Deployment Guide

Configuring the BIG-IP APM as a SAML 2.0 Identity Provider for Microsoft Office 365

Welcome to the F5® deployment guide for configuring the BIG-IP® Access Policy Manager (APM) to act as a SAML Identity Provider for Microsoft® Office 365. This document contains guidance on configuring the BIG-IP® APM as an IdP for Office 365 to perform Single Sign-On between the local Active Directory user accounts and Office 365-based resources such as Microsoft Outlook Web App and Microsoft SharePoint®.

Using this guide, you can configure the BIG-IP system version 11.3 and later using an iApp application template. There is also an appendix with manual configuration tables for users who prefer to create each individual object.

Products and applicable versions

Product	Version
BIG-IP APM	11.3, 11.4, 11.4.1, 11.5, 11.5.1, 11.6
iApp Template Version	f5.microsoft_office_365_idp.v1.1.0rc1
Deployment guide version	1.1

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/microsoft-office-365-idp-dg-rc1.pdf.*

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com*

Contents

What is F5 iApp™?

New to BIG-IP version 11, 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. The iApp template for Office 365 IdP acts as the single-point interface for managing this configuration.

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network:* *http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf*.

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- This guide assumes the person configuring this implementation is (or is working with) the administrator of their respective Office 365 tenant.
- For this guide, the BIG-IP system ***must*** be running version 11.3 or later. The configuration described in this guide does not apply to previous versions.
- You must have the APM module fully licensed and provisioned. You must have the LTM module provisioned, even if it is not licensed. You can ignore the provisioning warning when LTM is not licensed.
- This document provides guidance for using the iApp for configuring the BIG-IP APM to act as a SAML IdP using the downloadable iApp template available from *downloads.f5.com*. For users familiar with the BIG-IP system, there is a manual configuration table at the end of this guide. However, because the configuration can be complex, we recommend using the iApp template.
- We assume you have already obtained the appropriate SSL certificate(s) and key(s), and they are installed on the BIG-IP system. See *Generating or importing certificates on page 5* for specific information.

Configuring F5 BIG-IP to act as a SAML 2.0 Identity Provider for Office 365

The first task in federating user identify with Office 365 is to setup your BIG-IP APM to act as the SAML Identify Provider.

You need to complete the following tasks:

1. Configuring the DNS and NTP settings on the BIG-IP system, on this page.
2. Generate a self-signed certificate or import a certificate/key combination to the BIG-IP system that is used to sign the IdP SAML assertions. See *Generating or importing certificate used to sign your SAML Assertion on page 5.*
3. Import the SSL certificate and key that will be used by your IdP Virtual Server. See *Importing a valid SSL certificate for authentication on page 5*
4. Import the Office 365 iApp template on to your BIG-IP system. See *Downloading and importing the Office 365 iApp template on page 5*
5. Run the iApp to configure BIG-IP as SAML IdP Provider for Office 365. See *Configuring the BIG-IP system using the iApp template on page 6.*
6. Configuring your Active Directory implementation for federation and single sign-on. See *Setting up your internal Active Directory infrastructure for federation and Single Sign-On with Office 365 on page 12*

As an alternative to steps 4 and 5, you can use the manual configuration guidance in *Appendix A: Manual Configuration table on page 14* to configure the BIG-IP system. However, we strongly recommend using the iApp template.

Configuring DNS and NTP settings on the BIG-IP system

If you are configuring the iApp to use BIG-IP APM, you must configure DNS and NTP settings on the BIG-IP system before beginning the configuration.

Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP system to point to a DNS server that can resolve your Active Directory server or servers. In many cases, this IP address will be that of your Active Directory servers themselves.

Note

DNS lookups go out over one of the interfaces configured on the BIG-IP system, not the management interface. The management interface has its own, separate DNS settings.

Important

*The BIG-IP system must have a self IP address in the same local subnet and VLAN as the DNS server, or a route to the DNS server if located on a different subnet. The route configuration is found on the Main tab by expanding **Network** and then clicking **Routes**. For specific instructions on configuring a route on the BIG-IP system, see the online help or the product documentation.*

To configure DNS settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **DNS**.
3. In the **DNS Lookup Server List** row, complete the following:
   a. In the **Address** box, type the IP address of a DNS server that can resolve the Active Directory server.
   b. Click the **Add** button.
4. Click **Update**.

Configuring the NTP settings

The next task is to configure the NTP settings on the BIG-IP system for authentication to work properly.

To configure NTP settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **NTP**.
3. In the **Address** box, type the fully-qualified domain name (or the IP address) of the time server you want to add to the Address List.
4. Click the **Add** button.
5. Click **Update**.

To verify the NTP setting configuration, you can use the **ntpq** utility. From the command line, run **`ntpq -np`**.

