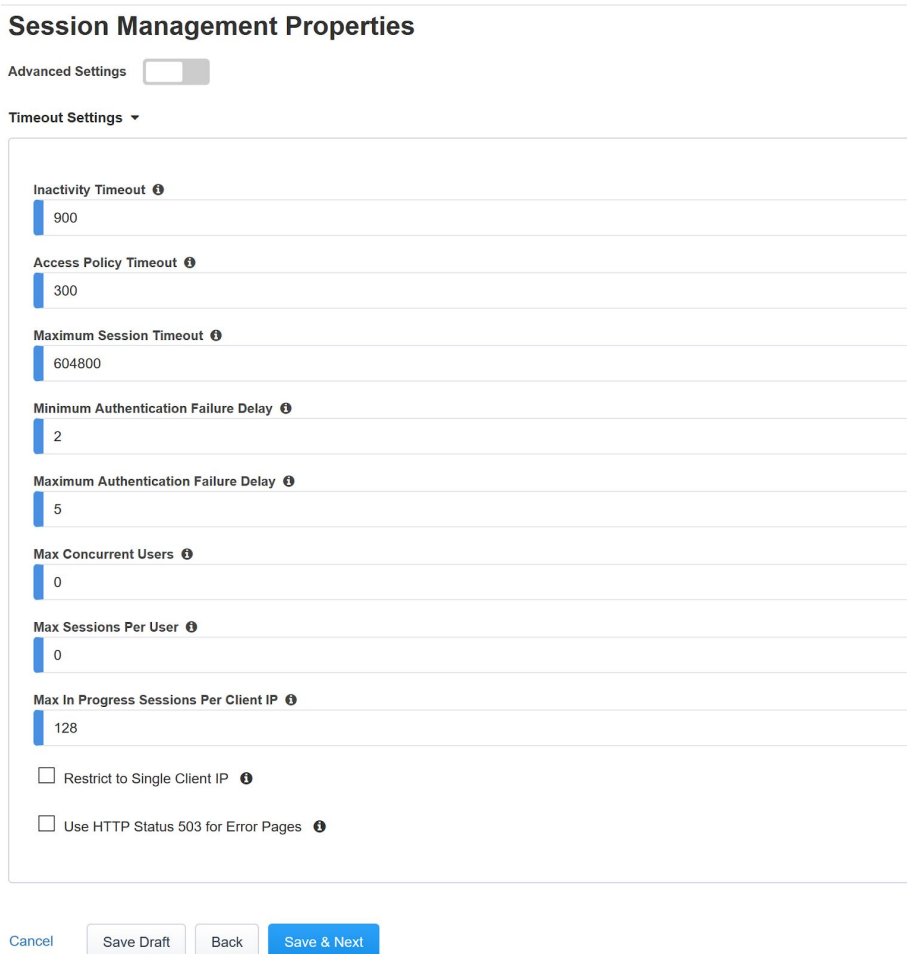


Step 12: For SSO, you will need to configure and pass two, (2) headers to the backend application. The header values will be derived from claims delivered via the SAML assertion. In the **Single Sign-On Settings** page, click **Enable Single Sign-On**, and then click on **Show Advanced Settings**, configure the following information, leave default settings and click **Save & Next**.

