Microsoft Azure Virtual Desktop



Azure Virtual Desktop for Business Premium Hands-on Lab

Version:

**V4**

Created by:

**Bogdan Grozoiu**

**&**   
**Joke Feije-Edelman**

# Table of Contents

[1 Table of Contents 2](#_Toc150348043)

[2 About the document 5](#_Toc150348044)

[3 Version history 5](#_Toc150348045)

[4 MFA Enforcement 5](#_Toc150348046)

[5 System requirements 6](#_Toc150348047)

[6 Account requirements 6](#_Toc150348048)

[7 Configure your lab environment 6](#_Toc150348049)

[7.1 Remote Desktop client 6](#_Toc150348050)

[7.2 Create a Microsoft Edge profile for your administrator account 7](#_Toc150348051)

[7.3 Naming conventions Azure resources 8](#_Toc150348052)

[8 Multi Factor Authentication (MFA) 9](#_Toc150348053)

[8.1 Review of Conditional Access Policies 9](#_Toc150348054)

[9 Prerequisites – Virtual network 10](#_Toc150348055)

[9.1 Create an Azure Virtual Network 11](#_Toc150348056)

[10 Prerequisites – Log Analytics workspace 12](#_Toc150348057)

[10.1 Create a Log Analytics workspace. 12](#_Toc150348058)

[11 Pre-requisites - Users and groups 13](#_Toc150348059)

[11.1 Create user 13](#_Toc150348060)

[11.2 Onboard user 14](#_Toc150348061)

[11.3 Create groups 14](#_Toc150348062)

[12 Azure Virtual Desktop 15](#_Toc150348063)

[12.1 Create a Host pool 16](#_Toc150348064)

[12.2 Create VMs for Hostpool 17](#_Toc150348065)

[12.3 Configure the Application group for the workspace 18](#_Toc150348066)

[12.4 Create an Application group for Azure Virtual Desktop Applications 20](#_Toc150348067)

[12.5 Check the Workspace settings. 21](#_Toc150348068)

[13 Additional configuration for Azure Active Directory Azure Virtual Desktop 22](#_Toc150348069)

[13.1 Host pool configuration 22](#_Toc150348070)

[13.2 Permissions on the Virtual Machines 23](#_Toc150348071)

[13.3 AADJoined check 24](#_Toc150348072)

[13.4 Assign licenses 25](#_Toc150348073)

[13.5 Conditional Access policy exception 25](#_Toc150348074)

[14 Azure Virtual Desktop workspace 26](#_Toc150348075)

[14.1 Connect to the Azure Virtual Desktop environment with the browser 26](#_Toc150348076)

[14.2 Connect to the Azure Virtual Desktop environment with the Remote Desktop application 28](#_Toc150348077)

[15 Best Practice 1: Scale the host pool for demand 28](#_Toc150348078)

[16 Best Practice 2: Hybrid Scenarios 28](#_Toc150348079)

[17 Appendix 1 - Migration from On-Premises to Azure Virtual Desktop 29](#_Toc150348080)

[18 Appendix 2 – Language settings 29](#_Toc150348081)

[18.1 Language settings in the Azure portal 29](#_Toc150348082)

[19 Appendix 3 - Enable Multi Factor Authentication (MFA) 29](#_Toc150348083)

[19.1 Prepare for Conditional Access 30](#_Toc150348084)

[19.2 Conditional access - enforce MFA for administrators 30](#_Toc150348085)

[19.3 Conditional access - enforce MFA for all users (configuration) 31](#_Toc150348086)

[20 Appendix 4 – Training prerequisites 32](#_Toc150348087)

[20.1 Tenant prerequisites 33](#_Toc150348088)

[Resources 33](#_Toc150348089)

[21 Appendix 5 – Resources 34](#_Toc150348090)

Disclaimer

© 2023 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

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.

Microsoft customers and partners may copy, use, and share these materials for planning, deployment, and operation of Microsoft products.

# About the document

Azure Virtual Desktop is a desktop and app virtualization service that runs on the cloud.

Here's what you can do when you run Azure Virtual Desktop on Microsoft Azure:

* Set up a multi-session Windows 11 or Windows 10 deployment that delivers a full Windows experience with scalability
* Present Microsoft 365 Apps for enterprise and optimize it to run in multi-user virtual scenarios
* Bring your existing Remote Desktop Services (RDS) and Windows Server desktops and apps to any computer
* Virtualize both desktops and apps
* Manage desktops and apps from different Windows and Windows Server operating systems with a unified management experience

If your current customer is hosting its remote desktop services on-premises. This Microsoft Learn page might be of value to you.

[Move on-premises Remote Desktop Services to Azure Virtual Desktop - Cloud Adoption Framework | Microsoft Learn](https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/migrate/azure-best-practices/contoso-migration-rds-to-wvd)

# Version history

V1 (May 2023):

* Initial version

V2 (June 2023)

* Updated based on the feedback initial runs

V3 (June 2023)

* Update on the Flow to configure your lab environment

V4 (October 2023)

* Major update on the training setup

# MFA Enforcement

Once you will receive your username and password, you will be forced to use your authenticator for the MFA with number matching. At the end of the event you can remove the entry from your authenticator

System requirements

As most configuration will be browser based, **a standard PC with recent Internet browser** with the “Remote Desktop” application (.msi version) installed on it or the ability to install the “Remote Desktop” application via .msi ([Windows 64-bit](https://go.microsoft.com/fwlink/?linkid=2139369)) will be sufficient for this lab.

The system used for this lab should contain a recent internet browser and the “Remote Desktop” application (msi deployment) or the ability to install the “Remote Desktop” application.

In these hands-on lab instructions we assume the usage of a PC with the Microsoft Edge browser.

To prevent constantly changing screens, it might be an idea to bring a small tablet or similar to keeping this lab document open during the hands-on lab.

**Note**: The embedded Remote Desktop Connection application (or the one that can be downloaded from the app store) cannot be used with Azure Virtual Desktop due to .draw file requirements.

More information about available clients to connect to Azure Virtual Desktop can be found here, [Remote Desktop clients for Azure Virtual Desktop - Azure Virtual Desktop | Microsoft Learn](https://learn.microsoft.com/en-us/azure/virtual-desktop/users/remote-desktop-clients-overview).

# Account requirements

During this hands-on lab, we will make use of a dedicated hands-on lab environment. There are no account pre-requisites.

Your trainer will let you know which administrator account will be used during this training. In many cases it is your own Azure Entra ID account which will be added as a guest account to the training tenant. But sometimes a new cloud-only account will be provided to you.

# Configure your lab environment

## Remote Desktop client

To be able to connect to the Azure Virtual Desktop as a user, the Remote Desktop client needs to be installed on your computer.

Check if the application has been installed on your computer:

1. In the search bar in your Windows task bar, type “Remote Desktop”
2. If installed the application will be available in the search results
3. Open the application
4. Click the ellipses (…) in the right upper hand corner and select **About**
5. Check the version number of your application, this should be 1.2.5105.0 or higher. There should as well be a green checkmark with the text “You’re up to date”.
6. If you are up to date, no further action is necessary, if not please follow the next steps to install the correct Remote Desktop application

Install the Remote Desktop application:

1. Use the following link to download the [Windows 64-bit](https://go.microsoft.com/fwlink/?linkid=2139369) version of the application.
2. Click on the downloaded file to install the application.
3. After the installation, follow the steps in the previous paragraph, to ensure the application installed successfully.

## Create a Microsoft Edge profile for your administrator account

In case you are not using your own Microsoft Entra ID as the administrator account for this training, it is recommended to work with a Microsoft Edge-profile linked to the account in this hands-on lab.

