2019

Windows Virtual Desktop ADFS\SSO

INTERNAL FACING

JOHN JENNER

Contents

Windows Virtual Desktop and ADFS \WAP\CA SSO

The following guide describes the process for you to set up single sign-on for end-users connecting to resources in a Windows Virtual Desktop modern infrastructure (WVD) environment. In this single-sign on flow, the end-users authenticate to Azure AD when subscribing to their feed but then do not face any other credential prompts as they select their remote desktop or RemoteApp and establish their connection. The assumption is the environment being modified for ADFS has been successfully configured for managed authentication and is reporting no critical errors.

Pre-requisites

To configure single sign-on, there are several requirements of the end-user environment:

- Certificate Authority Server – Domain joined – Not covered in this document (Enterprise CA Root)
- ADFS Server – Domain joined and up to date
- Web Access Proxy Server – Domain joined and up to date
- Wildcard Certificate – Not covered here
- Latest version of AD Connect installed on your Domain Controller

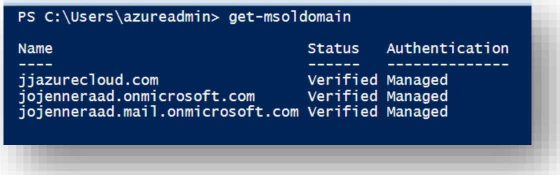
Assumptions

- There is an already configured Active Directory configured with AD Connect syncing to Azure AD
- All Servers are patched and up to date
- You are using the latest version of AD Connect. This is crucial as older versions will not implement or configure all appropriate settings for this solution.
- You have a custom domain and wildcard or SSL certificate
- Certificate Authority Server is already configured
- Access to the registrar where the custom domain is hosted

Quick Check of your current MSOL environment

Make sure your AD Connect Server has the below installed, if not go ahead and prep it out as its good practice to have this all setup in the event you need to redo ADFS in the future or remove it. Can you achieve this is a much simpler way? Yes you can but I like to be prepared 😊

```
# install this on the AD Connect Box (Domain Controller)
# https://www.microsoft.com/en-us/download/details.aspx?id=41950
# Install-Module AzureAD
# Install-Module MSOnline
# Connect-AzureAD
```



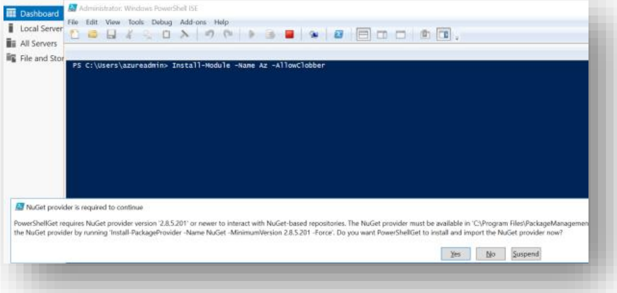
```
PS C:\Users\azureadmin> get-msoldomain

Name                              Status   Authentication
----                              ------   --------------
jjazurecloud.com                  Verified Managed
jojenneraad.onmicrosoft.com       Verified Managed
jojenneraad.mail.onmicrosoft.com  Verified Managed
```

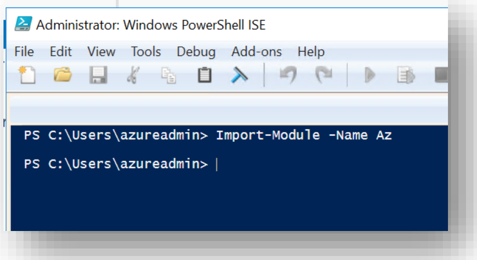
From elevated PS on your Domain Controller with Ad Connect Installed run get-msoldomain after you connect.

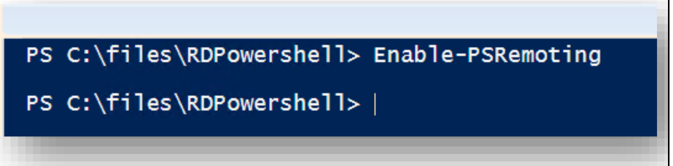
This is all you need to do for verification.

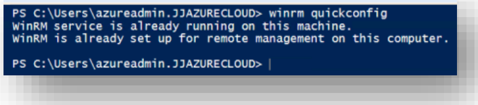
Prep your ADFS Windows 2016 Server

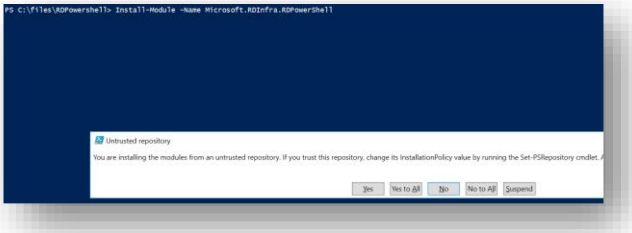
The assumption is you have built a Windows 2016 Server, patched it to current levels and it has been added to the domain. Turn off IE Enhanced mode and the Firewall (turn it back on later). In the Azure Portal make sure to set the local IP for your ADFS server to static.

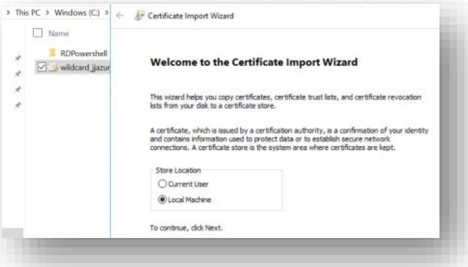
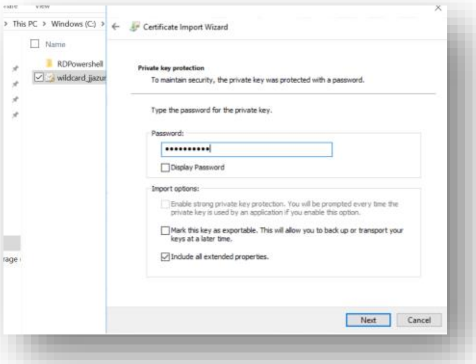
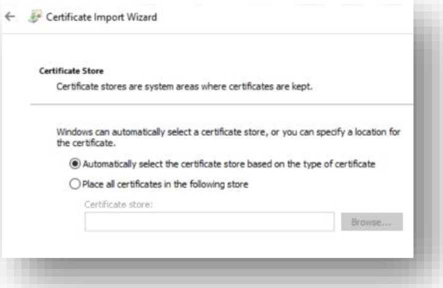
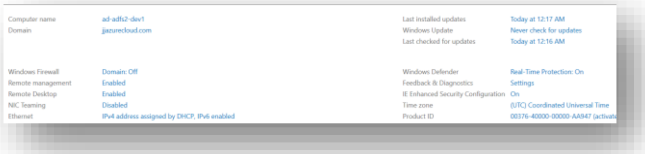
PowerShell Module Installs: Install-Module -Name AZ -AllowClobber	 Dashboard Local Server All Servers File and Stor Administrator: Windows PowerShell ISE File Edit View Tools Debug Add-ons Help `PS C:\Users\azureadmin> Install-Module -Name Az -AllowClobber` NuGet provider is required to continue PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet provider must be available in 'C:\Program Files\PackageManagemen the NuGet provider by running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import the NuGet provider now?


 Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
`PS C:\Users\azureadmin> Import-Module -Name Az`
`PS C:\Users\azureadmin>`
	Import-Module -Name AZ

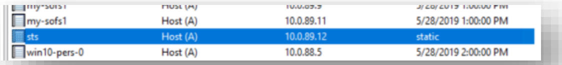
Enable-PSRemoting	
	`PS C:\files\RDPowershell> Enable-PSRemoting`
	`PS C:\files\RDPowershell>`


`PS C:\Users\azureadmin.JJAZURECLOUD> winrm quickconfig`
`WinRM service is already running on this machine.`
`WinRM is already set up for remote management on this computer.`
`PS C:\Users\azureadmin.JJAZURECLOUD>`
	Winrm Quickconfig

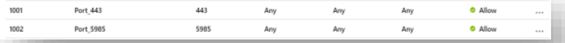
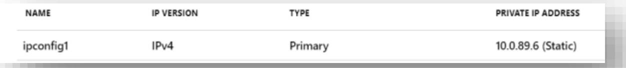
Install-Module -Name Microsoft.RDInfra.RDPowerShell Yes to All	 `PS C:\files\RDPowershell> Install-Module -Name Microsoft.RDInfra.RDPowerShell` Untrusted repository You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy value by running the Set-PSRepository cmdlet. A

