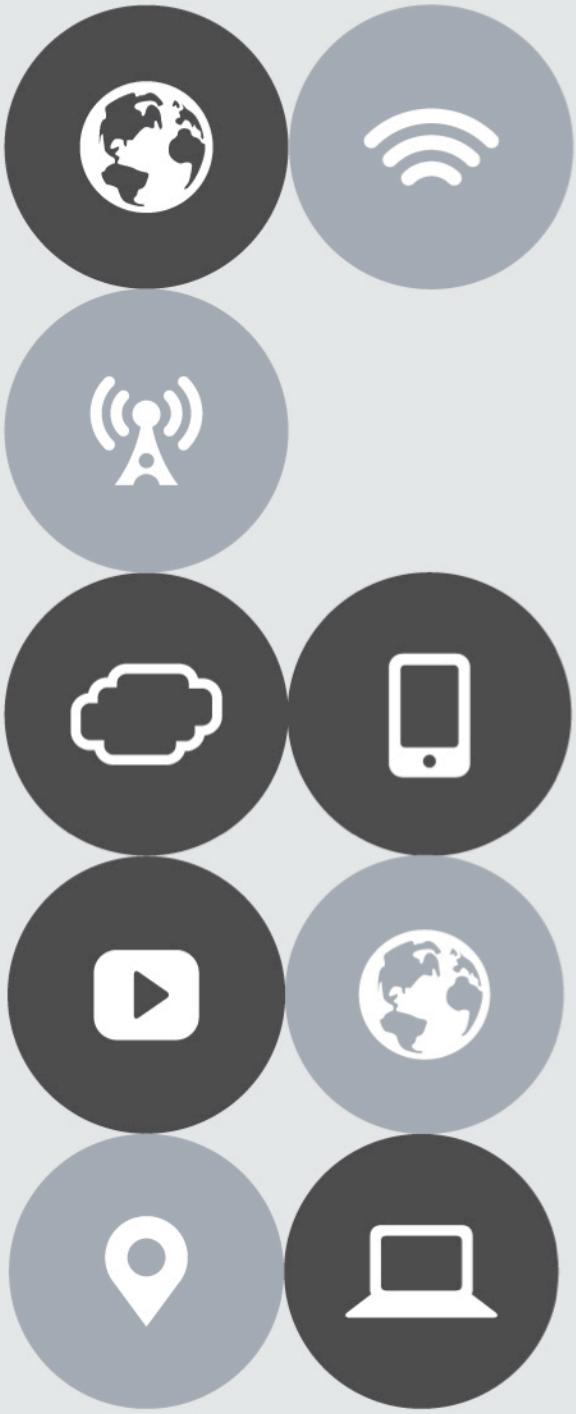


O365 Solutions

Three Phase Approach

msfttechteam@f5.com

Contents

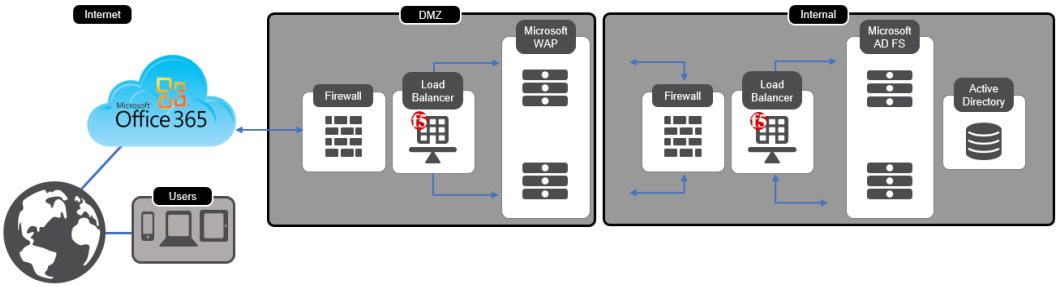
Document Version History

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



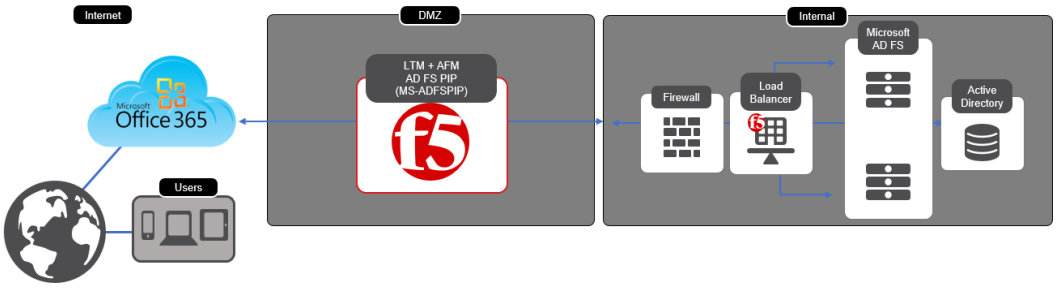
Scenario | Your organizations O365 tenancy requires an advanced Traffic Management engine

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 *and* 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

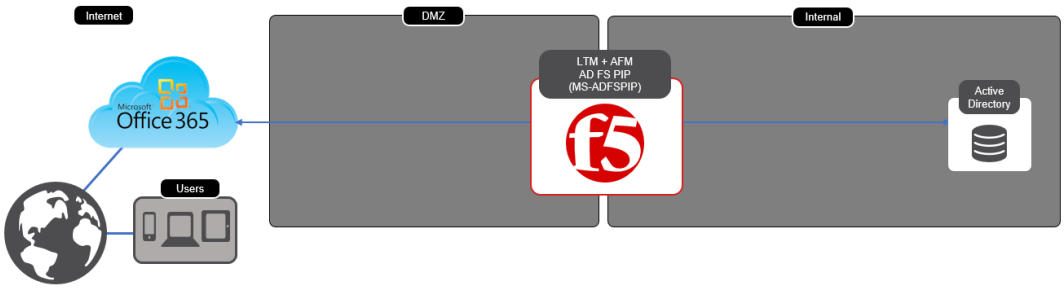
BIG-IP Access Policy Manager can now replace the need for Web Application Proxy servers providing security for your modern AD FS deployment with MS-ADFSPIP support released in BIG-IP v13.1.

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

- 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 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

- System Requirements and Installation Information for Windows Server 2012 R2
- Preparing to deploy a Windows Domain Controller
- Build and Deploy the First Domain Controller
- 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

- 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.

