Configuring BIG-IP as SAML Identity Provider for Office 365

The first task in federating user identity with Office 365 is to setup BIG-IP APM to act as the SAML Identity Provider as follows:

* Configure DNS and NTP settings
* Generate or import a certificate to the BIG-IP system to sign the ldp SAML
* Import SSL certificate to be used by the ldp Virtual Server
* Use the Office 365 iApp template for the BIG-ip system – just add configurations
* Configure AD implementation for federation and SSO

## Configuring DNS and NTP

1. On Main tab 🡪 System 🡪 Configuration
2. Device menu 🡪 DNS
3. DNS Lookup Server List 🡪 Adress
4. Update
5. System 🡪 Configuration
6. Device menu 🡪 NTP
7. Add address
8. Update

## Generationg or importing certificates

This configuration requires two different certificates (one to sign the SAML assertion, and the other to be used by external users to connect to ldp)

System🡪File Management🡪SSL Certificate List

Here we can use either **Import** or **Create** for the SAML certificate.

For the SSL certificate we will have to take the same steps.

System🡪File Management🡪SSL Certificate List🡪Import🡪Import type

## Download and import Office 365 iApp template

1. Download iApp file
2. In the BIG-IP web-based config Main🡪iApp🡪Templates🡪Import
3. Check Overwrite Existing Templates
4. Browse for the file and Upload.

## Configure iApp according to requirements

Configure iApp according to wizard propts.

## Set up internal AD infrastructure for federation and SSO

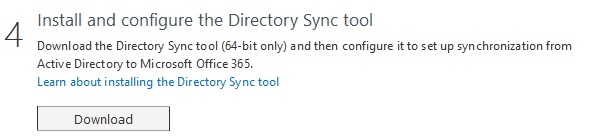
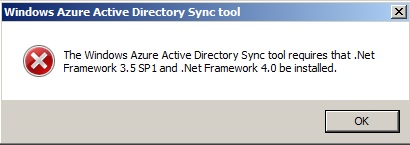
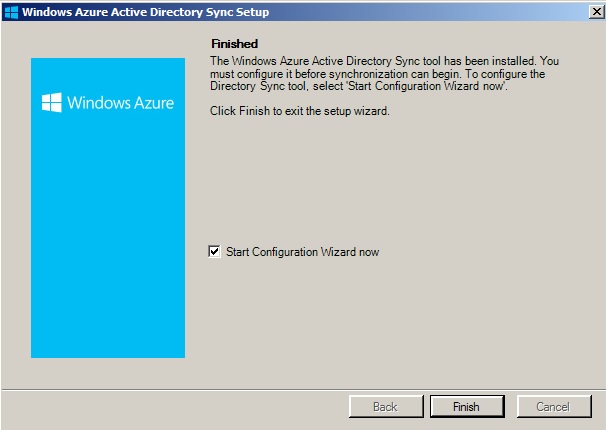
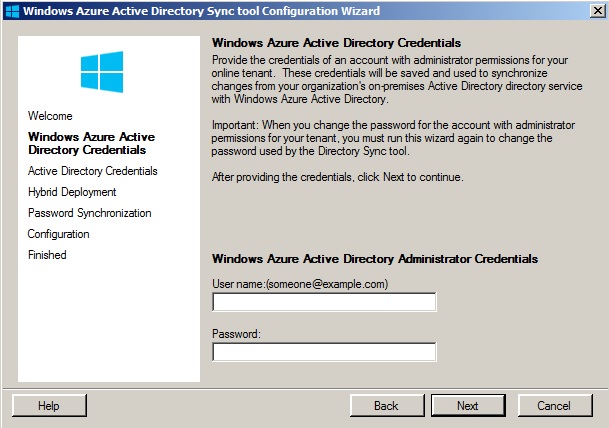
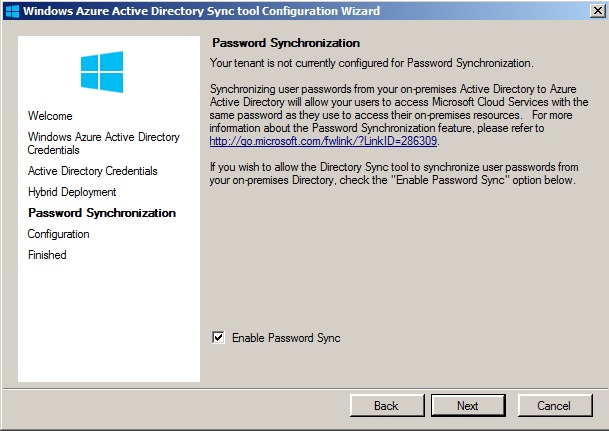
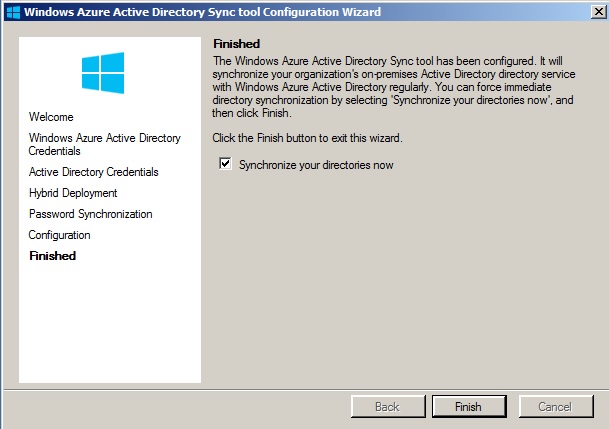
1. Install Office 365 DirSync tool