 This PC › Windows (C:) › Certificate Import Wizard □ Name RDPowershell ☑ wildcard_jjazur **Welcome to the Certificate Import Wizard** This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. Store Location ○ Current User ● Local Machine To continue, click Next.	Install your wildcard cert on the **ADFS server and WAP Server**. Right click your certificate and install or open up MMC and add Cert Snap-in and follow that method. Make sure to put it in Local Machine. Also make sure the certificate is in both **Personal and Trusted Root Certificate Authority.**
Password input	 This PC › Windows (C:) › Certificate Import Wizard □ Name RDPowershell ☑ wildcard_jjazur **Private key protection** To maintain security, the private key was protected with a password. Type the password for the private key. Password: •••••••••• □ Display Password Import options: □ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option. □ Mark this key as exportable. This will allow you to back up or transport your keys at a later time. ☑ Include all extended properties. Next Cancel
 Certificate Import Wizard **Certificate Store** Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate. ● Automatically select the certificate store based on the type of certificate ○ Place all certificates in the following store Certificate store: Browse...	Take defaults
Turn off Firewall and IE enhanced if not already done so.	 Computer name ad-adfs2-dev1 Domain jjazurecloud.com Last installed updates Today at 12:17 AM Windows Update Never check for updates Last checked for updates Today at 12:16 AM Windows Firewall Domain: Off Remote management Enabled Remote Desktop Enabled NIC Teaming Disabled Ethernet IPv4 address assigned by DHCP, IPv6 enabled Windows Defender Real-Time Protection: On Feedback & Diagnostics Settings IE Enhanced Security Configuration On Time zone (UTC) Coordinated Universal Time Product ID 00376-40000-00000-AA947 (activate

Add DNS Entry for ADFS

Add DNS entry for this ADFS server ‘A record’ for local ip to ADFS Service name you are going to use. In most practical cases this is called ‘STS’ so for example sts.jjazurecloud.com	 my-sofs1 Host (A) 10.0.89.9 5/28/2019 1:00:00 PM my-sofs1 Host (A) 10.0.89.11 5/28/2019 1:00:00 PM sts Host (A) 10.0.89.12 static win10-pers-0 Host (A) 10.0.88.5 5/28/2019 2:00:00 PM

Set NSG inbound Rules for ADFS and WAP

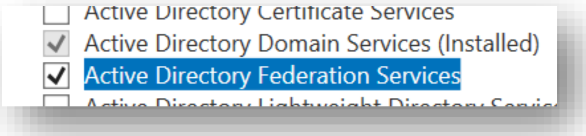
Add 443 inbound Add 5985 inbound	 1001 Port_443 443 Any Any Any Allow ... 1002 Port_5985 5985 Any Any Any Allow ...
Make sure your local IPs are static!	 NAME IP VERSION TYPE PRIVATE IP ADDRESS ipconfig1 IPv4 Primary 10.0.89.6 (Static)

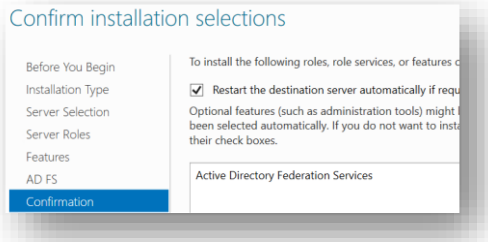
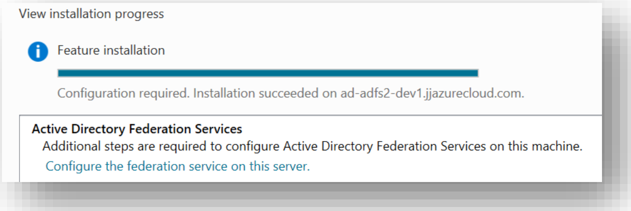
Windows Virtual Desktop PowerShell Script

Download or copy the following file to your ADFS server as you will need this file later.

https://www.powershellgallery.com/packages/ConfigureWVDSSO

Install the ADFS Role

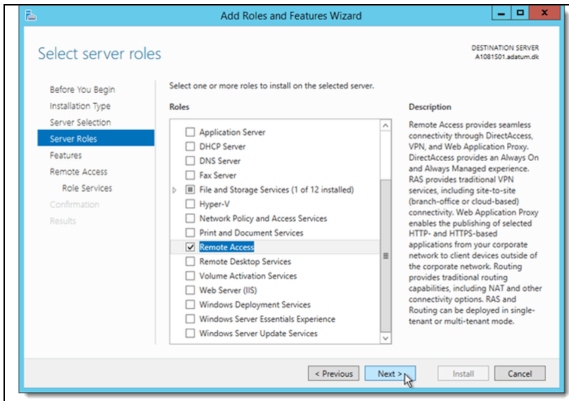
 □ Active Directory Certificate Services ☑ Active Directory Domain Services (Installed) ☑ Active Directory Federation Services □ Active Directory Lightweight Directory Servic	Select Active Directory Federation Services

Check restart if required.	 Confirm installation selections Before You Begin Installation Type Server Selection Server Roles Features AD FS Confirmation To install the following roles, role services, or features o ☑ Restart the destination server automatically if requ Optional features (such as administration tools) might b been selected automatically. If you do not want to insta their check boxes. Active Directory Federation Services
 View installation progress Feature installation Configuration required. Installation succeeded on ad-adfs2-dev1.jjazurecloud.com. Active Directory Federation Services Additional steps are required to configure Active Directory Federation Services on this machine. Configure the federation service on this server.	Stop here, you do not need to configure ADFS, we are going to let AD Connect do the lifting. Reboot the server if it was not rebooted automatically.

Prep your Web Application Proxy Server

The assumption is you have built a Windows 2016 Server, patched it to current levels and it has been added to the domain. Turn off IE Enhanced mode and the Firewall (turn it back on later). In the Azure Portal make sure to set the local IP for your ADFS server to static.

<table>
<tr>
<td>



Select server roles

DESTINATION SERVER
A1081S01.adatum.dk

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

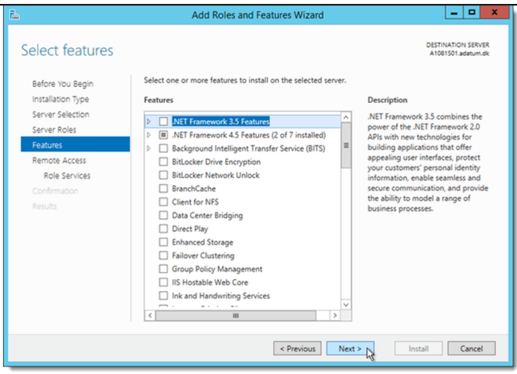
Roles

- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☑ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Essentials Experience
- ☐ Windows Server Update Services

Description

Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. 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. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.

</td>
<td>Add Roles and select ‘Remote Access’</td>
</tr>
<tr>
<td>Take defaults</td>
<td>



Select features

DESTINATION SERVER
A1081S01.adatum.dk

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

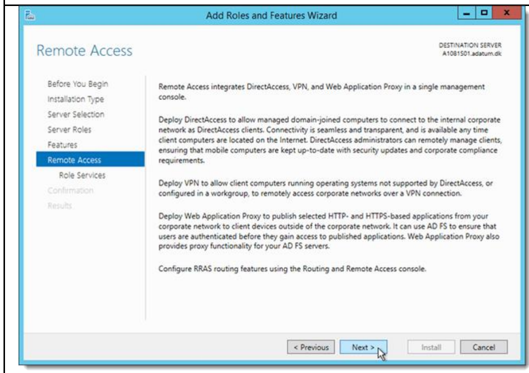
Features

- ☐ .NET Framework 3.5 Features
- ▣ .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.

</td>
</tr>
<tr>
<td>



Remote Access

DESTINATION SERVER
A1081S01.adatum.dk

Remote Access integrates DirectAccess, VPN, and Web Application Proxy in a single management console.