See *http://support.f5.com/kb/en-us/solutions/public/10000/200/sol10240.html* for more information on this command.

Generating or importing certificates

The next task is to import (or generate a self-signed) certificates on to the BIG-IP system. This configuration requires two different certificates, one that is used to sign your SAML assertion, and the other used by your external users to connect to your IdP service.

Generating or importing certificate used to sign your SAML Assertion

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.

Downloading and importing the Office 365 iApp template

The next task is to download and import the Office 365 iApp template.

To download and import the iApp

1. Open a web browser and go to *downloads.f5.com*.
2. Click **Find a Download**, and then click **BIG-IP v11.x / Virtual Edition**.
3. If necessary, select a BIG-IP product version from the list, and then click **iApp-Templates**.
4. Accept the EULA, and then download the iapps zip file to a location accessible from your BIG-IP system.
5. Extract the files. This Release Candidate version of this iApp is in the **RELEASE-CANDIDATE** folder.
6. Follow the instructions to download the **f5.microsoft_office_365_idp.v1.1.0rc1** iApp template.
7. Log on to the BIG-IP system web-based Configuration utility.
8. On the Main tab, expand **iApp**, and then click **Templates**.

9. Click the **Import** button on the right side of the screen.
10. Click a check in the **Overwrite Existing Templates** box.
11. Click the **Browse** button, and then browse to the location you saved the iApp file.
12. Click the **Upload** button. The iApp is now available for use.

Configuring the BIG-IP system using the iApp template

To begin the iApp Template, use the following procedure.

To start the iApp template

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **Office365-.**
5. From the **Template** list, select **f5.microsoft_office_365_idp.v1.1.0rc1** (or newer if applicable).

Template Options

This section of the iApp template asks general questions about the deployment and iApp options.

1. ***Do you want to see inline help***
   Select whether you want to see informational and help messages inline throughout the template. If you are unsure, we recommend leaving the default, **Yes, show inline help text**.
   Important and critical notes are always shown, no matter which selection you make.
   - **Yes, show inline help text**
     Select this option to show inline help for most questions in the template.
   - **No, do not show inline help text**
     Select this option if you do not want to see inline help. If you are familiar with this iApp template, or with the BIG-IP system in general, select this option to hide the inline help text.

2. ***Which configuration mode do you want to use?***
   Select whether you want to use F5 recommended settings, or have more granular, advanced options presented.
   - **Basic - Use F5's recommended settings**
     In basic configuration mode, options like load balancing method, parent profiles, and settings are all set automatically. The F5 recommended settings come as a result of extensive testing, so if you are unsure, choose Basic.
   - **Advanced - Configure advanced options**
     In advanced configuration mode, you have more control over individual settings and objects, such as server-side optimizations and advanced options such as configuring the ability to restrict traffic to specific VLANs. You can also choose to attach iRules you have previously created to the Citrix application service. This option provides more flexibility for advanced users.

     Advanced options in the template are marked with the Advanced icon: Advanced. If you are using Basic/F5 recommended settings, you can skip the questions with this icon.

BIG-IP APM configuration

This section of the template asks questions about the BIG-IP APM configuration. You must know your EntityID and the FQDN of your Active Directory implementation to complete this section.

1. ***What is the Entity ID that you want to use for your Office 365 IdP?***
   Type the EntityID for your Office 365 IdP. The EntityID is a required configuration setting, and is used by the Office 365 SAML Service Provider (SP) to properly identify and match the SAML assertion coming from the BIG-IP system. The format of the IdP Entity ID should be the URL to the federation service URL that users will use to authenticate themselves to the BIG-IP system. For example, if our Entity ID is **https://login.example.com/idp/f5**, the host name of the federation service is login.example.com. The URI part of the Entity ID, **/idp/f5/**, simply helps build a unique IdP identifier string for the SAML assertion for this particular IdP instance.

2. ***Should the iApp create a new AAA server or use an existing one?***
   The AAA Server contains the authentication mechanism for the BIG-IP APM Access Policy.

   Select whether you want to the template to create a new BIG-IP APM AAA Server object, or if you have already created an AAA object for this implementation on the BIG-IP system. We recommend letting the iApp template create a new AAA server unless you have specific requirements that necessitate a custom AAA Server.

   - *Select an existing AAA Server*
     If you have already created an AAA Server object for this deployment, select it from the list. If you want to create your own AAA Server but have not already done so, you must exit the template and create the object before it is available in the list. Continue with *BIG-IP IdP Virtual Server on page 8*.
   - **Create a new AAA Server**
     Select this option (the default) to have the template create a new Active Directory AAA Server object for the Citrix environment.

     a. *Which Active Directory server IP address in your domain can this BIG-IP system contact?*
        Type both the FQDN and IP address of all Active Directory servers in your domain that this BIG-IP system can contact. Make sure this BIG-IP system and the Active Directory servers have routes to one another and that firewalls allow traffic between the two. Click **Add** to include additional servers.

     b. *What is the FQDN of the Active Directory implementation for your Office 365 users?*
        Type the Active Directory domain name for your Office 365 implementation in FQDN (fully qualified domain name) format. This is the FQDN for the whole domain, and not the FQDN for a specific host.

     c. *Does your Active Directory domain allow anonymous binding?*
        Select whether anonymous binding is allowed in your Active Directory environment.

