



Desktop-as-a-Service (DaaS) Using Windows Virtual Desktop (WVD) Compliance & Identity with SSO & MFA

Prepared for:

Service Provider Partners
Oct. 2019

Prepared by:

Microsoft – **One Commercial Partner (OCP)**

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation. Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers. © 2016 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

1. Overview	5
2. Prerequisites	5
Azure & Windows Active Directory Prerequisites	5
General Best Practices	6
Azure Networking	6
Azure Architectural Diagram	6
3. Plan user rollout	7
User communications	7
Deployment considerations	8
Enabling Multi-Factor Authentication with Conditional Access	8
Defining network locations	9
Configuring a named location	9
Plan authentication methods	11
Notification through mobile app	11
Verification code from mobile app	11
Call to phone	11
Text message to phone	11
Choose verification options	11
Plan a registration policy	13
Registration with Identity Protection	13
Azure Multi-Factor Authentication registration policy	14
Policy settings	15
4. Securing WVD with Conditional Access and MFA	16
Configure WVD in Azure with Conditional Access and MFA	16
Create a new Conditional Access Policy	16
5. Enabling Single-Sign-on (SSO)	18
Design principles	18
Steps to deploy AD FS in Azure	19

Deploying the network	19
Create DMZ virtual subnet	20
Creating the DMZ network security group.....	20
Create storage accounts.....	22
Create availability sets.....	23
Deploy WAP virtual machines	23
Configuring the domain controller / AD FS servers	24
Deploying Internal Load Balancer (ILB).....	31
Configuring the Web Application Proxy (WAP) server	31
6. Support	31

1. Overview

People are connecting to organizational resources in increasingly complicated scenarios. People connect from organization-owned, personal, and public devices on and off the corporate network using smart phones, tablets, PCs, and laptops, often on multiple platforms. In this always-connected, multi-device and multi-platform world, the security of user accounts is more important than ever. Passwords, no matter their complexity, used across devices, networks, and platforms are no longer sufficient to ensure the security of the user account, especially when users tend to reuse passwords across accounts. Sophisticated phishing and other social engineering attacks can result in usernames and passwords being posted and sold across the dark web.

Azure Multi-Factor Authentication (MFA) helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs.

This document is a walk-through of implementing Azure user authentication services with MFA enabled, and streamlining the user logon experience with Single Sign-on (SSO).

2. Prerequisites

Azure & Windows Active Directory Prerequisites

Before getting started, **all** items listed below **must** be checked/validated to ensure the most basic requirements are in place to proceed with executing the remaining steps in this guide.

- An Azure Active Directory
- A Windows Server Active Directory in sync with Azure Active Directory. This can be enabled through:
 - Azure AD Connect
 - Azure AD Domain Services
- An Azure subscription, containing a virtual network that either contains or is connected to the Windows Server Active Directory

General Best Practices

Since everyone's business and technical requirements vary across the board, it is always a good idea to familiarize yourselves with the standard best practices across the different Azure technologies & services.

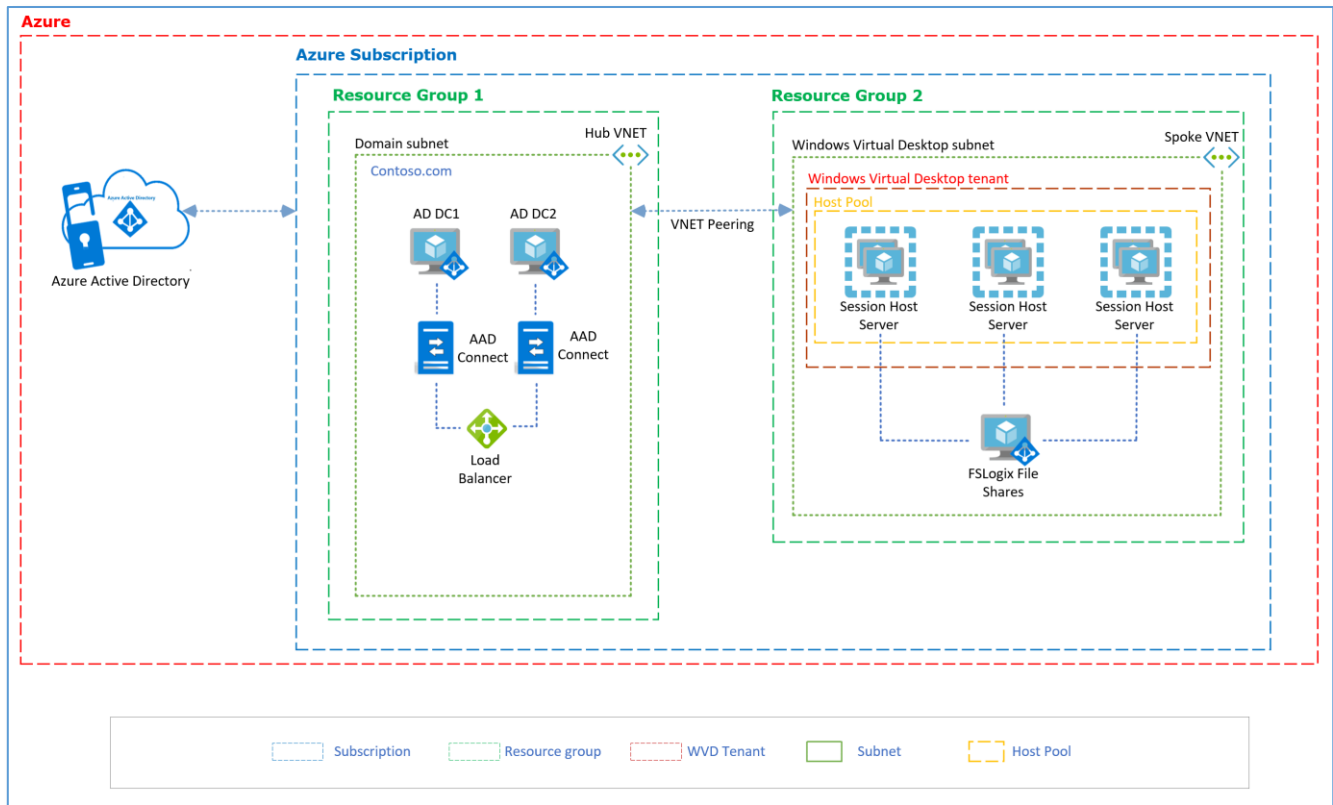
- Please follow the guidance [here](#) to maintain a consistent naming convention across your resources, unless you are already using a naming system.
- [Azure security best practices and patterns](#)
- Azure Active Directory Hybrid Identity [best practices](#)
- [Azure identity management and access control security best practices](#)
- Azure Networking & security [Best Practices](#)
- Azure Storage security [overview](#)
- [Best practices for Azure VM security](#)

Azure Networking

The recommendation is to design your Azure Networking using a [Hub-Spoke topology](#). Consider the HUB like a DMZ deployed with your Virtual network Gateways and other security/edge appliances like Firewalls Etc. while the Spoke will act as the backend zone where your session hosts servers are deployed to and is peered with the HUB. This is our design for this walk-through, so you'll need this already setup before proceeding.

Azure Architectural Diagram

Below is a diagram of the Azure environment that we'll use. It shows the objects created in Azure and their relationships within the environment. In this example, the company name will be Contoso.



3. Plan user rollout

Your MFA rollout plan should include a pilot deployment followed by deployment waves that are within your support capacity. Begin your rollout by applying your Conditional Access policies to a small group of pilot users. After evaluating the impact on the pilot users, processes used, and registration behaviors, you can either add more user groups to the policy, or, add more users to the existing groups.

User communications

It is critical to inform users, in planned communications, about upcoming changes, Azure MFA registration requirements, and any necessary user actions. We recommend communications are developed in concert with representatives from within your organization, such as a Communications, Change Management, or Human Resources departments.

Microsoft provides communication templates and end-user documentation to help draft your communications. You can send users to <https://myprofile.microsoft.com> to register directly by selecting the **Security Info** links on that page.

Deployment considerations

Azure Multi-factor Authentication is deployed by enforcing policies with Conditional Access. A Conditional Access policy can require users to perform multi-factor authentication when certain criteria are met such as:

- All users, a specific user, member of a group, or assigned role
- Specific cloud application being accessed
- Device platform
- State of device
- Network location or geo-located IP address
- Client applications
- Sign-in risk (Requires Identity Protection)
- Compliant device
- Hybrid Azure AD joined device
- Approved client application

Use the customizable posters and email templates in multi-factor authentication rollout materials to roll out multi-factor authentication to your organization.

Enabling Multi-Factor Authentication with Conditional Access

Conditional Access policies enforce registration, requiring unregistered users to complete registration at first sign-in, an important security consideration.