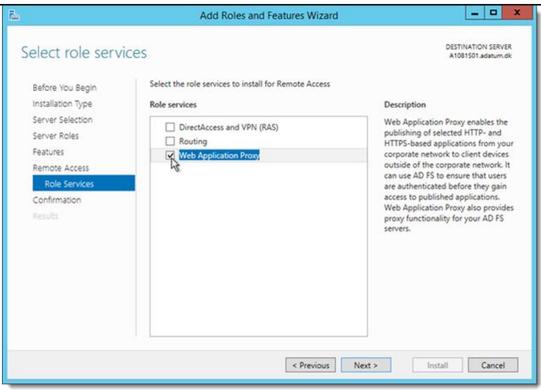
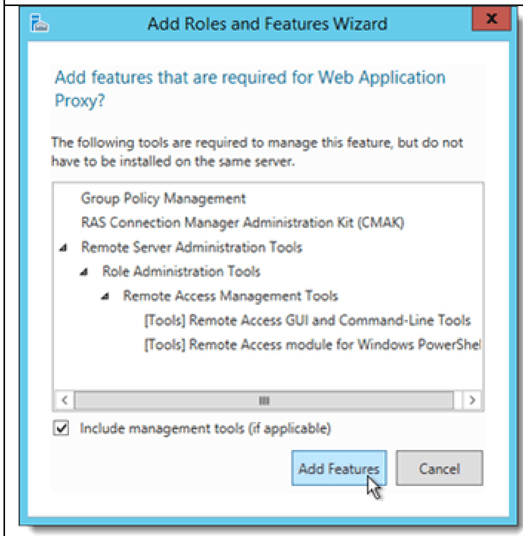
Deploy DirectAccess to allow managed domain-joined computers to connect to the internal corporate network as DirectAccess clients. Connectivity is seamless and transparent, and is available any time client computers are located on the Internet. DirectAccess administrators can remotely manage clients, 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.

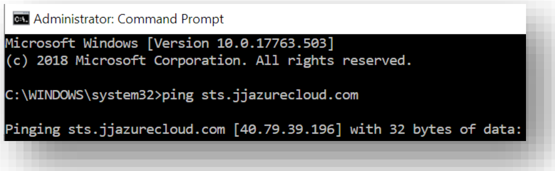
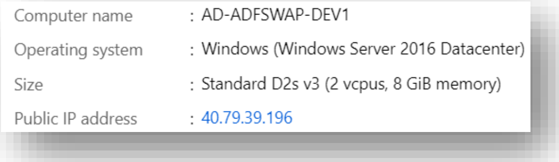
Deploy Web Application Proxy to publish selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. It can use AD FS to ensure that users are authenticated before they gain access to published applications. Web Application Proxy also provides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

Configure RRAS routing features using the Routing and Remote Access console.

</td>
<td>Defaults</td>
</tr>
</table>

Select 'Web Application Proxy'	 Add Roles and Features Wizard Select role services DESTINATION SERVER A1081S01.adatum.dk Before You Begin Installation Type Server Selection Server Roles Features Remote Access Role Services Confirmation Results Select the role services to install for Remote Access Role services ☐ 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. < Previous Next > Install Cancel
 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 [Tools] Remote Access GUI and Command-Line Tools [Tools] Remote Access module for Windows PowerShel ☑ Include management tools (if applicable) Add Features Cancel	Add Features and **STOP**. This is all you need to do.

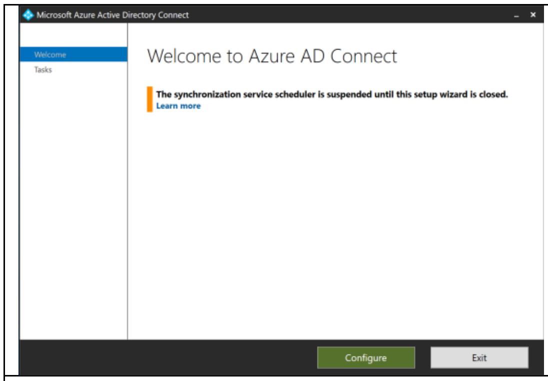
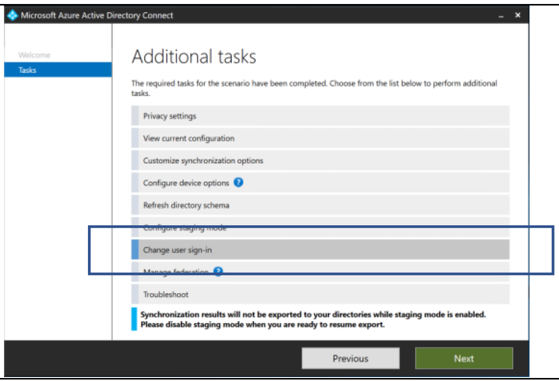
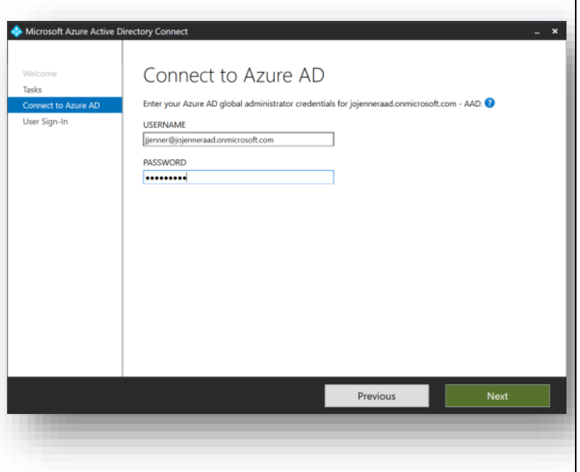
The Public IP of your WAP should also be a entry in your custom domain registrar and point to your ADFS service name. For example, **sts**.jjazurecloud.com should resolve to the public IP of your WAP server.

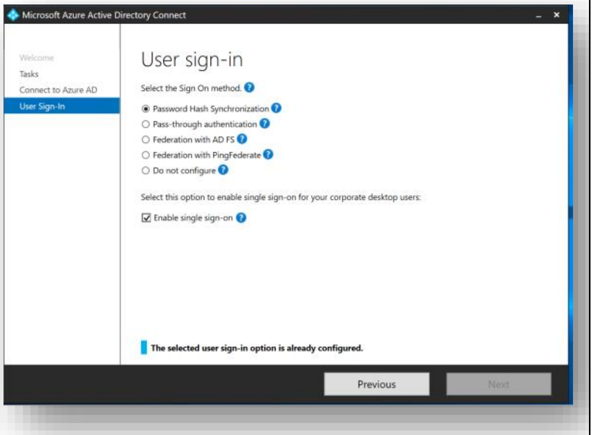
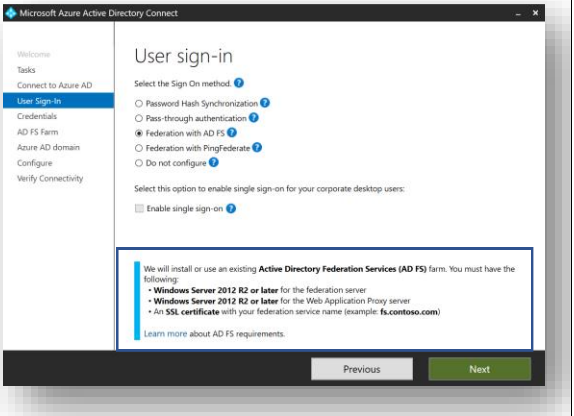
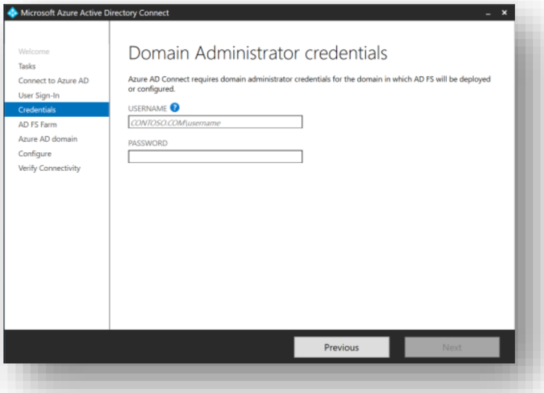

Administrator: Command Prompt
`Microsoft Windows [Version 10.0.17763.503]`
`(c) 2018 Microsoft Corporation. All rights reserved.`
 	
`C:\WINDOWS\system32>ping sts.jjazurecloud.com`
 	
`Pinging sts.jjazurecloud.com [40.79.39.196] with 32 bytes of data:`
	
	Computer name : AD-ADFSWAP-DEV1
	Operating system : Windows (Windows Server 2016 Datacenter)
	Size : Standard D2s v3 (2 vcpus, 8 GiB memory)
	Public IP address : 40.79.39.196

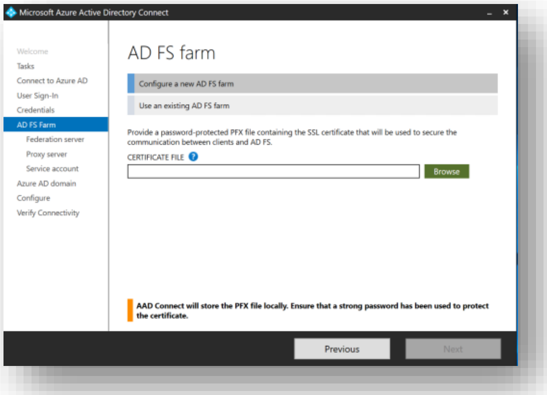
Summary - One

We have built two servers (ADFS and WAP). We prepped both servers and installed the roles on them. We added the proper PowerShell Modules for administration and we created an internal DNS record for the name you are going to use for ADFS service name (STS), in my case sts.jjazurecloud.com and pointed it to the private IP of your ADFS server. At this point we are ready to use AD Connect to create\configure the ADFS Farm, trust and WAP.