Usage of a profile will allow for quick switching between this demo-environment and your production environment

1. Open a new instance of Microsoft Edge.
2. Click on the circle with your profile picture or initials in the top bar. (Depending on your browser version, it can be found in the top left or top right corner)
3. Click the settings icon in the top right corner
4. Click **Add a Browser**.
5. Click **Add**.
6. Click **Choose an account** and select **+ Add new account.**
7. Click **Sign in to sync data.**
8. Fill in the sign in information. (*Hint: username is* [*avdadmin01@xxxx.onmicrosoft.com*](mailto:avdadmin01@xxxx.onmicrosoft.com)) click **Next**.
9. Fill in the password and click **Sign in**.
10. The “More information is required” message will appear to setup MFA for this user. Click **Next**.
11. On the next page follow the steps to get the Authenticator app if not already installed on your device. Click **Next** when the Authenticator is installed.
12. In the Authenticator app click **Add an account** and select **Work or School**. In the browser wizard click **Next**.
13. In the Authenticator app click **Scan the QR code** and scan the QR code in the wizard in the browser and click Next
14. A number will appear in the wizard that should be filled in in the Authenticator and click **Yes.**
15. After that approve with your personal Authenticator pin code, a “Notification approved” message will appear in the wizard in the browser.
16. Click **Next** in the browser wizard.
17. A success message will appear, click **Done**.
18. If the question arises or you would like to stay signed in, click “**No**”.
19. Click **Next**.
20. Click **Finish**.

## Naming conventions Azure resources

Just as with an on-premises environment, it makes sense to use a naming convention for the resources created within Azure. Give this naming convention some thought before creating any resources within the Azure tenant. Not all resources can be renamed after the creation, and you will end up with inconsistent named resources.

An example of a naming convention:

<max 4 letter abbreviation of the azure resource>-<environment>-<Azure region the resource resides>-<optional: purpose>-<serial number>

For a resource group in the Production environment, hosted in Western Europe, supporting the platform networking resources, the following name would suit the naming convention: “rg-p-we-network-01”.

For a Log Analytics Workspace in the acceptance environment, hosted in Northern Europe, the following name would suit the naming convention: “law-a-ne-01”.

# Multi Factor Authentication (MFA)

To perform the steps in this chapter, make sure that the Global Reader role is enabled for your administrator account.

The primary security measure for every organization **MUST** be to enable multi-factor authentication for **ALL USERS**. Always confirm that MFA is enabled for all users in every tenant that you work.

Although a “Man in the Middle” phishing attack can go around MFA, by injecting the MFA token (see <https://aka.ms/EvilGinx>) is provides more security than Single Factor Authentication.

This hands-on-lab will start with a check if the **Security Standards** have been enabled in this tenant. These “Security Standards” are by default enabled for all Azure-tenants provisioned after November 2020.

The Security Standards” are a limited set of minimal security settings to enable MFA for the Tenant.

## Review of Conditional Access Policies

In this step you will check, or a custom policy has been created to configure a conditional access policy which enables a more fine-grained MFA implementation.

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “entra” or “aad”.
2. In the **search results**, click “**Microsoft Entra ID**” under “Services”, the Microsoft Entra ID page will open.
3. On the Microsoft Entra ID page, in the left select the tab **Properties**.
4. At the very bottom of the page, under the “Security Defaults” section, make sure the following text is displayed “*Your organization is currently using Conditional Access policies which prevents you from enabling security defaults. You can use Conditional Access to configure custom policies that enable the same behavior provided by security defaults*.” A close-up of a text

   Description automatically generated
5. Click on the **Manage Conditional Access** link. The Conditional Access Policies page will open.
6. The first policy which we want to make sure is enforced is MFA for all accounts with privileged access, like global administrators or Helpdesk administrators.

Click on the “MFA for admins”. The policy configuration pages will open.

1. Click on the “Specific users included” link in the Assignments>Users section.
2. On the **Include** tab, check that **Select users and groups** is selected and the box in front of **Directory roles** is checked. A number of roles should be selected.
3. Check if in the section “Target resources”, All cloud apps are selected.
4. Under the section “Access controls>Grant access” click on the link “1 control selected”.
5. In the Grant information ensure that **Require multifactor authentication** has been selected.
6. Exit the policy and return to the Conditional access policies overview page.
7. The second policy which we want to make sure is enforced is conditional access for all users who sign in on the M365 applications, like Exchange Online and Microsoft Teams as well as the Azure portal.
8. Click on the “MFA for all users” policy. The policy configuration pages will open.
9. Click on the “All users included and specific users excluded” link in the Assignments>Users section.
10. On the **Include** tab, check that **All users** is selected.
11. On the **Exclude** tab, check that no one is excluded.
12. Click on the “All cloud apps included and 1 app excluded” link in the Target Resources section.
13. On the **Include** tab, check that **All Cloud apps** is selected.
14. On the **Exclude** tab, check that the **Azure Windows VM Sign-in** app is excluded.
15. Under the section “Access controls>Grant access” click on the link “1 control selected”.
16. In the Grant information ensure that **Require multifactor authentication** has been selected.

If any of these settings are incorrect, please use Appendix 3 - Enable Multi Factor Authentication (MFA) to configure these policies for your tenant.

# Prerequisites – Virtual network

To perform the steps in this chapter, make sure that the Owner role for your Management Group is enabled for your administrator account.

To be able to set up an Azure Virtual Desktop environment, an Azure Virtual Network (vnet) is required. For every network it is important to use a range of unique IP addresses. Connected networks cannot use the same IP address ranges. As this hands-on lab is a green field situation, no interference is expected but in a customer environment you most likely enter a brownfield situation.

## Create an Azure Virtual Network

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “vnet”.
2. In the **search results**, click “**Virtual Networks**” under “Services”, the virtual networks page will open.
3. On the Virtual Networks page, click “**Create**” in the menu bar to start the creation of a new Virtual Network.
4. In the “Create Virtual Network wizard” select the **subscription** in which this Virtual Network will reside.
5. For the Resource group, select “**Create new**” and fill in the name of the Resource Group, e.g., “rg-p-su-network-01<uniqueID>”
6. On the Instance details, fill in the **Name** of the Virtual Network, e.g., “vnet-p-su-01<uniqueID>”.
7. Select the **Region** in which the Virtual Network will be created, “South UK Europe”.
8. Click **Next : Security** to continue to the next tab in the wizard.
9. For now a **BastionHost** is not necessary, keep it disabled.
10. **DDoS Network Protection** is a valuable service to protect resources exposed to the internet. However this also is a more expensive service, so be conscious if the risk is worth the costs. For this lab we will leave the option for DDoS Network Protection disabled.
11. In a real-life scenario it is recommended to consider the usage of an [Azure Firewall](https://learn.microsoft.com/en-us/azure/firewall/overview) in your Virtual Network. As the focus of the hands-on-lab is on the Azure Virtual Desktop we select “Disable”.
12. Click **Next : IP Addresses**, to continue to the next tab in the wizard.
13. In the **IPv4 address space**, fill in the IP range for this Virtual Network, e.g., 10.0.0.0/24. By default, the wizard will propose an IP range. You are able to adjust the range or remove it for the IP ranges for this network by using the recycle bin icon behind the range. Make sure you have an appropriate amount of IP addresses available within the network. How many is dependent on which workloads will land in this virtual network. Proper network planning is just as important for Azure as it is for an on-premises environment.
14. Every Virtual Network needs one or more subnets. The wizard already proposes a default subnet for this network. You are able to adjust the configuration of this subnet by clicking it. You can add more than one subnet at this moment or add more in a later stage. For now we will adjust the default subnet, containing all ip-addresses in the Virtual Network, without a NAT gateway or Service Endpoints selected and give it a name following our naming conventions, e.g. “snet-p-su-01<uniqueID>”.  
    *NOTE: If the wizard does not propose a default subnet then click on “****Add subnet”*** *and give the subnet the same range as the IPv4 address space as you added in the previous step.*
15. Click **Next : Tags** to continue to the next tab in the wizard
16. Optionally add one or more tags to this resource. Tags can be used for all kinds of purposes but are mostly configured to associate resources to a cost center to enable the split of costs.
17. Click **Next : Review + Create** to continue to the next tab in the wizard.
18. Review all selections and if all is well, click **Create** to deploy the Virtual Network and its subnet.
19. A notification will be displayed when the deployment of the resources has been completed.