        - **Yes, anonymous binding is allowed**
          Select this option if anonymous binding is allowed. No further information is required for this question.
        - **No, credentials are required for binding**
          If credentials are required for binding, you must specify an Active Directory user name and password.

          i). *Which Active Directory user with administrative permissions do you want to use?*
              Type a user name with administrative permissions.

          ii). *What is the password for that user?*
               Type the associated password.
               These credentials are stored in plaintext on your BIG-IP system.

     d. *How do you want to handle health monitoring for this pool?*
        Specify whether you want the template to create a new LDAP monitor or a new ICMP monitor, or if you select an existing monitor. For more accurate monitoring, we recommend using an LDAP monitor.

        - **Select an existing monitor for the Active Directory pool**
          Select this option if you have already created a health monitor (only monitors with a **Type** of LDAP or External can be used) for the Active Directory pool that will be created by the template. If you want to create a health monitor, but have not already done so, you must exit the template and create the object before it becomes available from the list.

The iApp allows you to select monitors that are a part of another iApp Application Service. If you select a monitor that is a part of another Application Service, be aware that any changes you make to the monitor in the other Application Service will apply to this Application Service as well.

i). *Which monitor do you want to use?*
From the list, select the LDAP or External monitor you created to perform health checks for the Active Directory pool created by the template. Only monitors that have a Type value of LDAP or External appear in this list. Continue with the next section.

- **Use a simple ICMP monitor for the Active Directory pool**
Select this option if you only want a simple ICMP monitor for the Active Directory pool. This monitor sends a ping to the servers and marks the server UP if the ping is successful. Continue with the next section.
- **Create a new LDAP monitor for the Active Directory pool**
Select this option if you want the template to create a new LDAP monitor for the Active Directory pool. You must answer the following questions:

i). *Which Active Directory user name should the monitor use?*
Specify an Active Directory user name to use when attempting to log on as a part of the health check. This should be a user account created specifically for this health monitor, and *must* be set to never expire.

ii). *What is the associated password?*
Specify the password associated with the Active Directory user name.

iii). *What is the LDAP tree for this user account?*
Specify the LDAP tree for the user account. As noted in the inline help, ADSI editor, an tool for Active Directory LDAP administration, is useful for determining the correct LDAP tree value. For example, if the user name is 'user1' which is in the organizational unit 'F5 Users' and is in the domain 'f5.example.com', the LDAP tree would be: ou=F5 Users, dc=f5, dc=example, dc=com.

iv). *Does your Active Directory domain require a secure protocol for communication?*
Specify whether your Active Directory implementation requires SSL or TLS for communication, or does not require a secure protocol. This determines the port the health monitor uses.

- **No, a secure protocol is not required**
Select this option if your Active Directory domain does not require a secure protocol.
- **Yes, SSL communication is required**
Select this option if your Active Directory domain requires SSL communication. The health check uses port 636 as the Alias Service Port.
- **Yes, TLS communication is required**
Select this option if your Active Directory domain requires TLS communication. The health check uses port 389 as the Alias Service Port.

v). *How many seconds between Active Directory health checks?*
Specify how many seconds the system should use as the health check Interval for the Active Directory servers. We recommend the default of 10 seconds.

vi). *Which port is used for Active Directory communication?*
Specify the port being used by your Active Directory deployment. The default port displayed here is determined by your answer to the secure protocol question. When using the TLS security protocol, or no security, the default port 389. The default port used when using the SSL security protocol is 636.

BIG-IP IdP Virtual Server

This section gathers information about your Office 365 IdP environment that will be used in the BIG-IP virtual server.

1. ***What is the IP address clients will use to access the BIG-IP IdP Service?***
Type the IP address to use for the BIG-IP virtual server. Clients will resolve the FQDN of the Identity Provider to this IP address.

2. ***What port do you want to use for the virtual server?***
Type the port number you want to use for the BIG-IP virtual server IP address you specified in the previous question. The default port is 443 (HTTPS).

3. ***Do you want to redirect inbound HTTP traffic to HTTPS?*** Advanced
Select whether you want the BIG-IP system to automatically redirect HTTP traffic to the HTTPS virtual server. This is useful when users forget to use HTTPS when attempting to connect to the environment.