AD Connect Configuration for ADFS\WAP

 Microsoft Azure Active Directory Connect Welcome Tasks Configure Exit Welcome to Azure AD Connect **The synchronization service scheduler is suspended until this setup wizard is closed.** **Learn more**	Launch AD Connect from the domain controller.
Select 'Change User Sign-in'	 Microsoft Azure Active Directory Connect Welcome Tasks Previous Next Additional tasks The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks. Privacy settings View current configuration Customize synchronization options Configure device options Refresh directory schema Configure staging mode Change user sign-in Manage federation Troubleshoot **Synchronization results will not be exported to your directories while staging mode is enabled. Please disable staging mode when you are ready to resume export.**
 Microsoft Azure Active Directory Connect Welcome Tasks Connect to Azure AD User Sign-In Previous Next Connect to Azure AD Enter your Azure AD global administrator credentials for jojenneraad.onmicrosoft.com - AAD. USERNAME jjenner@jojenneraad.onmicrosoft.com PASSWORD •••••••••	Fill in the credentials needed.

This should reflect the current working setup. We are going to change from Password Hash to Federation.	 Microsoft Azure Active Directory Connect Welcome Tasks Connect to Azure AD User Sign-In Previous Next User sign-in Select the Sign On method. ● Password Hash Synchronization ○ Pass-through authentication ○ Federation with AD FS ○ Federation with PingFederate ○ Do not configure Select this option to enable single sign-on for your corporate desktop users: ☑ Enable single sign-on **The selected user sign-in option is already configured.**
 Microsoft Azure Active Directory Connect Welcome Tasks Connect to Azure AD User Sign-In Credentials AD FS Farm Azure AD domain Configure Verify Connectivity Previous Next User sign-in Select the Sign On method. ○ Password Hash Synchronization ○ Pass-through authentication ● Federation with AD FS ○ Federation with PingFederate ○ Do not configure Select this option to enable single sign-on for your corporate desktop users: □ Enable single sign-on We will install or use an existing **Active Directory Federation Services (AD FS)** farm. You must have the following: • **Windows Server 2012 R2 or later** for the federation server • **Windows Server 2012 R2 or later** for the Web Application Proxy server • An **SSL certificate** with your federation service name (example: **fs.contoso.com**) Learn more about AD FS requirements.	Please select Federation with ADFS and note the below statements.
Login with your AD credentials here.	 Microsoft Azure Active Directory Connect Welcome Tasks Connect to Azure AD User Sign-In Credentials AD FS Farm Azure AD domain Configure Verify Connectivity Previous Next Domain Administrator credentials Azure AD Connect requires domain administrator credentials for the domain in which AD FS will be deployed or configured. USERNAME *CONTOSO.COM\username* PASSWORD



AD FS farm

Configure a new AD FS farm

Use an existing AD FS farm

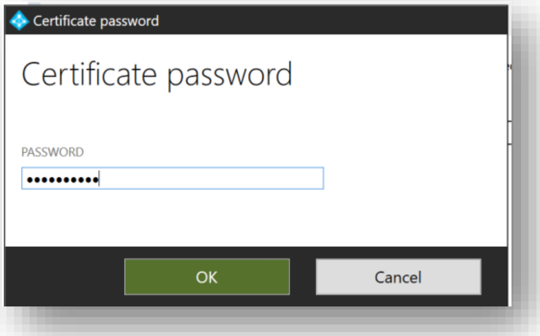
Provide a password-protected PFX file containing the SSL certificate that will be used to secure the communication between clients and AD FS.

CERTIFICATE FILE

AAD Connect will store the PFX file locally. Ensure that a strong password has been used to protect the certificate.

Browse to your Certificate file and I hope you have the password handy. This might seem redundant since we installed the certificate already in previous steps however this step is taking the certificate and tying it to your ADFS Farm.

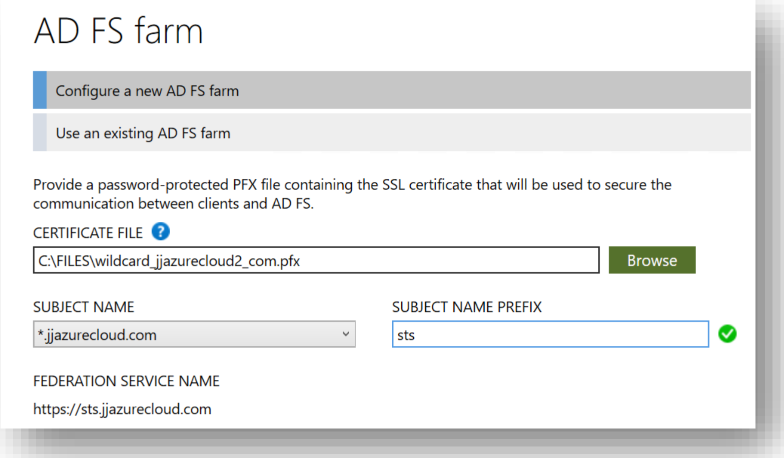
Password for your certificate



Certificate password

PASSWORD

••••••••••



AD FS farm

Configure a new AD FS farm

Use an existing AD FS farm

Provide a password-protected PFX file containing the SSL certificate that will be used to secure the communication between clients and AD FS.

CERTIFICATE FILE

C:\FILES\wildcard_jjazurecloud2_com.pfx

SUBJECT NAME

*.jjazurecloud.com

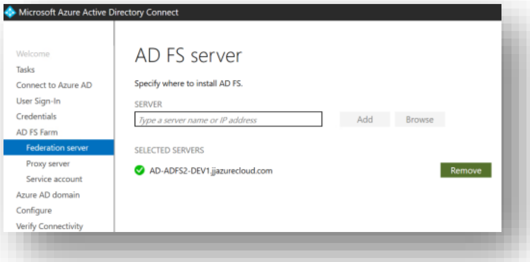
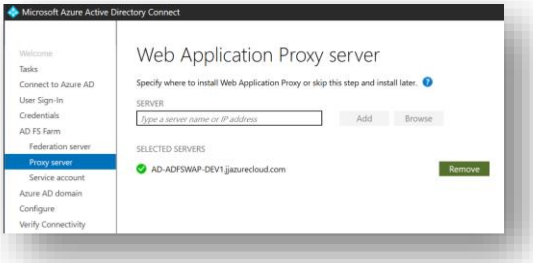
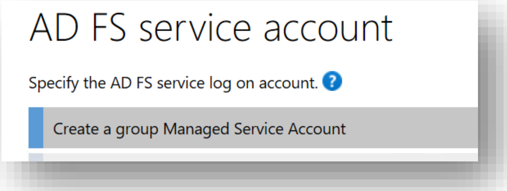
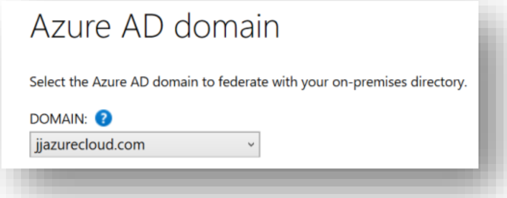
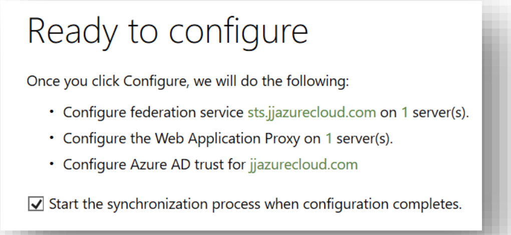
SUBJECT NAME PREFIX

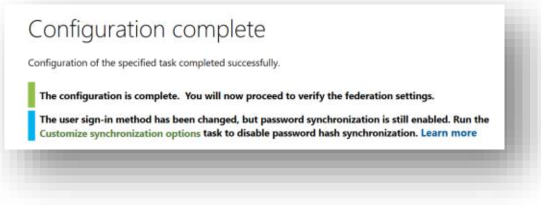
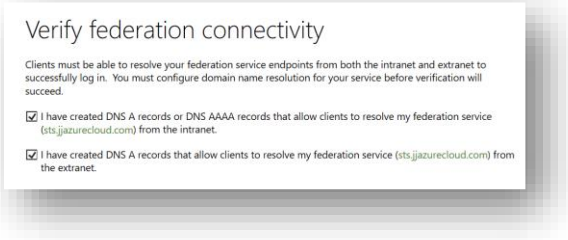
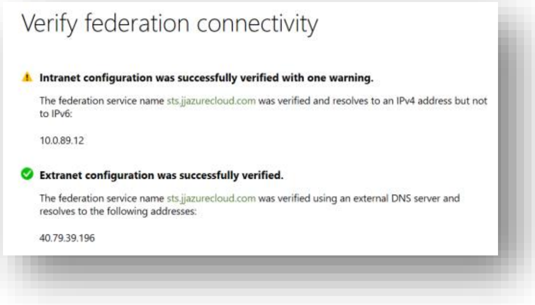
sts ✓

FEDERATION SERVICE NAME

https://sts.jjazurecloud.com

The Subject name drop down should have two options displayed. If using a wildcard certificate, select the *. Otherwise, select the other one per domain SSL. Subject name please use STS.

