

O365 Solutions

Three Phase Approach

msfttechteam@f5.com



Contents

Use Cases	2
Use Case One Advanced Traffic Management for WAP and ADFS farms	2
Use Case Two BIG-IP with ADFS-PIP.....	3
Phase Three BIG-IP as IdP.....	4
Lab Environment	5
Solution Prerequisites.....	5
Directory Services.....	5
Public Key infrastructure.....	5
Public Domain Naming Service (DNS).....	5
BIG-IP Access Policy Manager (APM).....	6
Federate via PowerShell	7
BIG-IP iApp	8
Download the ADFS iApp v 1.7 from https://downloads.f5.com	8
Import the iApp to the BIG-IP.....	10
Upgrading an Application Service from previous version of the iApp template	12
Use Case One Configuring Local Traffic Management (LTM) for WAP and ADFS farms.....	13
iApp Configuration.....	13
Configure LTM to Load Balance Active Directory Federation Services (ADFS).....	13
Create a Route to the DMZ	18
Configure LTM to Load Balance Web Application Proxy (WAP) servers.....	22
Use Case Two BIG-IP with ADFS-PIP	25
Reconfigure ADFS iApp to include ADFS Proxy support.....	25
Use Case Three BIG-IP as IdP.....	28
Delete existing ADFS iApps.....	28
iApp Configuration.....	29
Verify Successful Federation	32



Document Version History

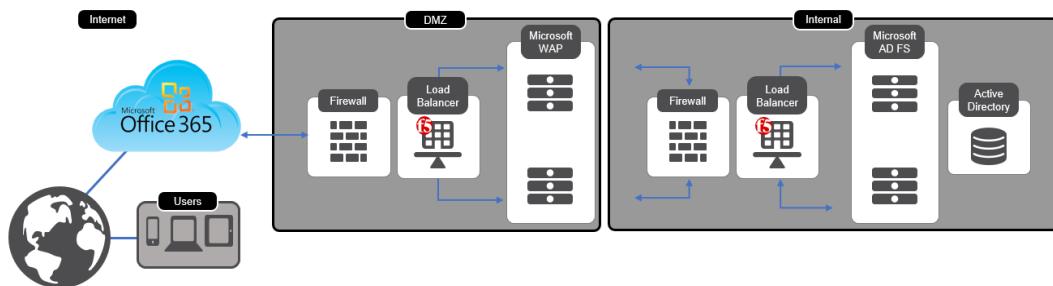
Date		Revision History	Revision Class	Comments
4/8/2018		1.0.0		Initial Availability



Use Cases

Use Case One | Advanced Traffic Management for WAP and ADFS farms

Use Case One | Configuring Local Traffic Management (LTM) for WAP and ADFS farms



Scenario | Your organizations O365 tenancy requires an advanced Traffic Management engine

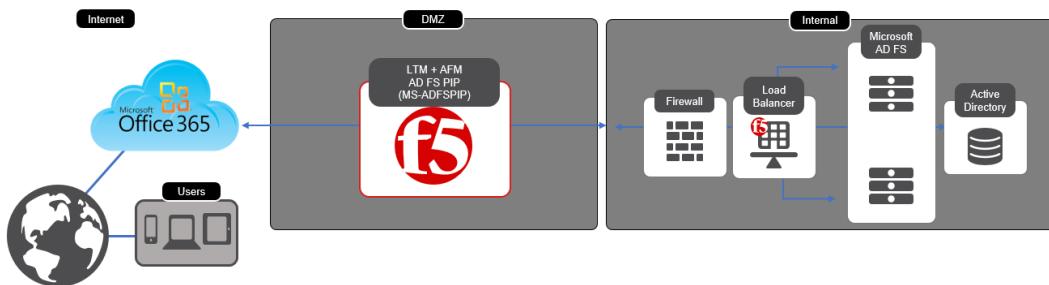
BIG-IP LTM is a full proxy, used to inspect, manage, and report on application traffic entering *and* exiting your network. From basic load balancing to complex traffic management decisions based on client, server, or application status, BIG-IP LTM gives you granular control over app traffic.

Full Proxy	SSL	iRules	iApp
Granular control over app traffic.	Cost-effectively protect the end-to-end user experience by encrypting everything from the client to the server	Event-driven scripting language adaptable to defeating zero-day attacks	Enables quick and smooth configuration of standard load balancing with the provided iApp Application template
Manage, and report on application traffic entering <i>and</i> exiting your network	Includes levels of inspection necessary to block bad traffic and allow good traffic to pass through.	From defeating zero-day attacks to cloning specific app requests or dealing with custom application protocols	Gives you greater visibility and control over app delivery
Optimize the speed and reliability of your applications via both network and application layers	Scales on-demand and absorbs potentially crippling DDoS attacks	Adaptable to application delivery challenges across the data center, virtual infrastructure, and the cloud.	you can deploy in hours instead of weeks.



Use Case Two | BIG-IP with ADFS-PIP

Phase Two | BIG-IP with ADFS-PIP



Scenario | Your O365 Architecture has Windows Application Proxy Servers (WAP) in your DMZ. Microsoft now officially supports the use of third party proxies as an alternative if those proxies support ADFS-PIP

BIG-IP Access Policy Manager can now replace the need for Web Application Proxy servers providing security for your modern AD FS deployment with MS-ADFSPIP support released in BIG-IP v13.1.

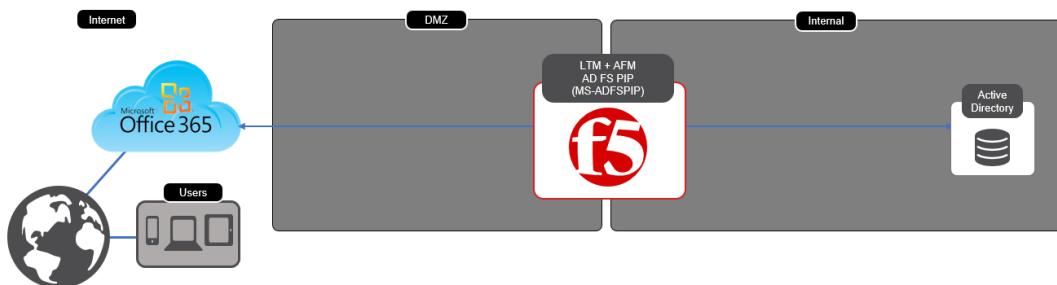
Benefits of using APM as a WAP Alternative

Simplified Architecture	Consolidate load balancing and secure access with BIG-IP APM with an AD FS PIP -compliant proxy Limit your exposure by only placing security hardened devices in the DMZ
Simple to Deploy	F5 iApp uses information gathered by the administrator to configure a service for a new application
Pre-Authentication	Providing a layer of security further isolating internal resources from external access
Multi-Factor Authentication (MFA)	Azure MFA included in iApp template
WAF features	Brute force, credential stuffing, bot protection, and more...



Phase Three | BIG-IP as IdP

Use Case Three | BIG-IP as IdP



F5 Access Federation architecture uses Security Assertion Markup Language (SAML), an XML-based, open standard data format for exchanging authentication and authorization data between parties. SAML technology eliminates the need to manage independent user accounts across SaaS providers. The most important element that SAML addresses is web browser single sign-on (SSO).

Furthermore, the F5 Access Federation architecture enables the deployment of stronger authorization solutions, including two-factor authentication, IP geolocation enforcement, and device inspection.

F5 BIG-IP Local Traffic Manager (LTM) and BIG-IP Access Policy Manager (APM) together provide the required platform

- ④ SAML communication between an organization's private IAM system and external SaaS providers. Consistent, multi-factor authentication for all users across all systems accessed using the BIG-IP devices

Consistent, multi-factor authentication for all users across all systems accessed using the BIG-IP devices

In this document we will describe how one would configure a BIG-IP for SSO user attempts to access a resource without being logged on. The user has a domain account and a federated organization. The BIG-IP acts as the identity provider ("IdP"). Both the request and the returned SAML assertion are sent through the user's browser via HTTP POST.