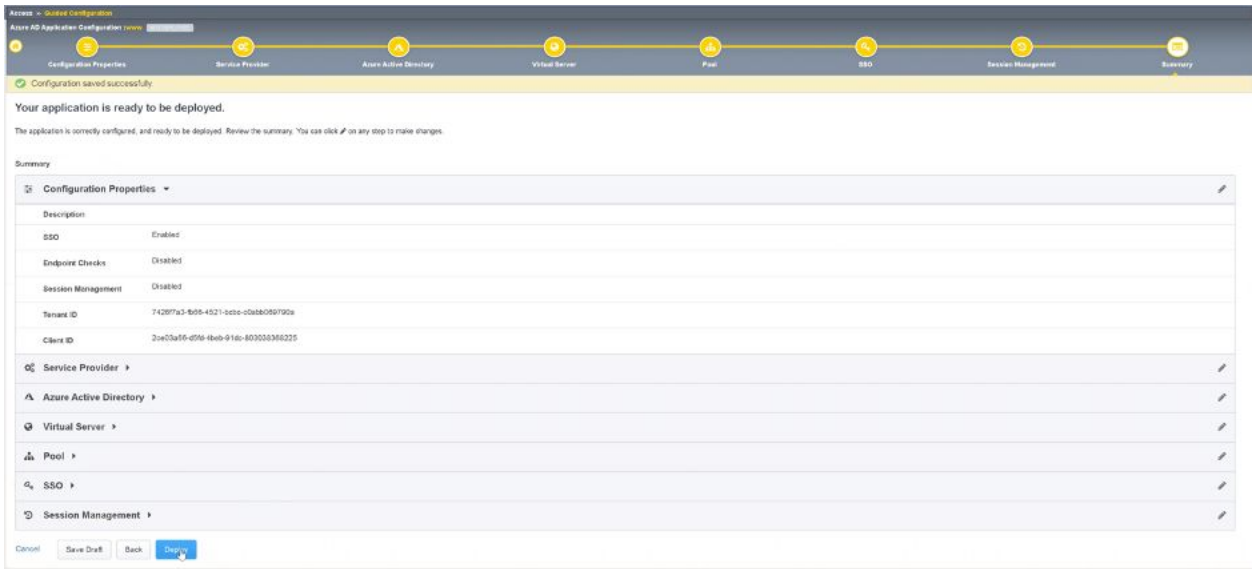
- **Select Single Sign-On Type:** HTTP header-based
- **Username Source:** session.saml.last.identity
- **SSO Headers**
    - **Header Operation:** insert
    - **Header Name:** EMPLID
    - **Header Value:** %{session.saml.last.attr.EMPLID}
    - **Header Operation:** insert
    - **Header Name:** NAME
    - **Header Value:** %{session.saml.last.attr.name.http://schemas.xmlsoap.org/ws/2005/identity/claims/givenname}



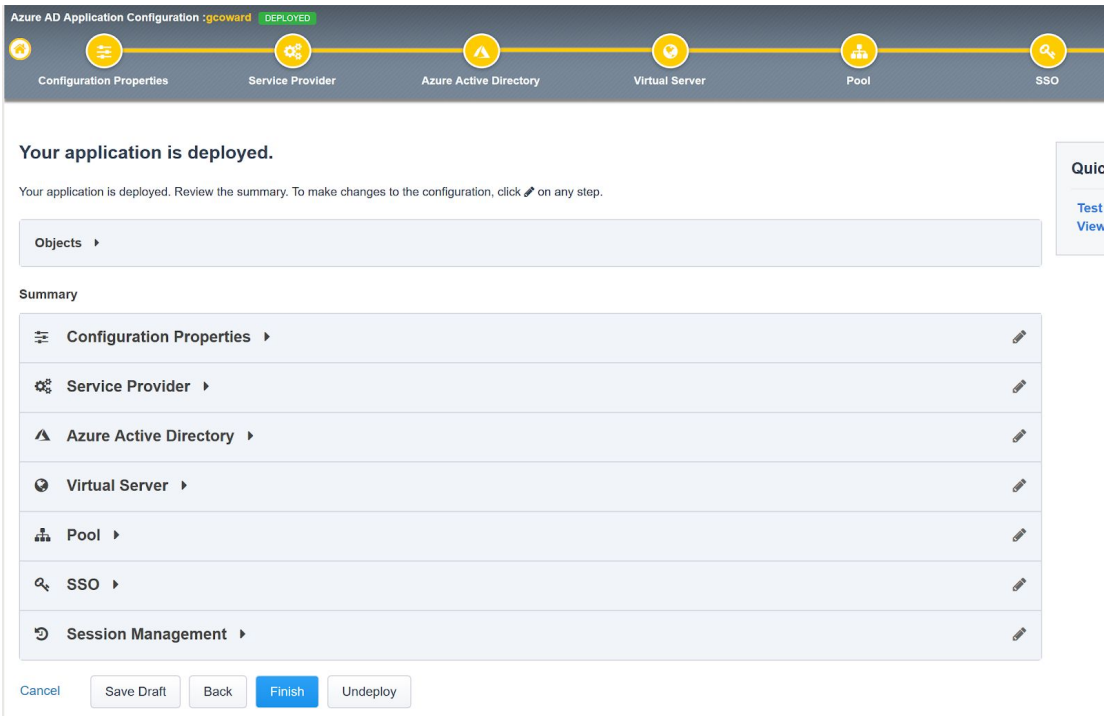
Step 13: In the **Session Management Properties** page, leave default settings and click **Save & Next**.