 Microsoft Azure Active Directory Connect Welcome Tasks Connect to Azure AD User Sign-In Credentials AD FS Farm Federation server Proxy server Service account Azure AD domain Configure Verify Connectivity AD FS server Specify where to install AD FS. SERVER Type a server name or IP address SELECTED SERVERS ✓ AD-ADFS2-DEV1.jjazurecloud.com 	Add your IP or FQDN of your ADFS server
Add your IP or FQDN of your WAP server	 Microsoft Azure Active Directory Connect Welcome Tasks Connect to Azure AD User Sign-In Credentials AD FS Farm Federation server Proxy server Service account Azure AD domain Configure Verify Connectivity Web Application Proxy server Specify where to install Web Application Proxy or skip this step and install later. SERVER Type a server name or IP address SELECTED SERVERS ✓ AD-ADFSWAP-DEV1.jjazurecloud.com
 AD FS service account Specify the AD FS service log on account. Create a group Managed Service Account	You have three options on this screen, choose Managed Service Account as that is best practice.
Select your domain from the drop-down	 Azure AD domain Select the Azure AD domain to federate with your on-premises directory. DOMAIN: jjazurecloud.com
 Ready to configure Once you click Configure, we will do the following: • Configure federation service sts.jjazurecloud.com on 1 server(s). • Configure the Web Application Proxy on 1 server(s). • Configure Azure AD trust for jjazurecloud.com ☑ Start the synchronization process when configuration completes.	Review the details before clicking.

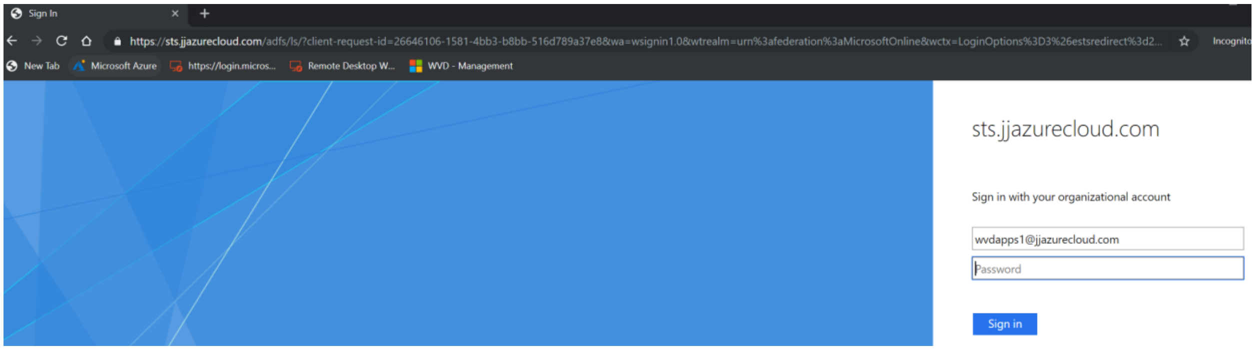
Configuration is complete	 Configuration complete Configuration of the specified task completed successfully. **The configuration is complete. You will now proceed to verify the federation settings.** **The user sign-in method has been changed, but password synchronization is still enabled. Run the Customize synchronization options task to disable password hash synchronization. Learn more**
 Verify federation connectivity Clients must be able to resolve your federation service endpoints from both the intranet and extranet to successfully log in. You must configure domain name resolution for your service before verification will succeed. ☑ I have created DNS A records or DNS AAAA records that allow clients to resolve my federation service (sts.jjazurecloud.com) from the intranet. ☑ I have created DNS A records that allow clients to resolve my federation service (sts.jjazurecloud.com) from the extranet.	Make sure to check off both boxes, by default only the top box is selected.
You should see this picture if everything was configured correctly. You can ignore the IP6 warning. The most important piece here is the extranet GREEN check!	 Verify federation connectivity ⚠ **Intranet configuration was successfully verified with one warning.** The federation service name sts.jjazurecloud.com was verified and resolves to an IPv4 address but not to IPv6: 10.0.89.12 ✓ **Extranet configuration was successfully verified.** The federation service name sts.jjazurecloud.com was verified using an external DNS server and resolves to the following addresses: 40.79.39.196

Validate your ADFS setup

We can validate the ADFS setup in a few ways. I will cover a few of them here to make sure we are sure it is working.

Open a browser and login to the below url with a synced account that is in your AD\AAD any synced.

https://login.microsoftonline.com



https://sts.jjazurecloud.com/adfs/ls/?client-request-id=26646106-1581-4bb3-b8bb-516d789a37e8&wa=wsignin1.0&wtrealm=urn%3afederation%3aMicrosoftOnline&wctx=LoginOptions%3D3%26estsredirect%3d2...

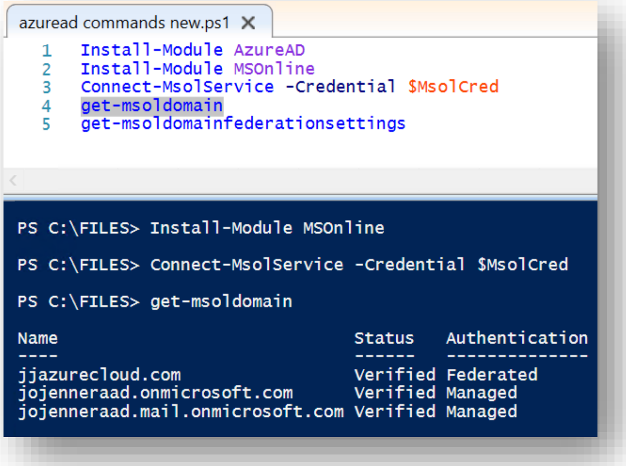
sts.jjazurecloud.com

Sign in with your organizational account

wvdapps1@jjazurecloud.com

Password

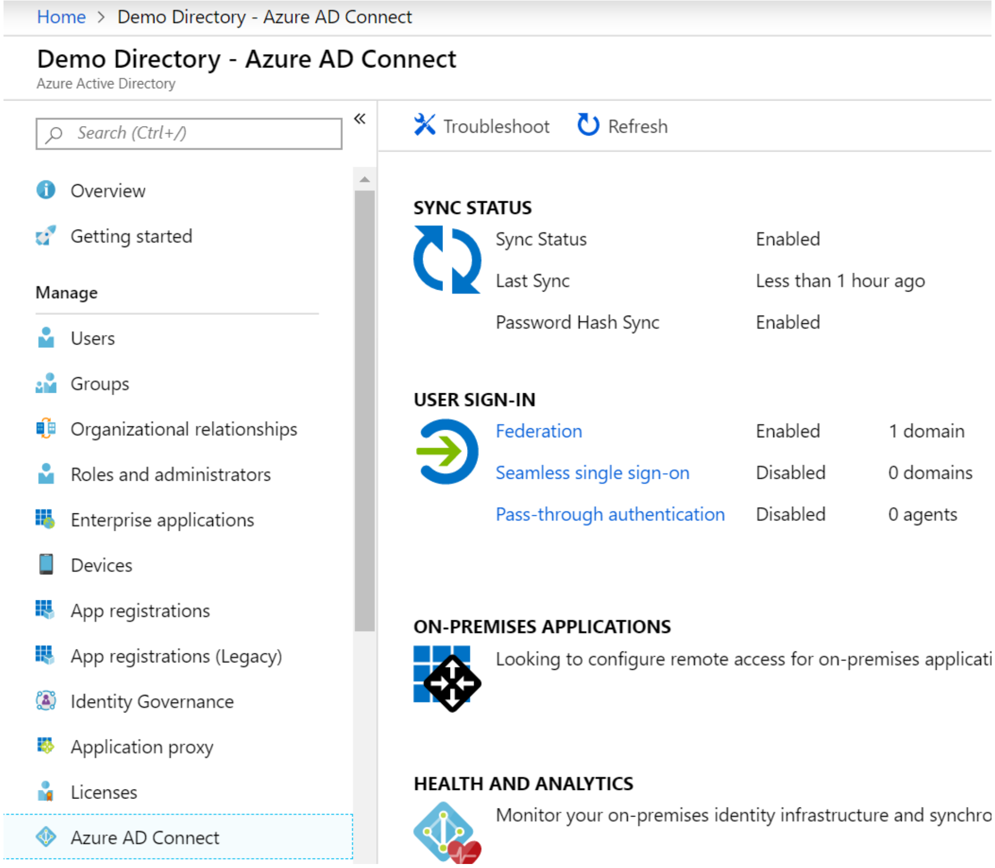
You can also check from your PowerShell, Federated should now be seen for the domain



```
Install-Module AzureAD
Install-Module MSOnline
Connect-MsolService -Credential $MsolCred
get-msoldomain
get-msoldomainfederationsettings
```

```
PS C:\FILES> Install-Module MSOnline

PS C:\FILES> Connect-MsolService -Credential $MsolCred

PS C:\FILES> get-msoldomain

Name                               Status   Authentication
----                               ------   --------------
jjazurecloud.com                   Verified Federated
jojenneraad.onmicrosoft.com        Verified Managed
jojenneraad.mail.onmicrosoft.com Verified Managed
```