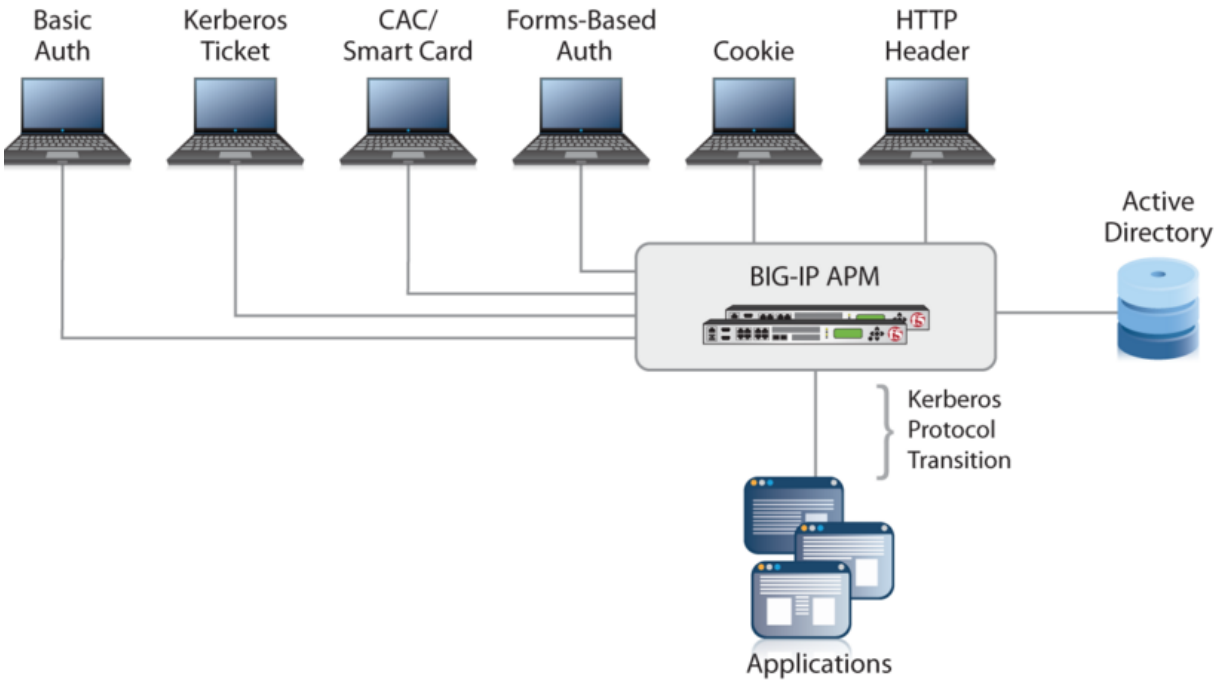
BIG-IP APM supports connections initiated by SAML identity providers (IdPs) and service providers (SPs), extending secure single sign-on (SSO) capabilities to SaaS, cloud-based, web-based, and virtual applications; remote access (VPN) authentication and authorization; and client-based apps and browser-less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

- If you don't already have a F5 ID you can register for one here | Account Registration
- Navigate to the following link | Login
- After authentication navigate to the following link | Downloads | Click **Find a Download**

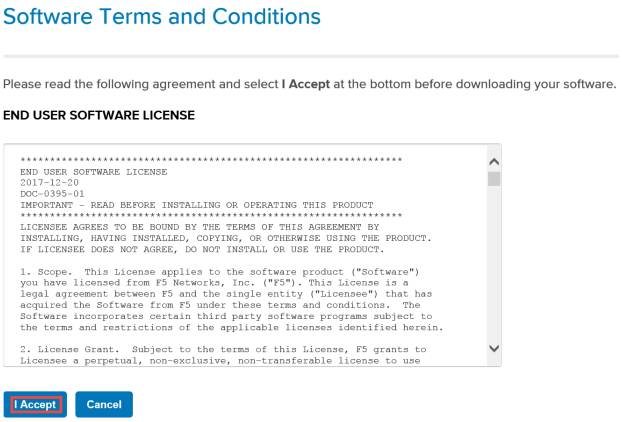
1. **Select** | iApp Template

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**



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

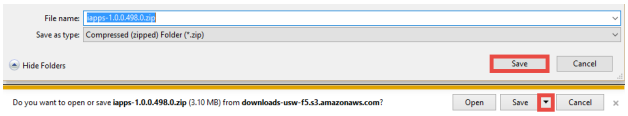
Now that you have selected the file you wish to download, please select one of the locations or methods below.

For the best performance, please select the link from the location nearest you:

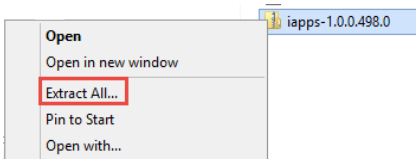
Download - iapps-1.0.0.498.0.zip

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

6 **Note** | The location of the saved zip file



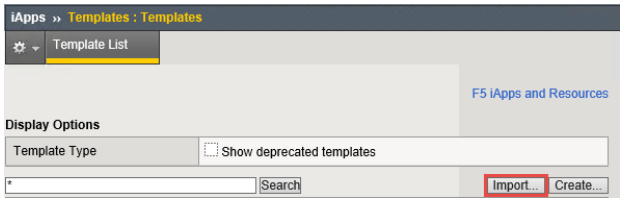
7 **Right Click** the .zip | Choose Extract All from the dropdown



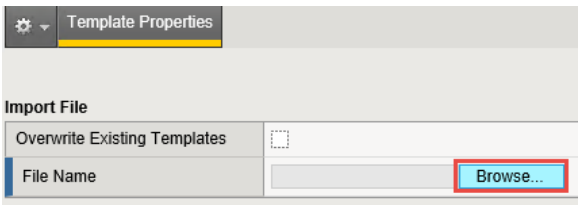
Import the iApp to the BIG-IP

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

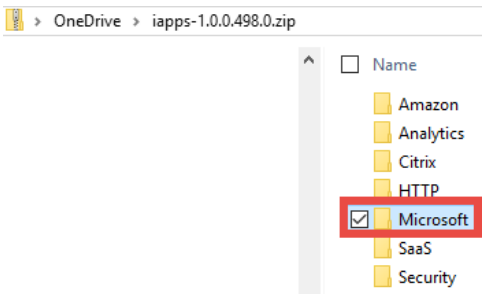
2. **Click** | Import



3. **Click** | Browse

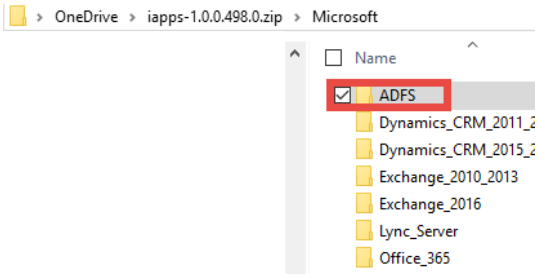


4. **Navigate** to the extracted iApp File | **Select** | Microsoft



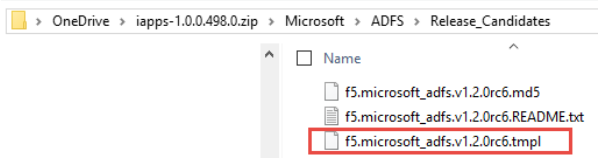
*Note: At the time this article was written **v1.2** of the iApp was a release candidate*

5 **Select** | ADFS

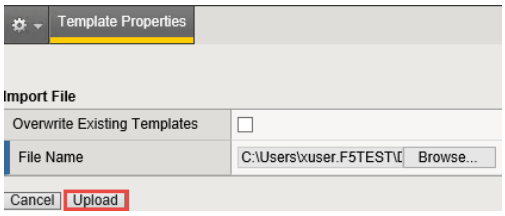


6 **Select** | Release Candidate

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

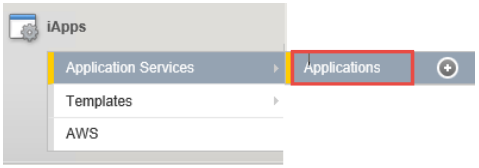


8 **Click** | Upload

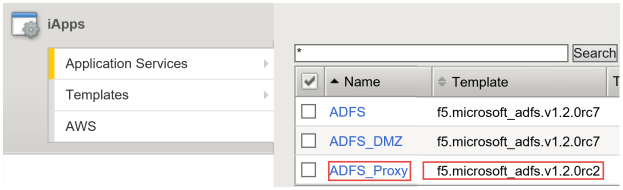


Upgrading an Application Service from previous version of the iApp template

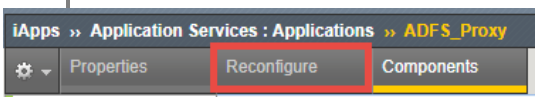
1. **On the** BIG-IP | Select iApps | Application Services | Applications