   - **Redirect HTTP to HTTPS**
   Select this option to redirect HTTP traffic to HTTPS. If you select this option (the default), the BIG-IP system creates an HTTP virtual server and attaches a very small redirect iRule to ensure users get to the correct location.

     a. *From which port should traffic be redirected?*
     Type the port number for the traffic that you want to redirect to HTTPS. The most common is port 80 (the default).

   - **Do not redirect HTTP to HTTPS**
   Select this option if you do not want to enable the automatic redirect.

4. ***Do you want to restrict client traffic to specific VLANs?*** Advanced
The BIG-IP system allows you to restrict client traffic to specific VLANs that are present on the system. This can provide an additional layer of security, as you can allow or deny traffic from the VLANs you choose. By default, all VLANs configured on the system are enabled. If you select to enable or disable traffic on specific VLANs, you must specify the VLANs in the next question. The VLAN objects must already be configured on this BIG-IP system before you can select them.

   - **Enable traffic on all VLANs and Tunnels**
   Choose this option to allow traffic from all VLANs and Tunnels. If you select this option, the question asking about VLANs disappears. Continue with the next question.

   - **Yes, enable traffic only on the VLANs I specify**
   Choose this option to restrict client traffic to specific VLANs that you choose in the following question. The system will accept client traffic from these VLANs, and deny traffic from all other VLANs on the system.

     a. *On which VLANs should traffic be enabled or disabled?*
     Use this section to specify the VLANs that accept client traffic. By default, all VLANs on the BIG-IP system appear in the Selected box, so click the VLANs and then use the Move buttons to adjust list membership.

     Note

     If you choose to allow traffic from certain VLANs, when additional VLANs are added to the BIG-IP system at a later time, this iApp configuration will deny traffic from these VLANs by default. To accept traffic from these VLANs, you must re-enter the template and add the VLAN(s).

   - **Yes, disable traffic only on the VLANs I specify**
   Choose this option to deny client traffic from the specific VLANs that you choose in the following question. The system will refuse client traffic from these VLANs, and accept traffic from all other VLANs on the system.

     a. *On which VLANs should traffic be enabled or disabled?*
     Use this section to specify the VLANs that should not accept client traffic. By default, all VLANs on the BIG-IP system appear in the Selected box, so it is critical in this case that you click the VLANs and then use the Move button (>>) to adjust list membership.

     Warning

     If you choose to disable certain VLANs, you must move at least one VLAN to the Options list. Otherwise, the system will deny traffic from all VLANs on the box, and the configuration, although valid, will not pass any traffic.

5. ***Will clients be connecting to this BIG-IP virtual server primarily over a LAN or a WAN?*** Advanced
Select whether most clients are connecting over a WAN or LAN. The iApp uses your selection to determine the default TCP optimization settings in the next question.

   - **Most clients connect over a WAN**
   Select this option if most of your clients are coming into the environment over a Wide Area Network.

   - **Most clients connect over a LAN**
   Select this option if most your clients are coming into the environment over a Local Area Network.

6. ***How do you want to optimize client-side connections?*** Advanced
   The client-side TCP profile optimizes the communication between the BIG-IP system and the client by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - **Create the appropriate tcp-optimized profile (recommended)**
     Select this option to have the system create the recommended TCP profile. The parent profile (either WAN or LAN optimized) is determined by your selection to the "What type of network connects clients to the BIG-IP system" question.
   - *Select the TCP profile you created from the list*
     If you created a custom TCP profile for this implementation, select it from the list.

7. ***Which HTTP profile do you want to use?*** Advanced
   The HTTP profile contains settings for instructing the BIG-IP system how to handle HTTP traffic. Choose whether you want the iApp to create a new HTTP profile or if you have previously created an HTTP profile for this deployment.

   Unless you have requirements for configuring specific HTTP settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Services : HTTP** to create a HTTP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - *Select an existing HTTP profile from the list*
     If you already created an HTTP profile for this implementation, select it from the list.
   - **Create a new HTTP profile (recommended)**
     Select this option for the iApp to create a new HTTP profile.

8. ***Do you want to create a new client SSL profile or use an existing one?***
   This question only appears if you selected Advanced configuration mode, however if you selected Basic mode, the Certificate and Key questions (a and b) under "Create a new Client SSL profile" appear.

   The iApp can create a new Client SSL profile, or if you have created a Client SSL profile which contains the appropriate SSL certificate and key for your implementation, you can select it from the list.

   Unless you have requirements for configuring specific Client SSL settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** > **Profiles** > **SSL** > **Client** to create a Client SSL profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - *Select the Client SSL profile you created from the list*
     If you manually created a Client SSL profile that includes the appropriate certificate and key, select it from the list.
   - **Create a new Client SSL profile**
     Select this option if you want the iApp to create a new Client SSL profile.

     a. *Which certificate do you want this BIG-IP system to use for client authentication?*
        Select the SSL certificate you imported onto the BIG-IP system for client authentication.