# Prerequisites – Log Analytics workspace

To create an Azure Virtual Desktop environment, we first need a Log Analytics workspace. A Log Analytics workspace is a unique environment that logs data from Azure Monitor and other Azure services, such as Azure Virtual Desktop, but it is also used by Microsoft Sentinel and Microsoft Defender for Cloud. Each workspace has its own data repository and configuration but might combine data from multiple services. It is recommended to centralize the usage of Log Analytics workspaces, as the power of the data resides in the ability to combine the data and find correlations. In many SMB Azure environments, only one Log Analytics workspace will be needed within the Azure environment.

## Create a Log Analytics workspace.

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “log”.
2. In the **search results**, click “**Log Analytics workspaces**” under “Services”, the Log Analytics workspaces page will open.
3. On the Log Analytics workspaces page, click “**Create**” in the menu bar to start the creation of a new Log Analytics workspace.
4. In the “Create Log Analytics workspace wizard” select the **subscription** in which this Log Analytics workspace will reside.
5. For the Resource group, select “**Create new**” and fill in the name of the Resource Group, e.g., “rg-p-su-management-01<uniqueID>”
6. On the Instance details, fill in the **Name** of the Log Analytics workspace, e.g., “law-p-su-01<uniqueID>”.
7. Select the **Region** in which the Log Analytics workspace will be created, “South UK”.
8. Click **Next : Tags** to continue to the next tab in the wizard.
9. Optionally add one or more tags to this resource. Tags can be used for all kinds of purposes but are mostly configured to associate resources to a cost center to enable the split of costs.
10. Click **Next : Review + Create** to continue to the next tab in the wizard.
11. Review all selections and if all is well, click **Create** to deploy the Log Analytics workspace.
12. A notification will be displayed when the deployment of the resource has been completed.

# Pre-requisites - Users and groups

To perform the steps in this chapter, make sure that the User administrator role is enabled for your administrator account.

When deploying an Azure Virtual Desktop environment, this usually is to support a particular set of users within an organization. In a real-life scenario, you will need to investigate which users have what requirements and specifications and then design the solution for the different user types. In this hands-on-lab we assume we will have a user base for a workspace environment and a user base for the availability of specific applications via Azure Virtual Desktop. As there is a limited number of licenses available, you will create one user.

In this hands-on-lab, we will create 2 groups of users to represent this user base and grant access to the solution. Please make use of users created by other participants to play around by placing users in one of the two different security groups, or in both to notice the difference.

## Create user

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “entra” or “aad”.
2. In the **search results**, click “**Microsoft Entra ID**” under “Services”, the Microsoft Entra ID page will open.
3. On the Microsoft Entra ID page, in the left-hand navigation , under manage, click “**Users**”.
4. Click **New user**.
   1. Username: johnd (or be creative)
   2. Name: John Doe (or be creative)
   3. Configure password: be creative and write the password down
5. Click **Create**.

## Onboard user

The newly created user in the previous section will need to reset its password and configure MFA. To get this out of the way the newly created user will logon to the azure portal to kickstart this process.

1. Open an InPrivate browser session in Microsoft Edge.
2. Open the Azure Portal (<https://portal.azure.com>)
3. Login with the email address of <your newly created user> and sign in.
4. Update the password
5. Configure MFA
6. Logoff

## Create groups

In this section 2 groups which will be created which each represent a user base.

* SG-AVD workspace users<uniqueID>
* SG-AVD application users<uniqueID>

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

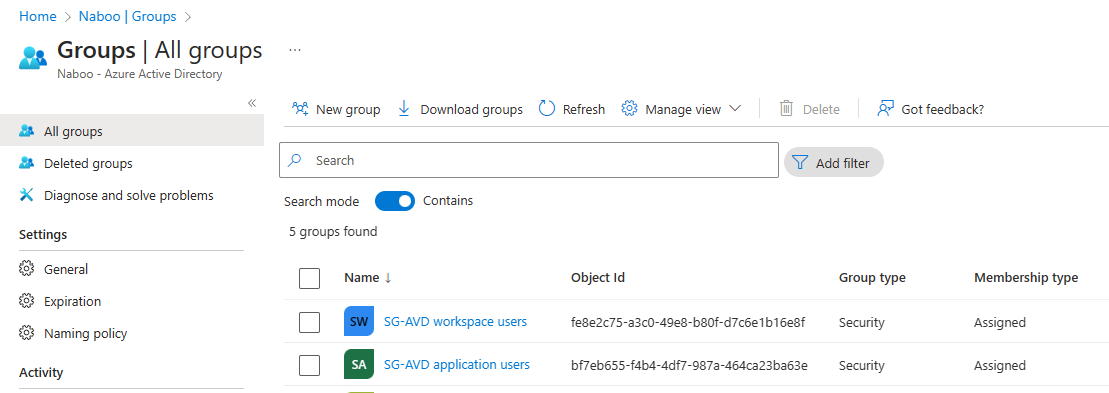
1. In the **search bar** at the top of the Azure Portal, type “entra” or “aad”.
2. In the **search results**, click “**Microsoft Entra ID**” under “Services”, the Microsoft Entra ID page will open.
3. On the Microsoft Entra ID page, in the left-hand navigation , under manage, click “**Groups**”.
4. Click **New group**.
5. Group type: **Security**  
   Group name: **SG-AVD workspace users**  
   Group description: **Security group for all users which use the Azure Virtual Desktop workspace**  
   Azure AD roles can be assigned to the group: **No**

Membership type: **Assigned**

1. Owner: Select yourself as an owner.
2. Members: Select the users:  
   **<Your own created user>**  
   **<User created by the participant at your left-hand side>**
3. Click **Create**.
4. Click **New group** .
5. Group type: **Security**  
   Group name: **SG-AVD application users**  
   Group description: **Security group for all users which use the Azure Virtual Desktop applications**  
   Azure AD roles can be assigned to the group: **No**

Membership type: **Assigned**

1. Owner: Select yourself as an owner.
2. Members: Select the users   
   **<Your own created user>**  
   **<User created by the participant at your right-hand side>**
3. Click **Create.**
4. Click **Refresh** to view the 2 newly created Security groups.



# Azure Virtual Desktop

To perform the steps in this chapter, make sure that the Owner role for your Management Group is enabled for your administrator account.

A host pool holds the compute power necessary for Azure Virtual Desktop. It is a collection of Azure virtual machines that register to Azure Virtual Desktop as session hosts when you run the Azure Virtual Desktop agent. All session host virtual machines in a host pool should be sourced from the same image for a consistent user experience. You control the resources published to users through application groups.

A host pool can be one of two types:

* Personal, where each session host (Virtual Machine) is assigned to an individual user. Personal host pools provide dedicated desktops to end-users that optimize environments for performance and data separation.
* Pooled, where user sessions can be load balanced to any session host (Virtual Machine) in the host pool. There can be multiple different users on a single session host at the same time. Pooled host pools provide a shared remote experience to end-users, which ensures lower costs and greater efficiency.

## Create a Host pool

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “avd”.
2. In the **search results**, click “**Azure Virtual Desktop**” under “Services”, the Azure Virtual Desktop page will open.
3. On the Azure Virtual Desktop page, click the “**Create a host pool**” button to start the creation of a new Host pool.
4. In the “Create a host pool wizard” select the **subscription** in which this Azure Virtual Desktop Host pool will reside.
5. For the Resource group, select “**Create new**” and fill in the name of the Resource Group, e.g., “rg-p-su-avd-01<uniqueID>”.
6. On the Instance details, fill in the **Name** of the host pool, e.g., “hp-p-su-01<uniqueID>”.
7. Select the **Region** in which the Virtual Network will be created, “South UK”.
8. Validation environment: This setting is used for testing configuration changes i.e.. a production environment. As this is an initial deployment, Select **No**.
9. Preferred app group type: You can choose here whether you want a full Azure Virtual Desktop available to your users on only want to make applications available. In this lab we start with a Azure Virtual desktop, so select **Desktop**.
10. Host pool type, in most SMB cases you want users to share the host pool to be as efficient with the resources as possible. In some cases, you need dedicated resources for users and in that case you can decide to use a personal host pool. For this hands-on-lab, select **Pooled**.
11. Load balancing algorithm, keep the selected **Breadth-first**.