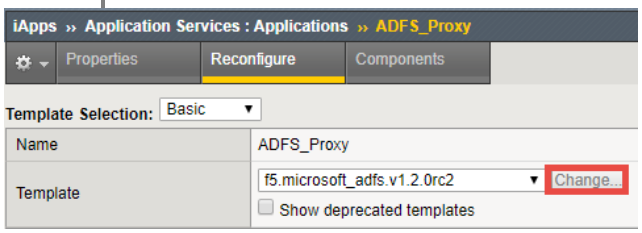
2. **Click** | The name of your existing f5.microsoft_adfs application service from the list



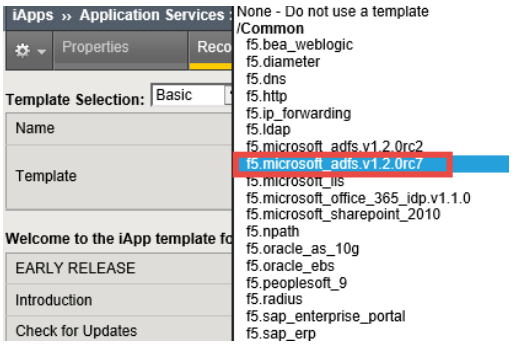
3. **Click** | Reconfigure.



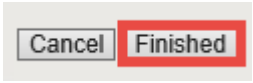
4. **Click** | the Change button to the right of the list.



5. **Select** | f5.microsoft_adfs.<latest version> from the Dropdown list

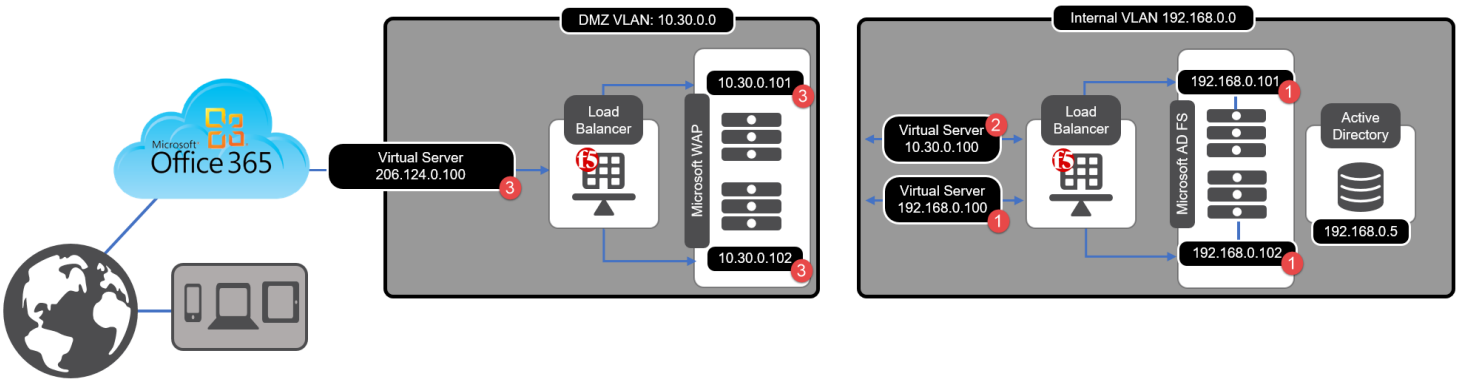


6. **Click** | Finished at the bottom of the template



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

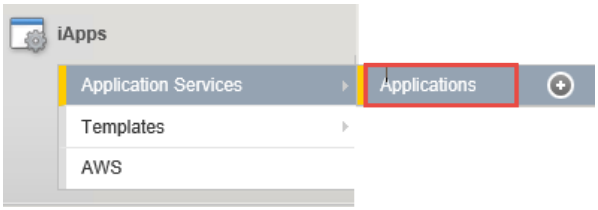
Phase One | Advanced Traffic Management for WAP and ADFS farms



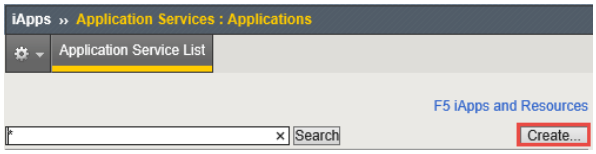
iApp Configuration

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

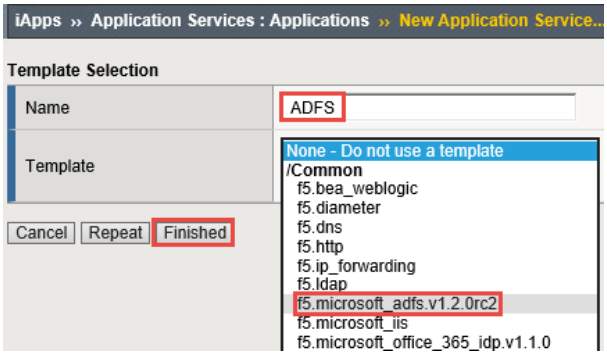
1. **On the** BIG-IP | Select iApps | Application Services | Applications



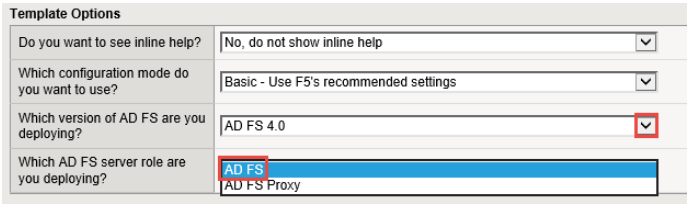
2. **Click** | Create



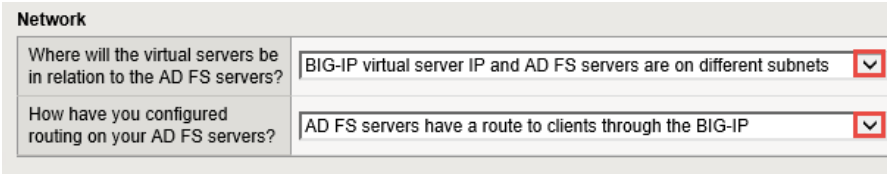
3 **Provide a name** | Select the iApp you uploaded previously | **Click** Finished



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



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



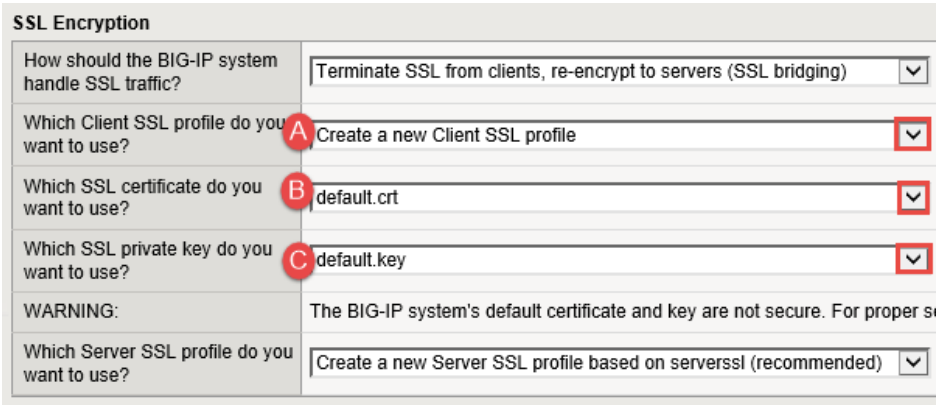
SSL Encryption | Select this method if you want the BIG-IP system to terminate SSL to process it, and then re-encrypt the traffic to the servers