Azure AD Identity Protection contributes both a registration policy for and automated risk detection and remediation policies to the Azure Multi-Factor Authentication story. Policies can be created to force password changes when there is a threat of compromised identity or require MFA when a sign-in is deemed risky by the following events:

- Leaked credentials
- Sign-ins from anonymous IP addresses
- Impossible travel to atypical locations
- Sign-ins from unfamiliar locations
- Sign-ins from infected devices
- Sign-ins from IP addresses with suspicious activities

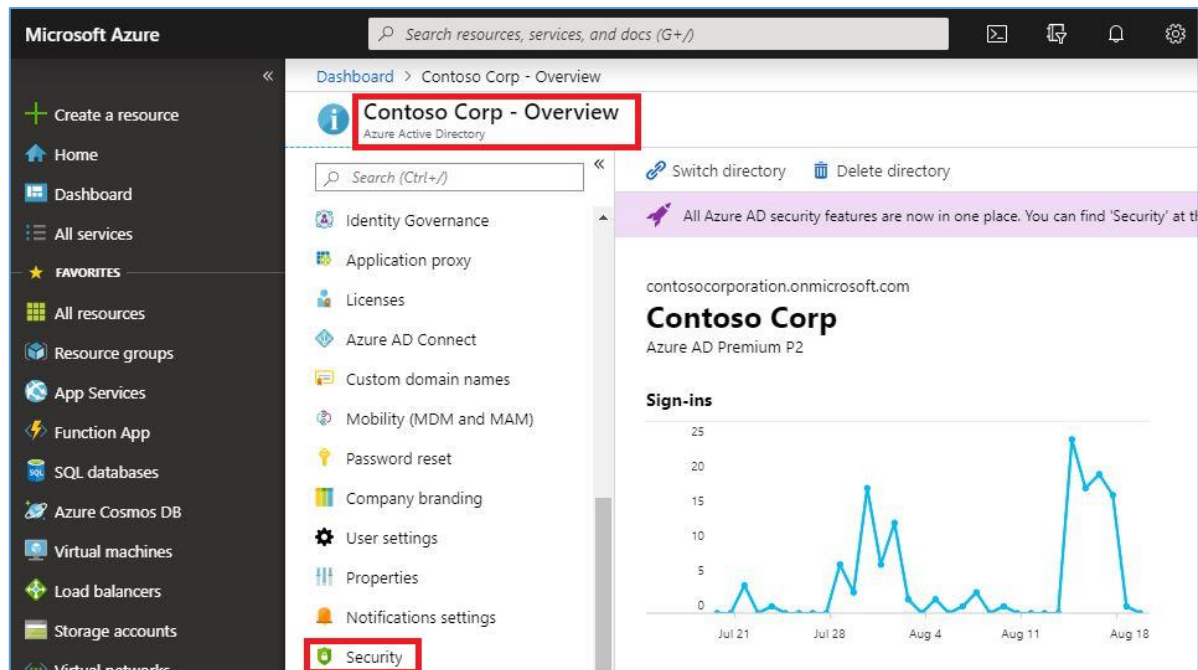
Some of the risk events detected by Azure Active Directory Identity Protection occur in real time and some require offline processing. Administrators can choose to block users who exhibit risky behaviors and remediate manually, require a password change, or require a multi-factor authentication as part of their Conditional Access policies.

Defining network locations

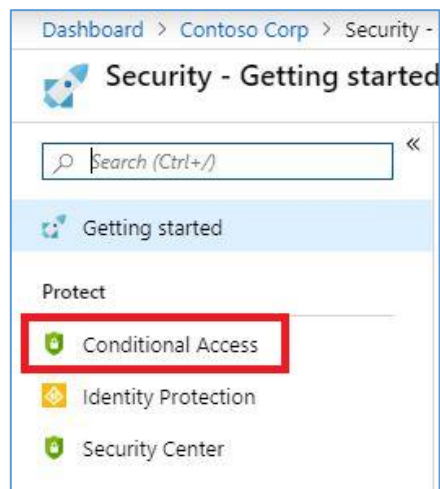
We recommended that organizations use Conditional Access to define their network using named locations. If your organization is using Identity Protection, consider using risk-based policies instead of named locations. In this section, we'll create a named location called **Contoso-MFA**.

Configuring a named location

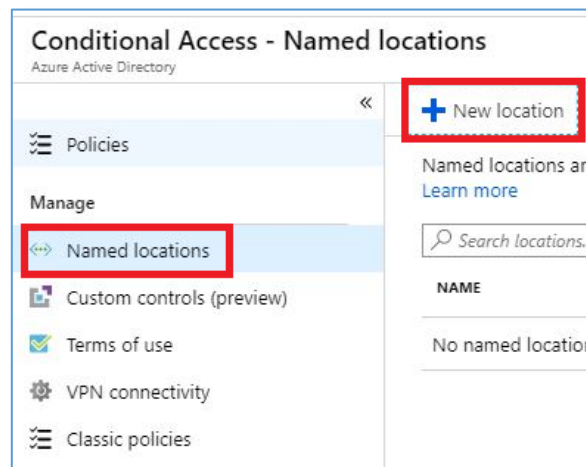
1. Open **Azure Active Directory** in the Azure portal and click on **Security**



2. Click **Conditional Access**



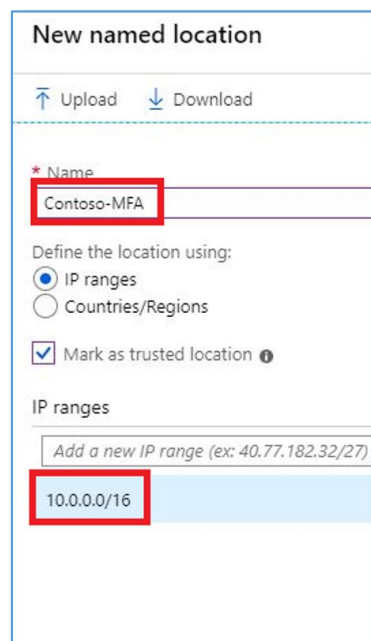
3. Click **Named Locations > New Location**



4. In the **Name** field, provide a meaningful name. *We're using Contoso-MFA.*

5. Select whether you are defining the location using IP ranges or Countries/Regions.

- If using **IP Ranges** (*we're using the IP range 10.0.0.0/16 for the example below*)
 1. Decide whether to mark the location as Trusted. Signing in from a trusted location lowers a user's sign-in risk. Only mark this location as trusted if you know the IP ranges entered, are established and credible in your organization.
 2. Specify the IP Ranges
- If using **Countries/Regions**
 1. Expand the drop-down menu and select the countries or regions you wish to define for this named location.
 2. Decide whether to Include unknown areas. Unknown areas are IP addresses that can't be mapped to a country/region.



Plan authentication methods

Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. The following methods are available for administrators to enable:

Notification through mobile app

A push notification is sent to the Microsoft Authenticator app on your mobile device. The user views the notification and selects **Approve** to complete verification. Push notifications through a mobile app provide the least intrusive option for users. They are also the most reliable and secure option because they use a data connection rather than telephony.

Verification code from mobile app

A mobile app like the Microsoft Authenticator app generates a new OATH verification code every 30 seconds. The user enters the verification code into the sign-in interface. The mobile app option can be used whether or not the phone has a data or cellular signal.

Call to phone

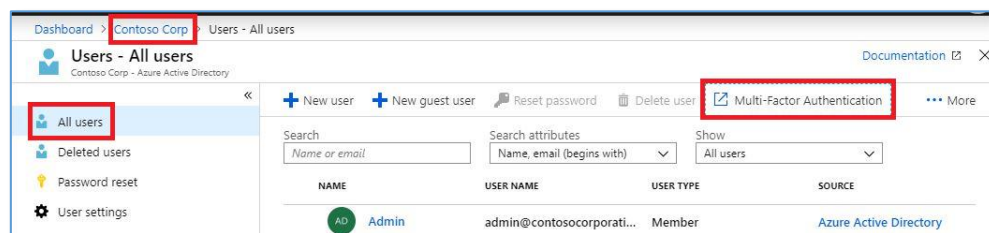
An automated voice call is placed to the user. The user answers the call and presses # on the phone keypad to approve their authentication. Call to phone is a great backup method for notification or verification code from a mobile app.

Text message to phone

A text message that contains a verification code is sent to the user. The user is prompted to enter the verification code into the sign-in interface.

Choose verification options

1. Browse to **Azure Active Directory, Users, Multi-Factor Authentication:**



2. In the new tab that opens browse to **service settings**.
3. Under **verification options**, check all of the boxes for methods available to users.