Lab Environment

For the purposes of verifying a working solution we deployed the following.

Appliance	Roles	Version
Windows Server 2016	Active Directory Services Remote Access Certificate Services	Version 1607 (OS Build 14393.2068)
BIG-IP VE	(APM) Access Policy Manager (LTM) Local Traffic Management	BIG-IP 13.1.0.1 Build 0.0.8 Point Release 1
Office 365	NA	NA

Solution Prerequisites

Directory Services

LDAP (Lightweight Directory Access Protocol) can be used by systems to perform LDAP lookups against existing users in order to verify their Access and Identity. We utilized Microsoft's [Active Directory](#) to import user accounts. Creating your first Active Directory Domain Controller can be achieved by following the steps outlined here

- ④ [System Requirements and Installation Information for Windows Server 2012 R2](#)
- ④ [Preparing to deploy a Windows Domain Controller](#)
- ④ [Build and Deploy the First Domain Controller](#)
- ④ [Create a User Account in Active Directory Users and Computers](#)

Public Key Infrastructure

Before you begin configuring the iApp, you need to make sure that you either create or import the certificate that will be used to sign your assertions to the BIG-IP system. That certificate can be either a self-signed certificate generated by the BIG-IP system, or you can import any certificate on the BIG-IP system for this purpose. The only restriction is that a wildcard certificate cannot be used to sign SAML assertions to Office 365.

To generate or import a certificate, go to System > File Management > SSL Certificate List. If you are using a certificate from a third-party CA, click Import. If you want the BIG-IP system to generate a self-signed certificate, click Create.

Importing a valid SSL certificate for authentication

You also need to import a valid SSL certificate onto the BIG-IP system that is trusted by all browsers, as it will be used by your external users to connect to your IdP service and authenticate themselves to the Office 365 cloud.

To import a certificate, go to System > File Management > SSL Certificate List, and then click Import. From the Import Type list, select the appropriate value, such as Certificate. Repeat for the key if necessary

- ④ [Managing SSL certificates for BIG-IP systems using the Configuration utility](#)

Public Domain Naming Service (DNS)

A publicly routable A record that points to the destination address of your Virtual Server is required



BIG-IP Access Policy Manager (APM)

BIG-IP APM federates user identity across multiple domains using numerous authentication and attribute-sharing standards and protocols, including SAML 2.0.

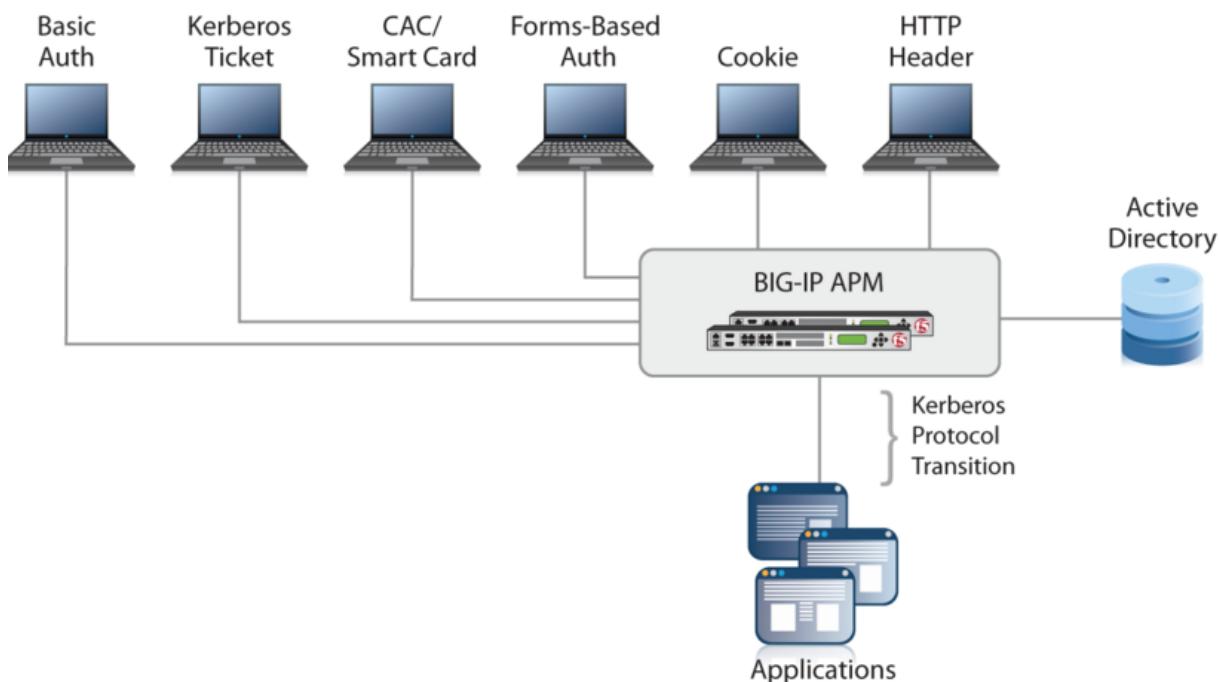
BIG-IP APM supports connections initiated by SAML identity providers (IdPs) and service providers (SPs), extending secure single sign-on (SSO) capabilities to SaaS, cloud-based, web-based, and virtual applications; remote access (VPN) authentication and authorization; and client-based apps and browser-less environments.

With BIG-IP APM, it's faster and easier to provision and de-provision user access to resources, no matter where they're located.

Access Policy Manager provides a Single Sign-On (SSO) feature which leverages credential caching and proxy. This mechanism acts as a two-phase security mechanism that only requires your users to enter their credential once to access their secured web applications.

By leveraging this technology, users request access to the secured back-end web server. Once that occurs, Access Policy Manager creates a user session and collects the user identity based on the access policy. Upon successful completion of the access policy, the user identity is saved (*cached*), in a session database. Lastly, the **WebSSO** plugin retrieves (*proxies*) the cached user credentials and authenticates the user based on the configured authentication method. Additional information can be found in the Hyperlinks below

- [Centralized, Secure Application Access Anytime, Anywhere](#)
- [BIG-IP Access Policy Manager: SAML Configuration Guide](#)
- [Simplifying Single Sign-On with F5 BIG-IP APM and Active Directory](#)





Federate via PowerShell

For the purposes of this document It is assumed that you have a O365 Tenancy that is federated you're your domain. If that is not the case there are a few links below to help you get started.

[BIG-IP Access Policy Manager](#) (APM) lets you to provide secure, federated identity management from your existing Active Directory to Office 365, without the complexity of additional layers of Active Directory Federation Services (ADFS) servers and proxy servers. You can use many of the enhanced APM security features, such as geographical restrictions and multi-factor authentication, to further protect access to Office 365.

[↳ Securing Identity for Office 365](#)

[↳ Convert a Managed Domain in Azure AD to a Federated Domain using ADFS for On-Premises Authentication – Step by Step](#)

[↳ PowerShell commands for federated identity for Office 365 dev/test](#)

[↳ Powershell script for Office365 Federation](#)



BIG-IP iApp

F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center.

Download the ADFS iApp v 1.7 from <https://downloads.f5.com>

- ④ If you don't already have a F5 ID you can register for one here | [Account Registration](#)
- ⑤ Navigate to the following link | [Login](#)
- ⑥ After authentication navigate to the following link | [Downloads](#) | Click [Find a Download](#)

① Select | iApp Template

F5 Product Family	Product Line
BIG-IP	BIG-IP v13.x / Virtual Edition
	BIG-IP v12.x / Virtual Edition
	BIG-IP v11.x / Virtual Edition
	BIG-IP v10.x / Virtual Edition
	BIG-IP v9.x
	APM Clients
	BIG-IP
	F5 Application Connector
	iApp Templates
	iAppLX Templates

② Choose | iApp Templates

Name	Version	Type
iApp-Templates	iApps	Patches

- ③ Review the end user software license [Click](#) | [I Accept](#)

Software Terms and Conditions

Please read the following agreement and select [I Accept](#) at the bottom before downloading your software.