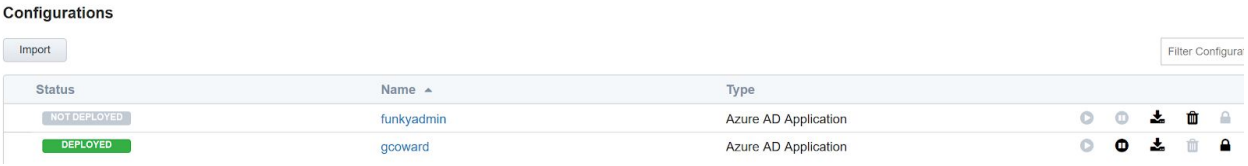
Step 14: In the **Your application is ready to be deployed** page, click **Deploy**.



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



The application has now been deployed.

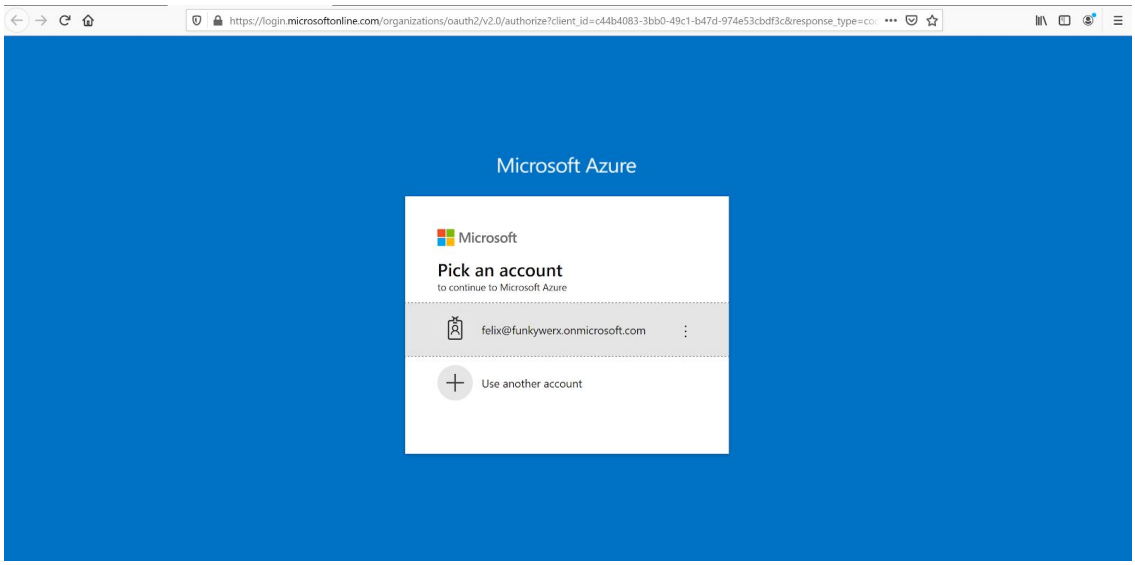


Verify the Application Deployment

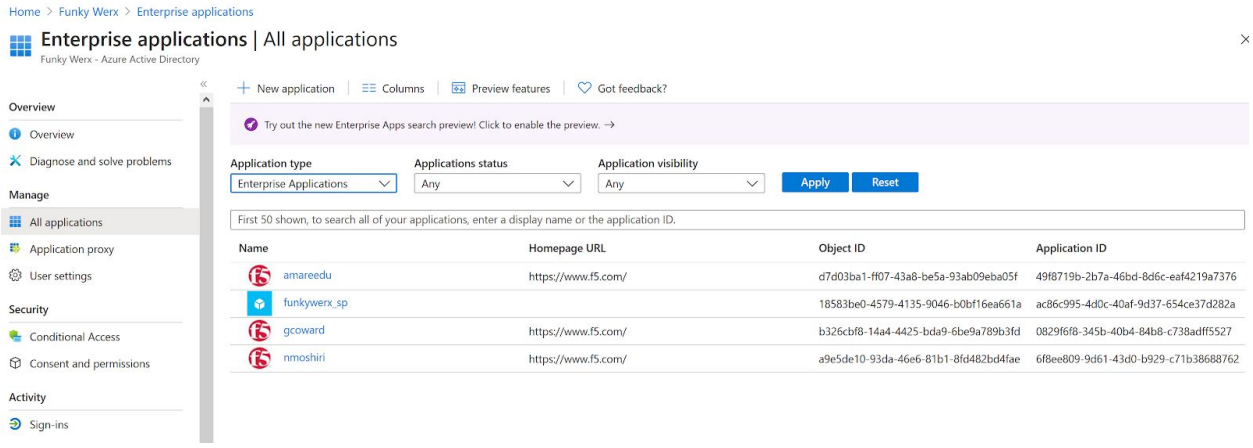