Microsoft contosouser@contosocorporation.onmicrosoft.com

multi-factor authentication

users service settings

app passwords [\(learn more\)](#)

☒ Allow users to create app passwords to sign in to non-browser apps
☐ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

☐ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/27

192.168.1.0/27

192.168.1.0/27

verification options [\(learn more\)](#)

Methods available to users:

☐ Call to phone

☒ Text message to phone

☒ Notification through mobile app

☒ Verification code from mobile app or hardware token

remember multi-factor authentication [\(learn more\)](#)

☐ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60):

save

4. Click **Save** & close the **service settings** tab.

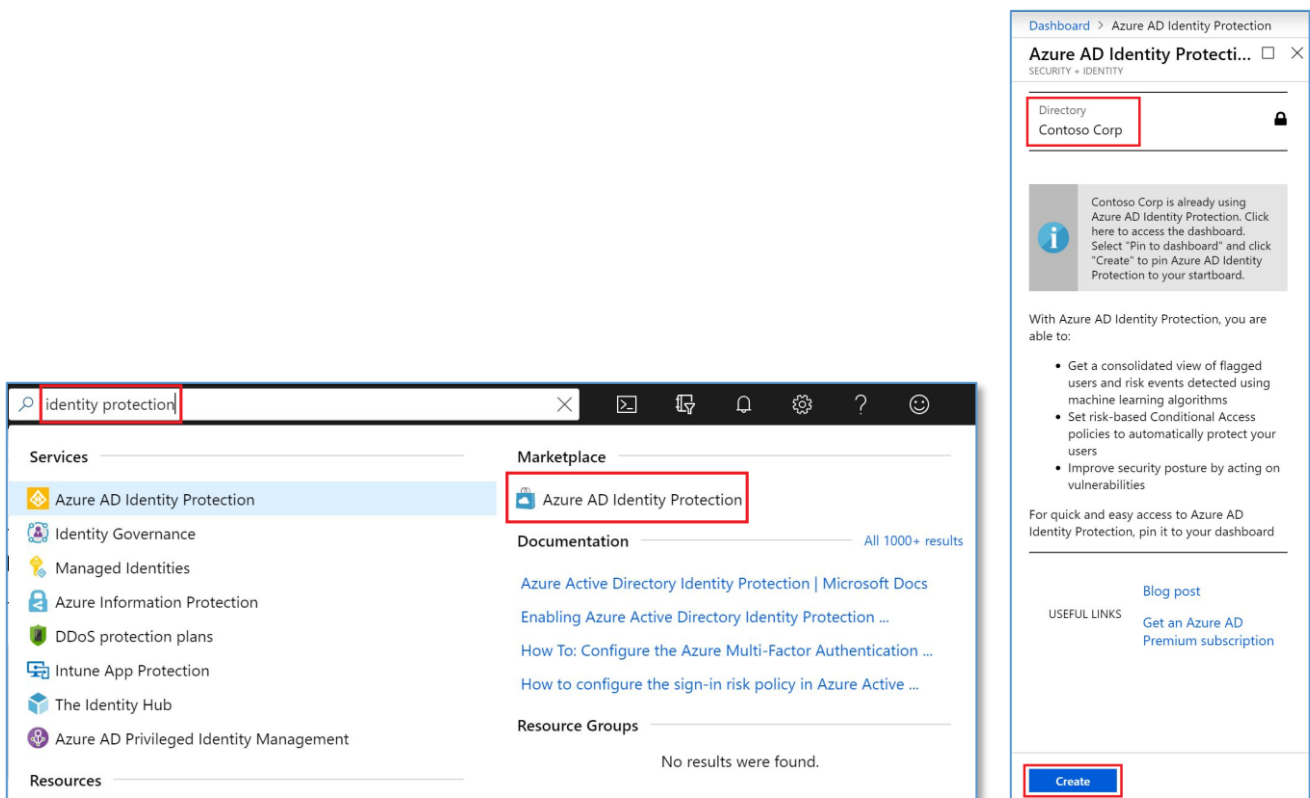
Plan a registration policy

Organizations should enable the newly combined registration experience for Azure MFA and self-service password reset (SSPR). SSPR allows users to reset their password in a secure way, using the same methods they use for multi-factor authentication. We recommend this combined registration method, currently in public preview, because it's a great experience for users, providing the ability to register once, for both services.

Registration with Identity Protection

If your organization is using Azure Active Directory Identity Protection, configure the MFA registration policy to prompt your users to register the next time they sign in interactively.

To activate the Azure Active Directory Identity Protection, add the Identity protection services at the Marketplace. Once is added, it will ask for the Directory creation "**Azure Active Directory**" selected and click **Create**:



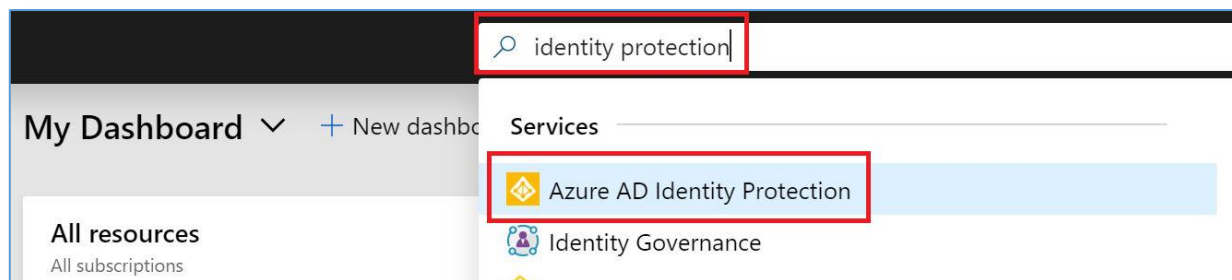
Azure Multi-Factor Authentication registration policy

Azure Multi-Factor Authentication provides a means to verify who you are using more than just a username and password. It provides a second layer of security to user sign-ins. In order for users to be able to respond to MFA prompts, they must first register for Azure Multi-Factor Authentication.

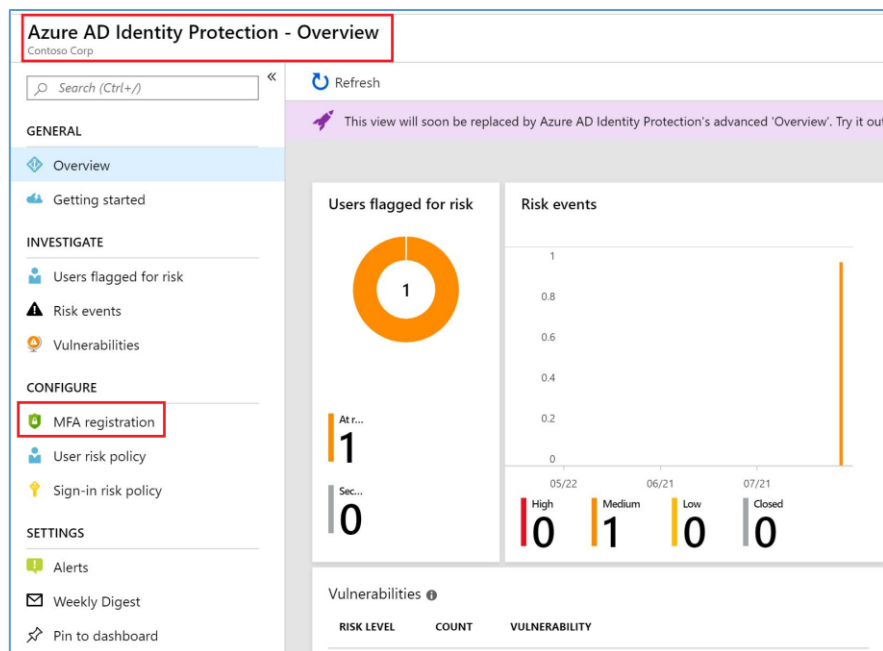
We recommend that you require Azure Multi-Factor Authentication for user sign-ins because it:

- Delivers strong authentication with a range of easy verification options
- Plays a key role in preparing your organization to protect and recover from risk events in Identity Protection

The MFA registration policy is in the **Configure** section on the Azure AD Identity Protection page found at search field as shown below:



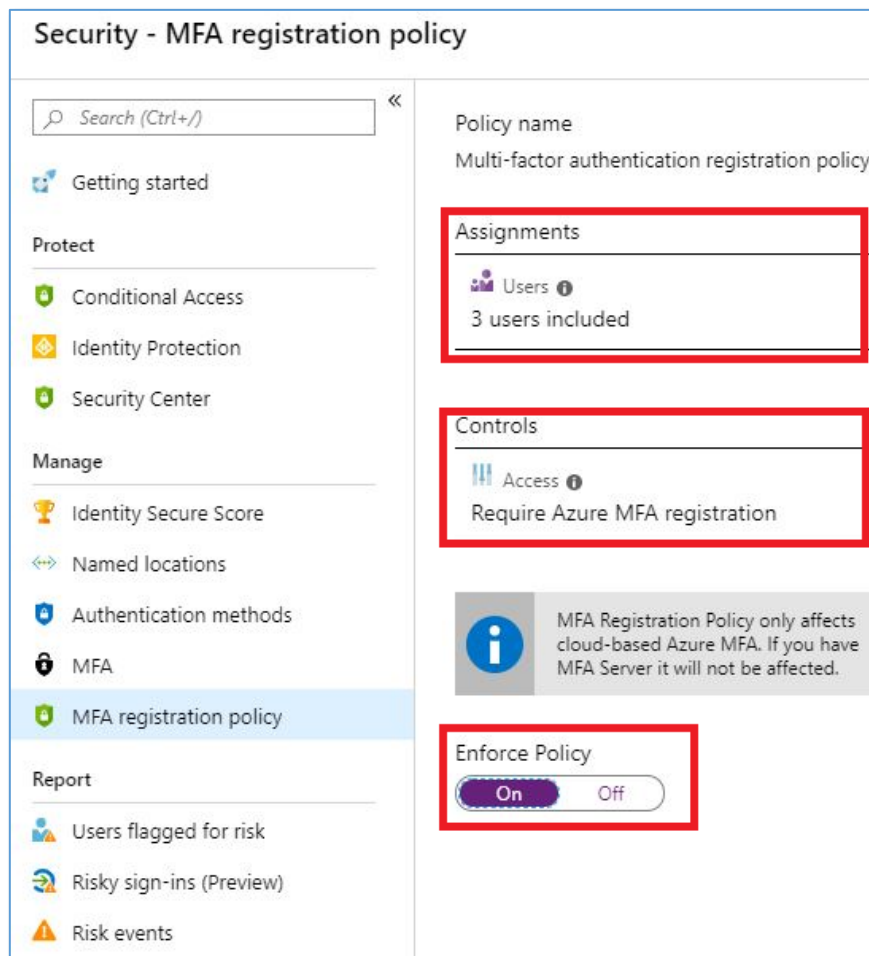
1. Click on **Azure AD Identity Protection** to show the console and click on **MFA Registration**:



Policy settings

When you configure the MFA registration policy, you need to make the following configuration changes:

- The users and groups the policy applies to. Remember to exclude your organization's emergency access accounts.
- The control you want to enforce - **Require Azure MFA registration**
- Enforce Policy should be set to **On**.
- **Save** your policy



Azure Active Directory Identity Protection will prompt your users to register the next time they sign in interactively.

4. Securing WVD with Conditional Access and MFA

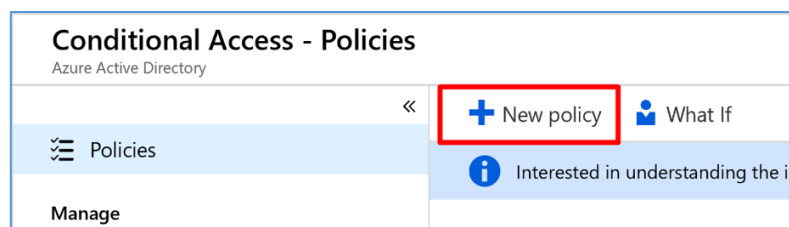
Azure MFA enabled on a traditional RDS deployment, via RADIUS authentication, issues an MFA challenge on every login. Fortunately, securing Windows Virtual Desktop in Azure with Conditional Access and MFA is a breeze and dramatically improves the user experience!

Configure WVD in Azure with Conditional Access and MFA

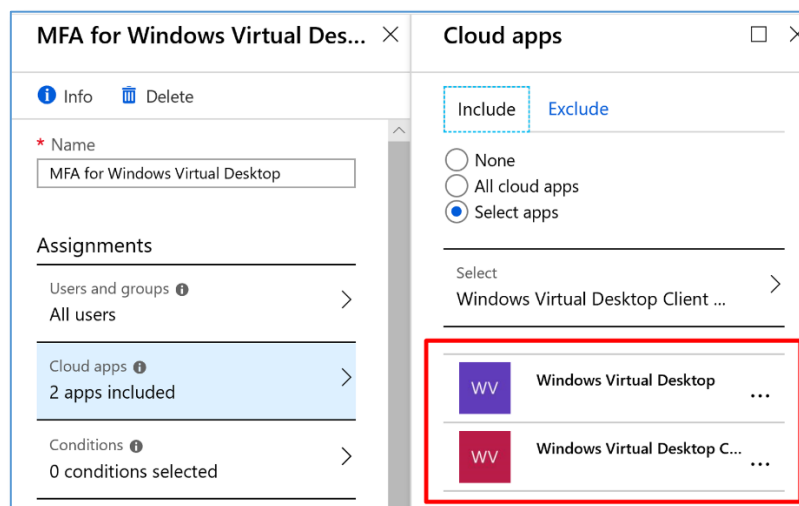
When you integrate any application with Azure SSO as either a SAML 2.0 endpoint or Enterprise Application, it's simple to create a conditional access policy to enforce MFA challenges for that application. In this section, we'll create a Conditional Access Policy for Contoso.

Create a new Conditional Access Policy

1. Navigate to the Conditional Access blade in the Azure management portal.
2. Click **New Policy** and name it: **MFA for Windows Virtual Desktop**



3. Under **Assignments**, target **All Users** or choose a pilot group.
4. Select **Cloud Apps**, search for **Windows Virtual Desktop**, and select the apps that are registered in your tenant: *(we're selecting WVD Desktop & WVD Desktop Client)*



5. Under **Conditions** exclude **Devices marked as compliant** to allow your enrolled and healthy devices to bypass MFA challenges:

The screenshot shows the 'Conditions' pane for an MFA policy named 'MFA for Windows Virtual Desktop'. The 'Device state (preview)' pane on the right is active, showing the 'Exclude' button and the 'Device marked as compliant' condition selected. The 'Configure' button is also visible.

Conditions

- Sign-in risk: Not configured
- Device platforms: Not configured
- Locations: Not configured
- Client apps (preview): Not configured
- Device state (preview): Not configured

Device state (preview)

Configure: Yes No

Include Exclude

Select the device state condition used to exclude devices from policy.

☐ Device Hybrid Azure AD joined

☒ Device marked as compliant

6. Under **Access Control** select **Require multi-factor authentication**

The screenshot shows the 'Grant' pane for the same MFA policy. The 'Require multi-factor authentication' checkbox is selected. The 'Access controls' pane on the left shows '1 control selected'.

Grant

Select the controls to be enforced.

☐ Block access

☒ Grant access

☒ Require multi-factor authentication

☐ Require device to be marked as compliant

☐ Require Hybrid Azure AD joined device

☐ Require approved client app
[See list of approved client apps](#)

For multiple controls

☐ Require all the selected controls

☒ Require one of the selected controls

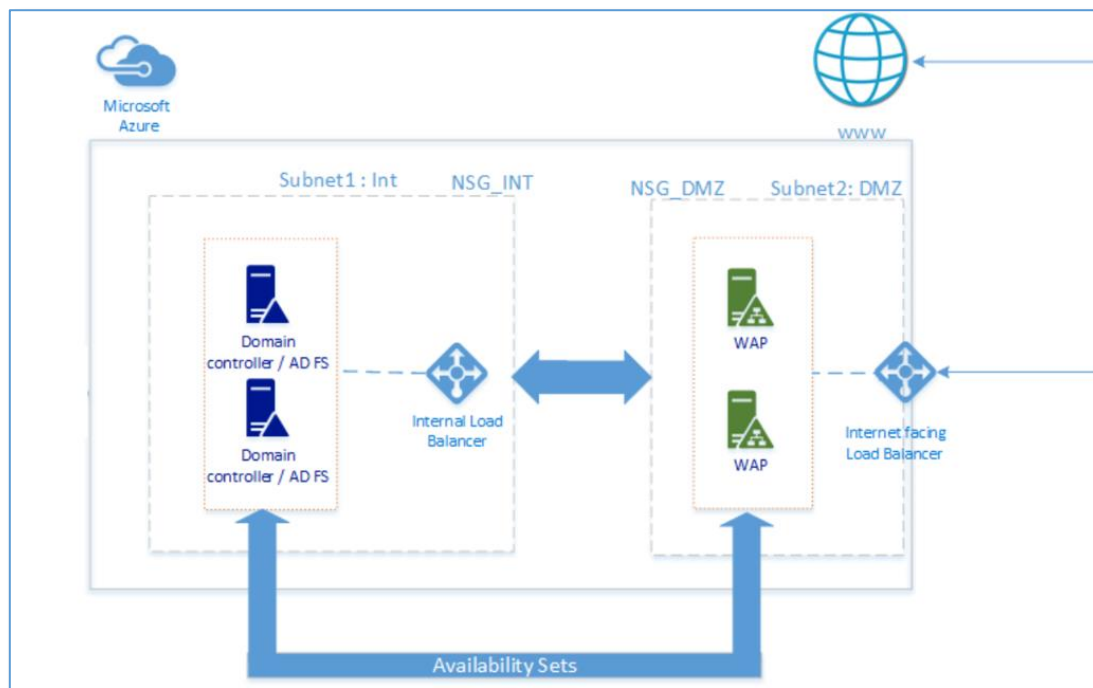
7. Click **Save** and make sure you **enable** the policy
8. Test your policy by logging into the Windows Virtual Desktop environment from an *unmanaged* computer.