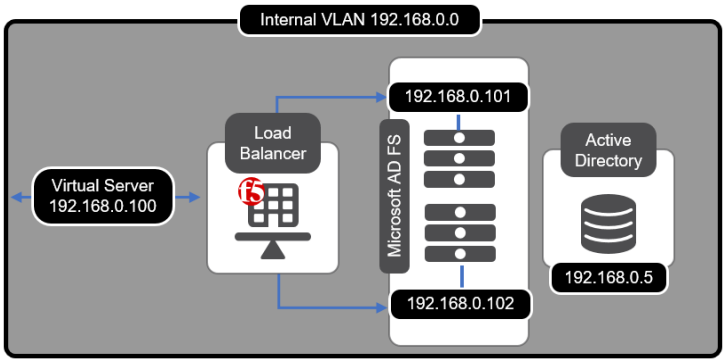
6

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.





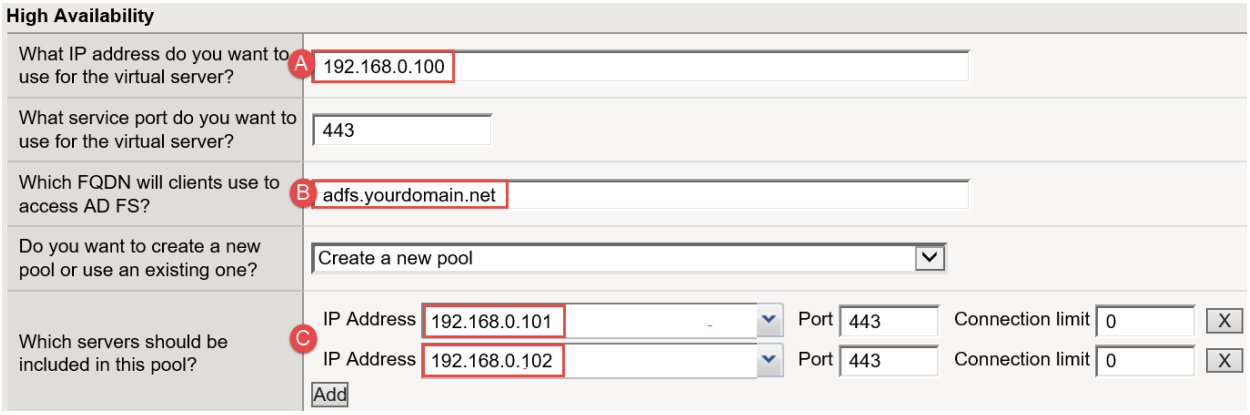
7

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

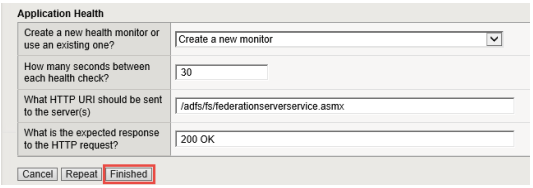
A. Virtual Server | This is the address clients use (or a DNS entry resolves to this address) to access the ADFS deployment via the BIG-IP system

B. FQDN | Type the fully qualified domain name clients will use to access the AD FS deployment.

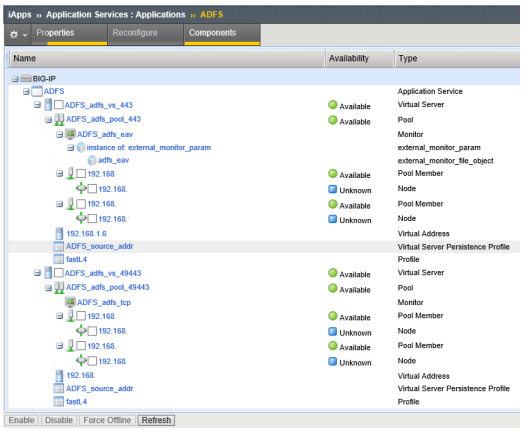
C.Pool | Enter the IP address of your ADFS servers



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

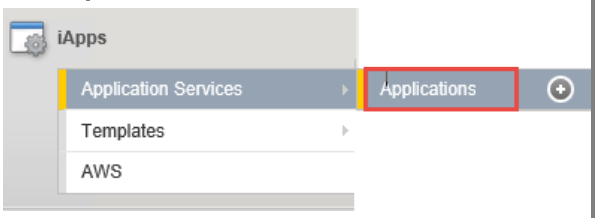


9 **Behold!** | The iApp has completed! | **Note:** the green health monitors reporting the health of the service.

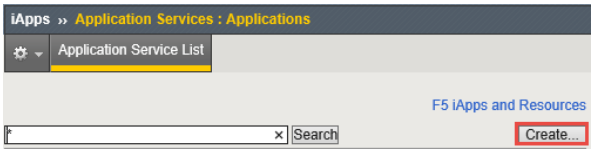


Create a Route to the DMZ

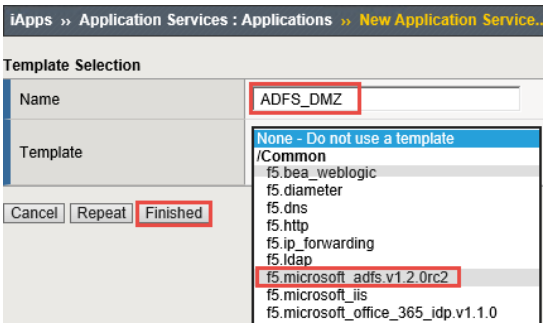
1. **On the** BIG-IP | Select iApps | Application Services | Applications



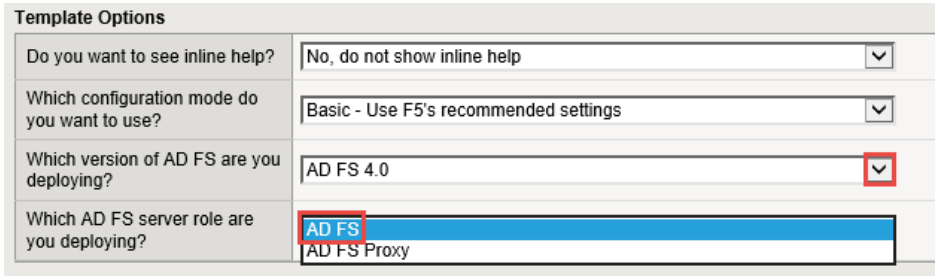
2. **Click** | Create



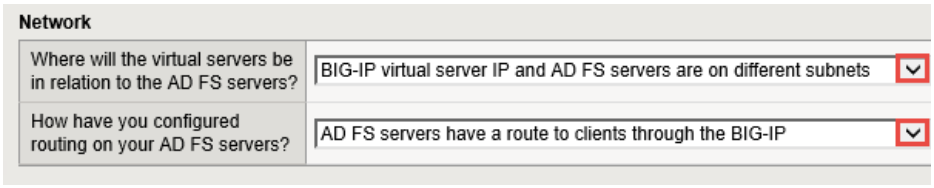
3. **Provide a name** | Select the iApp you uploaded previously | **Click** Finished



