This is a typical highly available setup into Office 365. Ideally this server will be installed as virtual servers on multiple Hyper-V hosts. Think about redundancy, not only in the virtual servers, but in the Hyper-V servers as well. Install one AD FS and one AD FS Proxy on one Hyper-V host and the other AD FS and AD FS Proxy on another Hyper-V host. This prevents loss of service from a hardware failure. Keep in mind that once you are using Single Sign-on with Office 365, you rely on your local Active Directory for authentication. Both video and printed steps have provided to ease your implementation of AD FS and SSO.

**Prepare the Base Servers**

**AD FS Server**

1. Base build the AD FS server with Windows Server 2012
2. Setup a connection to the internal network
3. Add the server to the local domain
4. Update the server with all Windows Updates

**AD FS Proxy Server**

1. Base Build the AD FS Proxy server with Windows Server 2012
2. Setup a connection to the DMZ network (verify connectivity to the AD FS server on port 443)
3. DO NOT add the server to the local domain
4. Update the server with all Windows Updates

**Directory Sync Server**

1. Base build the Directory Synchronization server with Windows Server 2012
2. Setup a connection to the internal network
3. Add the server to the local domain
4. Update the server with all Windows Updates

**Prepare Active Directory**

Add UPN Suffix

If you are using and internal domain name that doesn’t match the domain that you want to federate with Office 365 you will have to add a custom UPN suffix that matches that external name space. If you need to add the UPN suffix, please follow these instructions, http://www.thatlazyadmin.com/add-upn-suffixes-forest/

Example

Internal Domain Name – contoso.local

Desired Federated Domain – contoso.com

**Clean up Active Directory**

This makes sense for so many reasons, but the most for Directory Sync. I generally make an OU for all the Office 365 Services; then create more OUs within that one for all the user accounts, services accounts, groups, servers and computers. This will allow us to filter on user accounts and groups when we enable Directory Synchronization with Office 365. The less number of objects that you sync with Office 365 is better. If you have thousands of objects replicating, that don’t need to be, things will get messy really quick. Keep it clean and neat. This will prevent mistakes and keep you head ache free.

Setting up AD FS requires the use of a third party SSL certificate. In a production situation, I would recommend that a single name SSL certificate. Wildcard and multi-name certificates will work, but I like to keep things simple and use a standard SSL certificate in a production situation. Make sure that the common name matches what you plan to call the AD FS server farm. Microsoft best practices recommends that you use the host name, STS (secure token service). In the example below, I have used the value *sts.domain.com*.

**Create the SSL Certificate Request (CSR)**

1. Open Server Manager
2. Click Tools
3. Click Internet Information Services (IIS) Manager
4. Select the local server
5. Select Server Certificates
6. Click Open Feature (actions pane)
7. Click Create Certificate Request
8. Fill out the certificate request properties. Make sure that the common name matches what you plan to call the AD FS server farm. Microsoft best practices recommends that you use the host name STS (secure token service). In the example below, I have used the value*sts.domain.com*.
9. Click Next
10. Leave the Cryptographic service provider at the default
11. Change the Bit Length to 2048
12. Click Next
13. Select a location for the request file
14. Click Finish

Fulfill the Certificate Signing Request (CSR)

We need to take the CSR generated in the last step to a third party SSL certificate provider. I choose to use GoDaddy. Here are GoDaddy’s instructions to fulfill the CSR at their site – https://www.godaddy.com/help/request-an-ssl-certificate-deluxe-or-extended-validation-562?locale=en

Once the certificate is issued, download the completed CSR to the AD FS server. A wildcard can be used for other things so I recommend that.

**Complete the Certificate Request (CSR)**

1. Open Server Manager
2. Click Tools
3. Click Internet Information Services (IIS) Manager
4. Select the local server
5. Select Server Certificates
6. Click Open Feature (actions pane)
7. Click Complete Certificate Request
8. Select the path to the complete CSR file that you competed and downloaded from the third party certificate provider
9. Enter the friendly name for the certificate
10. Select Personal as the certificate store
11. Click Ok
12. The certificate will be added

*\*\*\*Note\*\*\* The certificate shown below is a multi-name SSL certificate for my lab environment. When your certificate is added, it should show sts.domain.com, which matches the request.*

Assign the Completed SSL Certificate

Now that we have the third party certificate completed on the server, we need to assign and bind it to the default website (HTTPS port 443).

1. Expand the local server
2. Expand Sites
3. Select Default Web Site
4. Click Bindings (actions pane)
5. Click Add
6. Change the type to HTTPS
7. Select your certificate from the drop down menu.

*\*\*\*Note\*\*\* The certificate shown below is a multi-name SSL certificate for my lab environment. When you select your certificate, it should show sts.domain.com, which matches the competed certificate.*

1. Click OK
2. Click Close
3. Close IIS Manager

Now that we have the required software installed and the certificate in place, we can finally configure the AD FS role and federate with Microsoft.

**Configure Local AD FS Federation Server**

1. Open Server Manager
2. Click Tools
3. Click AD FS Management
4. Click AD FS Federation Server Configuration Wizard
5. Create a new Federation Service
6. New Federation Server Farm – Choose this option all the time, even if you only plan on deploying one server. If you choose Stand-alone federation server, then you won’t be able to add more servers.
7. Click Next
8. SSL Certificate – This should be pre-populated. If it isn’t, go back and assign/bind the third party certificate to the default web site
9. Federation Service Name – This should match the SSL certificate name

\*\*\* NOTE \*\*\* Since I am using a multi-name certificate in a lab environment, my SSL certificate name and Federation Service name don’t match. This is not recommended for production environments. Use best practices always; a single name certificate.

1. Click Next
2. Enter the AD FS service account name and password
3. Click Next
4. Click Next
5. All green check marks mean everything is setup correctly
6. Click Close

**Configure Federation Trust with Office 365**

Now that we have our side of the federation setup, we can complete the federation with Office 365

* Open the Desktop on the AD FS server
* Windows Azure Active Directory Module for Windows PowerShell
* Right Click and Run As Administrator
* Set the credential variable
  + *$cred=Get-Credential*
* Enter a Global Administrator account from Office 365. I have a dedicated tenant (@domain.onmicrosoft.com) service account setup for AD FS and Directory Syncronization.
* Connect to Microsoft Online Services with the credential variable set previously
  + *Connect-MsolService –Credential $cred*
* Set the MSOL ADFS Context server, to the ADFS server
  + *Set-MsolADFSContext –Computer adfs\_servername.domain\_name.com*
* Convert the domain to a federated domain
  + *Convert-MsolDomainToFederated –DomainName domain\_name.com*
* Successful Federation
  + *Successfully updated ‘domain\_name.com‘ domain.*
* Verify federation
  + *Get-MsolFederationProperty –DomainName domain\_name.com*

This completes the setup for federation to Office 365. Keep in mind that before you can successfully use single sign-on with Office 365, you will need to setup and configure Directory Synchronization. After Directory Synchronization is setup, you will have to license the synchronized user in Office 365. This will provision the services for the user. If they want to access Office 365 from outside the internal network, the AD FS Proxy server needs to be setup and configured.