The following load-balancing algorithms are available in Azure Virtual Desktop:

*Breadth-first load balancing* allows you to evenly distribute user sessions across the session hosts in a host pool. You don't have to specify a maximum session limit for the number of sessions.

*Depth-first load balancing* allows you to saturate a session host with user sessions in a host pool. You have to specify a maximum session limit for the number of sessions. Once the first session host reaches its session limit threshold, the load balancer directs any new user connections to the next session host in the host pool until it reaches its limit, and so on.

1. Max session limit, set to **2** users per session host.
2. Click **Next : Virtual Machines** to continue to the next tab in the wizard.
3. On the Virtual Machines page in the wizard, there is the ability to configure the Virtual Machines used in the host pool. The advantage of adding the Virtual Machines here is that the Azure Virtual Desktop agent will already be installed on the Virtual Machines. But as joining the Microsoft Entra will sometimes fail as not all resources are fully provisioned yet, we will skip this stap for now. For **Add Azure virtual machines**, select **No**.
4. Click **Next : Workspace** to continue to the next tab in the wizard.
5. On the workspace page, select **Yes** for Register desktop app group.
6. To this workspace, click **Create new** and type a name, e.g., wsp-p-su-01<uniqueID>
7. Click **Next : Advanced** to continue to the next tab in the wizard.
8. Enable diagnostic settings, for this hands-on-lab, keep the box **unchecked**. In a real-life scenario these diagnostics logs can be stored in the Log Analytics workspace. However, you need to be aware that data that you store will have a cost associated with that.
9. Click **Next : Tags** to continue to the next tab in the wizard.
10. Optionally add one or more tags to this resource. Tags can be used for all kinds of purposes but are mostly configured to associate resources to a cost center to enable the split of costs, e.g. Name: workload, Value: Azure Virtual Desktop-tailspintoys.
11. Click **Next : Review + Create** to continue to the next tab in the wizard.
12. Review all selections and if all is well, click **Create** to deploy the host pool and workspace.
13. A notification will be displayed when the deployment of the resources has been completed. **Please wait until the deployment succeeds before moving to the next step.**

## Create VMs for Hostpool

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “host pools”.
2. In the **search results**, click “**Host pools**” under “Services”, the Azure Host pool page will open.
3. Click the Host pool created in the previous section. The details page will open.
4. Click under the section Virtual Machines on the “**Total machines**” box to go the Session hosts overview.
5. Click **Add** to add new hosts (virtual machines) to the host pool.
6. On the Basics tab, all options are greyed out. Click **Next : Virtual Machines** to continue to the next tab in the wizard.
7. On the Virtual Machines page in the wizard, there is the ability to configure the Virtual Machines used in the host pool. The option **Add Azure virtual machines** has already been set to **Yes**.
8. Resource group for the virtual machines, here is the resource group of the host pool prefilled. Keep this value unless you are in favor of hosting the Virtual Machines in another resource group.
9. Name prefix, type the prefix which will be used for these virtual machines, e.g., “avd<uniqueID>”.
10. Virtual machine location, select **South UK**.
11. Availability options, select for this hands-on-lab **No infrastructure redundancy required**. In a real-life scenario, this setting will depend on the level of availability necessary. A higher level of availability will impact the costs.

For West Europe, where not all zones are freely available for every Virtual Machine type, it is highly recommended to use the “No Infrastructure redundancy” setting. This allows the hypervisor to select the most appropriate zone for every Virtual Machine and will result (for every region) in a higher SLA.

1. Security type, select for this hands-on-lab **Standard**. In a real-life scenario, this setting will depend on the level of security the service needs to enforce.
2. Image, select the most recent image for this hands-on-lab, **Windows 11**. **Enterprise multi-session, version 22H2 + Microsoft 365 Apps - Gen 2**.   
   Note: Because you have the Microsoft Business Premium licenses in your tenant, the Windows 11 Enterprise license is available to you.
3. Select the required Virtual Machine size: e.g., **D4as\_v5**. Please note that by default quotas are applied to your Azure tenant, also with regards to the amount of CPUs per region per subscription. In many cases this quota can be adjusted when there is a need for more than the current quota allows. Some quotas can be adjusted by the global administrator of your tenant, but for others a support ticket is needed.
4. Number of VMs, type **2** for this hands-on-lab.
5. OS disk type, keep the preselected **Standard SSD**.
6. OS disk size, keep the preselected **Default size (128GiB)**.
7. Boot diagnostics, for this hands-on-lab, select **Disable**.
8. Virtual Network, select here the Virtual Network created in paragraph 9.1 Create an Azure Virtual Network.
9. Subnet, select here the subnet created in paragraph 9.1 Create an Azure Virtual Network.
10. Network Security Group, for this hands-on-lab, select **None**. In a real-life scenario, plan for security using Network Security Groups, Firewalls etcetera.
11. Select which directory you would like to join, select **Microsoft Entra ID**.
12. Enroll VM in Intune, for this hands-on-lab, select **No**, in a real-life scenario enrolling the VMs in Intune is a cloud native way to manage these devices.
13. Fill in your own Virtual Machine Administrator account and password, e.g. account avdadmin and make a note of the username and password.
14. Custom Configuration script URL, is not applicable for this hands-on-lab.
15. Click **Next : Review + Create** to continue to the next tab in the wizard.
16. Review all selections and if all is well, click **Create** to deploy the Virtual Machines in the host pool.

## Configure the Application group for the workspace

An application group is a logical grouping of applications installed on session hosts in the host pool.

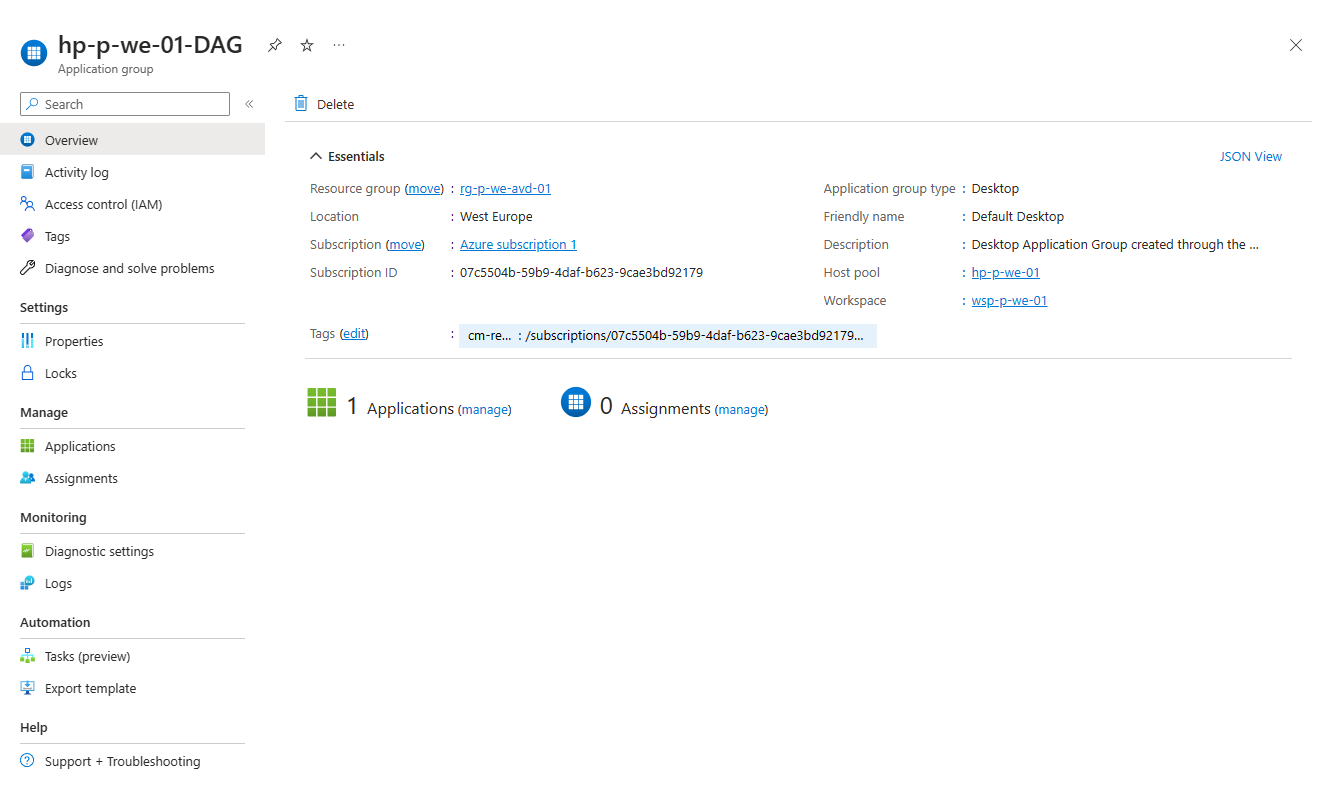
An application group can be one of two types:

* RemoteApp, where users access the RemoteApps you individually select and publish to the application group. Available with pooled host pools only.
* Desktop, where users access the full desktop. Available with pooled or personal host pools.