        If you have not yet imported a certificate, you can leave the default selections and reconfigure this iApp after obtaining the certificates. Using the default certificate and key results in an incomplete configuration which is not secure until you import and assign a trusted certificate and key that are valid for all fully qualified domain names used to access the application.

        ⚠ ***Warning***

        The default certificate and key on the BIG-IP system is not secure and should never be used in production environments. The trusted certificate must be valid for all fully qualified domain names used to access the application. For more information on importing certificates and keys, see the BIG-IP documentation.

b. *What is the associated private key?*
Select the SSL private key associated with the certificate you selected above.

c. *Do you need to use an intermediate certificate?*
Select whether you need to use an intermediate certificate in this implementation. Immediate certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown. See http://support.f5.com/kb/en-us/solutions/public/13000/300/sol13302.html for help creating an intermediate certificate chain.

- **Do not use an intermediate certificate**
  Select this option if you do not require an intermediate certificate for this deployment. Continue with the next section.
- *Select the certificate you imported from the list*
  If you imported an intermediate certificate onto the BIG-IP system for this implementation, select it from the list.

IDP Encryption Certificate and Key

This section gathers information about your Office 365 IdP environment that will be used in the BIG-IP virtual server.

1. ***Which certificate do you want to use to encrypt your SAML Assertion?***
   Select the name of the certificate you imported to use to encrypt your SAML Assertion. The certificate must already be present on the BIG-IP system in order to select it. To select any new certificates and keys you import, you need to restart or reconfigure this template.

   Important

   The certificate can be either self-signed certificate generated by the BIG-IP system, or you can import a certificate for this purpose. The only restriction is you cannot use a wildcard certificate to sign SAML assertions to Office 365.

2. ***What is the associated private key?***
   Select the SSL private key associated with the certificate you selected above.

iRules

In this section, you can add custom iRules to the deployment. This entire section is available only if you selected Advanced mode.

iRules are a scripting language that allows an administrator to instruct the system to intercept, inspect, transform, direct and track inbound or outbound application traffic. An iRule contains the set of instructions the system uses to process data flowing through it, either in the header or payload of a packet.

1. ***Do you want to add any custom iRules to the configuration?*** Advanced
   Select if have preexisting iRules you want to add to your IIS implementation.

   Warning

   While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.

   If you do not want to add any iRules to the configuration, continue with the following section.

   If you have iRules you want to attach to the virtual server the iApp creates for your IIS servers, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (**<<**) button to move them to the **Selected** box.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects.

Setting up your internal Active Directory infrastructure for federation and Single Sign-On with Office 365

This section contains guidance on configuring your internal Windows infrastructure in order to enable directory replication and setup federation trust between your newly-configured BIG-IP system and the Office 365 cloud.

1. Install the Office 365 **DirSync** tool on a domain-joined server that replicates your Active Directory into the Office 365 tenant cloud.
2. Convert your domain to Federated status in the Office 365 cloud

Instructions on setting up Directory Synchronization and installation of the DirSync tool are available at the following location: *https://portal.microsoftonline.com/DirSync/DirectorySynchronization.aspx*

If you already have Directory Synchronization configured, either because you have setup Office 365 federation with AD FS or another IdP provider such as Shibboleth, you can go straight to the next step and perform the following actions on your server that has DirSync tools installed (or, alternately, you can perform these steps from any domain-joined server that has Microsoft Online Services Module for PowerShell installed as referenced in the Microsoft TechNet article: *http://technet.microsoft.com/en-us/library/jj205464.aspx*).

Each Active Directory domain that you want to federate with Office 365 must either be added as a single sign-on domain or converted to be a single sign-on domain from a standard domain. Adding or converting a domain sets up a trust between F5 BIG-IP IdP and Office 365.

Note

*When synchronizing Active Directory to Office 365 using the Directory Sync tool, you do not need to check the **Enable Password Sync** box.*

Log on to the Windows Server that has either DirSync or Microsoft Online Services Module installed and perform the following actions:

1. Copy the SSL Certificate that you configured the BIG-IP IdP services to use for signing SAML assertions on the server. It is important, because there can be issues with cutting and pasting the text of the certificate for configuring it Office 365 federation through the PowerShell. You can easily export the certificate by logging onto the BIG-IP Configuration utility from the Windows Server, clicking **System > File Management > SSL Certificate list > name of certificate > Export** button. Save the certificate file to a location on your server that can be easily specified in the command line format. In the following example, we assume that you will save your certificate to **C:\temp**.
2. From the Windows server **Start** menu, open the **Microsoft Online Services Module**.
3. Run the following command in the Module's PowerShell window: **`$cred=Get-Credential`**
4. When you are prompted for credentials, type the Office 365 administrator credentials for your domain tenant instance (for example, admin@example.onmicrosoft.com) and the associated password.
5. Run the command: **`Connect-MsolService -Credential $cred`**
   This cmdlet connects your PowerShell session to your Office 365 tenant instance for your domain
6. If your domain is currently in a Federated status with Office 365, you need to convert it to the standalone by running this cmdlet:
   `Convert-MsolDomainToStandard -Domain example.com`
   Replace example.com with the actual domain name that you are federating with Office 365.
7. Run the command: **`$dom = "example.com"`**
   This variable specifies the domain name that will be federated with Office 365. Replace example.com with your actual domain name that you are federating.
8. Run the command: **`$FedBrandName = "Example Federated SSO"`**
   This variable is purely informational but is required, and provides verbal comment-style description of the configuration.
9. Run the command: **`$url = "https://login.example.com/saml/idp/profile/redirectorpost/sso"`**
   This variable specifies the authentication URL for your BIG-IP Federation service that you have setup at the beginning of the document. Replace login.example.com with the actual DNS name of your federation service. The URI section **/saml/idp/profile/redirectorpost/sso** is always static for all F5 IdP configurations and should not be changed.

10. Run the command: **$ecpUrl = "https://login.example.com/saml/idp/profile/redirectorpost/sso"**
    The value of this variable should be set identical to the $url above. It is used by Office 365 to submit Active Assertion Requests to the BIG-IP system on behalf of non-browser clients such as ActiveSync devices and OutlookAnywhere connections.
11. Run the command: **$uri = "https://login.example.com/idp/f5/"**
    The value of this variable must be set to the exact Entity ID value you used when configuring the IdP configuration on the BIG-IP system. Replace login.example.com/idp/f5 to match your Entity ID value.
12. Run the command: **$logouturl = "https://login.example.com/vdesk/hangup.php3"**
    The value of this variable is used to perform sign-out of the user from the Office 365 application. Once the user clicks on the Logout Button in their Office 365 Outlook Web Access of SharePoint, they are sent to this URL, and then BIG-IP APM terminates their authenticated session. Replace login.example.com with the DNS name of your BIG-IP federation service as in the previous steps.
13. Run the command: **$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("c:\temp\saml.crt")**
    This variable stores the certificate that Office 365 will use to verify the assertions submitted by the BIG-IP IdP. In this example, c:\temp\saml.crt specifies the path to the certificate that you have downloaded from the BIG-IP in step 1 to your local file system. Replace c:\temp\saml.crt with the correct path to the actual certificate you downloaded in step 1.
14. Run the command: **$certData = [system.convert]::tobase64string($cert.rawdata)**
15. Run the command: **Set-MsolDomainAuthentication –DomainName $dom –FederationBrandName $FedBrandName -Authentication Federated -PassiveLogOnUri $url -SigningCertificate $certData -IssuerUri $uri -ActiveLogOnUri $ecpUrl -LogOffUri $logouturl -PreferredAuthenticationProtocol SAMLP**
    This command takes all the variables that you have defined above, connects to your Office 365 tenant, and performs the necessary configuration there to convert your domain to the Federated status using the BIG-IP system as the SAML IdP provider. If you do not receive any errors after running this command, you are now ready to test your newly-federated domain.

Testing the newly Configured Federated setup

To test your newly-converted federated domain, open a web browser and go to *https://outlook.com/owa/example.com*, replacing example.com with the domain name you have just configured for federation. You should be redirected to your federation URL on your BIG-IP APM and see the login page.

Type your Active Directory credentials, and then the BIG-IP system should issue a SAML Assertion to Office 365. If the assertion was properly accepted, the user sees their Office 365 mailbox. If they are not provisioned with an Office 365 mailbox, they will see an error message informing them of that.

Appendix A: Manual Configuration table

We strongly recommend using the iApp template to configure the BIG-IP system for Microsoft Office 365 IdP. Users familiar with the BIG-IP system can use the following table to manually configure the BIG-IP system. The table contains a list of configuration objects along with any non-default settings you should configure as a part of this deployment. Settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object			Non-default settings/Notes
Profiles *(Local Traffic > Profiles)*	***HTTP*** *(Profiles > Services)*	Name	Type a unique name
		Parent Profile	**http**
		Insert X-Forwarded-For	**Enabled**
	TCP *(Profiles > Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized** or **tcp-lan-optimized** depending on where most clients are located
		Idle Timeout	**1800**
	Client SSL[3] *(Profiles > SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select the Certificate and Key you imported from the associated list
		Chain	If applicable, select the Chain certificate you imported
iRules (*Local Traffic-->Rules*)	***Name***		Type a unique name, such as **encode_ObjectGUID_irule**