With the application now deployed, verify a successful application deployment.

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***'

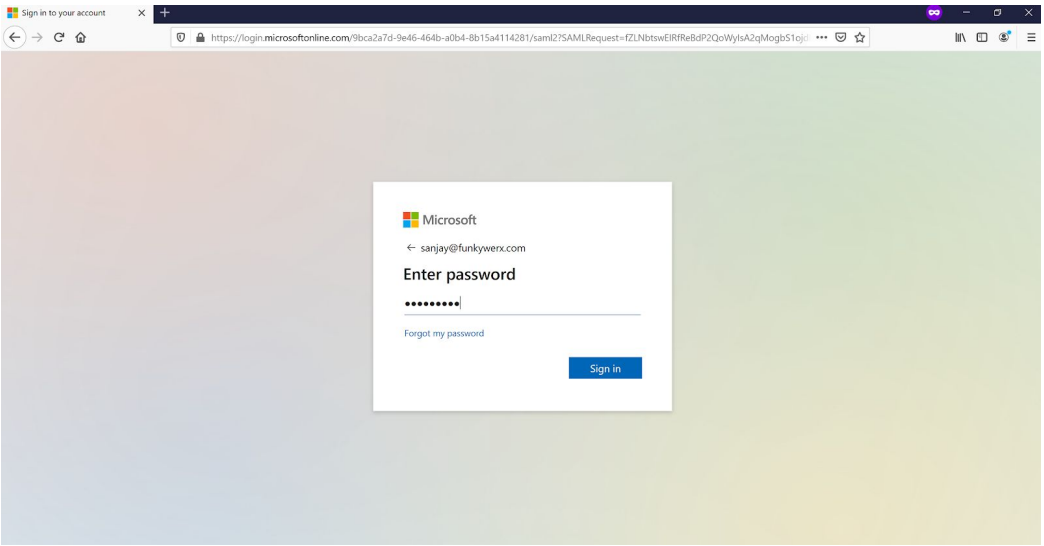


Step 16: Navigate to **Azure Active Directory → Enterprise Applications**
Upon successful deployment, you will see your application listed. Since this is a shared tenant, you may see other lab-generated applications in addition to your own.