To sync the local AD with the Office 365 service the installation of the Directory Synchronization Tool (Dirsync) is required. You can download the tool from Microsoft pages: <http://go.microsoft.com/fwlink/?LinkID=278924>. Bear in mind that the tool is available only in a 64 bit version.

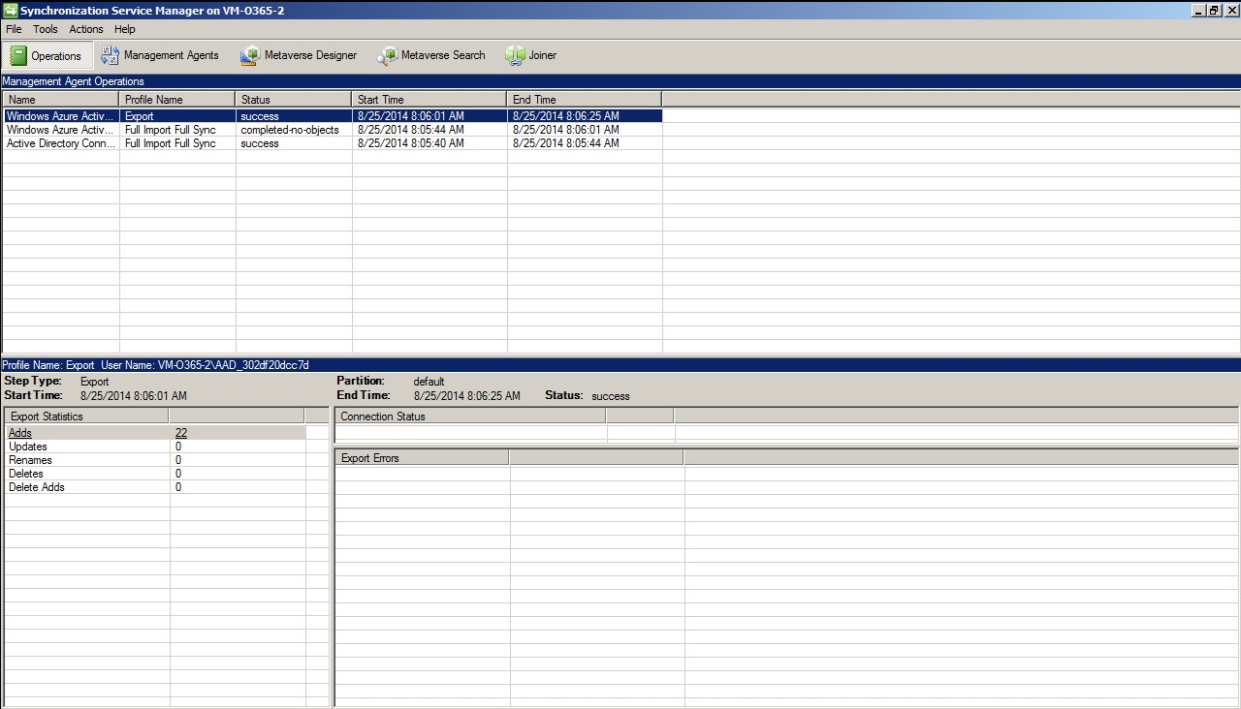
The program syncs all accounts, with their access passwords up to Office 365. However, it does not provide Single Sign-On (SSO) capability. To achieve SSO AD Federation Services (ADFS) needs to be configured.

Microsoft recommends installing Dirsync on a server within a domain, however, it should not be a domain controller. More specific system requirements are available on this Microsoft Technet website: <http://technet.microsoft.com/en-us/library/jj151831.aspx#BKMK_ComputerRequirements>.