	Definition		`when ACCESS_POLICY_AGENT_EVENT {`
			`  if {[ACCESS::policy agent_id] eq "encode"} {`
			`  set tmpVar [binary format H* [substr "[ACCESS::session data get session.ad.last.attr.objectGUID]" 2]]`
			`  ACCESS::session data set session.ad.last.attr.objectGUIDencoded [b64encode $tmpVar]`
			`  }`
			`}`

Health Monitor[1] (*Local Traffic--> Monitors*) **Note:** Only necessary if creating a pool of Active Directory servers Choose either ICMP or LDAP monitor.	***Simple ICMP Monitor***		
	Name		Type a unique name.
	Type		**Gateway ICMP**
	LDAP Monitor		
	Configuration		Select **Advanced** from the Configuration list (if necessary)
	Name		Type a unique name, such as AD_LDAP_monitor
	Type		**LDAP**
	Interval		**10** (recommended)
	Timeout		**31** (recommended)
	User Name		Type a user name with administrative permissions
	Password		Type the associated password
	Base		Specify your LDAP base tree. For example, CN=SharePoint Users,DC=example,DC=com
	Filter		Specify the filter. We type **cn=user1**, using the example above: user1 in OU group "SharePoint Users" and domain "example.com"
	Security		Select a Security option (either None, SSL, or TLS)
	Chase Referrals		**Yes**
	Alias Address		***All Addresses**
	Alias Address Port		**389** (for None or TLS) or **686** (for SSL)
AAA Server (*Access Policy-->AAA Servers*)	***If you are using a single Active Directory Server***		
	Name		Type a unique name.
	Type		**Active Directory**
	Domain Controller		Type the IP address or FQDN name of an Active Directory Domain Controller
	Domain Name		Type the Active Directory domain name
	Admin Name[2]		Type the AD user name with administrative permissions (optional)
	Admin Password[2]		Type the associated password (optional). Type it again in the Verify Password box

[1] Only necessary if using a pool of Active Directory servers
[2] Optional; Admin Name and Password are only required if anonymous binding to Active Directory is not allowed in your environment

BIG-IP LTM Object	Non-default settings/Notes	
AAA Server (*Access Policy-->AAA Servers*)	***If you are using a pool of Active Directory Servers***	
	Name	Type a unique name.
	Type	**Active Directory**
	Domain Name	Type the FQDN of the Windows Domain name
	Server Connection	Click **Use Pool** if necessary.
	Domain Controller Pool Name	Type a unique name
	Domain Controllers	**IP Address**: Type the IP address of the first domain controller **Hostname**: Type the FQDN of the domain controller Click **Add**. Repeat for each domain controller in this configuration.
	Server Pool Monitor	Select the monitor you created above.
	Admin Name[2]	Type the Administrator name
	Admin Password[2]	Type the associated password
SSO Configurations (*Access Policy-->SSO Configurations-->SSO Configurations By Type (on the menu bar)*)	***Name***	Type a unique name.
	SSO Method	**SAML**
	IdP Entity ID	Type your Entity ID, such as https://example.com/idp/f5.
	Assertion Settings	In the left pane of the Create New IdP Service box, click **Assertion Settings**. ***Assertion Subject Type:*** **Persistent identifier** ***Assertion Subject Value:*** **%{session.ad.last.attr.objectGUIDencoded}**
	SAML Attributes	In the left pane of the Create New IdP Service box, click **SAML Attributes**. ***Name***: **IDPEmail** ***Value:*** **%{session.ad.last.attr.userPrincipalName}**
	Security Settings	In the left pane of the Create New IdP Service box, click **Security Settings**. ***Assertion Signing Key:*** Select the appropriate Key ***Public Certificate:*** Select the appropriate Certificate
SAML Resource (*Access Policy-->SAML--> SAML Resources*)	***Name***	Type a unique name.
	Publish on Webtop	**Enabled**
	SSO Configuration	Select the SSO Configuration you just created
Connectivity Profile (*Access Policy--> Secure Connectivity*)	***Name***	Type a unique name
	Parent Profile	**connectivity**
Webtop (*Access Policy--> Webtops*)	***Name***	Type a unique name
	Type	**Full**
Access Profile (*Access Policy--->Access Profiles*)	***Name***	Type a unique name.
	SSO Configuration	Select the appropriate SSO Configuration you created.
	Languages	Move the appropriate language(s) to the **Accepted** box.
Access Policy	***Edit***	Edit the Access Profile you just created using the Visual Policy Editor using the guidance on the following page
Virtual Servers (*Local Traffic > Virtual Servers*)	**HTTP** *(only necessary if you want to redirect users from HTTP to HTTPS)*	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**80**
	iRule[4]	Enable the built-in **_sys_https_redirect** irule
	HTTPS	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	SSL Profile (Client)	Select the Client SSL profile you created above
	Access Profile	Select the Access Profile you created
	Connectivity Profile	Select the Connectivity profile you created above
	iRules	Enable the iRule you created **and** the built in **_sys_APM_Office365_SAML_BasicAuth** irule

Editing the Access Policy

The next step is to edit the Access Policy on the APM using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy.