In the Azure Portal you can view the User Sign-In setting below,



Demo Directory - Azure AD Connect
Azure Active Directory

SYNC STATUS

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Enabled	1 domain
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Disabled	0 agents

ON-PREMISES APPLICATIONS

Looking to configure remote access for on-premises applicati

HEALTH AND ANALYTICS

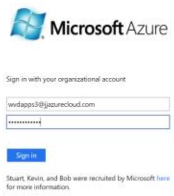
Monitor your on-premises identity infrastructure and synchro

If you want to brand your STS screens, you can use the below as an example.

```
Set-AdfsWebTheme -TargetName default -Illustration @{path="c:\Files\ADFS-illust.jpg"}
```

```
Set-AdfsWebTheme -TargetName default -Logo @{path="c:\Files\azure.jpg"}
```

```
Set-AdfsGlobalWebContent -SignInPageDescriptionText "<p>Stuart, Kevin, and Bob were recruited by Microsoft <A href='http://www.minionsmovie.com/'>here</A> for more information.</p>"
```



Sign in with your organizational account

wvdapps3@jjazurecloud.com

••••••••••••

Stuart, Kevin, and Bob were recruited by Microsoft here for more information.

Create the ADFS Certificates for Windows Virtual Desktop

Enterprise deployment: Enterprise CA issues certificates

In this deployment mode, the ADFS server acts as an enrollment agent [EA], also often referred to as a registration authority (RA). In this mode, ADFS has been granted the requisite privileges to enroll for user logon certificates on behalf of the end-user. The certificates are issued by the Enterprise CA, which has been configured to recognize ADFS as an enrollment agent capable of issuing smartcard logon certificates.

- Administrator configures and enables the enrollment agent certificate template on the enterprise CA to issue an enrollment agent certificate for ADFS.
- Administrator configures a certificate template for smartcard logon. This certificate template will be issued by the CA to issue smartcard logon certificates in response to requests from ADFS acting as the enrollment agent.

When the ADFS service is configured to use an enterprise CA for issuing logon certificates, it contacts the CA to enroll for an enrollment agent certificate. This is done on all nodes of the farm.

The administrator then creates the requisite trust relationships for the WVD session host, also known as the RDSH (as an RP trust) and the WVD App (as a client). The required application permissions are granted.

Thereafter, when a request for a logon certificate is received by ADFS, it performs all the required validation checks to ensure that certificates can be issued for the specified user.

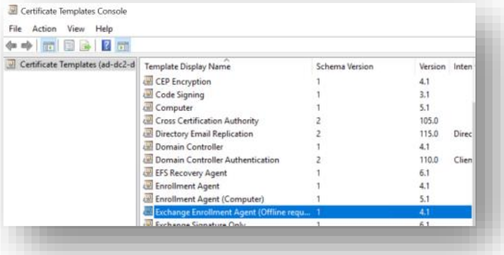
ADFS constructs a CMC request using the CSR generated by the requestor, signs and uses it enrollment agent certificate and then requests a smartcard logon certificate from the CA.

The CA validates the request and issues a smartcard logon certificate to ADFS. ADFS then responds to its caller with the smartcard logon certificate which can be used to interactively sign-in the user.

Configure the Enrollment Agent Certificate

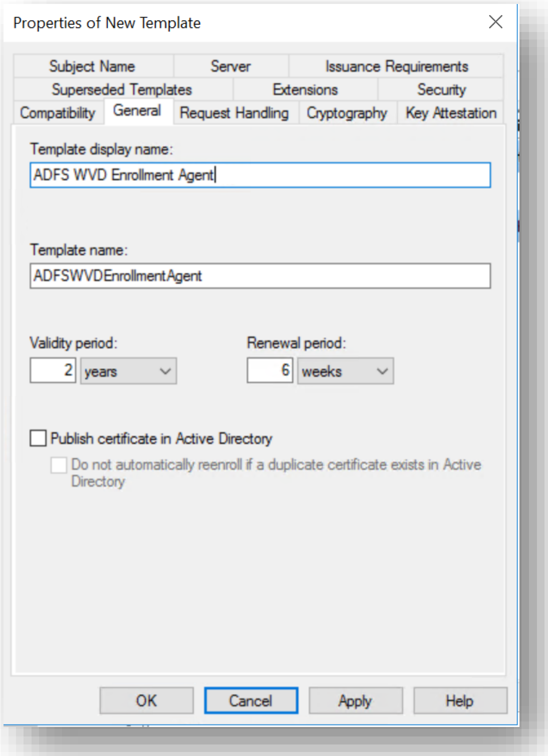
On the certificate authority server, launch MMC from the Start Menu. Select File…, Add/Remote Snap-in…, Certificate Templates, Add (USER ACOUNT)>, and OK to view the list of certificate templates.

Expand the Certificate Templates, right-click Exchange Enrollment Agent (Offline Request) and select Duplicate Template.



Certificate Templates Console
File Action View Help
Certificate Templates (ad-dc2-d

Template Display Name	Schema Version	Version	Inten
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Direc
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Clien
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	



Template display name: ADFS WVD Enrollment Agent

Template name: ADFSWVDEnrollmentAgent

Validity period: 2 years

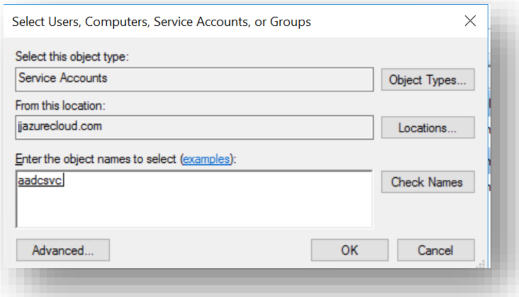
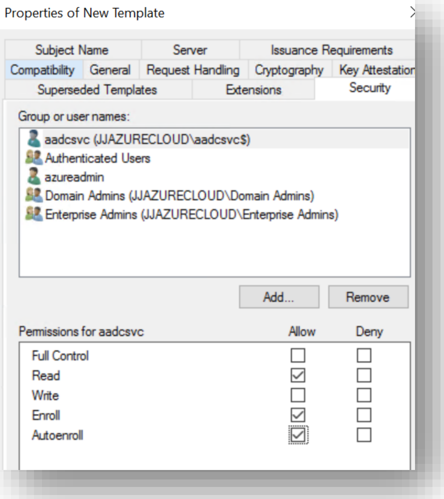
Renewal period: 6 weeks