5. Enabling Single-Sign-on (SSO)

AD FS provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. Federation with Azure AD or O365 enables users to authenticate using domain credentials and access all resources in cloud. Deploying AD FS in Azure can help achieve the high availability required with minimal efforts. There are several advantages of deploying AD FS in Azure, a few of them are listed below:

- **High Availability** - With the power of Azure Availability Sets, you ensure a highly available infrastructure.
- **Easy to Scale** – Need more performance? Easily migrate to more powerful machines by just a few clicks in Azure
- **Cross-Geo Redundancy** – With Azure Geo Redundancy you can be assured that your infrastructure is highly available across the globe
- **Easy to Manage** – With highly simplified management options in Azure portal, managing your infrastructure is very easy and hassle-free

Design principles



The diagram above shows the recommended basic topology to start deploying your AD FS infrastructure in Azure. The principles behind the various components of the topology are listed below:

- **DC / ADFS Servers:** If you have fewer than 1,000 users you can simply install AD FS role on your domain controllers. If you do not want any performance impact on the domain controllers or if you have more than 1,000 users, then deploy AD FS on separate servers.
- **WAP Server** – it is necessary to deploy Web Application Proxy servers, so that users can reach the AD FS when they are not on the company network also.
- **DMZ:** The Web Application Proxy servers will be placed in the DMZ and ONLY TCP/443 access is allowed between the DMZ and the internal subnet.
- **Load Balancers:** To ensure high availability of AD FS and Web Application Proxy servers, we recommend using an internal load balancer for AD FS servers and Azure Load Balancer for Web Application Proxy servers.
- **Availability Sets:** To provide redundancy to your AD FS deployment, it is recommended that you group two or more virtual machines in an Availability Set for similar workloads. This configuration ensures that during either a planned or unplanned maintenance event, at least one virtual machine will be available
- **Storage Accounts:** It is recommended to have two storage accounts. Having a single storage account can lead to creation of a single point of failure and can cause the deployment to become unavailable in an unlikely scenario where the storage account goes down. Two storage accounts will help associate one storage account for each fault line.
- **Network segregation:** Web Application Proxy servers should be deployed in a separate DMZ network. You can divide one virtual network into two subnets and then deploy the Web Application Proxy server(s) in an isolated subnet. You can simply configure the network security group settings for each subnet and allow only required communication between the two subnets. More details are given via the deployment scenario below.

Steps to deploy AD FS in Azure

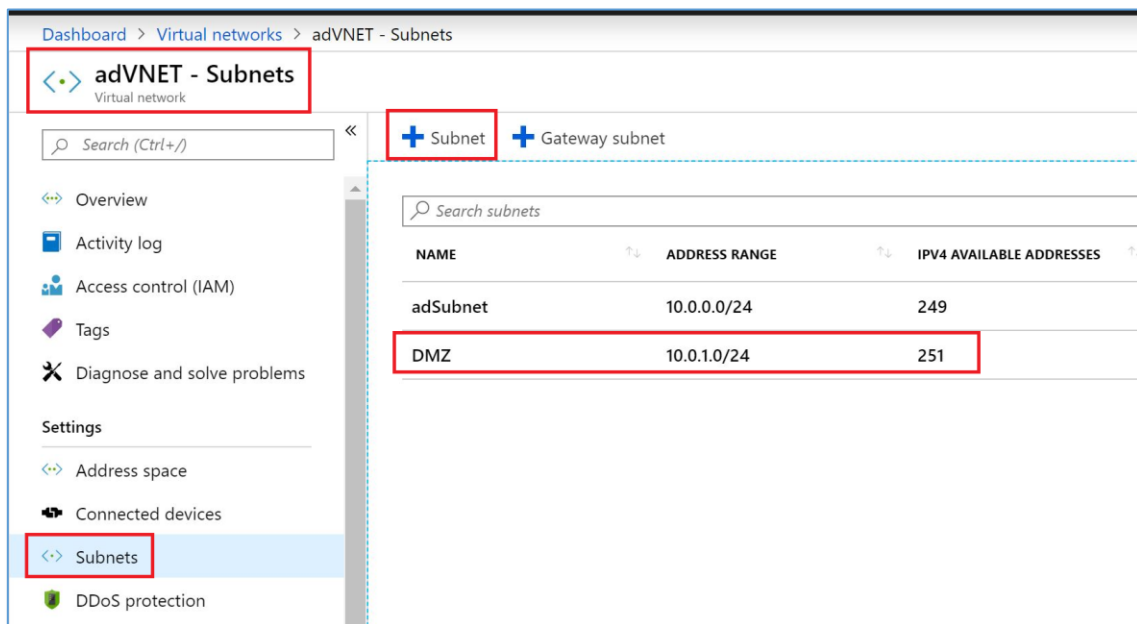
Deploying the network

As outlined above, you can either create two subnets in a single virtual network or else create two completely different virtual networks (VNet). This article will focus on deploying a single virtual network and divide it into two subnets. This is currently an easier approach as two separate VNets would require a VNet to VNet gateway for communications. In this scenario we already have a virtual network created. That's why we move forward and create the subnet for the DMZ.

Create DMZ virtual subnet

In the Azure portal, select virtual network and you can deploy the virtual network, and one subnet immediately, with just one click. An internal subnet is also defined and is then ready for VMs to be added. The next step is to add a DMZ subnet to the network. To create the DMZ subnet, simply:

- Select the network where you want to create the subnet. We're selecting our adVNET.
- In the properties select subnet
- In the subnet panel click on the add button
- Provide DMZ as the subnet name, and address space information, to create the subnet

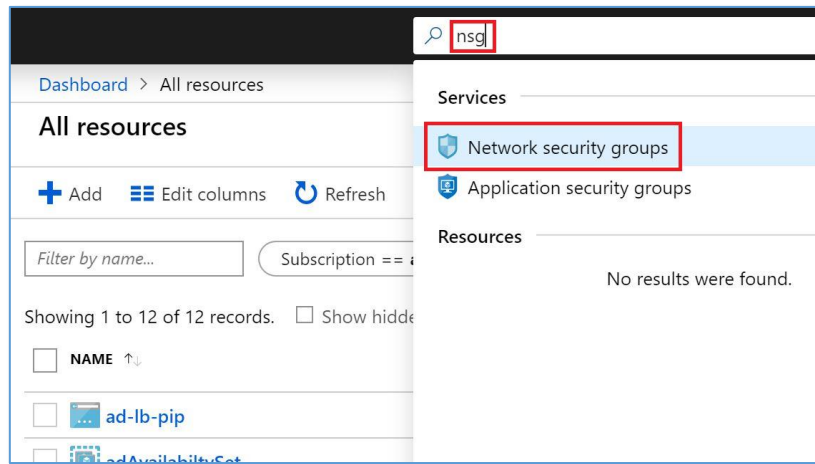


Creating the DMZ network security group

A Network security group (NSG) contains a list of Access Control List (ACL) rules that allow or deny network traffic to your VM instances in a Virtual Network. NSGs can be associated with either subnets or individual VM instances within that subnet. When an NSG is associated with a subnet, the ACL rules apply to all the VM instances in that subnet. For the purpose of this guidance, we will create a DMZ subnet NSG named DMZ_NSG.

After the NSG is created, there will be 0 inbound and 0 outbound rules. Once the roles on the respective servers are installed and functional, then the inbound and outbound rules can be opened according to the desired level of security.

1. **Search** resources, for **NSG**, click on “**Network security groups**”, and click +**Add**:



2. Complete the fields required and click on **Create**

Create network security g... □ ×

* Name
NSG_DMZ ✓

* Subscription
Contoso Subscription ▼

* Resource group
RG-ContosoCorpWSAD ▼
[Create new](#)

* Location
(US) East US ▼

Create Automation options

It is assumed that you already have an NSG for the network where your **domain controllers** are located. For the purposes of this example, we are using the name **NSG_INT** for that NSG.

After the DMZ NSG is created, associate it with subnet DMZ. An example screenshot is given below:

Dashboard > Virtual networks > adVNET - Subnets > DMZ 1

DMZ
adVNET

Save 3 Discard Delete Refresh

* Address range (CIDR block) ⓘ
10.0.1.0/24
10.0.1.0 - 10.0.1.255 (256 addresses)

Available addresses ⓘ
251

Network security group
NSG_DMZ 2

Route table
None

Users
Manage users >

Service endpoints
Services ⓘ
0 selected

Subnet delegation
Delegate subnet to a service ⓘ
None

NAME	ADDRESS RANGE	IPV4 AVAILABLE ADDRESSES	DELEGATED TO	SECURITY GROUP
adSubnet	10.0.0.0/24	249	-	-
DMZ	10.0.1.0/24	251	-	NSG_DMZ

Create storage accounts

In order to maintain high availability and avoid dependence on a single storage account, you can create two storage accounts. Divide the machines in each availability set into two groups and then

assign each group a separate storage account. On this step by step document we do not cover storage creation.