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



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

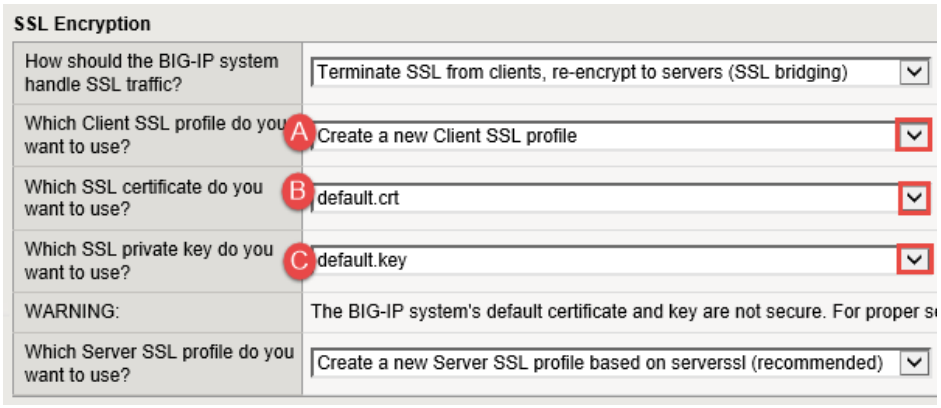


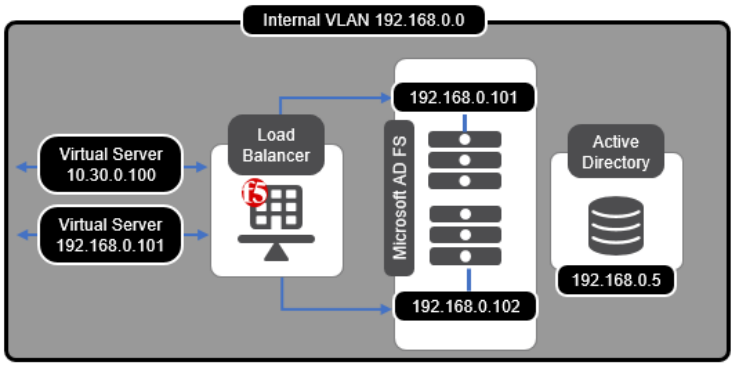
6 **SSL Encryption** | Select this method if you want the BIG-IP system to terminate SSL to process it, and then re-encrypt the traffic to the servers

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.





7

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

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.

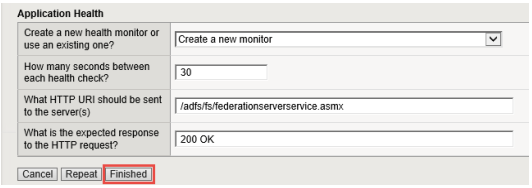
i.e. adfs.mydomain.com

C. Pool | Enter the IP address of your ADFS servers

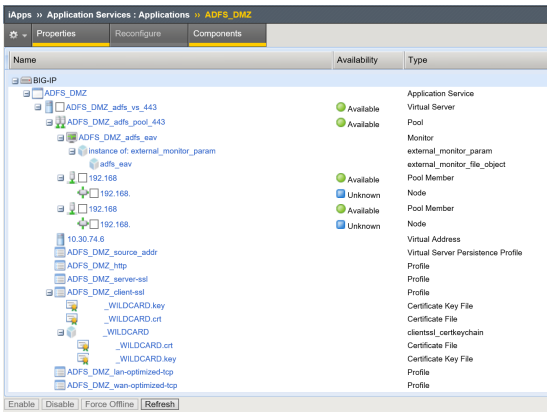
High Availability

What IP address do you want to use for the virtual server?	A 10.30.0.100
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 X IP Address 192.168.0.102 Port 443 Connection limit 0 X Add
Do you want the iApp to configure support for certificate authentication and Device Registration?	No, do not create the configuration

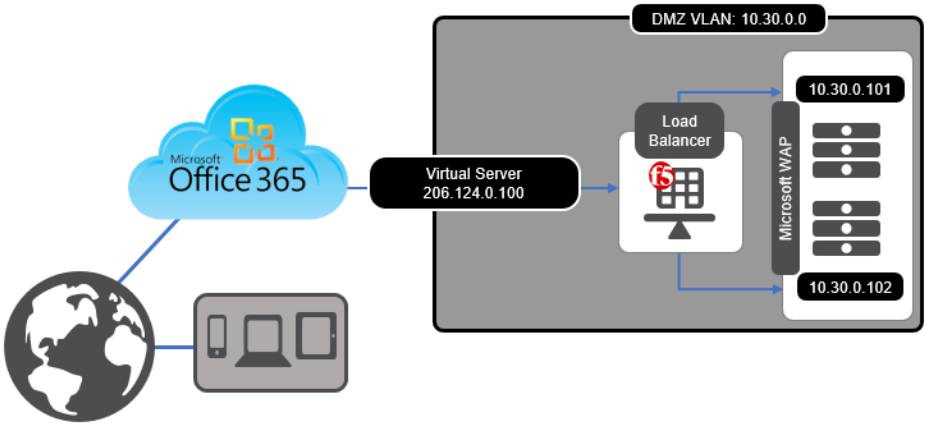
8 **Application Health** | the iApp can create a new monitor or use an existing Monitory | Click Finished



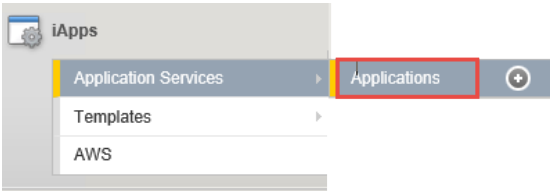
9 **Behold!** | The iApp has completed! | **Note:** the green health monitors reporting the health of the service.



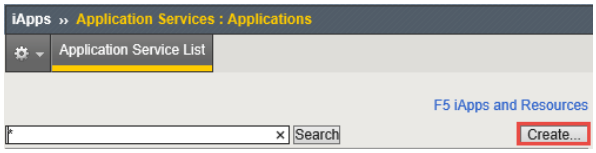
Configure LTM to Load Balance Web Application Proxy (WAP) servers.



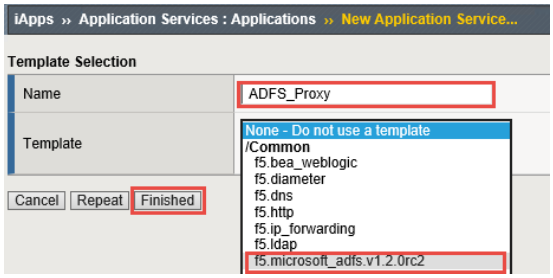
1. **On the BIG-IP** | Select iApps | Application Services | Applications



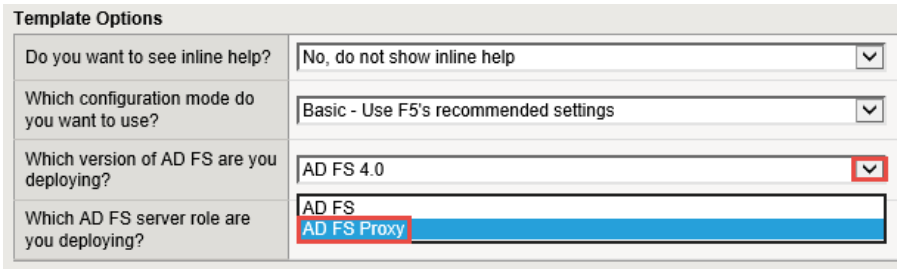
2. **Click** | Create



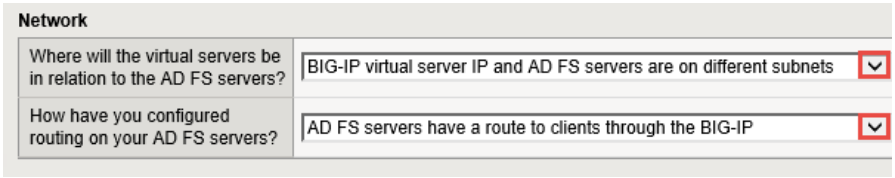
3. **Provide a name** | Select the iApp you uploaded previously | **Click** Finished