☐ Publish certificate in Active Directory

☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

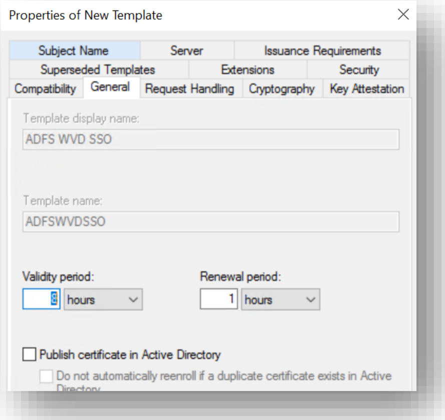
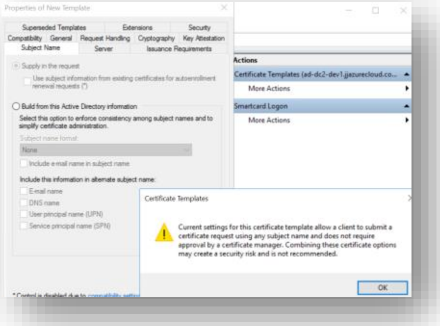
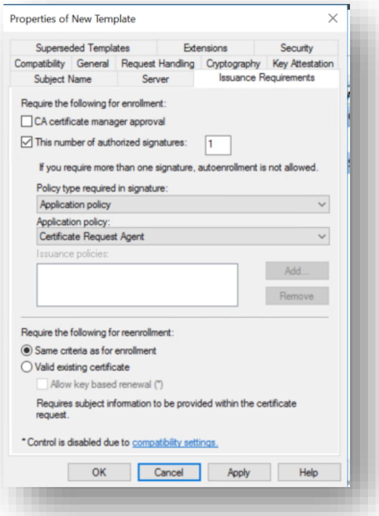
Select the General tab and rename the template accordingly, such as “ADFS WVD Enrollment Agent” for the Template display name which will automatically populate “ADFSWVDEnrollmentAgent” for the Template name.

Select the Security tab and Add… .
Select Object Types…, Service Accounts, and OK.

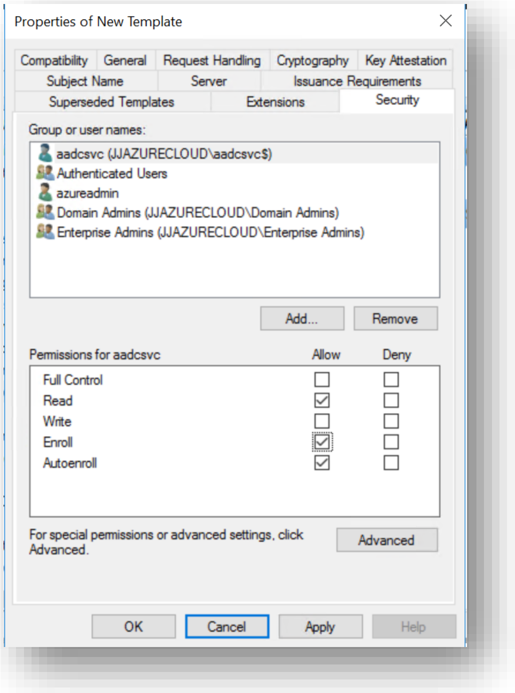
 Select Users, Computers, Service Accounts, or Groups Select this object type: Service Accounts From this location: jjazurecloud.com Enter the object names to select (examples): aadcsvc Object Types... Locations... Check Names Advanced... OK Cancel	Enter the service account for ADFS and select OK. If you setup ADFS via Azure AD Connect, the service account is “aadcsvc$”
After the service account is added and is visible in the Security tab, select it in the Group or user names pane, select Allow for both Enroll and Auto enroll, then select OK to save.	 Properties of New Template Subject Name Server Issuance Requirements Compatibility General Request Handling Cryptography Key Attestation Superseded Templates Extensions Security Group or user names: aadcsvc (JJAZURECLOUD\aadcsvc$) Authenticated Users azureadmin Domain Admins (JJAZURECLOUD\Domain Admins) Enterprise Admins (JJAZURECLOUD\Enterprise Admins) Permissions for aadcsvc — Allow — Deny Full Control ☐ ☐ Read ☑ ☐ Write ☐ ☐ Enroll ☑ ☐ Autoenroll ☑ ☐
Apply and this competes the first certificate	

Configure the smartcard logon certificate template for interactive logon

Expand the Certificate Templates, right-click Smartcard Logon and select Duplicate Template.	

 Properties of New Template Subject Name · Server · Issuance Requirements · Superseded Templates · Extensions · Security · Compatibility · General · Request Handling · Cryptography · Key Attestation Template display name: ADFS WVD SSO Template name: ADFSWVDSSO Validity period: 8 hours Renewal period: 1 hours ☐ Publish certificate in Active Directory ☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory	Select the General tab and rename the template accordingly, such as “ADFS WVD SSO” for the Template display name which will automatically populate “ADFSWVDSSO” for the Template name. Note: On this tab, you can shorten the validity period to 8 hours and the renewal period to 1 hour, since this certificate is requested on-demand.
Select the Subject Name tab and Supply in the request. Accept the warning and click ok.	 Properties of New Template Superseded Templates · Extensions · Security · Compatibility · General · Request Handling · Cryptography · Key Attestation · Subject Name · Server · Issuance Requirements ● Supply in the request ☐ Use subject information from existing certificates for autoenrollment renewal requests (*) ○ Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration. Subject name format: None ☐ Include e-mail name in subject name Include this information in alternate subject name: ☐ E-mail name ☐ DNS name ☐ User principal name (UPN) ☐ Service principal name (SPN) * Control is disabled due to compatibility settin Actions Certificate Templates (ad-dc2-dev1.jjazurecloud.co... More Actions Smartcard Logon More Actions Certificate Templates Current settings for this certificate template allow a client to submit a certificate request using any subject name and does not require approval by a certificate manager. Combining these certificate options may create a security risk and is not recommended. OK
 Properties of New Template Superseded Templates · Extensions · Security · Compatibility · General · Request Handling · Cryptography · Key Attestation · Subject Name · Server · Issuance Requirements Require the following for enrollment: ☐ CA certificate manager approval ☑ This number of authorized signatures: 1 If you require more than one signature, autoenrollment is not allowed. Policy type required in signature: Application policy Application policy: Certificate Request Agent Issuance policies: Add... · Remove Require the following for reenrollment: ● Same criteria as for enrollment ○ Valid existing certificate ☐ Allow key based renewal (*) Requires subject information to be provided within the certificate request. * Control is disabled due to compatibility settings. OK · Cancel · Apply · Help	Select Issuance Requirements Tab. Select ‘This number of authorized signatures and enter the value of’ 1. For Application policy select ‘Certificate Request Agent’.

Select the Security tab and Add. Select Object Types…, Service Accounts, and OK. Enter the service account for ADFS (same as above) and select OK. Select Enroll and AutoEnroll again, apply and ok.



Properties of New Template

Group or user names:

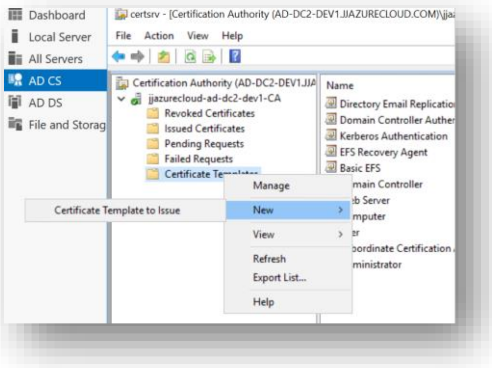
- aadcsvc (JJAZURECLOUD\aadcsvc$)
- Authenticated Users
- azureadmin
- Domain Admins (JJAZURECLOUD\Domain Admins)
- Enterprise Admins (JJAZURECLOUD\Enterprise Admins)

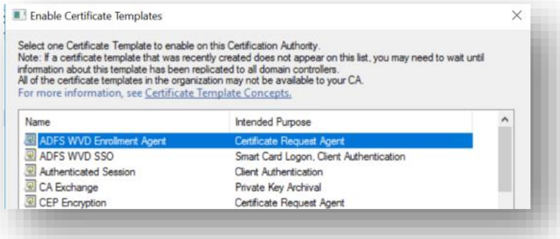
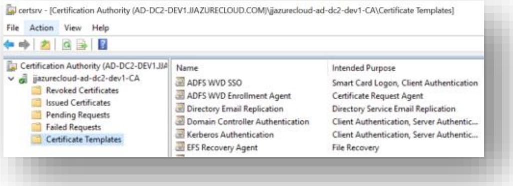
Permissions for aadcsvc	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□

For special permissions or advanced settings, click Advanced.

Enable the new WVD certificate templates on the certificate authority

Open the CA Manager. Click Certificate Templates, then right-click, select 'new' and then certificate template to issue.