For more information on how to create a storage account refer to this link:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-quickstart-create-account?tabs=azure-portal>

Create availability sets

For each role (DC/AD FS and WAP), it is advised to create availability sets that will contain 2 machines each at the minimum. This will help achieve higher availability for each role. While creating the availability sets. It is essential to decide on the following:

- **Fault Domains:** Virtual machines in the same fault domain share the same power source and physical network switch. A minimum of 2 fault domains are recommended. The default value is 3 and you can leave it as is for the purpose of this deployment
- **Update domains:** Machines belonging to the same update domain are restarted together during an update. You want to have minimum of 2 update domains. The default value is 5 and you can leave it as is for the purpose of this deployment

We do not cover this topic in the present document, it just more reference and recommendation about the relevance of the availability sets.

For more information on how to create an availability set, please refer to this link:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets>

Deploy WAP virtual machines

The next step is to deploy virtual machines that will host the WAP roles in your infrastructure. A minimum of two machines are recommended in an availability set. For our example, we created 2 VMs; ContosoWAP1 & ContosoWAP2 and put them into the DMZ subnet. We do not cover the creation of the virtual machines in this document. As reference please visit the link:

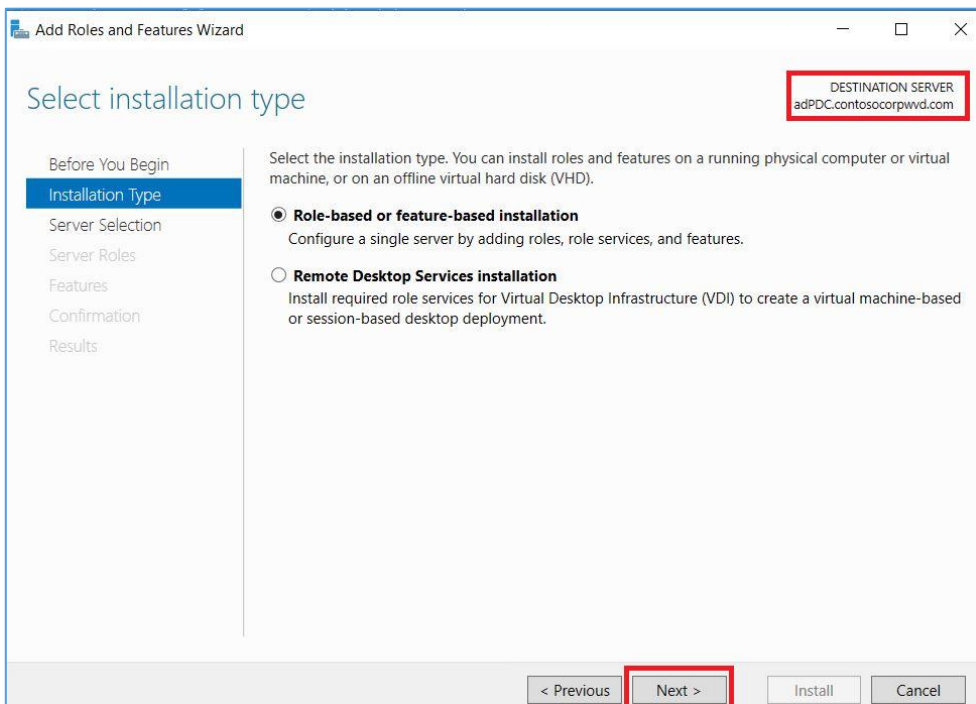
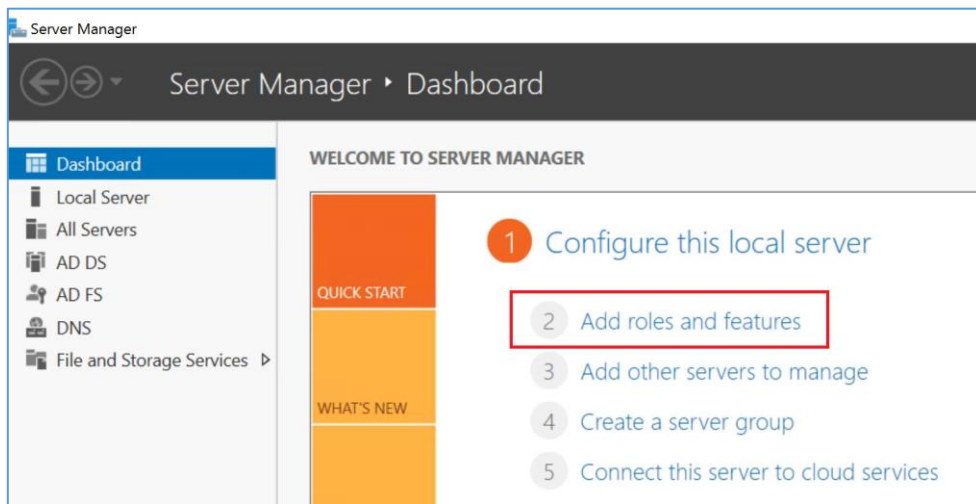
<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal>

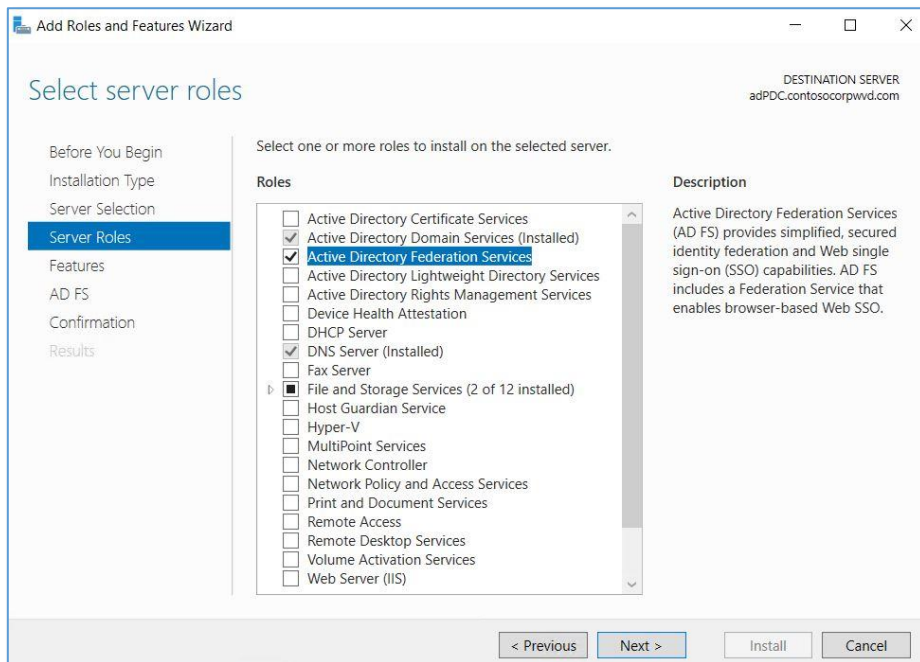
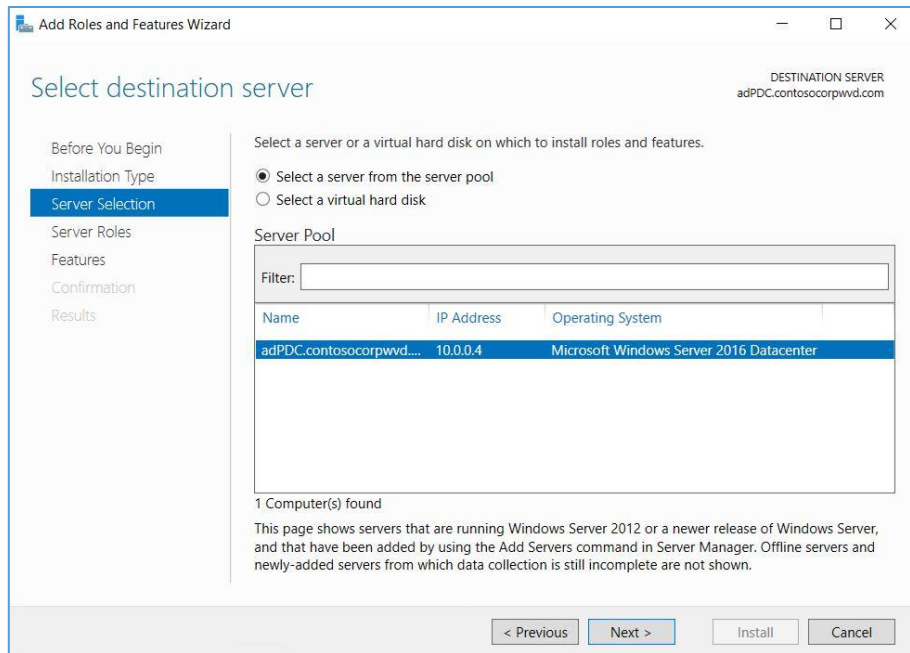
Configuring the domain controller / AD FS servers