END USER SOFTWARE LICENSE

END USER SOFTWARE LICENSE
2017-12-20
DOC-0395-01
IMPORTANT - READ BEFORE INSTALLING OR OPERATING THIS PRODUCT

LICENSEE AGREES TO BE BOUND BY THE TERMS OF THIS AGREEMENT BY
INSTALLING, HAVING INSTALLED, COPYING, OR OTHERWISE USING THE PRODUCT.
IF LICENSEE DOES NOT AGREE, DO NOT INSTALL OR USE THE PRODUCT.

1. Scope. This License applies to the software product ("Software")
you have licensed from F5 Networks, Inc. ("F5"). This License is a
legal agreement between F5 and the single entity ("Licensee") that has
acquired the Software from F5 under these terms and conditions. The
Software incorporates certain third party software programs subject to
the terms and restrictions of the applicable licenses identified herein.

2. License Grant. Subject to the terms of this License, F5 grants to
Licensee a perpetual, non-exclusive, non-transferable license to use

[I Accept](#) [Cancel](#)



4 | Select | iApps zip file

Select a Download

Product: iApp Templates
Version: iApps
Container: iApp-Templates

Please select the file you wish to download; make sure you have read the appropriate Release Notes before attempting to use the file.

Filename	Description	Size
README.txt	Readme.txt	1 KB
iapps-1.0.0.498.0.zip	iapps-1.0.0.498.0	3 MB
iapps-1.0.0.498.0.zip.md5	MD5 file for iapps-1.0.0.498.0	55 Bytes

5 | Select | Nearest location

Download Locations

Now that you have selected the file you wish to download, please select one of the locations or methods below. For the best performance, please select the link from the location nearest you:

Download - iapps-1.0.0.498.0.zip

- AUSTRALIA
- IRELAND
- JAPAN
- SINGAPORE
- USA - WEST COAST
- BRAZIL
- USA - EAST COAST

6 | Note | The location of the saved zip file

File name: iapps-1.0.0.498.0.zip
Save as type: Compressed (zipped) Folder (*.zip)

Save Cancel

Do you want to open or save iapps-1.0.0.498.0.zip (3.10 MB) from downloads-usw-f5s3.amazonaws.com?

Open Save Cancel

7 | Right Click the .zip | Choose Extract All from the dropdown

iapps-1.0.0.498.0

- Open
- Open in new window
- Extract All...**
- Pin to Start
- Open with...

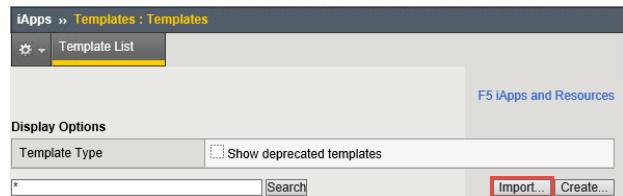


Import the iApp to the BIG-IP

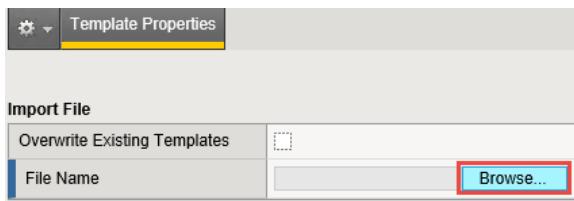
① On the Big-IP Main Menu | Select iApps | Templates | Templates



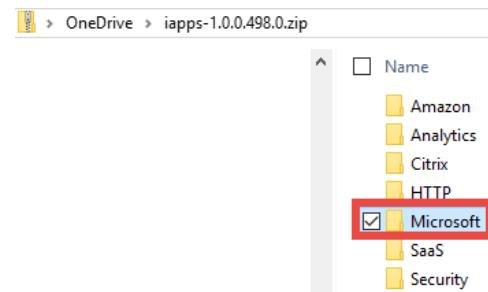
② Click | Import



③ Click | Browse



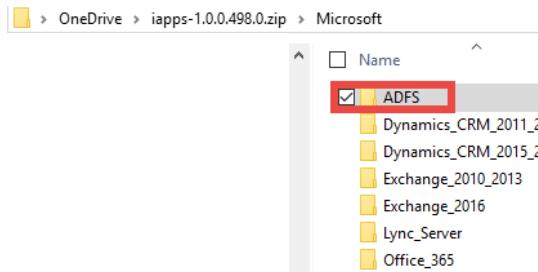
④ Navigate to the extracted iApp File | Select | Microsoft



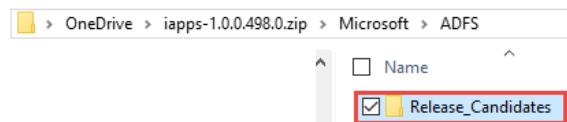


Note: At the time this article was written v1.2 of the iApp was a release candidate

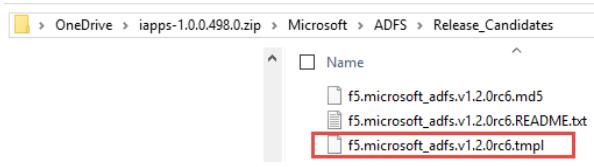
5 | Select | ADFS



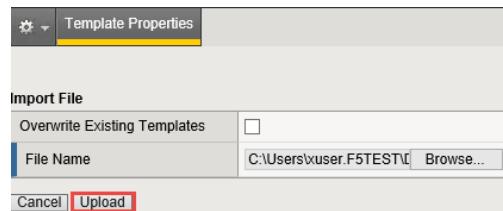
6 | Select | Release Candidate



7 | Note: | The location of the .tmpl file to import into your BIG-IP

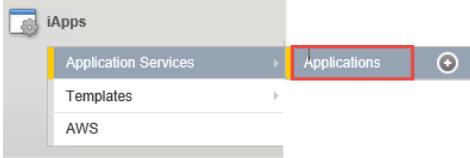
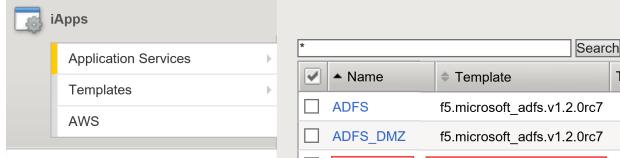
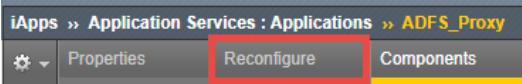
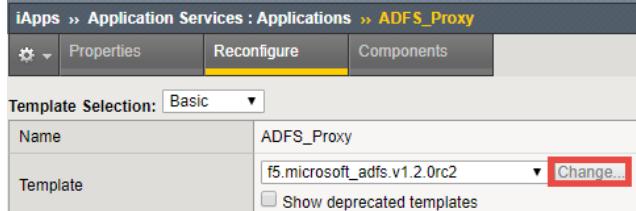
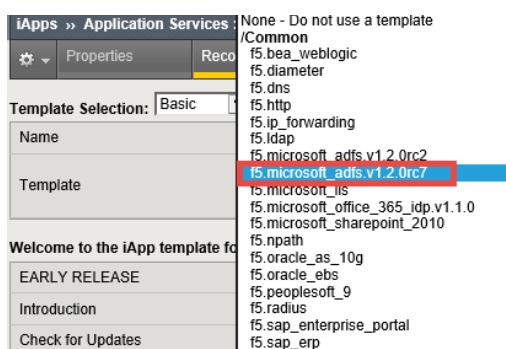