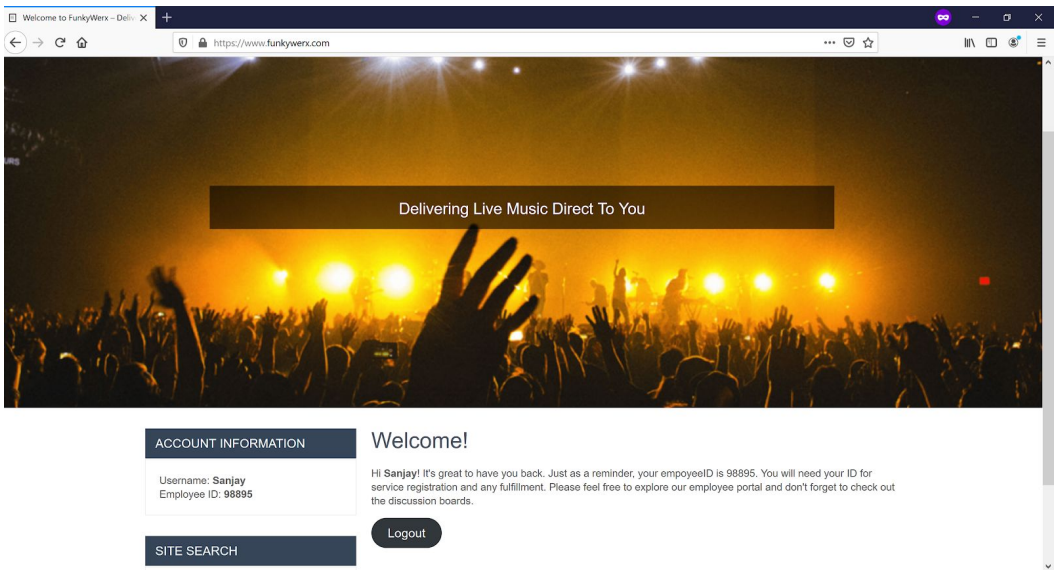


Step 17: From the Jump Box open a new firefox browser private window session by right-clicking the Firefox icon and selecting *'New Private Window'*. From the browser navigate to the application, (*https://www.funkywerx.com*). Login to the application using the below user credentials.

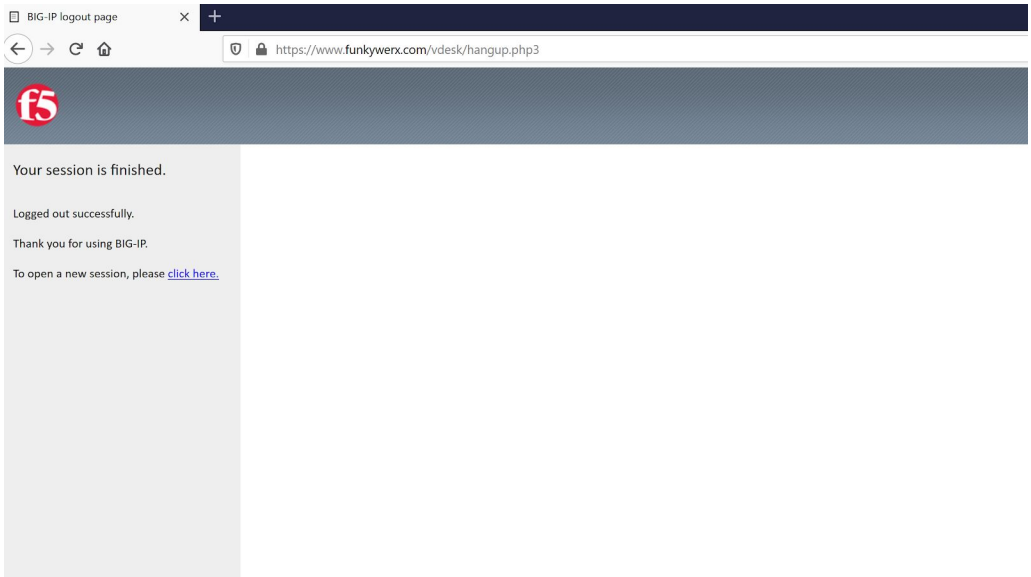
User - '***sanjay@funkywerx.com"*** Password - ***'F5demonet'***



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).