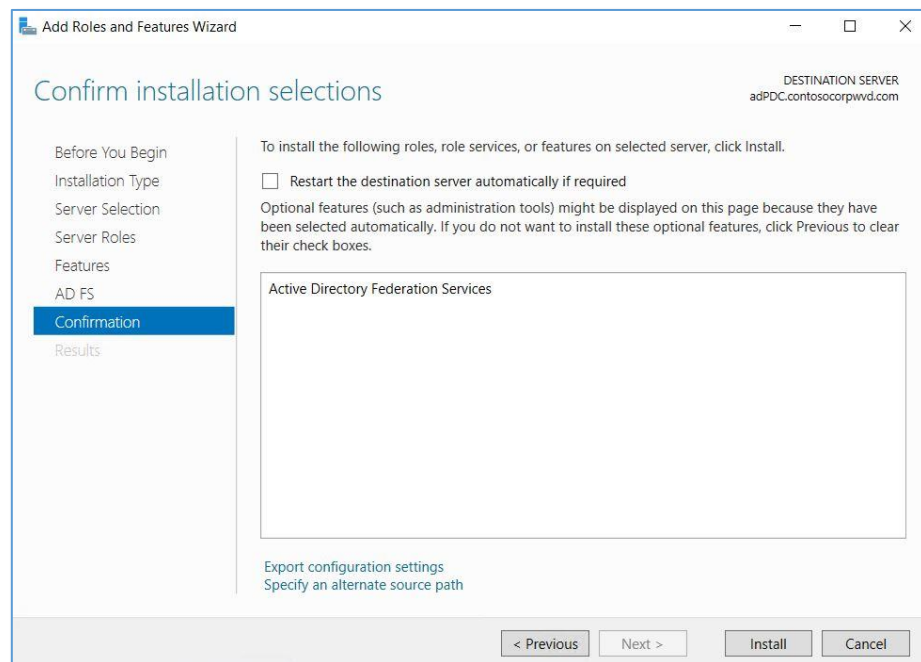
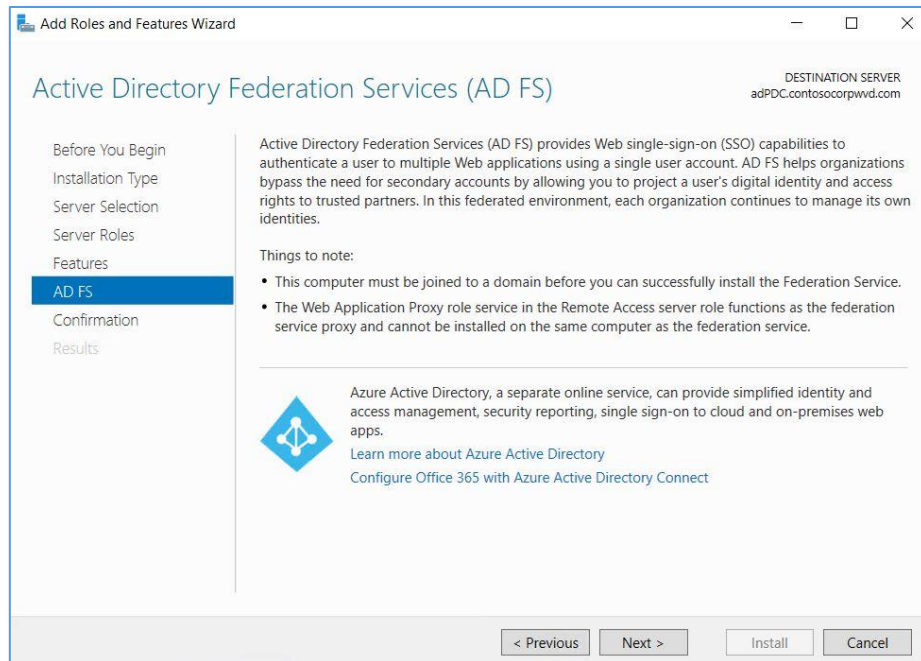
In order to authenticate an incoming authentication request, the AD FS service will need to contact the domain controller. In order to attain high availability, it is recommended to create an availability set of at-least 2 domain controllers. We will setup AD FS on our domain controllers.

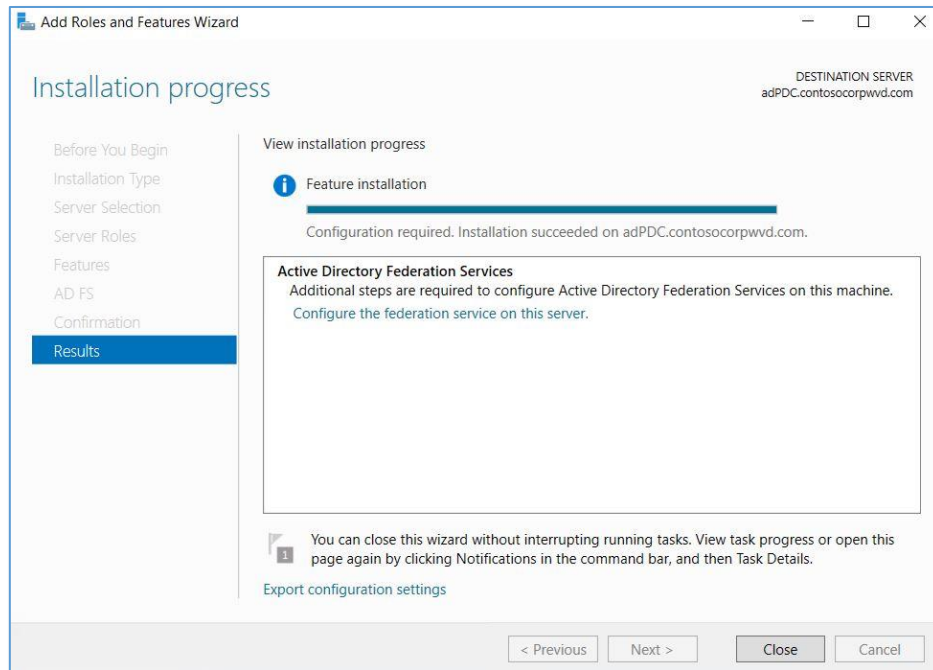
For this example, we show screen shots of the creation wizard for ADFS on contosocorpwvd.com

1. Log to your DC, open server manager, and ADD the ADFS role:

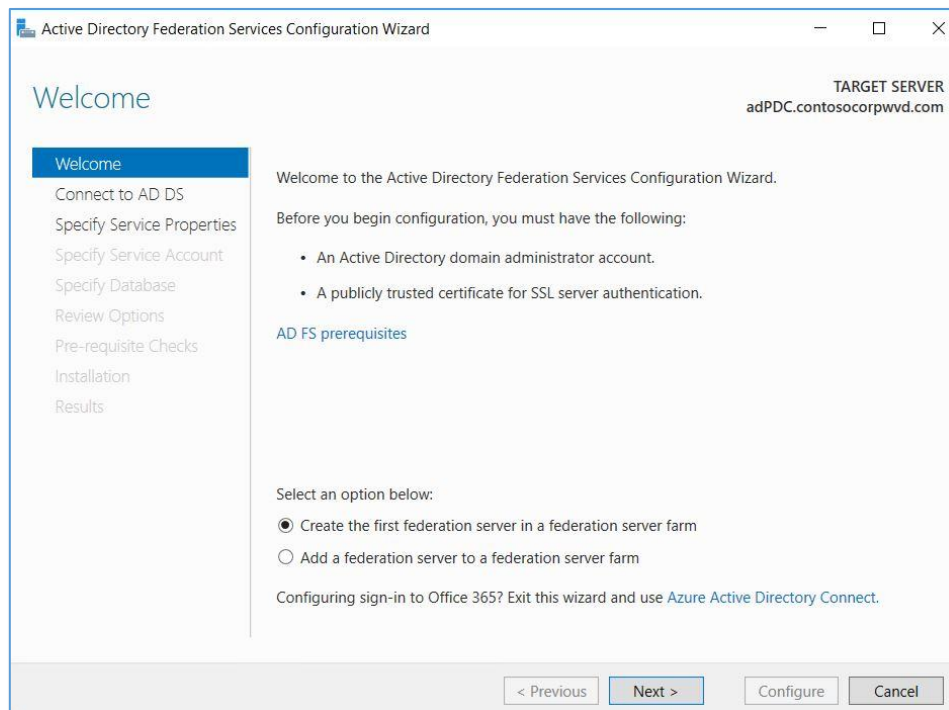
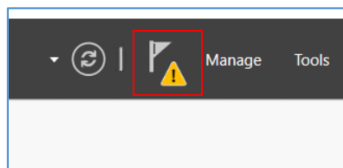








2. Configure AD FS by clicking the yellow alert at the top of Server Manager:



Active Directory Federation Services Configuration Wizard

Connect to Active Directory Domain Services

TARGET SERVER
adPDC.contosocorpwvd.com

Welcome

Connect to AD DS

Specify Service Properties

Specify Service Account

Specify Database

Review Options

Pre-requisite Checks

Installation

Results

Specify an account with Active Directory domain administrator permissions to perform the federation service configuration.