8 | Click | Upload





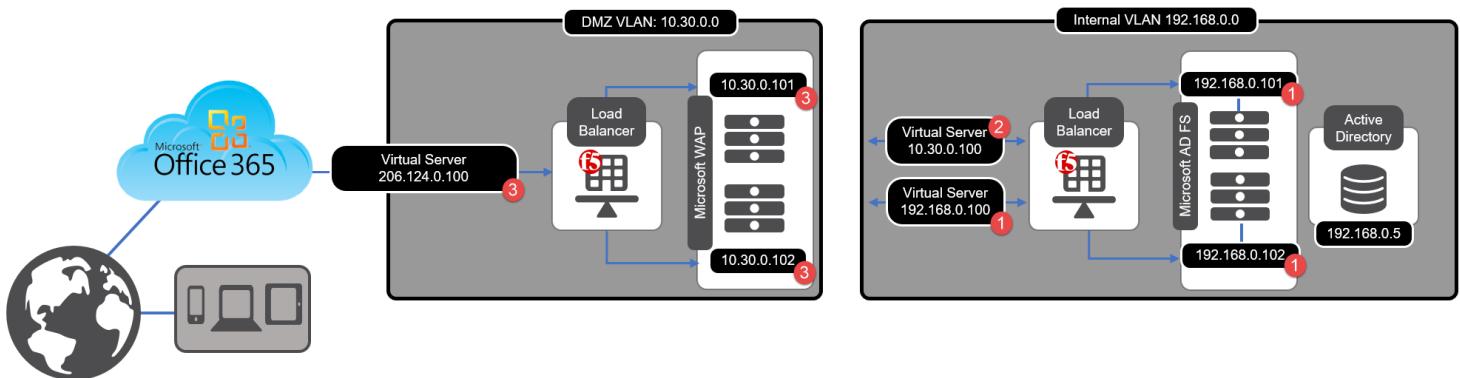
Upgrading an Application Service from previous version of the iApp template

- 1 On the BIG-IP | Select iApps | Application Services | Applications
- 2 Click | The name of your existing f5.microsoft_adfs application service from the list
- 3 Click | Reconfigure.
- 4 Click | the Change button to the right of the list.
- 5 Select | f5.microsoft_adfs.<latest version> from the Dropdown list
- 6 Click | Finished at the bottom of the template



Use Case One | Configuring Local Traffic Management (LTM) for WAP and ADFS farms

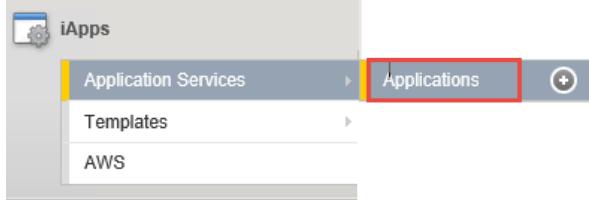
Phase One | Advanced Traffic Management for WAP and ADFS farms



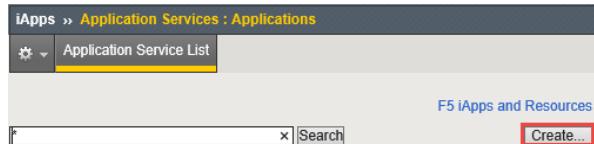
iApp Configuration

Configure LTM to Load Balance Active Directory Federation Services (ADFS)

- ① On the BIG-IP | Select iApps |
Application Services | Applications



- ② Click | Create





- ③ Provide a name | Select the iApp you uploaded previously | Click Finished

iApps » Application Services : Applications » New Application Service..

Template Selection

Name	ADFS
Template	None - Do not use a template /Common f5.bea_weblogic f5.diameter f5.dns f5.http f5.ip_forwarding f5.ldap f5.microsoft_adfs.v1.2.0rc2 f5.microsoft_iis f5.microsoft_office_365_idp.v1.1.0

Cancel Repeat **Finished**

- ④ Template Options | Use the dropdown chevron to choose your version of ADFS | Select the ADFS Server Role.

Template Options

Do you want to see inline help?	No, do not show inline help
Which configuration mode do you want to use?	Basic - Use F5's recommended settings
Which version of AD FS are you deploying?	AD FS 4.0
Which AD FS server role are you deploying?	AD FS AD FS Proxy

- ⑤ Network | Use the dropdown chevron to choose

Network

Where will the virtual servers be in relation to the AD FS servers?	BIG-IP virtual server IP and AD FS servers are on different subnets
How have you configured routing on your AD FS servers?	AD FS servers have a route to clients through the BIG-IP



SSL Encryption | Select this method if you want the BIG-IP system to terminate SSL to process it, and then re-encrypt the traffic to the servers

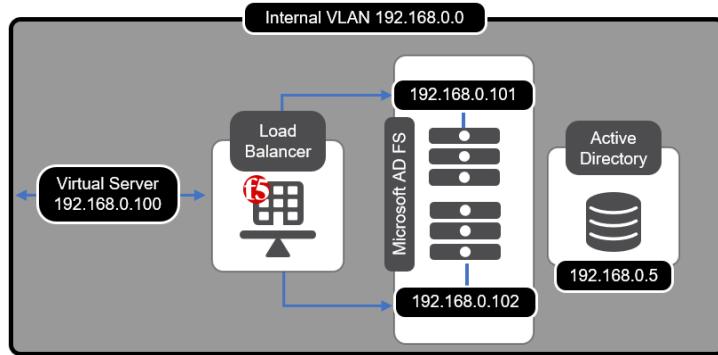
6

A. SSL Profile | This creates a new Client SSL profile.

B. SSL Certificate | Select the SSL certificate you imported for this implementation.

C. SSL Private Key | Select the associated SSL private key.

SSL Encryption	
How should the BIG-IP system handle SSL traffic?	Terminate SSL from clients, re-encrypt to servers (SSL bridging) <input type="button" value="▼"/>
Which Client SSL profile do you want to use?	A Create a new Client SSL profile <input type="button" value="▼"/>
Which SSL certificate do you want to use?	B default.crt <input type="button" value="▼"/>
Which SSL private key do you want to use?	C default.key <input type="button" value="▼"/>
WARNING:	The BIG-IP system's default certificate and key are not secure. For proper security, consider using a self-signed certificate or a certificate issued by a trusted authority.
Which Server SSL profile do you want to use?	Create a new Server SSL profile based on serverssl (recommended) <input type="button" value="▼"/>



High Availability | Create a virtual server to load balance the ADFS servers

7

- A. **Virtual Server** | This is the address clients use (or a DNS entry resolves to this address) to access the ADFS deployment via the BIG-IP system
- B. **FQDN** | Type the fully qualified domain name clients will use to access the AD FS deployment.
- C. **Pool** | Enter the IP address of your ADFS servers

High Availability

What IP address do you want to use for the virtual server?	A 192.168.0.100
What service port do you want to use for the virtual server?	443
Which FQDN will clients use to access AD FS?	B adfs.yourdomain.net
Do you want to create a new pool or use an existing one?	Create a new pool
Which servers should be included in this pool?	C IP Address 192.168.0.101 Port 443 Connection limit 0 IP Address 192.168.0.102 Port 443 Connection limit 0 Add



8 Application Health | the iApp can create a new monitor or use an existing Monitor | Click Finished

Application Health

Create a new health monitor or use an existing one?	<input type="checkbox"/> Create a new monitor
How many seconds between each health check?	<input type="text" value="30"/>
What HTTP URI should be sent to the server(s)?	<input type="text" value="/adfs/fs/federationserver/service.asmx"/>
What is the expected response to the HTTP request?	<input type="text" value="200 OK"/>

