How I did It #3 - "Integrating Azure MFA with Office 365 Federation"

Greg Coward, 2016-17-06

Isn't it great when two great things go great together? Well, it sure is if you're talking O365 federation and Azure multi-factor authentication. *Yeah, ok maybe a little over the top; but hey I'm a nerd.*

In a recent post I described how I integrated Azure MFA with BIG-IP and APM to enhance the security posture of my Hybrid cloud-hosted application. In this post we'll address the follow-up customer question; "Can I use this same functionality with my BIG-IP and the Microsoft Office 365 IdP iApp template?"

Let's take a look at how I did it.

Enabling iApp Deployment Modification

If you haven't heard yet, (*I hope you have*) Microsoft Office 365 supports SAML 2.0 federation with 3rd party identity providers. This now not only includes the web-based clients but the thick clients, (i.e. Skype for Business, CRM, Outlook) as well. To make deploying a BIG-IP for this functionality super easy, F5 has created an iApp template and guidance available for download. By simply answering a few questions, an administrator can create all the necessary LTM and APM components required to deploy a SAML IdP application service for use with Office 365.

For this post, I have already deployed the iApp template and have established federation with Office 365.

By default, the components deployed by the iApp can only be modified from with in the iApp template configuration. Since I'm going to add in additional functionality, (Azure MFA) I must first disable the strictness requirement. To do so, I will:
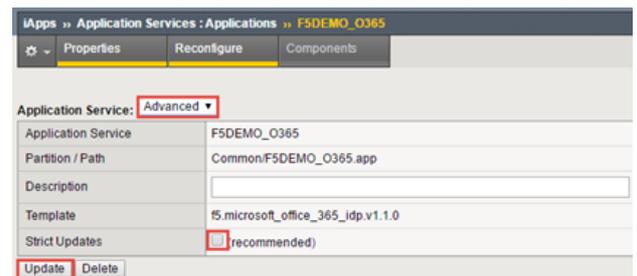
1. Navigate to | *iApps* | *Application Services*

2. Click on the o365 application service to open the application Components.
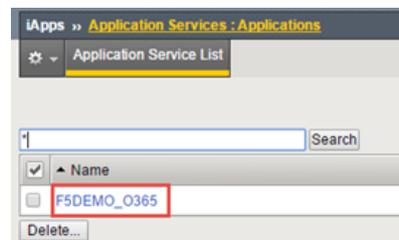

3. Select | *Properties*
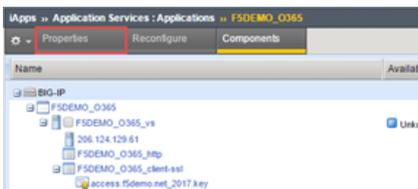
4. Select | *Advanced* | uncheck *Strict Updates* | *Update*. With *'Strict Updates'* disabled, the application service can now be modified outside of the iApp configuration.


Modify Existing O365 Access Policy

Now that I am able to modify the application service, I will need to modify the access policy to include the Azure MFA resource. For this post, I have already created the Azure MFA environment and the required APM object. I simply need to incorporate it into the policy using the Visual Policy Editor. For detailed guidance on creating the Azure MFA object, (*APM utilizes RADIUS authentication to query the MFA server*) refer to my previous blog post here. The steps I use are as follows:

1. Navigate to | *Access Profiles* | *Access Profiles List*. Click on the *'Edit'* under the Access Policy column to open the visual policy editor.
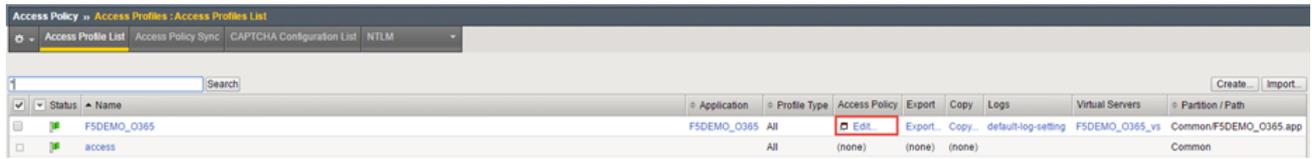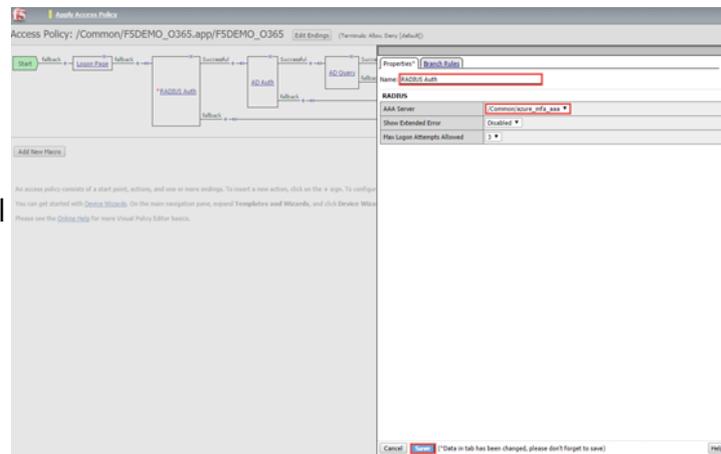

2. With the O365 policy opened, select | '+' to the right of the *'Logon Page'* object.

3. From the available resources dialog page, select | *Authentication* | *RADIUS Auth* | *Add Item*
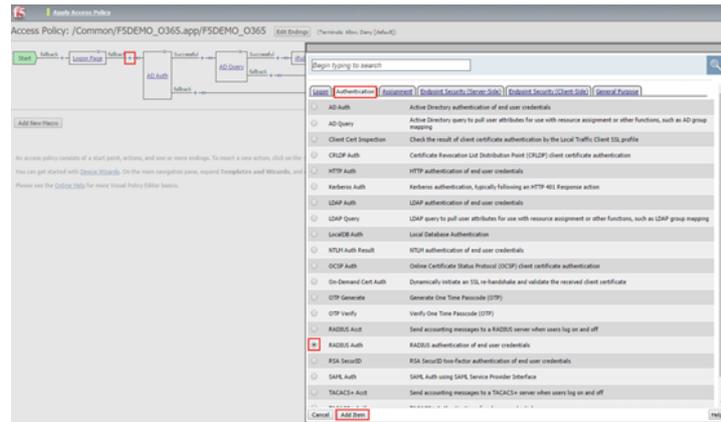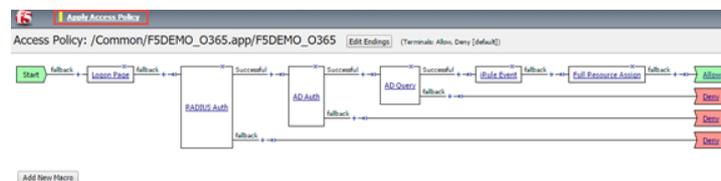

4. With the object configuration page opened, provide a name for the object, (*or leave default*).

5. Select the previously created AAA server object from the drop-down | Select *Save*

4. Select *Apply Access Policy* to finish the process.

That's it! You've added MFA to Office 365 with the BIG-IP.

Additional Links:

How I did It - "Integrating Azure MFA with the BIG-IP"

Azure Multi-Factor Authentication Documentation

F5 BIG-IP Access Policy Manager Resources and Support

The BIG-IP Platform and Microsoft Azure

Technorati Tags: Azure MFA multi-factor authentication BIG-IP Access Policy Manager F5 Azure