User Guide - ADFS and ADFS Proxy Installation and Configuration for O365 Hybrid deployment

Prepared by:
Vodafone Shared Services Limited

This document is meant for Vodafone cloud customers only and is confidential & legally privileged. Please do not reproduce copy or disclose this document or its contents with any third party/ies nor use it for purposes other than this document has been shared for.
Contents

Introduction – Active Directory Federation Services (ADFS) ................................................................. 3
Installing ADFS on Windows Server 2012 R2 .......................................................................................... 4
  ➢ Configure Windows NLB .................................................................................................................. 4
  ➢ Installing the ADFS Role on NODE (server) 1 .............................................................................. 4
Configuration of ADFS services .............................................................................................................. 10
  ➢ Installing the ADFS Role NODE (server) 2 .................................................................................. 15
Verifying the Federation Server farm is working properly: ................................................................. 16
Installing ADFS Proxy on Windows Server 2012 R2 ............................................................................. 18
  ➢ Configure Windows NLB ................................................................................................................ 18
  ➢ Installing the ADFS proxy Role in NODE 1: .............................................................................. 18
  ➢ Configuration of WAP (ADFS Proxy service) on NODE 1: .......................................................... 22
  ➢ Installing the ADFS proxy Role in NODE 2 .............................................................................. 26
  ➢ Configuration of WAP (ADFS Proxy service) on NODE 2: .......................................................... 26
Introduction – Active Directory Federation Services (ADFS)

ADFS is the primary choice for customers who want to use federated identities with Office 365. Since the availability of Office 365 relies upon the availability of ADFS when the domain is federated there is a strong recommendation to have at least two ADFS servers with a redundant ADFS proxy infrastructure. The act of deploying and configuring ADFS 2012 R2 for Office 365 will be broken down into three separate sections:

1. Install ADFS
2. Install ADFS Proxy
3. Leverage ADFS with Office 365

The ADFS role should be deployed within the corporate network, and not in the DMZ. The ADFS proxy role is intended to be installed into the DMZ.

Pre-requisites:

Require Following:

- ADFS Service account (No password Expiry)
- Domain admin account to configure the ADFS.
- Local Admin Account for ADFS Proxy server configuration.
- Wildcard certificate or the SAN certificates to be imported into the ADFS and ADFS proxy servers.
- Internet connectivity to ADFS Proxy Servers.
- Windows NLB to be configured for both ADFS and ADFS proxy servers.
Installing ADFS on Windows Server 2012 R2

Configure Windows NLB

Configure Windows Network Load Balancer (NLB) for ADFS Proxy servers. Post that you can follow below steps for ADFS Proxy role installation and configuration

Installing the ADFS Role on NODE (server) 1

Login to the ADFS server with Domain admin Credentials, Open Server Manager-> Add roles and Features

Click NEXT
Select as shown above and click **Next**.
Select destination server

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
- Select a virtual hard disk

Server Pool

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Microsoft Windows Server 2012 R2 Standard</td>
</tr>
</tbody>
</table>

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
Select the **Active Directory Federation Services** as shown above and hit **NEXT**.
Add Roles and Features Wizard

Select features

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD FS
Confirmation
Results

Select one or more features to install on the selected server.

Features
- .NET Framework 3.5 Features (1 of 3 installed)
- .NET Framework 4.5 Features (2 of 7 installed)
- Background Intelligent Transfer Service (BITS)
- BitLocker Drive Encryption
- BitLocker Network Unlock
- BranchCache
- Client for NFS
- Data Center Bridging
- Direct Play
- Enhanced Storage
- Failover Clustering
- Group Policy Management
- IIS Hostable Web Core
- Ink and Handwriting Services

Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
Active Directory Federation Services (AD FS)

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD FS
Confirmation
Results

Active Directory Federation Services (AD FS) provides Web single-sign-on (SSO) capabilities to authenticate a user to multiple Web applications using a single user account. AD FS helps organizations bypass the need for secondary accounts by allowing you to project a user’s digital identity and access rights to trusted partners. In this federated environment, each organization continues to manage its own identities.

Things to note:

• This computer must be joined to a domain before you can successfully install the Federation Service.

• The Web Application Proxy role service in the Remote Access server role functions as the federation service proxy and cannot be installed on the same computer as the federation service.

Confirm installation selections

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD FS
Confirmation
Results

To install the following roles, role services, or features on selected server, click Install.

- Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Federation Services

Export configuration settings
Specify an alternate source path
Thus Installation is completed.

**Configuration of ADFS services**

On Node 1, post installation Click on “Configure the federation service on this server” to start the configuration.
An Organization may have a Wildcard certificate, Import it on Both ADFS and ADFS Proxy Servers.

If certificate is not imported, it will show a Blank List in below Step.

(Here we are considering the Installation through Wildcard certificate)

Provide the **Federation service Name** which has a suffix same as that of your Wildcard certificate.

The **Federation service Display Name**: It can be given any name as it will be the Name which user will view on the ADFS login page.