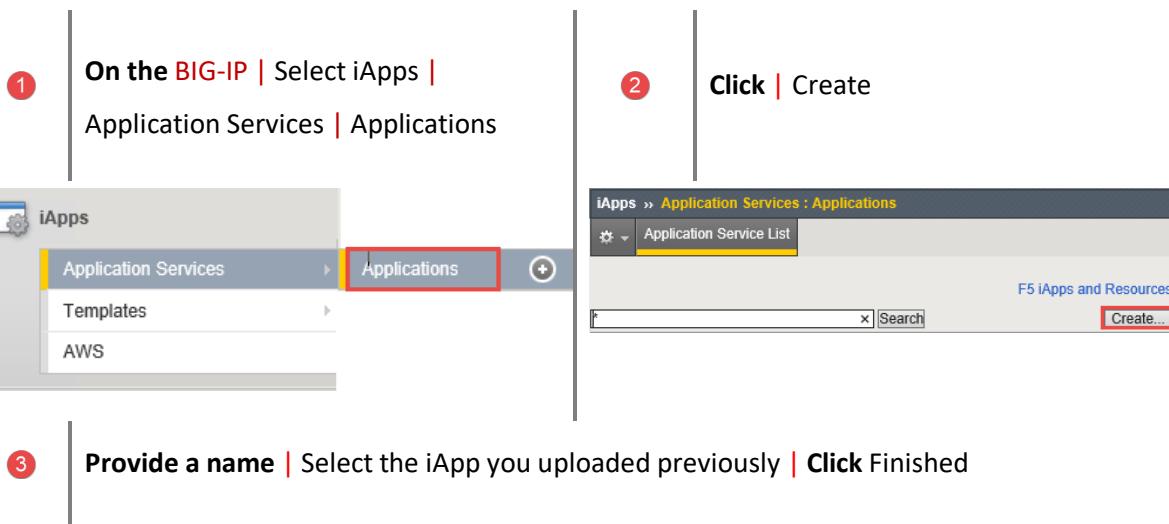
9 Behold! | The iApp has completed! | Note: the green health monitors reporting the health of the service.

iApps >> Application Services : Applications >> ADFS

Name	Availability	Type
BIG-IP	Available	Application Service
ADFS	Available	Virtual Server
ADFS_adfs_vg_443	Available	Pool
ADFS_adfs_pool_443	Available	Monitor
ADFS_adfs_eav	Available	external_monitor_param
instance_of_external_monitor_param	Available	external_monitor_be_object
adfs_eav	Available	Pool Member
192.168	Unknown	Node
192.168.	Available	Pool Member
192.168.	Unknown	Node
192.168.1.6	Available	Virtual Address
ADFS_source_addr	Available	Virtual Server Persistence Profile
test1.4	Available	Profile
ADFS_adfs_vg_49443	Available	Virtual Server
ADFS_adfs_pool_49443	Available	Pool
ADFS_adfs_tcp	Available	Monitor
192.168	Available	Pool Member
192.168.	Unknown	Node
192.168.	Available	Pool Member
192.168	Unknown	Node
192.168	Available	Virtual Address
ADFS_source_addr	Available	Virtual Server Persistence Profile
test1.4	Available	Profile



Create a Route to the DMZ



④ Template Options | Use the dropdown chevron to choose your version of ADFS | Select the ADFS Proxy Server Role.

Name: ADFS_DMZ

Template:

- None - Do not use a template
- /Common
- f5.bea_weblogic
- f5.diameter
- f5.dns
- f5.http
- f5.ip_forwarding
- f5.ldap
- f5.microsoft_adfs.v1.2.0rc2**
- f5.microsoft_iis
- f5.microsoft_office_365_idp.v1.1.0

Cancel Repeat **Finished**



Template Options

Do you want to see inline help?	No, do not show inline help
Which configuration mode do you want to use?	Basic - Use F5's recommended settings
Which version of AD FS are you deploying?	AD FS 4.0
Which AD FS server role are you deploying?	AD FS

- ⑤ **Network** | Use the dropdown chevron to choose

Network

Where will the virtual servers be in relation to the AD FS servers?	BIG-IP virtual server IP and AD FS servers are on different subnets
How have you configured routing on your AD FS servers?	AD FS servers have a route to clients through the BIG-IP

SSL Encryption | Select this method if you want the BIG-IP system to terminate SSL to process it, and then re-encrypt the traffic to the servers

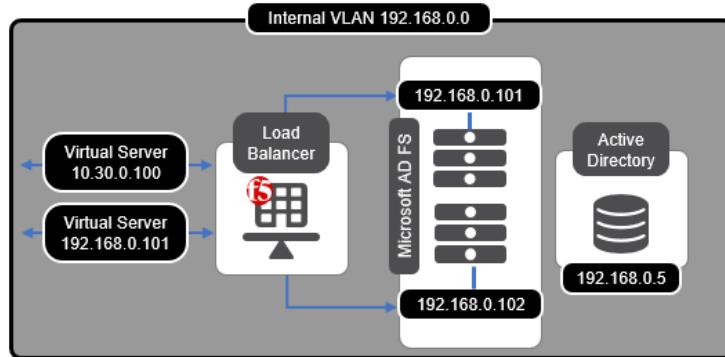
- ⑥ **A. SSL Profile** | This creates a new Client SSL profile.

B. SSL Certificate | Select the SSL certificate you imported for this implementation.

C. SSL Private Key | Select the associated SSL private key.

SSL Encryption

How should the BIG-IP system handle SSL traffic?	Terminate SSL from clients, re-encrypt to servers (SSL bridging)
Which Client SSL profile do you want to use?	A Create a new Client SSL profile
Which SSL certificate do you want to use?	B default.crt
Which SSL private key do you want to use?	C default.key
WARNING:	The BIG-IP system's default certificate and key are not secure. For proper security, generate a new certificate and key.
Which Server SSL profile do you want to use?	Create a new Server SSL profile based on serverssl (recommended)



High Availability | Create a virtual server to load balance the ADFS servers

7

- A. Virtual Server |** This is the address clients use (or a DNS entry resolves to this address) to access the ADFS deployment via the BIG-IP system
- B. FQDN |** Type the fully qualified domain name clients will use to access the AD FS deployment.
i.e. adfs.mydomain.com
- C. Pool |** Enter the IP address of your ADFS servers

High Availability										
What IP address do you want to use for the virtual server?	A <input type="text" value="10.30.0.100"/>									
What service port do you want to use for the virtual server?	<input type="text" value="443"/>									
Which FQDN will clients use to access AD FS?	B <input type="text" value="adfs.yourdomain.net"/>									
Do you want to create a new pool or use an existing one?	<input type="checkbox"/> Create a new pool <input checked="" type="checkbox"/>									
Which servers should be included in this pool?	C <table><tr><td>IP Address <input type="text" value="192.168.0.101"/></td><td>Port <input type="text" value="443"/></td><td>Connection limit <input type="text" value="0"/></td></tr><tr><td>IP Address <input type="text" value="192.168.0.102"/></td><td>Port <input type="text" value="443"/></td><td>Connection limit <input type="text" value="0"/></td></tr><tr><td colspan="3"><input type="button" value="Add"/></td></tr></table>	IP Address <input type="text" value="192.168.0.101"/>	Port <input type="text" value="443"/>	Connection limit <input type="text" value="0"/>	IP Address <input type="text" value="192.168.0.102"/>	Port <input type="text" value="443"/>	Connection limit <input type="text" value="0"/>	<input type="button" value="Add"/>		
IP Address <input type="text" value="192.168.0.101"/>	Port <input type="text" value="443"/>	Connection limit <input type="text" value="0"/>								
IP Address <input type="text" value="192.168.0.102"/>	Port <input type="text" value="443"/>	Connection limit <input type="text" value="0"/>								
<input type="button" value="Add"/>										
Do you want the iApp to configure support for certificate authentication and Device Registration?	<input type="checkbox"/> No, do not create the configuration									



8 Application Health | the iApp can create a new monitor or use an existing Monitor | Click Finished

Application Health

Create a new health monitor or use an existing one?	<input type="text" value="Create a new monitor"/>
How many seconds between each health check?	<input type="text" value="30"/>
What HTTP URI should be sent to the server(s)	<input type="text" value="/adfs/fs/federationserverservice.asmx"/>
What is the expected response to the HTTP request?	<input type="text" value="200 OK"/>