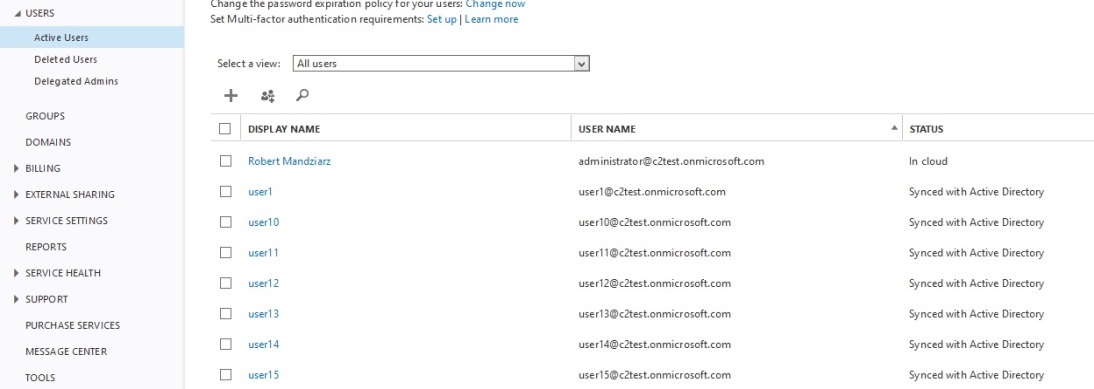
Steps are as follows:

* + 1. Log in to Office 365 with administrative user credentials.
    2. Go to **Users**, then **Active Users**.
    3. Click the **Active Directory synchronization Set up** link visible above the list of users.
    4. In point „**3**” on the list click the **Activate**button. A notification should appear that the synchronization is active:  
       [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/1.jpg)
    5. In point „**4**” click **Download** to get the Dirsync tool:  
       [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/2.jpg)
    6. On the machine, where you are installing the tool make sure that the **.net 3.5 sp1** and **.net 4.0** libraries are installed. Otherwise the Dirsync tool setup will return the following error:  
       [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/3.jpg)  
       In Windows Server 2008 R2 SP1 the .net 3.5 SP1 library is available for installation via the **Server Manager** program, in the **Features** tab, while the .net 4.0 needs to be downloaded from the following location: <http://www.microsoft.com/en-US/download/details.aspx?id=17718>.In Windows Server 2012 and 2012 R2 both libraries can be installed using the Server Manager console.
    7. Follow the installation wizard until finish. The process might take a couple of minutes.
    8. Once the installation is complete select **Start Configuration Wizard now**and click **Finish**.
    9. In the configuration wizard, enter credentials of a user with administrative privileges in Office 365. These credentials are stored within the tool – if they change (e.g. the password is changed) the program needs to be reconfigured.  
       [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/9.jpg)
    10. In the next step enter administrative user credentials of the on-premises AD. Opposite to step 9., these credentials are not stored, and there is no need to reconfigure the program if e.g. the password changes.
    11. Next step shows the Exchange settings for the hybrid deployment. Leave them unchecked, as they are not covered in this article. Click **Next**.
    12. In the following step, mark the **Enable Password Sync**checkbox. Click the **Next**button.  
        [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/11.jpg)
    13. Wait for the program to finish configuration. Once it’s done – click the **Finish** button. Leave the **Synchronize your directories now** option marked:  
        [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/12.jpg)

After Dirsync is installed, you need to verify that the process works as expected. To do so use the **Synchronization Service Manager** console:

* + 1. Go to the following disk location: C:\Program Files\Windows Azure Active Directory Sync\SYNCBUS\Synchronization Service\UIShell.
    2. Launch the **miisclient.exe** program. It might happen that the program will not start, right after Dirsync installation. In such situation simply log out and then log back on to the system.
    3. Once the program is running you can check the sync progress:  
       [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/13.jpg)

In the upper part of the window, there is a list of all current sync cycles. In lower left all current modifications to AD are listed.