Users/groups will be assigned to an application group. As an application group is part of a workspace, in this way, by assigning users/groups to an application group users will be assigned to workspaces.

In the previous step where you created a host pool using the wizard, you as well already created a Desktop application group. In this section you will further configure this Desktop Application group.

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “avd”.
2. In the **search results**, click “**Azure Virtual Desktop**” under “Services”, the Azure Virtual Desktop page will open.
3. On the Azure Virtual Desktop page, in the left-hand navigation click “**Application groups**” under Manage.
4. See that the creation of the host pool also created a matching application group named <host pool name>-DAG. Click on this resource.
5. In the middle of the page, you see that one applications is part of the application group and this application group has no assignments for now.  
   
6. Click on the **(manage)** link under Applications in the middle of the page and see that the Desktop is available in this Application group.
7. Click the X icon in the upper right corner to close the page and go back to the Application group page.
8. Click on the **(manage)** link under Assignments in the middle of the page and see that no users or groups have been assigned to this Application group.
9. Click **Add**.
10. Search for the **SG-AVD workspace users** group, select the group and confirm the selection by clicking the **Select** button at the bottom of the page.
11. Click the X icon in the upper right corner to close the page and go back to the Assignments page.
12. Click the X icon in the upper right corner to close the page and go back to the Application group page.

## Create an Application group for Azure Virtual Desktop Applications

You can also publish an (line of business) application instead of a full desktop for specific users. To configure this, we will create a new Application group (RemoteApp). After the creation of the new Application Group, it will be associated with the existing “wsp-p-su-01” resource.

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “avd”.
2. In the **search results**, click “**Azure Virtual Desktop**” under “Services”, the Azure Virtual Desktop page will open.
3. On the Azure Virtual Desktop page, in the left-hand navigation click “**Application groups**” under Manage.
4. Click **Create**.
5. In the “Create an application group” wizard select the **subscription** in which this Azure Virtual Desktop Application Group will reside.
6. For the Resource group, select the Resources group newly created in 12.1, Create a Host pool“, e.g. “rg-p-su-avd-01<uniqueID>”.
7. For the Host pool, select the Host pool newly created in 12.1, Create a Host pool“, e.g. hp-p-su-avd-01<uniqueID>. After the selection the Location will be prefilled and cannot be adjusted.
8. For Application group type, select **Remote App (RAIL)**.
9. For Application group type, add the abbreviation AAG (For Applications Application Group) to the host pool name to be consistent with the naming of the Desktop Application Group, e.g., “hp-p-su-avd-01-AAG<uniqueID>”.
10. Click **Next : Applications** to continue to the next tab in the wizard.
11. On the Applications in the wizard, there is the ability to add Applications, click **+Add applications** link to select applications.  
    *Note: Under* ***Application Source*** *you can select the option Start Menu, File path or MSIX Package for various scenarios. For this lab we focus on Start Menu applications.*
12. Select some of the M365 Apps (at least Word), by selecting the app and to confirm using the Save button at the bottom of the page. Repeat step 11-12 for all apps you want to include.
13. Click **Next : Assignments** to continue to the next tab in the wizard.
14. On the Assignments tab in the wizard, click the **+ Add Azure AD users or user groups** link.
15. Search for the **SG-AVD application users** group, select the group and confirm the selection by clicking the **Select** button at the bottom of the page.
16. Click the X icon in the upper right corner to close the page and go back to the Assignments page.
17. Click **Next : Workspace** to continue to the next tab in the wizard.
18. Set Register application group to **Yes**, the Workspace name will be prefilled as there can only be one Workspace been registered per Azure Virtual Desktop host pool.
19. Click **Next : Advanced** to continue to the next tab in the wizard.
20. On the Advanced tab in the wizard, you can enable diagnostic settings. For this hands-on-lab, keep the box **unchecked**. In a real-life scenario these diagnostics logs can be stored in the Log Analytics workspace. But be conscious of what to log as the amount of data has cost impact.
21. Click **Next : Tags** to continue to the next tab in the wizard.
22. Optionally add one or more tags to this resource. Tags can be used for all kind of purposes but are mostly configured to associate resources with a cost center to enable the split of costs.
23. Click **Next : Review + Create** to continue to the next tab in the wizard.
24. Review all selections and if all is well, click **Create** to deploy the Application group.
25. A notification will be displayed when the deployment of the resource has been completed.

## Check the Workspace settings.

In the previous section in this chapter, we’ve created and added Application groups to the Azure Virtual Desktop Workspace. In this section, just for reference we’ll look into the settings of the Azure Virtual Desktop Workspace, named wsp-p-su-01 associated with the Azure Virtual Desktop host pool.

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “avd”.
2. In the **search results**, click “**Azure Virtual Desktop**” under “Services”, the Azure Virtual Desktop page will open.
3. On the Azure Virtual Desktop page, in the left-hand navigation click “**Workspaces**” under Manage.
4. **Click** on the **wsp-p-su-01 resource**, the wsp-p-su-01 page opens.
5. On the Workspace page, in the left-hand navigation click “**Application groups**” under Manage.
6. Note that the 2 Application groups (DAG and AAG) are associated with this workspace.

# Additional configuration for Azure Active Directory Azure Virtual Desktop

To perform the steps in this chapter, make sure that the Owner role for your Management Group is enabled for your administrator account.

To support Azure Virtual Desktop with Azure Active Directory as an authentication provider without any Directory Services some additional configuration is needed. This chapter describes these additional configuration items.

* Host pool configuration
* Permissions on the Virtual Machine
* Active Directory joined hosts
* User licensing
* Conditional Access policy exception

Host pool configuration

In the Host pool properties, the RDP properties need to be set to use Azure Active Directory to sign in for RDP.

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “avd”.
2. In the **search results**, click “**Azure Virtual Desktop**” under “Services”, the Azure Virtual Desktop page will open.
3. On the Azure Virtual Desktop page, in the left-hand navigation click “**Host pools**” under Manage.
4. On the Azure Virtual Desktop page, click on the host pool created in 12.1
5. Click **RDP Properties** in the left-hand navigation under Settings.
6. On the Connection information tab, set the Azure AD authentication from “Not configured” to “**Connections will use Azure AD authentication to provide Single sign-on**”.
7. Leave the next option “Credential Security Support Provider” to the default **“RDP will use CredSSP if the operating system supports CredSSP**”
8. Check the options available under the tabs “Session behavior", “Device Redirection”, “Display Settings” and “Advanced”.
9. Leave all other options as is.
10. Click **Save** to confirm the new setting.

Permissions on the Virtual Machines

As Azure Active Directory is used as authentication and authorization provider, the users who will use the Azure Virtual Desktop Virtual Machines need permissions to logon to these Virtual Machines. The minimal set of permissions needed for is the “Virtual Machine User Login” role. You can assign the **Virtual Machine User Login** or **Virtual Machine Administrator Login** role either on the VMs, the resource group containing the VMs, or the subscription. In this lab we will assign the role on resource group level, to allow this permissions for every virtual machine in the AVD solution.