Buttons: Cancel | Repeat | **Finished**

9 Behold! | The iApp has completed! | Note: the green health monitors reporting the health of the service.

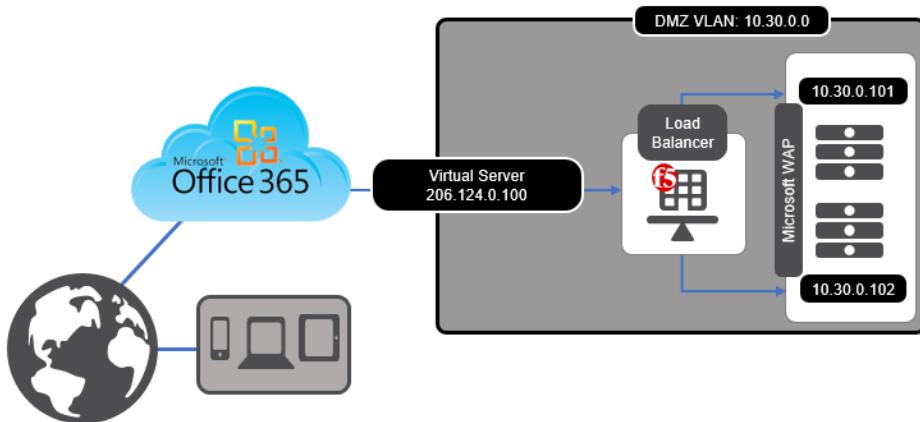
iApps > Application Services : Applications > ADFS_DMZ

Name	Availability	Type
ADFS_DMZ	Available	Application Service
ADFS_DMZ_adfs_vs_443	Available	Virtual Server
ADFS_DMZ_adfs_pool_443	Available	Pool
ADFS_DMZ_adfs_eav	Available	Monitor
Instance of external_monitor_param	Available	external_monitor_param
adfs_key	Available	external_monitor_ifc_object
192.168	Available	Pool Member
192.168	Unknown	Node
192.168	Available	Pool Member
192.168	Unknown	Node
10.90.7.1	Available	Virtual Address
ADFS_DMZ_source_addr	Available	Virtual Server Persistence Profile
ADFS_DMZ_hm	Available	Profile
ADFS_DMZ_server-ssl	Available	Profile
ADFS_DMZ_client-ssl	Available	Certificate Key File
_WILDCARD.key	Available	Certificate File
_WILDCARD.crt	Available	clientcert_keystorechain
_WILDCARD	Available	Certificate File
_WILDCARD.crt	Available	Certificate Key File
_WILDCARD.key	Available	Profile
ADFS_DMZ_lan-optimized-tcp	Available	Profile
ADFS_DMZ_wan-optimized-tcp	Available	Profile

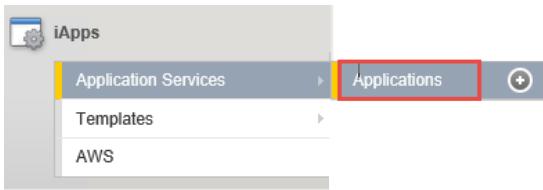
Buttons: Enable | Disable | Force Offline | Refresh



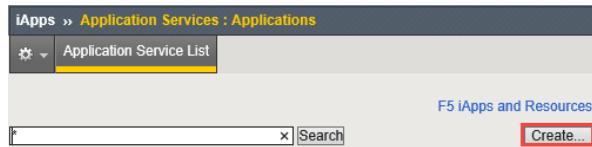
Configure LTM to Load Balance Web Application Proxy (WAP) servers.



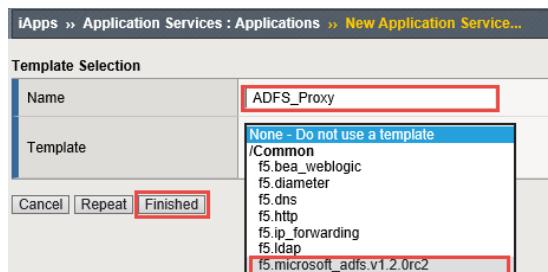
- ① On the BIG-IP | Select iApps | Application Services | Applications



- ② Click | Create



- ③ Provide a name | Select the iApp you uploaded previously | Click Finished





4

Template Options | Use the dropdown chevron to choose your version of ADFS | Select the ADFS Proxy Server Role.

Template Options	
Do you want to see inline help?	No, do not show inline help
Which configuration mode do you want to use?	Basic - Use F5's recommended settings
Which version of AD FS are you deploying?	AD FS 4.0
Which AD FS server role are you deploying?	AD FS AD FS Proxy

5

Network | Use the dropdown chevron to choose

Network	
Where will the virtual servers be in relation to the AD FS servers?	BIG-IP virtual server IP and AD FS servers are on different subnets
How have you configured routing on your AD FS servers?	AD FS servers have a route to clients through the BIG-IP

SSL Encryption | **SSL Bridging** is selected to terminate SSL and process it, the **BIG-IP** then re-encrypts and sends the traffic to the servers

6

- A. **SSL Profile** | The selected option creates a new Client SSL profile.
- B. **SSL Certificate** | Select the SSL certificate you imported for this implementation.
- C. **SSL Private Key** | Select the associated SSL private key.

SSL Encryption	
How should the BIG-IP system handle SSL traffic?	Terminate SSL from clients, re-encrypt to servers (SSL bridging)
Which Client SSL profile do you want to use? A	Create a new Client SSL profile
Which SSL certificate do you want to use? B	default.crt
Which SSL private key do you want to use? C	default.key
WARNING:	The BIG-IP system's default certificate and key are not secure. For proper security, generate a new certificate and key.
Which Server SSL profile do you want to use?	Create a new Server SSL profile based on serverssl (recommended)



High Availability | Create a virtual server to load balance the WAP servers

7

- A. **Virtual Server** | This is the address clients use (or a DNS entry resolves to this address) to access the WAP deployment via the BIG-IP system
- B. **FQDN** | Type the fully qualified domain name clients will use to access the AD FS deployment.
i.e. adfs.mydomain.com
- C. **Pool** | Enter the IP address of your WAP servers

High Availability

What IP address do you want to use for the virtual server?	A <input type="text" value="206.124.0.100"/>															
What service port do you want to use for the virtual server?	<input type="text" value="443"/>															
Which FQDN will clients use to access AD FS?	B <input type="text" value="adfs.mydomain.net"/>															
Do you want to create a new pool or use an existing one?	<input type="button" value="Create a new pool"/>															
Which servers should be included in this pool?	<table border="1"><tr><td>C</td><td>IP Address <input type="text" value="10.30.0.101"/></td><td>Port <input type="text" value="443"/></td><td>Connection limit <input type="text" value="0"/></td><td>X</td></tr><tr><td></td><td>IP Address <input type="text" value="10.30.0.102"/></td><td>Port <input type="text" value="443"/></td><td>Connection limit <input type="text" value="0"/></td><td>X</td></tr><tr><td></td><td>Add</td><td></td><td></td><td></td></tr></table>	C	IP Address <input type="text" value="10.30.0.101"/>	Port <input type="text" value="443"/>	Connection limit <input type="text" value="0"/>	X		IP Address <input type="text" value="10.30.0.102"/>	Port <input type="text" value="443"/>	Connection limit <input type="text" value="0"/>	X		Add			
C	IP Address <input type="text" value="10.30.0.101"/>	Port <input type="text" value="443"/>	Connection limit <input type="text" value="0"/>	X												
	IP Address <input type="text" value="10.30.0.102"/>	Port <input type="text" value="443"/>	Connection limit <input type="text" value="0"/>	X												
	Add															
Do you want the iApp to configure support for certificate authentication and Device Registration?	<input type="button" value="No, do not create the configuration"/>															

8

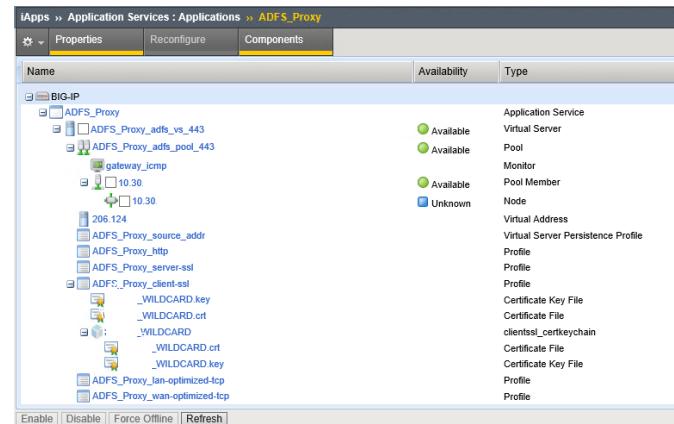
Application Health | the iApp can create a new monitor or use an existing Monitor | Click Finished