* + 1. Log on to the Office 365 portal again.
    2. In the **Users** section, in **Active Users** part you can check which accounts are already synced:[](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/14.jpg)

## Dirsync post-installation tweaks

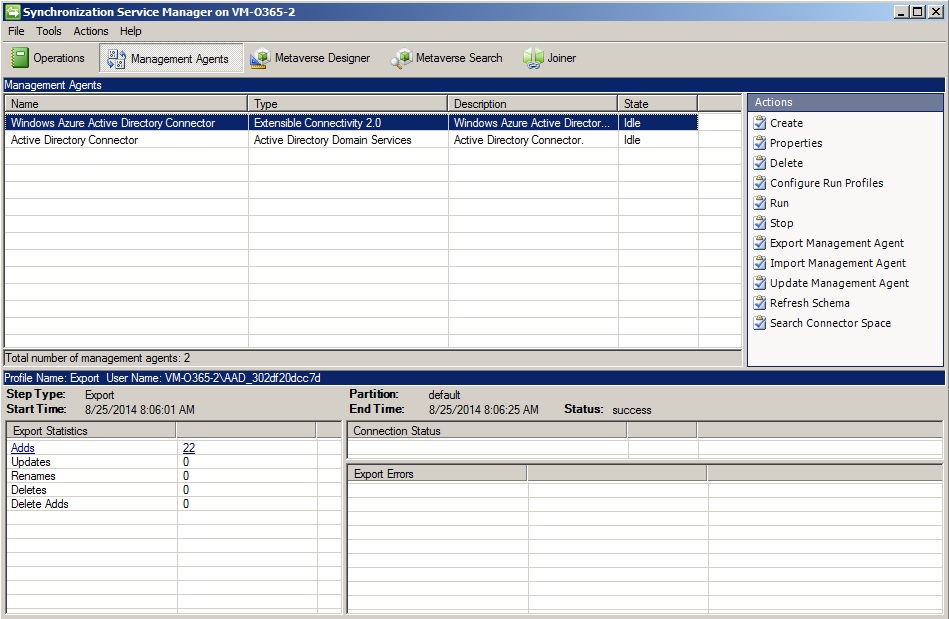
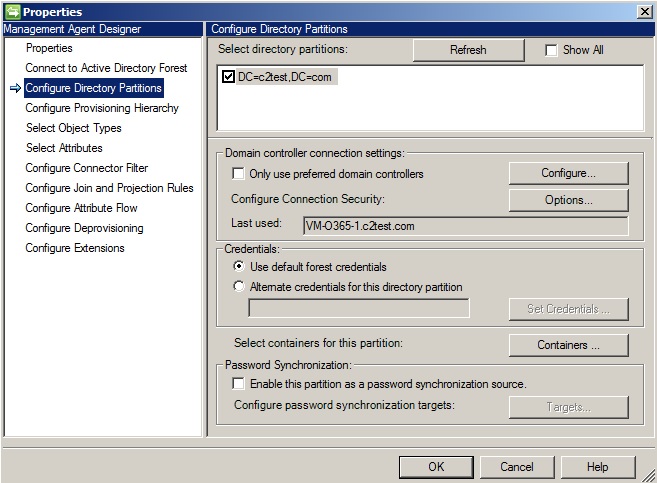
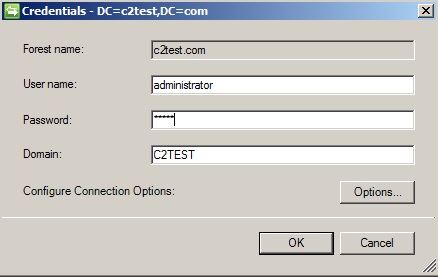
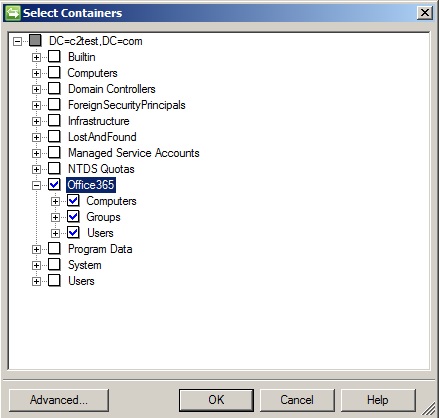
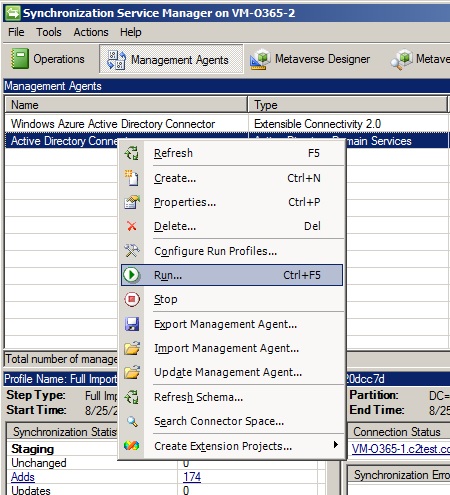
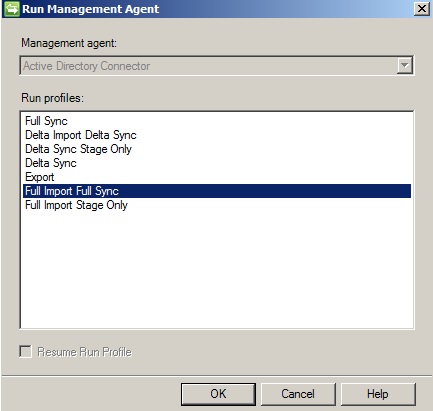
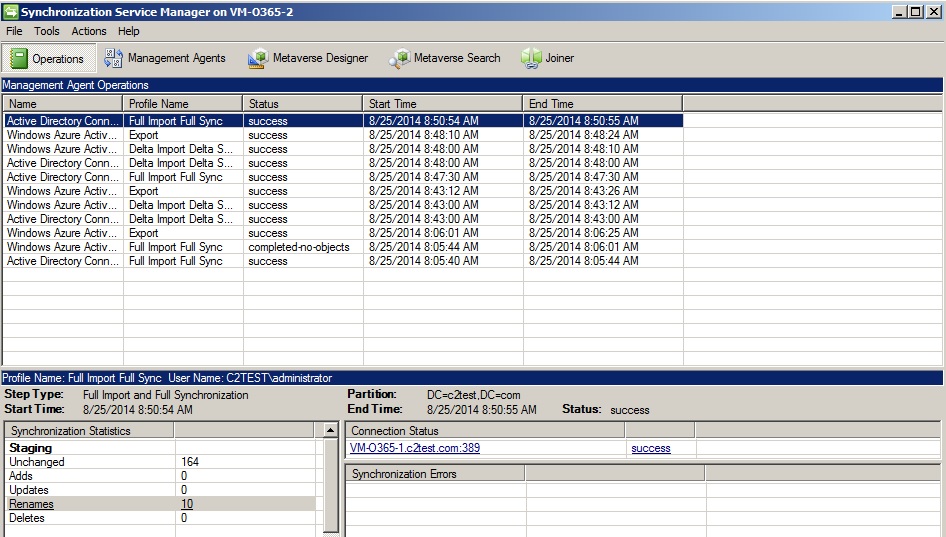
### Changing time between sync cycles