To grant users access to Microsoft Entra joined VMs, you must [configure role assignments for the VM](https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows" \l "configure-role-assignments-for-the-vm). You can assign the **Virtual Machine User Login** or **Virtual Machine Administrator Login** role either on the VMs, the resource group containing the VMs, or the subscription. We recommend assigning the Virtual Machine User Login role to the same user group you used for the application group at the resource group level to make it apply to all the VMs in the host pool.

The following instructions on assigning permissions to the Virtual Machines in the host pools needs to be performed for every Azure Virtual Desktop Virtual Machine.

Next to this the Virtual Machines need to be Azure Active Directory joined, as this configuration check has to be performed on every Virtual Machine, these steps will be combined to reduce clicking in the Azure Portal.

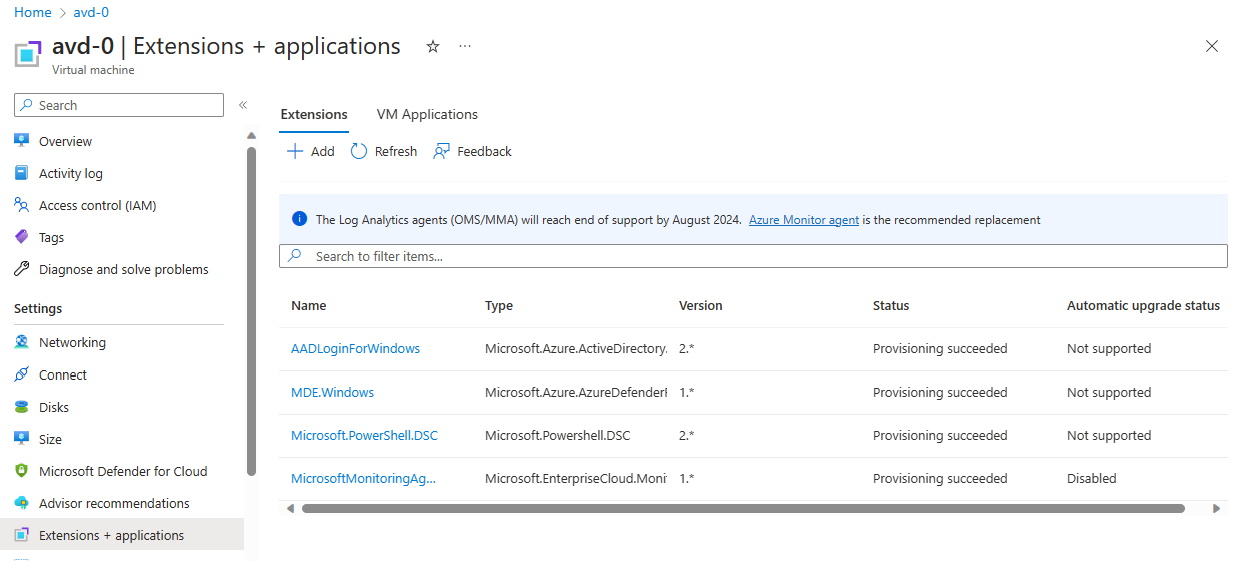
Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “rg”.
2. In the **search results**, click “**Resource group**” under “Services”, the Azure Resource Group page will open.
3. On the Azure Resource Group page, click on the resource group that hosts your host pools created in 12.1
4. Click **Access Control (IAM)** in the left-hand navigation.
5. Click on the “**Add**” button and choose “**Add role assignment**”
6. On the Add role assignment wizard, search for the **Virtual Machine User login** role, select this role and click **Next**.
7. On the Members tab, keep Assign Access to on **User, group, or service principal**
8. Click **+ Select members**.
9. Search for “SG-AVD” this will retrieve both AVD related groups created in section 11.2 Create groups.
10. Select both **groups** and confirm by clicking the **Select**-button at the bottom of the page.
11. Click **Next**.
12. Click the **Review + assign** button.
13. A notification will be displayed when the assignments have been completed.

AADJoined check

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the search bar at the top of the Azure Portal, type “avd”.
2. In the search results, click “Azure Virtual Desktop” under “Services”, the Azure Virtual Desktop page will open.
3. On the Azure Virtual Desktop page, in the left-hand navigation click “Host pools” under Manage. 4. On the Azure Virtual Desktop page, click on the host pool created in 12.1
4. Under Virtual Machines in the middle of the page, Click on Total machines, a screen with an overview of the Virtual Machines in the host pool is displayed.
5. Click on the first Virtual Machine, named <prefix>-0.
6. On the summary page, click again on the name of the Virtual Machine, which leads you to its homepage.
7. Click Extensions + applications in the left-hand navigation under Settings.
8. Check or the AADLoginforWindows extension is available.
9. Repeat steps 5 – 8 for every other Virtual Machine in the host pool.



In case the installation of the Virtual Machine extension has failed, use the following link [Troubleshoot deployment problems](https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#troubleshoot-deployment-problems).

Assign licenses

To perform the steps in this section, make sure that the User administrator role is enabled for your administrator account.

Although it is possible to assign licenses to individuals, it is easier to assign the licenses to a group. In this hands-on-lab we will assign the license for the usage of Windows Enterprise to the groups “SG-AVD workspace users” and “SG-AVD application users”.

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “entra” or “aad”.
2. In the **search results**, click “**Microsoft Entra ID**” under “Services”, the Microsoft Entra ID page will open.
3. On the Microsoft Entra ID page, in the left-hand navigation , under manage, click “**Groups**”.
4. Click **SG-** **AVD workspace users**.
5. In the left-hand navigation , under manage, click **Licenses**.
6. Click **Assignments** in the top menu bar.
7. Select **Windows 10/11 Business** or **Windows 10/11 Enterprise**.
8. Click **Save**.
9. Click twice on the X icon in the upper right corner.
10. Repeat step 4-9 voor **SG-AVD application users**.

Conditional Access policy exception

To perform the steps in this chapter, make sure that the Global Reader role is enabled for your administrator account.

In this section you will review the exception that has been made in the Conditional Access policy for the Azure Windows VM Sign-In.

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account as created in paragraph “7.2 Create a Microsoft Edge profile for your administrator account”.

1. In the **search bar** at the top of the Azure Portal, type “entra” or “aad”.
2. In the **search results**, click “**Microsoft Entra ID**” under “Services”, the Microsoft Entra ID page will open.
3. On the Microsoft Entra ID page, in the left-hand navigation , under manage, click **Security**.
4. On the Security page, in the left-hand navigation , under Protect, click **Conditional Access**.
5. On the **Conditional Access** page, click **Policies** in the left-hand menu.
6. Click the policy **MFA for all users** to review the policy.
7. On the Assignments>Cloud apps or actions, click **All cloud apps**.
8. On the **Exclude** tab, check that the **Azure Windows VM Sign-in** app is excluded.

# Azure Virtual Desktop workspace

The Azure Virtual Desktop environment for the workspace is now available and can be used. This chapter will test the workspace functionality.

The user used to login cannot be a Guest user in the Microsoft Entra ID tenant and needs to have MFA setup to be able to access the workspace.

Make sure you performed section 7.1, Remote Desktop client before attempting to start this chapter.

## Connect to the Azure Virtual Desktop environment with the browser

1. Open an InPrivate browser session in Microsoft Edge.
2. Open the following URL [Remote Desktop Web Client (microsoft.com)](https://client.wvd.microsoft.com/arm/webclient/index.html)
3. Login with the email address of <your left-hand participant created user> and sign in.
4. As <your left-hand participant created user> is member of only the SG-AVD workspace users group, he will only see the Workspace being available. Open the desktop and see a desktop available for this user while logging in with Microsoft Entra ID credentials.
5. Close the browser and open a new InPrivate browser session in Microsoft Edge.
6. Login with the email address of the <your right-hand participant created user> and sign in.
7. As <your right-hand participant created user> is member of only the SG-AVD application users group, he will only see the Applications (at least Word) being available. Open the Word application and see the app available for this user while logging in with Microsoft Entra ID credentials.
8. Close the browser and open a new InPrivate browser session in Microsoft Edge.
9. Login with the email address of the user <your own created user> and sign in.
10. As <your own created user> is a member of both SG-AVD users group, she will see as well the Applications (at least Word) as the Desktop being available. Open the Word application and see the app available for this user while logging in with Microsoft Entra ID credentials. Open the desktop and see a desktop available for this user while logging in with Microsoft Entra ID credentials.