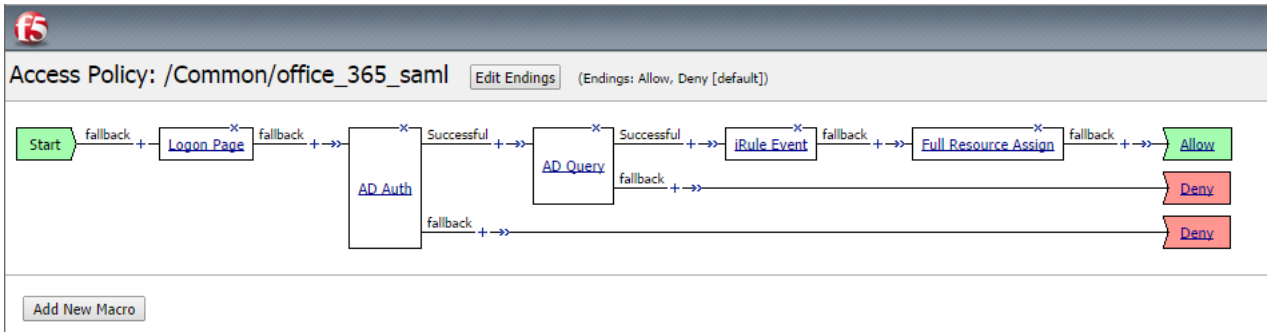
To edit the Access Policy

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you created, and then, in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Logon Page** option button, and then click the **Add Item** button.
    a. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
    b. Click **Save**.
5. Click the **+** symbol on the between **Logon Page** and **Deny**.
6. Click **AD Auth** option button (if using v11.4 or later, click the Authentication tab first), and then click the **Add Item** button.
    a. From the **Server** list, select the AAA server you configured in the table above.
    b. Click the Branch Rules tab.
    c. Click the **change** link.
    d. Click the delete (x) button next to the default branch rule to remove it.
    e. Click the Advanced tab.
    f. Type (or copy and paste) **expr {[mcget {session.ad.last.authresult}] == "1"}**.
    g. Click **Finished** and then click **Save**. You now see a Successful and Fallback path from AD Auth.
7. On the Successful path between **AD Auth** and **Deny**, click the **+** symbol.
8. Click the **AD Query** option button (if using v11.4 or later, click the Authentication tab), and then click **Add Item**.
    a. From the **Server** list, select the AAA server you created.
    b. In the **Search Filter** box, type **samAccountName=%{session.logon.last.username}**
    c. Click the Branch Rules tab and then click the delete (x) button next to the default branch rule to remove it.
    d. Click **Add Branch Rule**.
    e. In the **Name** box, type **Successful**.
    f. Click the **change** link.
    g. Click the **Add Expression** button.
    h. From the **Agent Sel** list, select **AD Query**.
    i. From the Condition list, select AD Query Passed, and then click the **Add Expression** button.
    j. Click **Finished** and then click **Save**.
9. On the Successful path between **AD Query** and **Deny**, click the **+** symbol.
10. Click the **iRule Event** option button (if using v11.4 or later, click the General Purpose tab), and then click **Add Item**.
    a. In the **Name** box, you can type a name.
    b. In the **ID** field, type **encode**.

c. Click **Save**.

11. On the fallback path between **iRule Event** and **Deny**, click the **+** symbol.
12. Click the **Advanced Resource Assign** (Full Resource Assign prior to v11.4) option button (if using v11.4 or later, click the Assignment tab), and then click **Add Item**.
    a. Click **Add new entry**.
    b. Click the **Add/Delete** link on the new entry.
    c. Click SAML tab.
    d. Check the box for the SAML SSO Configuration you created using the table.
    e. Click the Webtop tab.
    f. Click the option button for the Webtop profile you created using the table.
    g. Click **Update**, and then click the **Save** button.
13. On the path between **Advanced Resource Assign** and **Deny**, click the **Deny** box, click **Allow**, and then click **Save**.
14. Click the yellow Apply Access Policy link in the upper left part of the window, and then click the **Close** button on the upper right.

When complete, your VPE should look similar to the following example.



This completes the manual configuration.

Document Revision History

Version	Description	Date
1.0	New guide	10-06-2014
1.0	New Deployment Guide for the f5.microsoft_office_365_idp.v1.1.0rc1 version of the iApp template available in the Release-Candidate directory of the iApp package on downloads.f5.com. This version contains no new features, but has the following fixes: - Modified the iApp to allow certain special characters in passwords	12-16-2014

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com