CONTOSOCORPWVD\adAdministrator (Current user) [Change...](#)

< Previous Next > Configure Cancel

Active Directory Federation Services Configuration Wizard

Specify Service Properties

TARGET SERVER
adPDC.contosocorpwvd.com

Welcome

Connect to AD DS

Specify Service Properties

Specify Service Account

Specify Database

Review Options

Pre-requisite Checks

Installation

Results

SSL Certificate: [AzureDSCExtension-d977c05f-d8e3-4368-80e0-000000000000](#) [Import...](#)

[View](#)

Federation Service Name: [AzureDSCExtension-d977c05f-d8e3-4368-80e0-000000000000](#)

Example: fs.contoso.com

Federation Service Display Name:

Users will see the display name at sign in.
Example: Contoso Corporation

< Previous Next > Configure Cancel

Active Directory Federation Services Configuration Wizard

TARGET SERVER
adPDC.contosocorpwvd.com

Specify Service Account

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

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: CONTOSOCORPWVD\

☒ Use an existing domain user account or group Managed Service Account

Account Name: CONTOSOCORPWV... Clear Select...

Account Password:

< Previous Next > Configure Cancel

Active Directory Federation Services Configuration Wizard

TARGET SERVER
adPDC.contosocorpwvd.com

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.

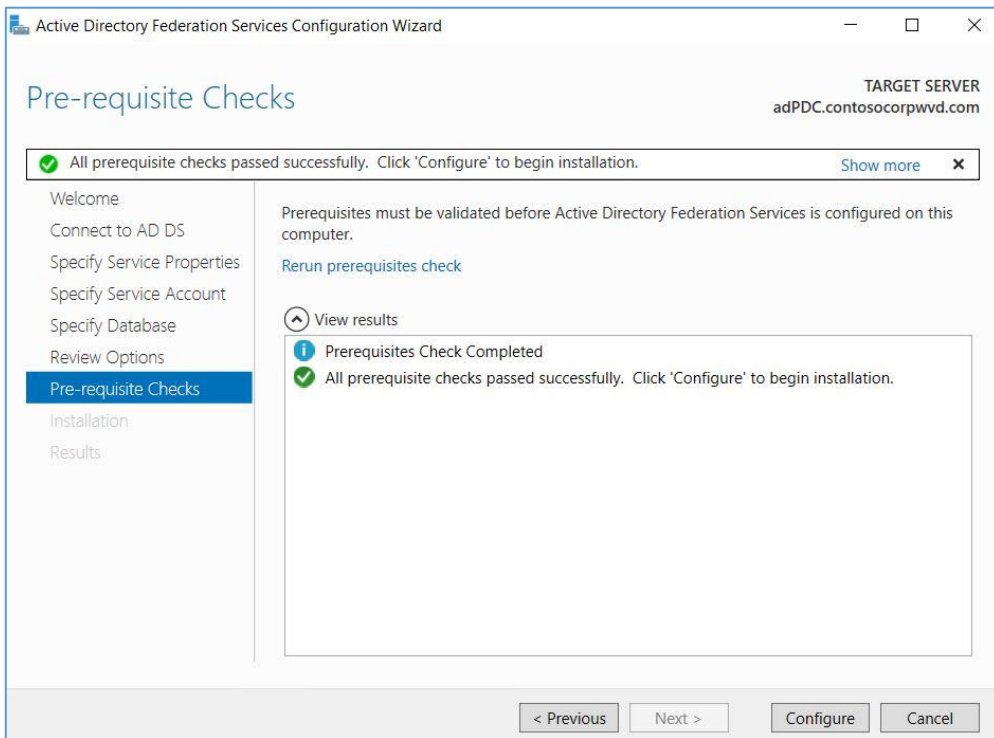
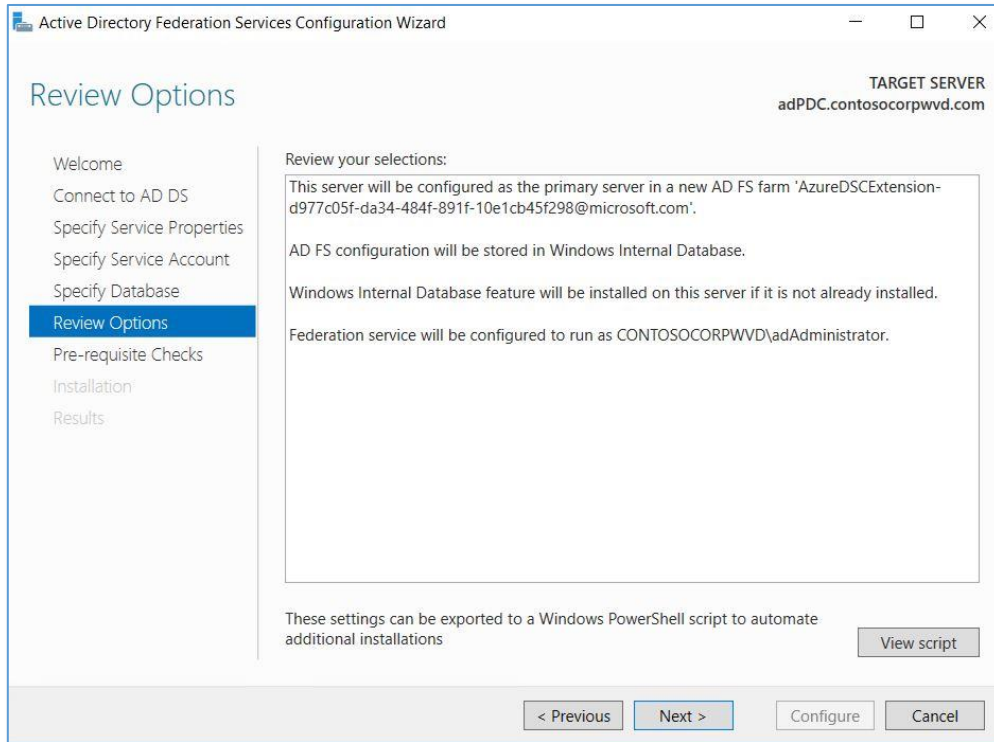
☐ Specify the location of a SQL Server database.

Database Host Name:

Database Instance:

To use the default instance, leave this field blank.

< Previous Next > Configure Cancel



Deploying Internal Load Balancer (ILB)

To ensure high availability of AD FS and Web Application Proxy servers, we recommend using a load balancer for AD FS servers *and* a load balancer for Web Application Proxy servers.

We do not cover this topic in this document. As a reference please visit the link for more information of creating load balancers in Azure: <https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-basic-internal-portal>

Configuring the Web Application Proxy (WAP) server

Web Application Proxy servers need not be joined to the domain, however, they do need to be able to communicate with the domain controllers. Install the Web Application Proxy roles on the two Web Application Proxy servers by selecting the Remote Access role, from Roles & Features. The setup wizard will guide you through completing the WAP installation. This topic is not covered on this document. For more information on how to deploy WAP, read [Install and Configure the Web Application Proxy Server](#).

Once we have the environment setup, it should have:

- Azure AD configured
- Synchronization with AD Connect running
- ADFS configured in a domain controller
- WAP configured, AD communication enabled
- Load balancers, **NSG secured**, ready and **published**

Now we can test the connection to the Windows Virtual Desktop Farm, to verify that a domain user of the Windows Server Active Directory network can access the Azure WVD PaaS without asking for user and password at the Azure Portal.

6. Support

Opening tickets

In case of an issue for Windows Virtual Desktop go to the Azure Portal and open a technical ticket based on your existing support plan at <https://azure.microsoft.com/en-us/support/create-ticket/>

Look for Service under **COMPUTE** and select **Windows Virtual Desktop-Preview**. You will find options to create tickets for the WVD service itself and for Office:

For Office issues you can file tickets during public preview in the Azure Portal when using Office in context of Windows Virtual Desktop.

Information you should provide for failed connection or management interactions when using the service:

- Use the diagnostics service to retrieve the **Activity ID** for failed connections or management interactions.
- Provide the approximate timeframe the issue happened

NOTE: This workflow will change post general availability.

Other resources you can leverage

Windows Virtual Desktop contains a number of knowledge articles as well as trouble shooting guides. Pay attention to the updated diagnostics chapter that provides Error scenarios you can mitigate: <https://docs.microsoft.com/azure/virtual-desktop/overview>

Exchange on our community forum on issues important to you for Windows Virtual Desktop: <https://techcommunity.microsoft.com/t5/Windows-Virtual-Desktop/bd-p/WindowsVirtualDesktop>

When setting up your environment you will be using other Azure Services. You can watch the health dashboard here to verify health state on any Azure service you are consuming: <https://azure.microsoft.com/en-us/status/>