Application Health

Create a new health monitor or use an existing one?	<input type="button" value="Create a new monitor"/>	
How many seconds between each health check?	<input type="text" value="30"/>	
What HTTP URI should be sent to the server(s)?	<input type="text" value="/adfs/fs/federationserverservice.asmx"/>	
What is the expected response to the HTTP request?	<input type="text" value="200 OK"/>	
<input type="button" value="Cancel"/>	<input type="button" value="Repeat"/>	<input type="button" value="Finished"/>

9

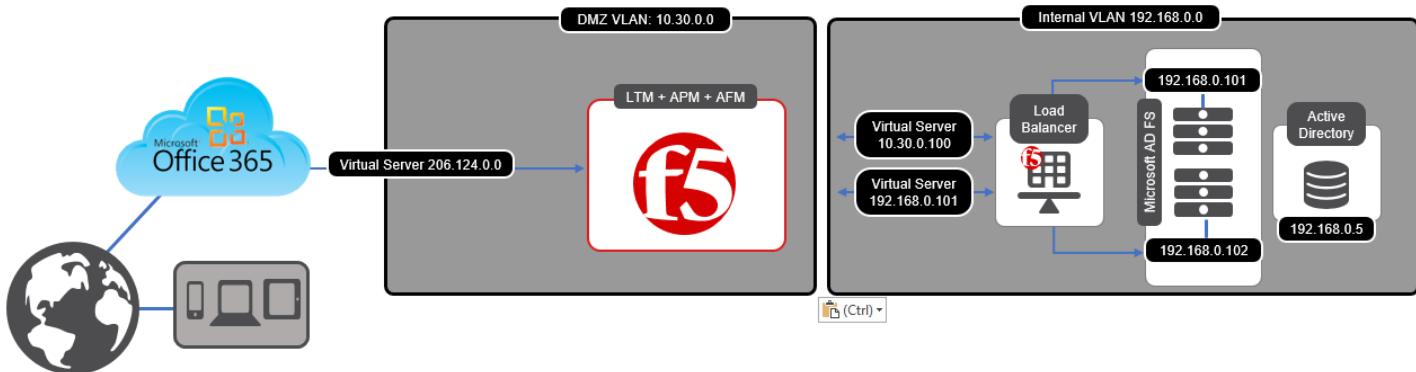
Behold! | The iApp has completed! | Note: the green health monitors reporting the health of the service.





Use Case Two | BIG-IP with ADFS-PIP

Use Case Two | BIG-IP with ADFS-PIP



Reconfigure ADFS iApp to include ADFS Proxy support

Third party proxies can be placed in front of the Web Application Proxy, but any third-party proxy must support the [MS-ADFSPIP protocol](#) to be used in place of the Web Application Proxy.

- ④ AD FS Frequently Asked Questions (FAQ)
- ④ [MS-ADFSPIP]: Active Directory Federation Services and Proxy Integration Protocol
- ④ Identity Federation and SSO for Microsoft and F5 Customers
- ④ F5 BIG-IP Appliance as Full-Fledged AD FS Web Application Proxy

Navigate to application Services **Delete** | The Existing ADFS Proxy Application Service if you have deployed WAP server load balancing previously.

The screenshot shows the iApps interface with the 'Application Services' list. The 'ADFS_Proxy' service is selected and highlighted with a red box. A red circle with the number '1' is on the left side of the interface.



Access Policy Manager (APM) | iApp Template

②

- A. From the dropdown **Select** | Yes, provide secure authentication using APM
- B. From the dropdown **Select** | Yes, Configure BIG-IP as an ADFS Proxy
- C. **Enter** | an account that has Admin rights on the BIG-IP
- D. **Enter** | the accounts password
- E. From the dropdown **Select** | Yes, configure Forms SSO for AD FS
- F. **Enter** | the FQDN for your domain and the IP address of your domain controller
- G. From the dropdown **Select** | Use a simple ICMP monitor for the Active Directory pool
- H. **Enter** | your Active directory domain

Access Policy Manager (BIG-IP APM)	
Do you want to provide secure authentication with BIG-IP APM?	<input type="text" value="Yes, provide secure authentication using APM"/> A
Would you like to configure BIG-IP as an ADFS Proxy?	<input type="text" value="Yes, configure BIG-IP as an ADFS Proxy"/> B
NOTE:	Please be aware that in order to setup BIG-IP as an ADFS Proxy, it requires running a utility on the management plane.
What is the account to be used for establishing proxy trust with ADFS?	<input type="text" value="yourserviceaccount"/> C
What is the password associated with that account?	<input type="password" value="*****"/> D
Which Access Profile do you want to use?	<input type="text" value="Use the iApp to create a new Access Profile"/> E
Do you want the iApp to configure Forms SSO?	<input type="text" value="Yes, configure Forms SSO for AD FS (/adfs/ls endpoint)"/> F
Which AAA Server object do you want to use?	<input type="text" value="Create a new AAA Server"/> G
Which Active Directory server/IP address in your domain can the BIG-IP system contact?	<input type="text" value="FQDN: yourdomain.domain.com IP: 192.168.0.5"/> H <input type="button" value="Add"/>
Does your Active Directory domain allow anonymous binding?	<input type="text" value="Anonymous binding is allowed"/> I
Create a new monitor for the Active Directory servers?	<input type="text" value="Yes, create a simple ICMP monitor"/> J
What is the FQDN of the Active Directory implementation for your AD FS users?	<input type="text" value="domain.com"/> K
Do you want to configure support for Azure MFA (via Azure MFA servers)?	<input type="text" value="No, do not configure support for Azure MFA"/> L
Which log settings would you like to use to log APM events?	<input type="text" value="default-log-setting"/> M



Modify | High Availability

- 3

- A. Virtual Server** | This is the public-address clients will use that resolves to a public DNS entry to access the ADFS deployment via the BIG-IP system
 - B. FQDN** | Type the fully qualified domain name clients will use to access the AD FS deployment.
i.e. adfs.mydomain.com
 - C. From the dropdown Select** | the publicly trusted certificate that you imported previously

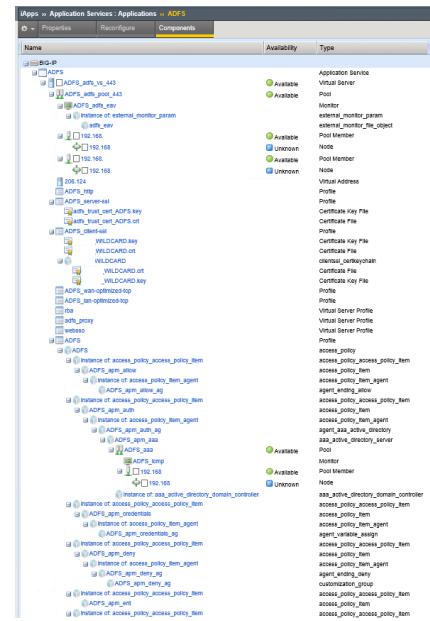
High Availability			
What IP address do you want to use for the virtual server?	<input type="text" value="206.124.0.0"/> A		
What service port do you want to use for the virtual server?	<input type="text" value="443"/>		
Which FQDN will clients use to access AD FS?	<input type="text" value="yourdomain.domain.com"/> B		
Do you want to create a new pool or use an existing one?	<input type="button" value="Create a new pool"/> ▾		
Which servers should be included in this pool?	<input type="text" value="192.168.0.5"/> C <input type="text" value="192.168.0.6"/>	<input type="button" value="Port 443"/> <input type="button" value="Port 443"/>	<input type="text" value="Connection limit 0"/> <input type="text" value="Connection limit 0"/>
Add			
Do you want to configure support for client certificate authentication?	<input checked="" type="checkbox" value="Yes, configure support for certificate authentication"/> ▾		
What Trusted CA would you like to use to validate the client certificate chain presented during certificate authentication?	<input type="text" value="WILDCARD.crt"/> D ▾		