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



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

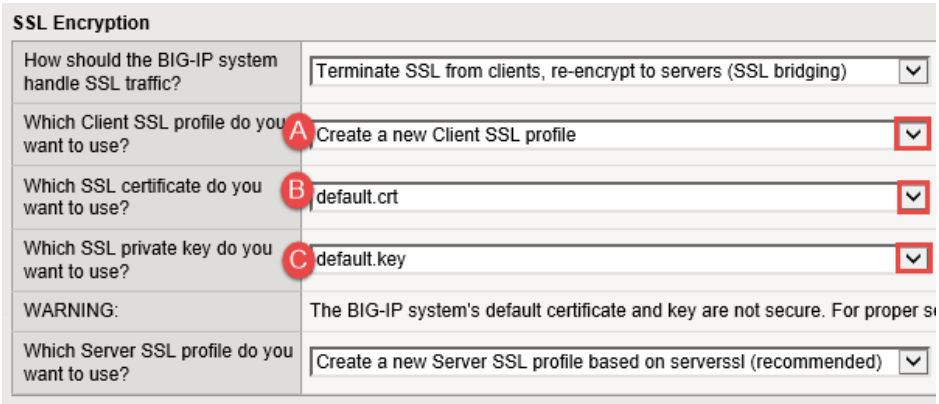


6 **SSL Encryption** | **SSL Bridging** is selected to terminate SSL and process it, the BIG-IP then re-encrypts and sends the traffic to the servers

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.



7

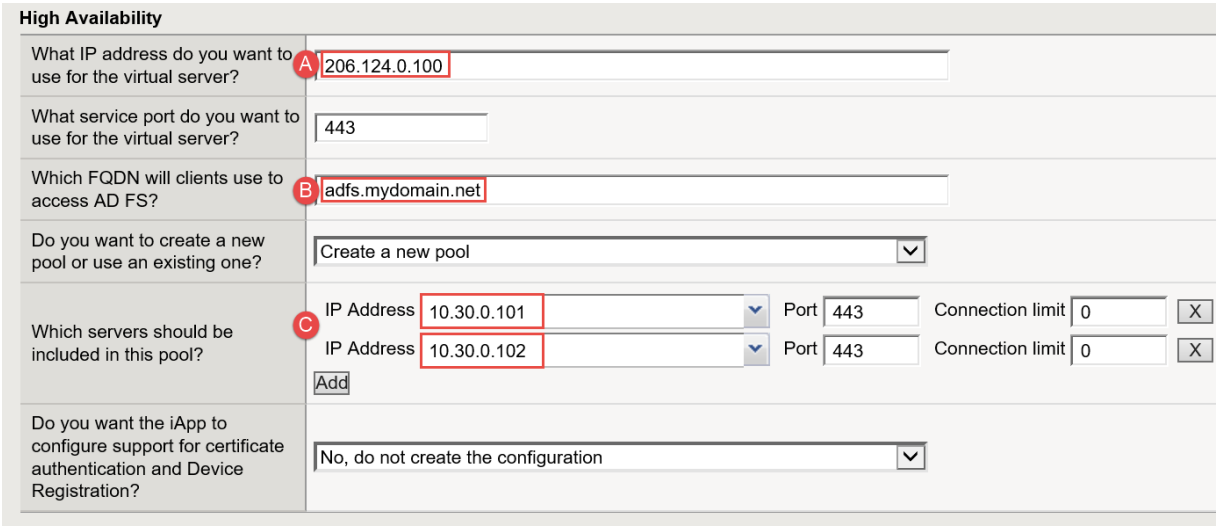
High Availability | Create a virtual server to load balance the WAP servers

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.

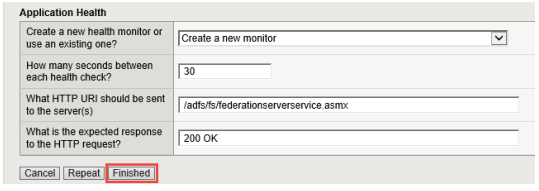
i.e. adfs.mydomain.com

C. Pool | Enter the IP address of you WAP servers



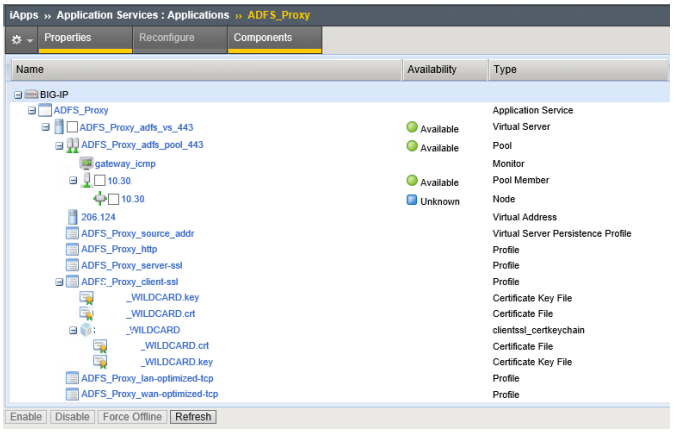
8

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



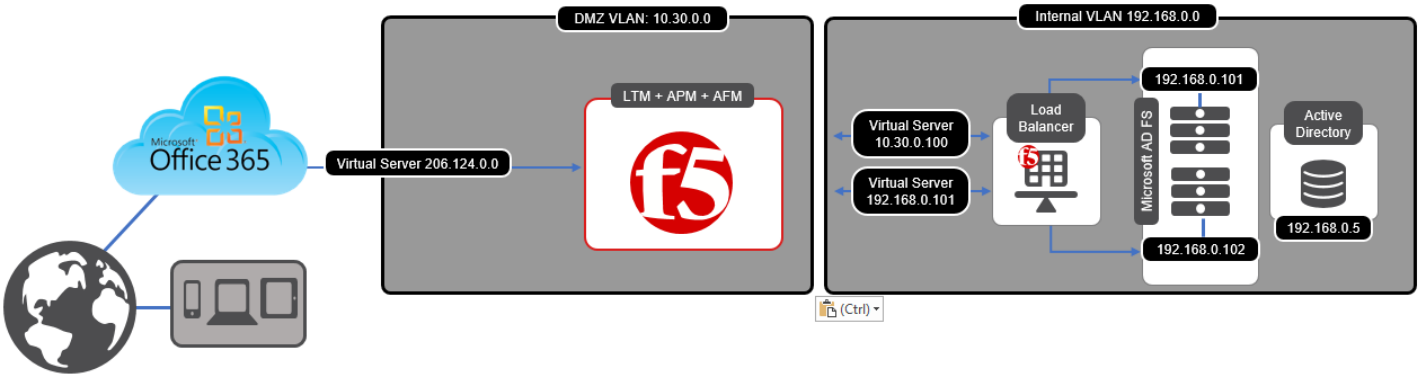
9

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

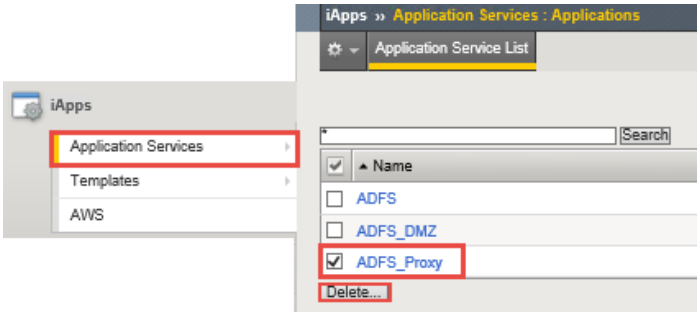


Reconfigure ADFS iApp to include ADFS Proxy support

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.