## Connect to the Azure Virtual Desktop environment with the Remote Desktop application

1. In the search bar in your Windows task bar, type “Remote Desktop”.
2. Open the application named “**Remote Desktop**” (not the “Remote Desktop Connection”)
3. Click the ellipses (…) in the right upper hand corner and select **Subscribe.** If you want to use the **Subscribe with URL**, use the following URL: <https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery> .
4. Fill in the email address of <your left-hand participant created user> and sign in.
5. As <your left-hand participant created user> is member of only the SG-AVD workspace users group, he will only see the Workspace being available. Open the desktop and see a desktop available for this user while logging in with Microsoft Entra ID credentials.
6. Click the ellipses (…) in the right upper hand corner and select **Subscribe.** If you want to use the **Subscribe with URL**, use the following URL: <https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery>.
7. Fill in the email address of the user <your right-hand participant created user> and sign in.
8. As <your right-hand participant created user> is member of only the SG-AVD applications users group, he will only see the Applications (at least Word) available. Open the Word application and see the app available for this user while logging in with Microsoft Entra ID credentials.
9. Click the ellipses (…) in the right upper hand corner and select **Subscribe.** If you want to use the **Subscribe with URL**, use the following URL: <https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery>.
10. Fill in the email address of the user <your own created user> and sign in.
11. As <your own created user> is a member of both SG-AVD users group, she will see as well the Applications (at least Word) as the Desktop being available. Open the Word application and see the app available for this user while logging in with Microsoft Entra ID credentials. Open the desktop and see a desktop available for this user while logging in with Microsoft Entra ID credentials.

# Best Practice 1: Scale the host pool for demand

To only pay for the resources needed, make sure you scale your host pool.

[Create an autoscale scaling plan for Azure Virtual Desktop | Microsoft Learn](https://learn.microsoft.com/en-us/azure/virtual-desktop/autoscale-scaling-plan)

# Best Practice 2: Hybrid Scenarios

# Appendix 1 - Migration from On-Premises to Azure Virtual Desktop

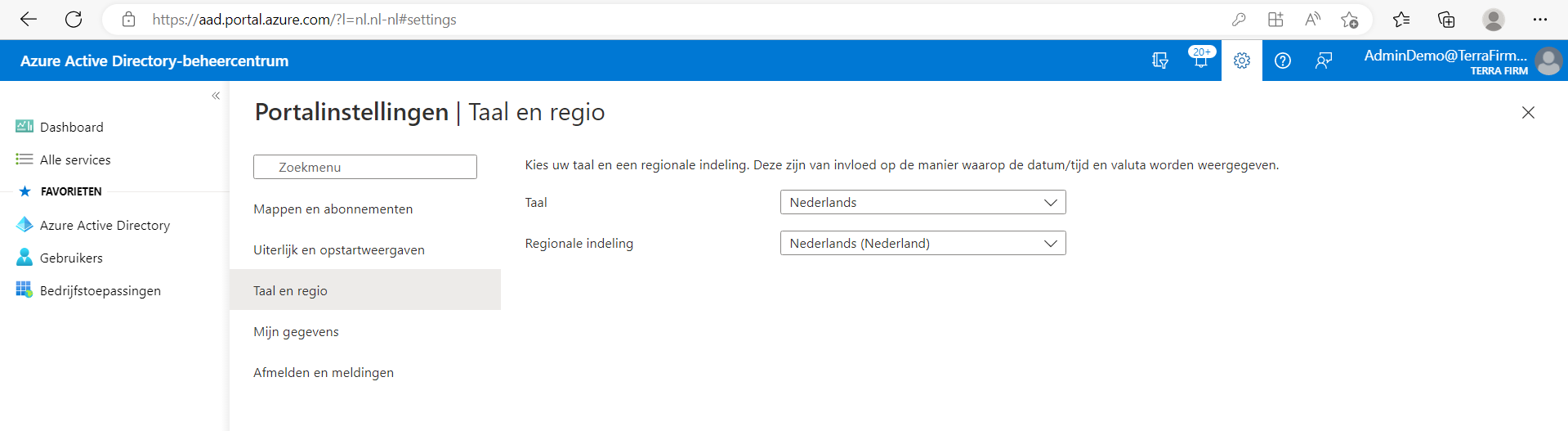
[About Azure Migrate - Azure Migrate | Microsoft Learn](https://learn.microsoft.com/en-us/azure/migrate/migrate-services-overview)

[Move on-premises Remote Desktop Services to Azure Virtual Desktop - Cloud Adoption Framework | Microsoft Learn](https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/migrate/azure-best-practices/contoso-migration-rds-to-wvd#current-architecture)

# Appendix 2 – Language settings

## Language settings in the Azure portal

In the Azure (Active Directory) portal in the upper right-hand corner, click on the clog icon. Go to Language and region settings. Select here your preferred language and the regional settings.



# Appendix 3 - Enable Multi Factor Authentication (MFA)

The primary security measure for every organization **MUST** be to enable multi-factor authentication for **ALL USERS**.

Although a “Man in the Middle” phishing attack can go around MFA, by injecting the MFA token (see <https://aka.ms/EvilGinx>) is provides more security than Single Factor Authentication.

This document contains the steps on how to set up Multi Factor Authentication in case you need it isn’t or isn’t configured correctly for your tenant. To perform the configuration of MFA the Global Administrator role needs to be enabled for your administrator account.

First it will start with a check if the **Security Standards** have been enabled in this tenant. These “Security Standards” are by default enabled for all Azure-tenants provisioned after November 2020. The Security Standards” are a limited set of minimal security settings to enable MFA for the Tenant.

## Prepare for Conditional Access

In this step the Security Defaults will be turned off, this will enable the creation of a custom policy to configure a conditional access policy which enables a more fine-grained MFA implementation.

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account.

1. In the **search bar** at the top of the Azure Portal, type “entra” or “aad”.
2. In the **search results**, click “**Microsoft Entra ID**” under “Services”, the Microsoft Entra ID page will open.
3. On the Microsoft Entra ID page, in the left select the tab **Properties**.
4. At the very bottom of the page, under the “Access management for Azure Resources” section, click on the **Manage security defaults** link.
5. By default, the Security defaults are enabled.
6. Turn the Security defaults off, by selecting **Disabled (not recommended)**.
7. Select **My organization uses Conditional Access**.
8. To confirm your selection, click **Save** at the bottom of the page
9. Confirm the pop-up prompt.
10. Click the X icon in the upper right corner.

## Conditional access - enforce MFA for administrators

The first policy which we will configure is to enforce MFA for all accounts with privileged access, like global administrators or Helpdesk administrators.

The policy will be enabled in the Report only mode, this is the safest way to start with conditional access (You want to avoid the possibility that you lock yourself out of the tenant).

Go to the Azure Portal (<https://portal.azure.com> ) using the Edge browser profile attached to your administrator account.

1. In the **search bar** at the top of the Azure Portal, type “entra” or “aad”.
2. In the **search results**, click “**Microsoft Entra ID**” under “Services”, the Microsoft Entra ID page will open.
3. On the Microsoft Entra ID page, in the left-hand navigation, under manage, click **Security**.
4. On the Security | Getting started page, in the left-hand navigation, under Protect, click **Conditional Access**.
5. Click **Create new policy**.
6. Name: **MFA for admins**.
7. Assignments>Users, click **0 users and groups selected**.
8. On the **Include** tab, select **Select users and groups** and check the box in front of **Directory roles**.
9. Select all roles on which you like to enable MFA. As a bare minimum select at least the Global Administrator role.
10. Under “Cloud apps or actions” click **No cloud apps, actions, or authentication contexts selected**.
11. On the **Include** tab, select **All cloud apps**.
12. Access control>Grant, click **0 controls selected**.
13. Under the section “Access controls” click on the option **Grant access**.
14. Check the box in front of **Require multifactor authentication**.
15. Confirm at the bottom, click **Select**.
16. Under the section “Session” click **0 controls selected**.
17. Select **Persistent browser session > Never persistent**.