By default, the sync cycles are launched in 3-hour intervals. To reduce the time between syncs (e.g. for testing purposes) do the following:

* + 1. On the server, where the Dirsync tool is installed go to the C:\Program Files\Windows Azure Active Directory Sync folder.
    2. Open the Microsoft.Online.DirSync.Scheduler.exe.Config file with the Notepad.
    3. Locate the following string:**<add key=”SyncTimeInterval” value=”3:0:0″ />**and change the “3:0:0” value to e.g. “0:5:0”. This changes the sync interval from 3 hours to 5 minutes.
    4. Save changes in the file and restart the Windows Azure Active Directory Sync Service in system services.

### Limiting the number of synced objects

In situations, when the on-premises organization is large, and only some users or groups are using Office 365 it is useful to limit the sync to specific Organizational Units (OU) only.

* + 1. On the Dirsync server open the C:\Program Files\Windows Azure Active Directory Sync\SYNCBUS\Synchronization Service\UIShell location.
    2. Open the **Synchronization Service Manager** console by launching miisclient.exe.
    3. Open the **Management Agents** tab:  
       [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/15.jpg)
    4. Right-click **Active Directory Connector** and select **Properties**.
    5. Navigate to **Configure Directory Partitions** and click the **Containers**button:  
       [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/16.jpg)
    6. In the next window enter credentials of the AD administrative user:  
       [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/17.jpg)
    7. Select the OU container of your choice and click **OK**:  
       [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/18.jpg)
    8. Click **OK** again to return to the main window (**Management Agents** tab).
    9. Right-click the **Active Directory Connector** agent and click **Run**:  
       [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/19.jpg)
    10. Select **Full Import Full Sync** and hit **OK**:  
        [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/20.jpg)
    11. You should already notice the effect of above settings in the main program window, in the **Operations** tab:  
        [](http://www.codetwo.com/admins-blog/wp-content/uploads/2014/10/21.jpg)

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

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 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 following command. This variable specifies the authentication URL for your BIG-IP Federation service that you 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: *$url = "https://login.example.com/saml/idp/profile/redirectorpost/sso"*

10. Run one of the following commands (this step depends on whether you are using BIG-IP v11.x or v12). 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. F5 Deployment Guide 13 Microsoft Office 365 as SAML IdP

• v11.x: $ecpUrl = "https://login.example.com/saml/idp/profile/redirectorpost/sso"

• v12: $ecpUrl = "https://login.example.com/saml/idp/profile/ecp/sso"

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.