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

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



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

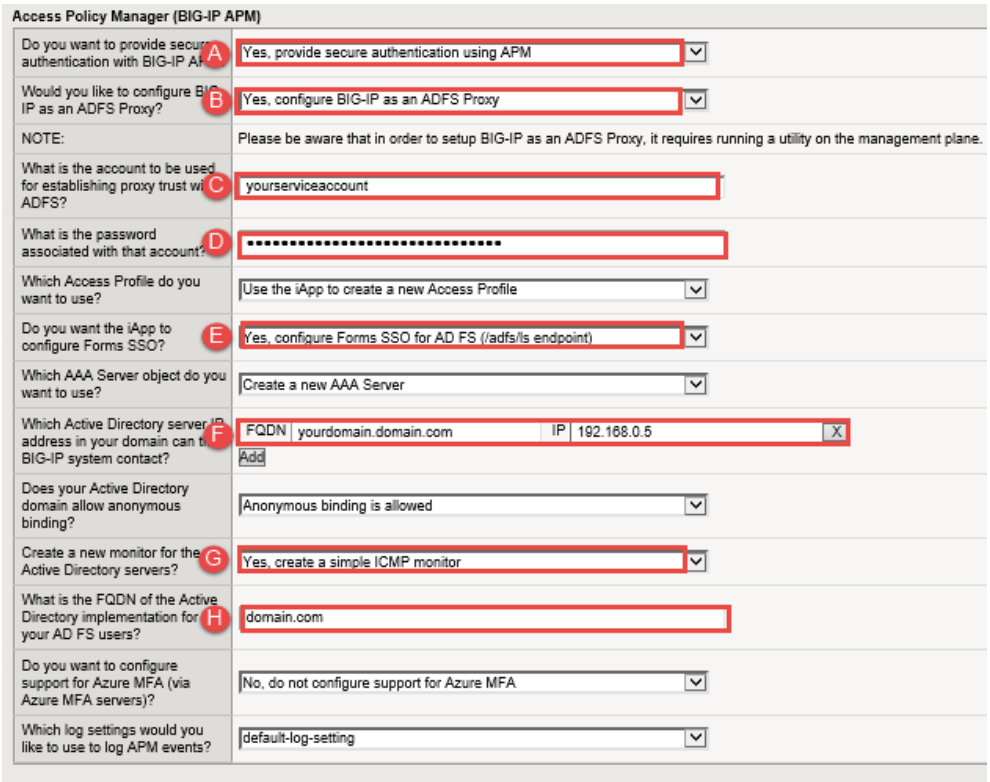
D. Enter | the accounts password

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 contorler

G. From the dropdown **Select** | Use a simple ICMP monitor for the Active Directory pool

H. Enter | your Active directory domain



Modify | High Availability

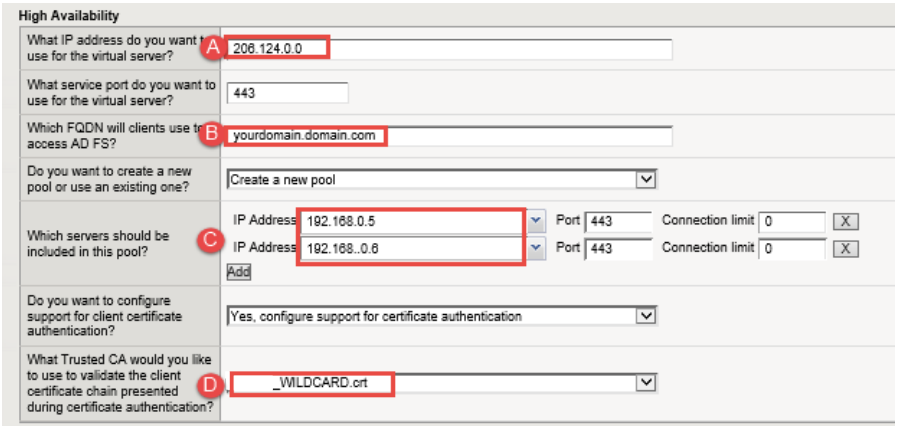
3

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

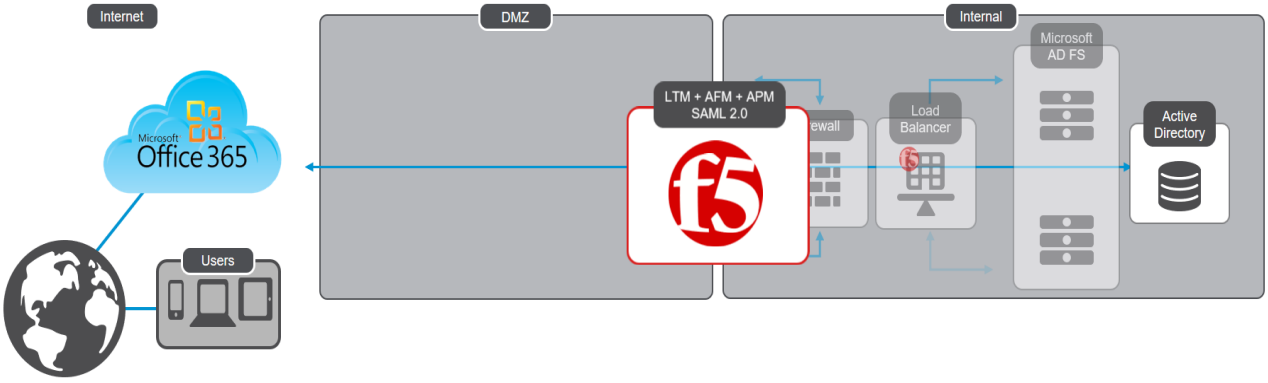


4

Click | Finished

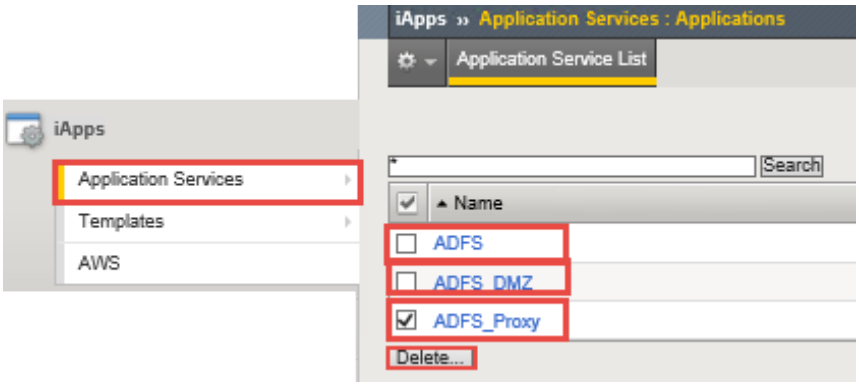
5

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



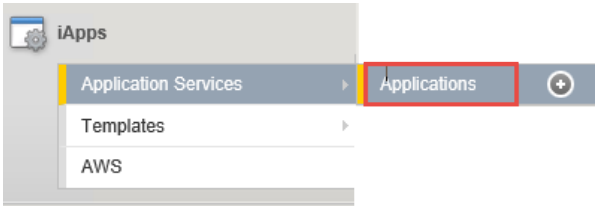
Delete existing ADFS iApps

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

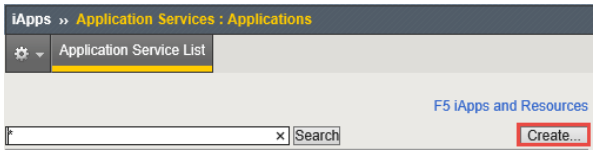


iApp Configuration

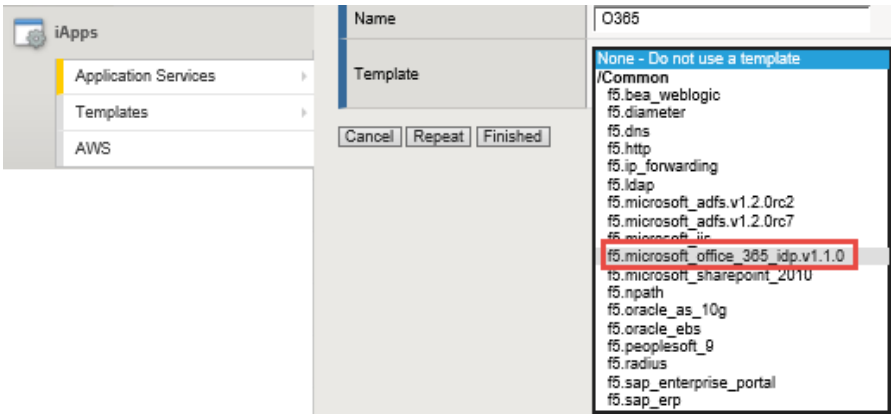
1. **On the** BIG-IP | Select iApps | Application Services | Applications



2. **Click** | Create