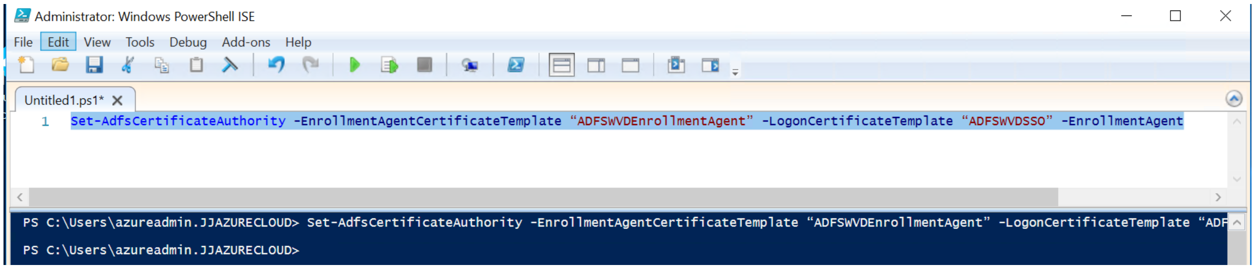


 Enable Certificate Templates Select one Certificate Template to enable on this Certification Authority. Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers. All of the certificate templates in the organization may not be available to your CA. For more information, see Certificate Template Concepts. Name — Intended Purpose ADFS WVD Enrollment Agent — Certificate Request Agent ADFS WVD SSO — Smart Card Logon, Client Authentication Authenticated Session — Client Authentication CA Exchange — Private Key Archival CEP Encryption — Certificate Request Agent	Do this for both certificates you created.
Once you have added both, you should now see them in the main panel.	 certsrv - [Certification Authority (AD-DC2-DEV1.JJAZURECLOUD.COM)\jjazurecloud-ad-dc2-dev1-CA\Certificate Templates] Certification Authority (AD-DC2-DEV1.JJA jjazurecloud-ad-dc2-dev1-CA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates Name — Intended Purpose ADFS WVD SSO — Smart Card Logon, Client Authentication ADFS WVD Enrollment Agent — Certificate Request Agent Directory Email Replication — Directory Service Email Replication Domain Controller Authentication — Client Authentication, Server Authentic... Kerberos Authentication — Client Authentication, Server Authentic... EFS Recovery Agent — File Recovery

Configure ADFS and WVD together

*The following steps need to be completed from elevated PowerShell on your ADFS server.

Set-AdfsCertificateAuthority -EnrollmentAgentCertificateTemplate “ADFSWVDEnrollmentAgent” -LogonCertificateTemplate “ADFSWVDSSO” -EnrollmentAgent



```
1  Set-AdfsCertificateAuthority -EnrollmentAgentCertificateTemplate “ADFSWVDEnrollmentAgent” -LogonCertificateTemplate “ADFSWVDSSO” -EnrollmentAgent
```

```
PS C:\Users\azureadmin.JJAZURECLOUD> Set-AdfsCertificateAuthority -EnrollmentAgentCertificateTemplate “ADFSWVDEnrollmentAgent” -LogonCertificateTemplate “ADF
PS C:\Users\azureadmin.JJAZURECLOUD>
```

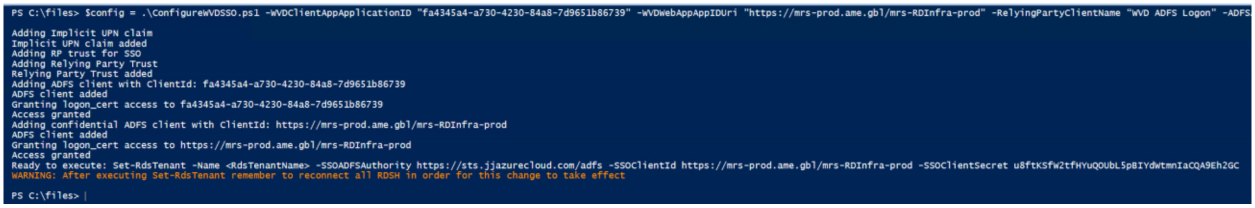
Configure a relying-party trust on your ADFS

Creating a relying-party trust between the ADFS and the Azure AD application tied to WVD is important so that ADFS can issue logon certificates for users you provision for RemoteApp and desktop access. To help in the creation of the relying-party trust, we can provide a script that requires the following parameters (and an example below):

- WVDClientAppApplicationID (AAD Application RDInfraClient) – THIS IS SET BY INTERNAL PG USE THE BELOW.
- WVDWebAppAppIDUri (AAD Application RDInfra Under settings and properties) – THIS IS SET BY INTERNAL PG USE THE BELOW.
- RelyingPartyClientName – Supply the name that will be used in ADFS to identify this relying-party trust. This is custom and does not rely on any deployment or Azure AD information.
- ADFSAuthority – Supply the URL where ADFS can be found, which is usually the public DNS name of the ADFS farm with the suffix of “/adfs”.
- RdWebURL – Supply the URL of the RDWeb app service of the WVD instance.

In the same PowerShell session run the below script: Make sure you are in the path of where you have the .\configurewvdsso.ps1 script **DO NOT CHANGE THE APPID OR APPIDURI**

$config = .\ConfigureWVDSSO.ps1 -WVDClientAppApplicationID "fa4345a4-a730-4230-84a8-7d9651b86739" -WVDWebAppAppIDUri "https://mrs-prod.ame.gbl/mrs-RDInfra-prod" -RelyingPartyClientName “WVD ADFS Logon” -ADFSAuthority "https://sts.jjazurecloud.com/adfs" -RdWebURL https://rdweb.wvd.microsoft.com



```
PS C:\files> $config = .\ConfigureWVDSSO.ps1 -WVDClientAppApplicationID "fa4345a4-a730-4230-84a8-7d9651b86739" -WVDWebAppAppIDUri "https://mrs-prod.ame.gbl/mrs-RDInfra-prod" -RelyingPartyClientName “WVD ADFS Logon" -ADFS

Adding Implicit UPN claim
Implicit UPN claim added
Adding RP trust for SSO
Adding Relying Party Trust
Relying Party Trust added
Adding ADFS client with ClientId: fa4345a4-a730-4230-84a8-7d9651b86739
ADFS client added
Granting logon_cert access to fa4345a4-a730-4230-84a8-7d9651b86739
Access granted
Adding confidential ADFS client with ClientId: https://mrs-prod.ame.gbl/mrs-RDInfra-prod
ADFS client added
Granting logon_cert access to https://mrs-prod.ame.gbl/mrs-RDInfra-prod
Access granted
Ready to execute: Set-RdsTenant -Name <RdsTenantName> -SSOADFSAuthority https://sts.jjazurecloud.com/adfs -SSOClientId https://mrs-prod.ame.gbl/mrs-RDInfra-prod -SSOClientSecret u8ftKSfW2tfHYuQOUbL5pBIYdWtmnIaCQA9Eh2GC
WARNING: After executing Set-RdsTenant remember to reconnect all RDSH in order for this change to take effect

PS C:\files> |
```

Update the RDS tenant object with single sign-on parameters

Run this from a machine that has the Azure PS modules and everything need, preferably in the same session as above.

Import-Module -Name Microsoft.RDInfra.RDPowerShell

Add-RDSAccount -DeploymentUrl https://rdbroker.wvd.microsoft.com

--STOP---

IF YOU HAVE MORE THAN ONE TENANT THAT YOU WANT TO HAVE ADFS SSO TIED TO USING THE SAME AZURE AD AND LOCAL AD, JUST KEEP SETTING THE RDSTENANT -NAME TO EACH ONE AND THEN RUN THE LAST LINE BELOW. YOU DO NOT NEED TO RUN THE $CONFIG ABOVE AGAIN.

Set-RdsTenant -Name "XXXXXX"

Set-RdsTenant -Name jojenner -SSOADFSAuthority $config.SSOADFSAuthority -SSOClientId $config.SSOClientId -SSOClientSecret $config.SSOClientSecret

```
After executing Set-RdsTenant remember to restart all session hosts in order for these
changes to take effect.
```

Final Validation everything is working

If you have already successfully configured this solution and have added more tenants to your environment and want to add SSO to them, then you will need to execute the below: These values are constant and apply to all environments.

```
Remove-AdfsClient -TargetClientId fa4345a4-a730-4230-84a8-7d9651b86739
Remove-AdfsClient -TargetClientId https://mrs-prod.ame.gbl/mrs-RDInfra-prod
Remove-AdfsRelyingPartyTrust -TargetIdentifier https://mrs-prod.ame.gbl/mrs-RDInfra-
prod
```

Re-run the $config command above and follow the steps to add to multiple tenants.

Link to the script which contains the above 3 lines.

https://www.powershellgallery.com/packages/UnConfigureWVDSSO