Note: for safety reasons, you don’t want to allow permanent browser sessions as these browser sessions can remain active even when the browser is restarted.

1. Confirm at the bottom, click **Select**.
2. Confirm that the Enable policy is set to **Report only**.
3. Click **Create**.

Note: the conditional access policy can exclude users from signing in. By default, the user configuring the policy will be excluded from the policy to prevent a lockout of the tenant.

1. Click **I understand that my account will be impacted by this policy. Proceed anyway**.
2. Confirm at the bottom, click **Create**.

As an example, this policy will be configured as Report only. The next policy for the users will be configured as enforce.

## Conditional access - enforce MFA for all users (configuration)

This second policy will enforce conditional access for all users who sign in on the M365 applications, like Exchange Online and Microsoft Teams as well as the Azure portal.

1. We assume you are still in the Microsoft Entra ID portal on the Conditional Access policy page. If this is not the case please follow step 1-5 from the previous section.
2. Click **Create new policy**.
3. Name: **MFA for users**.
4. Assignments>Users, click **0 users and groups selected**.
5. On the **Include** tab, select **Select users and groups** and check the box in front of **All Users**.
6. Assignments>Cloud apps or actions, click **No cloud apps, actions, or authentication contexts selected**.
7. On the **Include** tab, select **Select apps**.
8. Click **None** under Select
9. On the **Include** tab, check that **All Cloud apps** is selected
10. On the **Exclude** tab, check that the **Azure Windows VM Sign-in** app is excluded.
11. **5**
12. Confirm at the bottom, click **Select**.
13. Access control>Grant, click **0 controls selected**.
14. Select **Grant access**.
15. Check the box in front of **Require multifactor authentication**.
16. Confirm at the bottom, click **Select**.
17. Toggle the Enable policy switch to **On**.
18. Click **Create**.
19. Click **I understand that my account will be impacted by this policy. Proceed anyway**.
20. Confirm at the bottom, click **Create**.

# Appendix 4 – Training prerequisites

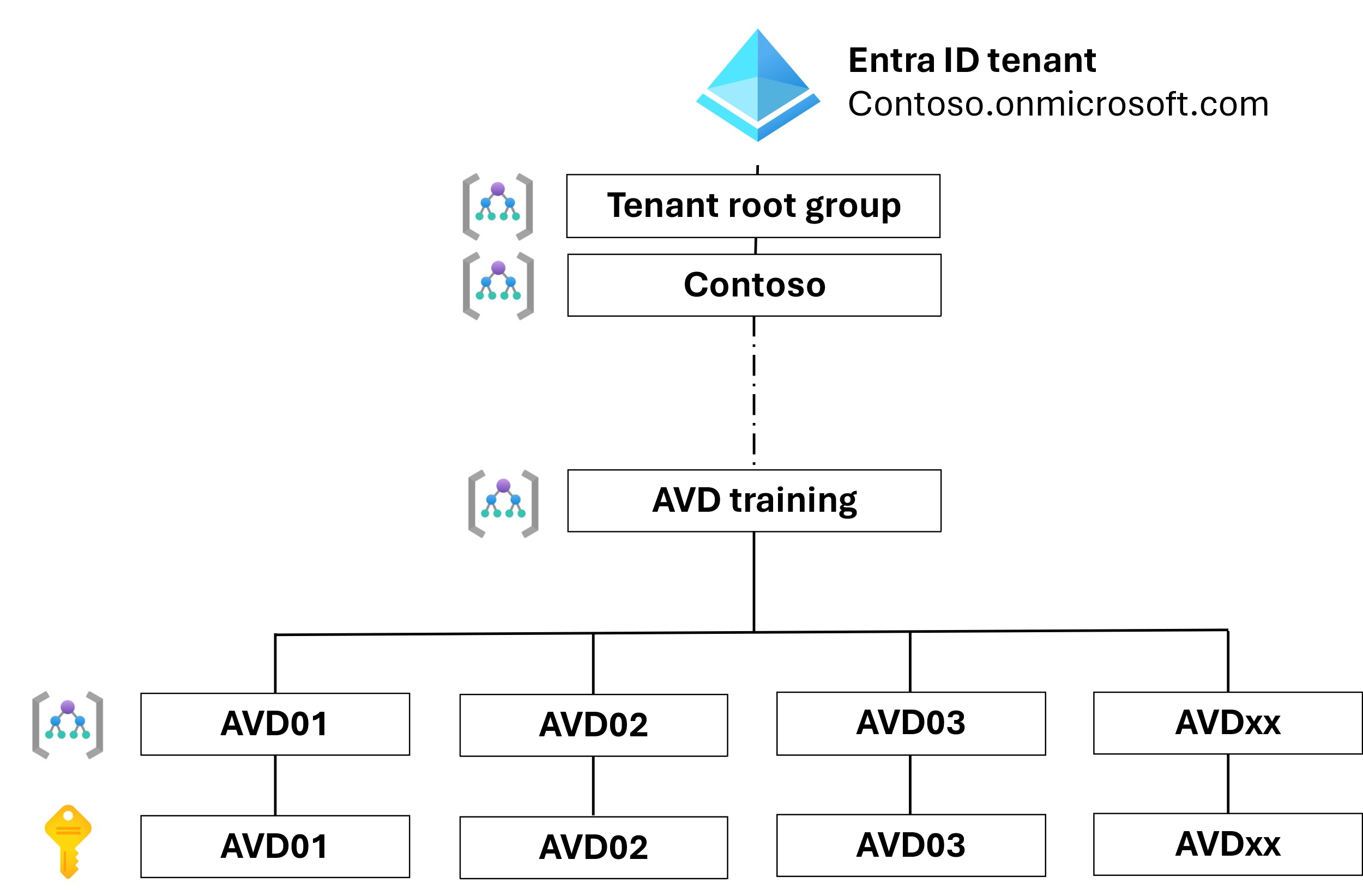
To be able to run this training session a training environment is needed. Previous attempts in using trial tenants for the participants have been less successful. In this chapter the prerequisites for this training are described.

Ideally, we recommend the usage of Privileged Identity Management (PIM) to assign the administrator role to the participants this will give the advantage that you can only grant them administrator access during a specific timeframe.

## Tenant prerequisites

For this training an Azure needs to be available with the following configuration

* MFA enabled for all users and admins
* One account per participant (overhead/scripts/provision-hackathon-participants.ps1)
* One subscription per participant
* Management groups enabled
* One root Management group
* One Management Group per subscription
  + Per Management group, one participant eligible for Owner permissions via PIM
* All participants member of a group which has:
  + Automatic License assignment (A license including P2 for PIM purpose - M365 E5/ Premium Business for SMB)
  + Eligible for Global Reader permissions via PIM
  + Eligible for User Administrator permissions via PIM
* Availability of Business Premium licenses (**Windows 10/11 Business**) for the Azure Virtual Desktop users (1 per participant)



Resources

Pipelines and scripts which can be used as a foundation for automation for this setup can be found here

Management group creation without the need for global admin permissions

[Endor/.github/workflows/1-process-management-groups.yml at main · msft-nl-gps/Endor · GitHub](https://github.com/msft-nl-gps/Endor/blob/main/.github/workflows/1-process-management-groups.yml)

Participant creation, role assingment and licensing

[overhead/.github/workflows/create-all-users.yml at main · msft-nl-gps/overhead · GitHub](https://github.com/msft-nl-gps/overhead/blob/main/.github/workflows/create-all-users.yml)

Resource cleanup after training, including users (groups, management groups and sunscriptions will remain)

[overhead/.github/workflows/deprovision-everything.yml at main · msft-nl-gps/overhead · GitHub](https://github.com/msft-nl-gps/overhead/blob/main/.github/workflows/deprovision-everything.yml)

# Appendix 5 – Resources

[Azure Virtual Desktop documentation | Microsoft Learn](https://learn.microsoft.com/en-us/azure/virtual-desktop/)