3. **Select** | the O365 iApp from the dropdown



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

4

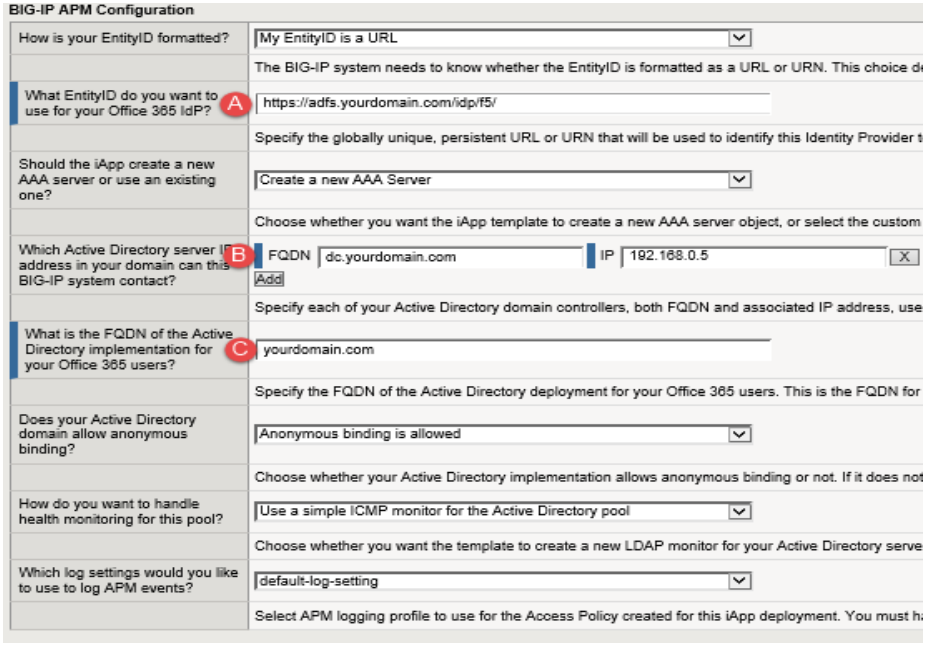
A. Entity ID | Enter an IdP Entity ID

i.e. https://adfs.yourdomin.com/idp/f5/

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



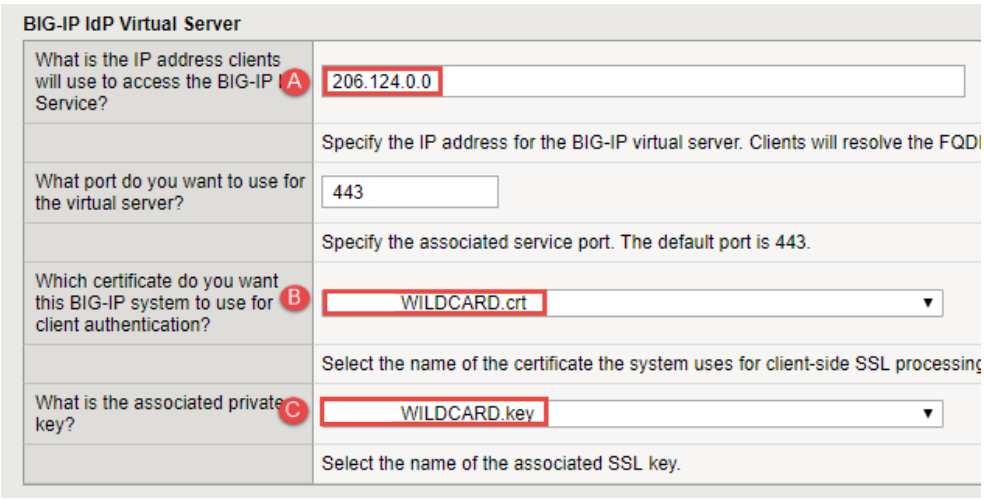
BIG-IP IdP Virtual Server

5

A. IdP address IP adress | 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.

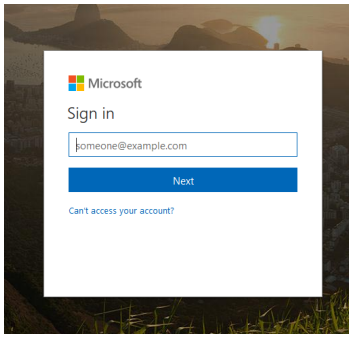


Verify Successful Federation

1. Open a Browser | navigate to your O365 Subscription

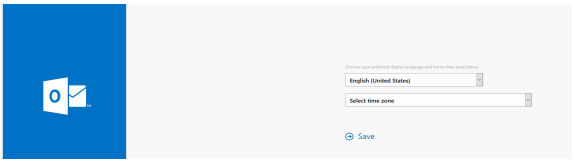
   i.e.outlook.com/yYourDomainName.net

2. Enter Credentials | For a Licensed O365 User

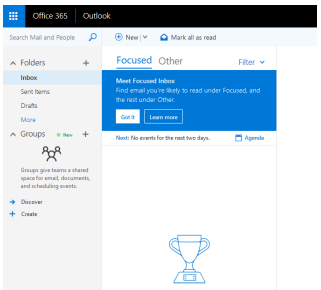


3. **Redirect to the BIG-IP as IdP** | Enter the licensed users credentials for SSO

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



5. **Behold**! | Successful Federation



Note: *If you receive an error while verifying federation like "The requested Federation relm object does not exist"*

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