Example:

- SSL certificate name is: `*.abcservices.com`
- Federation Service Name should be: `<AnyName>.abcservices.com`
  
  *Eg: adfs.abcservices.com*
- Federation Service Display Name: `<AnyName>`
  
  *Eg: ABCSERVICESGroup*
Provide the **ADFS service account** as shown below and click **Next**.
Specify Service Account

Group Managed Service Accounts are not available because the KDS Root Key has not been set. Use the foll... Show more

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Specify a domain user account or group Managed Service Account.

Create a Group Managed Service Account

Account Name: [Redacted]

Use an existing domain user account or group Managed Service Account

Account Name: [Redacted]
Account Password: [Redacted]

< Previous  Next >  Configure  Cancel

Specify Configuration Database

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Specify a database to store the Active Directory Federation Service configuration data.

Create a database on this server using Windows Internal Database.
Specify the location of a SQL Server database.

Database Host Name: [Redacted]
Database Instance: [Redacted]

To use the default instance, leave this field blank.

< Previous  Next >  Configure  Cancel
Click On **Configure**
Installing the ADFS Role NODE (server) 2

Similarly Install the ADFS role on Node 2 and configure as shown be:

Now, We have to add the Node 2 ADFS server in the existing federation Farm:

Post Installation of Role, ADD node 2 into the existing federation Farm:
Provide the same federation server name, Click NEXT and complete the configuration

Verifying the Federation Server farm is working properly:

- https://<adfs_server_FQDN>/FederationMetadata/2007-06/FederationMetadata.xml
- In event Viewer open the AD FS Admin log and look for event 100
Installing ADFS Proxy on Windows Server 2012 R2

- Configure Windows NLB

Configure Windows Network Load Balancer (NLB) for ADFS Proxy servers. Post that you can follow below steps for ADFS Proxy role installation and configuration

- Installing the ADFS proxy Role in NODE 1:
Before you begin

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:
* The Administrator account has a strong password
* Network settings, such as static IP addresses, are configured
* The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

Select destination server

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
- Select a virtual hard disk

Server Pool

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Deploy DirectAccess to allow managed domain-joined computers to connect to the internal corporate network as DirectAccess clients. Connectivity is seamless and transparent, and is available any time client computers are located on the Internet. DirectAccess administrators can remotely manage clients, ensuring that mobile computers are kept up-to-date with security updates and corporate compliance requirements.

Deploy VPN to allow client computers running operating systems not supported by DirectAccess, or configured in a workgroup, to remotely access corporate networks over a VPN connection.

Deploy Web Application Proxy to publish selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. It can use AD FS to ensure that users are authenticated before they gain access to published applications. Web Application Proxy also provides proxy functionality for your AD FS servers.

Configure RRAS routing features using the Routing and Remote Access console.
Add Roles and Features Wizard

Add features that are required for Web Application Proxy?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Group Policy Management
- RAS Connection Manager Administration Kit (CMAK)
- Remote Server Administration Tools
- Role Administration Tools
- Remote Access Management Tools

Include management tools (if applicable)

Add Features
Cancel

Select role services

Select the role services to install for Remote Access

- [ ] DirectAccess and VPN (RAS)
- [ ] Routing
- [√] Web Application Proxy

Description
Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. It can use AD FS to ensure that users are authenticated before they gain access to published applications. Web Application Proxy also provides proxy functionality for your AD FS servers.
Configuration of WAP (ADFS Proxy service) on NODE 1:

- First Make a host entry for NLB IP of ADFS Service.
- Then, Navigate to Server Manager -> top right corner -> notification -> Click to configure the ADFS proxy (WAP) Service.

- Enter the Federation Service Name and the Local Admin Account of ADFS Proxy Server:
  - For Example: here we have created a local admin account named O365svc
Select the Wild Card Certificate:
Thus we have configured with WAP.
Installing the ADFS proxy Role in NODE 2
Similarly Install the Role on NODE 2 of ADFS Proxy Server

Configuration of WAP (ADFS Proxy service) on NODE 2:
Similarly Configure ADFS proxy services (WAP) on NODE 2 of ADFS Proxy Farm.

(NOTE: Publish the ADFS Proxy server using the NLB IP on the Public Domain through ISP provider. And for ADFS server Create a A record in Local DNS server using the NLB IP of ADFS Server)

Verify ADFS Proxy Configuration:
  • open the AD FS Admin log and look for event 100
Verify Federation Service Metadata:

This URL identifies whether the ADFS is configured.

https://<federation Service name>/federationmetadata/2007-06/federationmetadata.xml

Example: https://adfs.abcservices.com/federationmetadata/2007-06/federationmetadata.xml

Verify ADFS Sign-In Page:

The below URL is used to check whether the user is able to get the ADFS sign in page

https://<Federation service name>/adfs/ls/idpinitiatedsignon.htm

Example: https://adfs.abcservices.com/adfs/ls/idpinitiatedsignon.htm
Reference Links:


http://blogs.catapultsystems.com/smcneill/archive/2014/01/04/setting-up-adfs-3-0-server-2012-r2-for-office-365/