4

Click | Finished

5

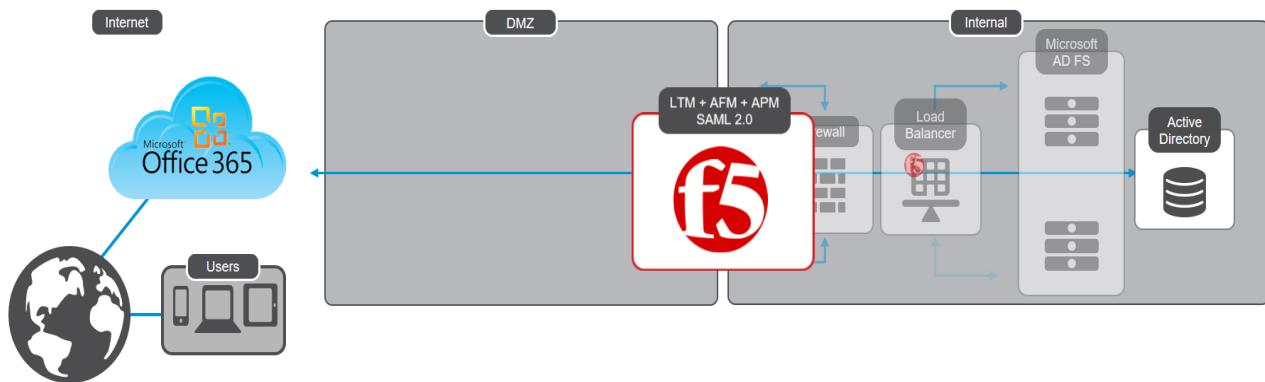
Behold! | The iApp has completed! | **Note:** the green health monitors reporting the health of the service.





Use Case Three | BIG-IP as IdP

Phase Three | BIG-IP as IdP



Delete existing ADFS iApps

1

Navigate to application Services **Delete** | The Existing ADFS Proxy Application Service if you have deployed WAP server load balancing previously.

iApps > Application Services : Applications

Application Service List

iApps

Application Services

Templates

AWS

Name

ADFS

ADFS_DMZ

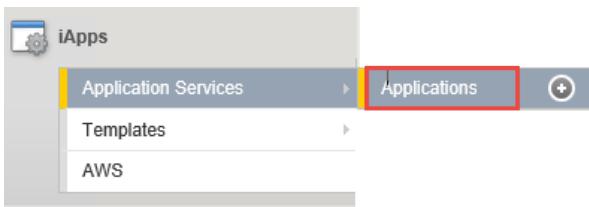
ADFS_Proxy

Delete...

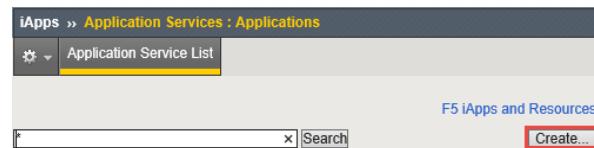


iApp Configuration

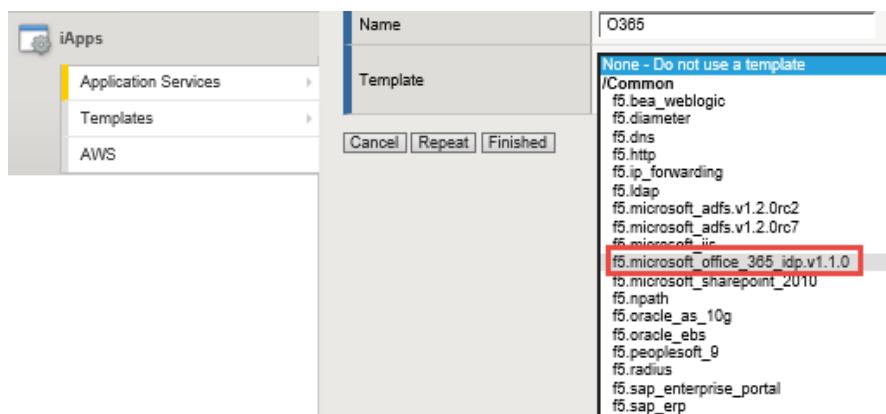
- ① On the BIG-IP | Select iApps | Application Services | Applications



- ② Click | Create



- ③ Select | the O365 iApp from the dropdown





BIG-IP APM Configuration | the O365 iApp from the dropdown

A. Entity ID | Enter an IdP Entity ID

i.e. <https://adfs.yourdomain.com/idp/f5/>

4

B. Active Directory | Enter the FQDN then the IP address of your AD server | Click Add to provide an additional server

C. Active Directory FQDN | Enter your Domian FQDN

i.e. yourdomain.com

BIG-IP APM Configuration

How is your EntityID formatted?	<input type="checkbox"/> My EntityID is a URL
What EntityID do you want to use for your Office 365 IdP? A	<input type="text"/> https://adfs.yourdomain.com/idp/f5/
Should the iApp create a new AAA server or use an existing one?	<input type="checkbox"/> Create a new AAA Server
Which Active Directory server IP address in your domain can this BIG-IP system contact?	<input type="text"/> FQDN dc.yourdomain.com IP 192.168.0.5 <input type="button" value="X"/> <input type="button" value="Add"/>
What is the FQDN of the Active Directory implementation for your Office 365 users? B	<input type="text"/> yourdomain.com
Does your Active Directory domain allow anonymous binding?	<input type="checkbox"/> Anonymous binding is allowed
How do you want to handle health monitoring for this pool?	<input type="checkbox"/> Use a simple ICMP monitor for the Active Directory pool
Which log settings would you like to use to log APM events?	<input type="text"/> default-log-setting
	Select APM logging profile to use for the Access Policy created for this iApp deployment. You must have at least one APM logging profile defined.



BIG-IP IdP Virtual Server

5

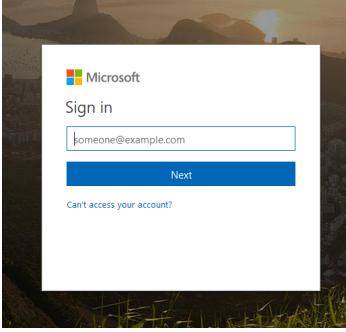
- A. IdP address IP address** | Enter the public address the BIG-IP Virtual Server
- B. Client Authentication Certificate** | Select the SSL certificate you imported for this implementation.
- C. Associated Private Key** | Select the associated SSL private key.

BIG-IP IdP Virtual Server	
What is the IP address clients will use to access the BIG-IP Service?	<input type="text" value="206.124.0.0"/> A
What port do you want to use for the virtual server?	<input type="text" value="443"/> Specify the IP address for the BIG-IP virtual server. Clients will resolve the FQDN.
Which certificate do you want this BIG-IP system to use for client authentication?	<input type="text" value="WILDCARD.crt"/> B Specify the associated service port. The default port is 443.
What is the associated private key?	<input type="text" value="WILDCARD.key"/> C Select the name of the certificate the system uses for client-side SSL processing.
	Select the name of the associated SSL key.



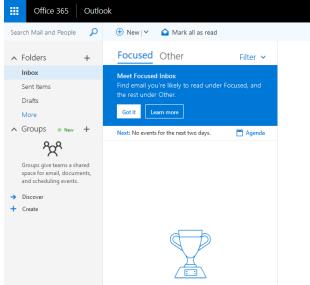
Verify Successful Federation

- 1 Open a Browser | navigate to your O365 Subscription
i.e.outlook.com/yYourDomainName.net
- 2 Enter Credentials | For a Licensed O365 User


- 3 Redirect to the BIG-IP as IdP | Enter the licensed users credentials for SSO


- 4 Select the time zone | If this is the first time the account has accessed O365. They will be prompted to select their time zone


- 5 Behold! | Successful Federation



Note: If you receive an error while verifying federation like “*The requested Federation realm object does not exist*”

You may need to convert your federated domain to standard and then re-federate.