chawn
+44 (0)121 314 2253
info@chawn.com

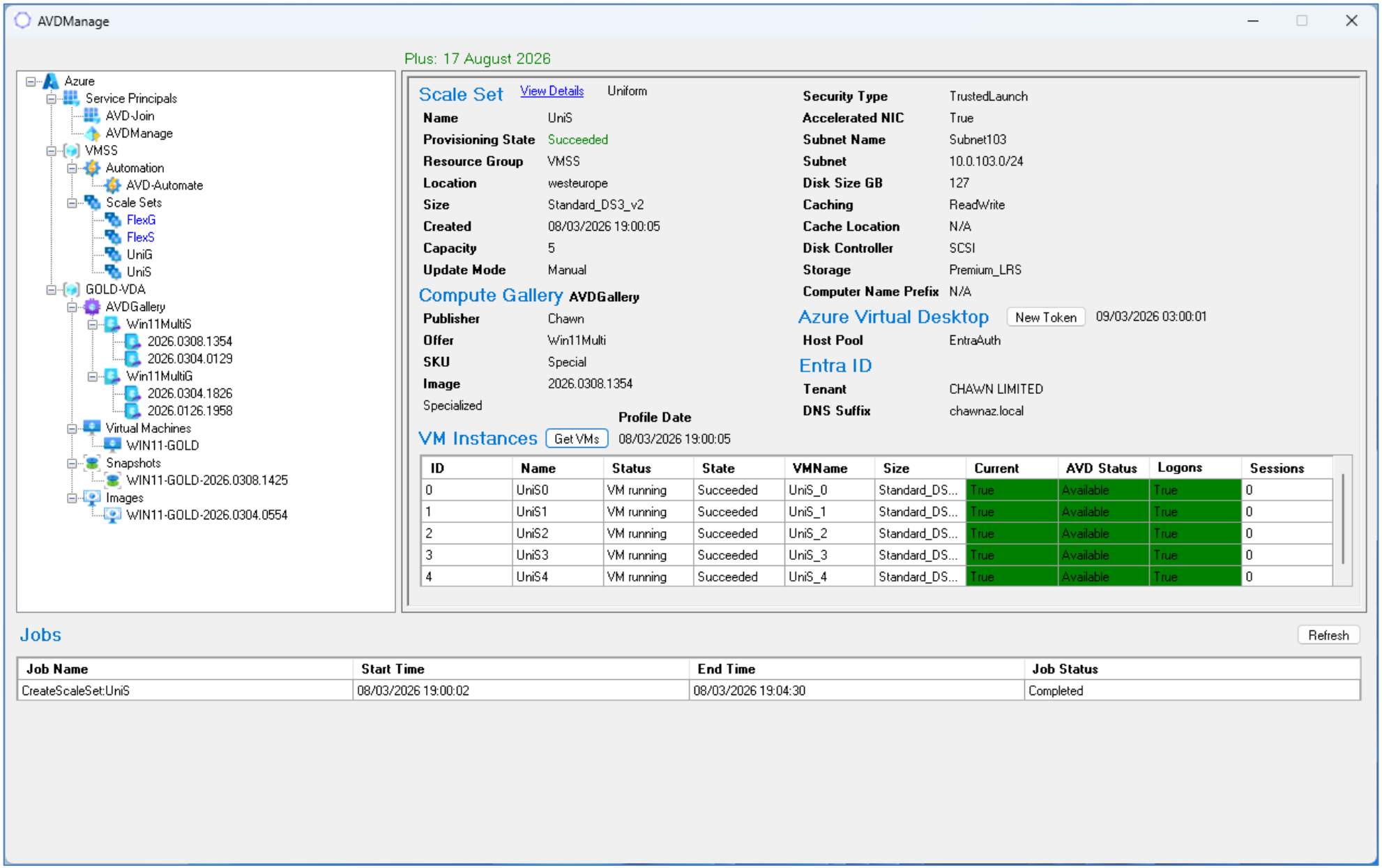
Desktops & Applications Virtualisation & Integration

AVDManage 2.5.0.0 Administration

Master Image Management for Azure Virtual Desktops

Document Details

Document Name	AVDManage 2.5.0.0 Administration
Author	DG – Chawn Limited
Version	1.0 (AVDManage Version 2.5.31.0)
Date	4th March 2026
Status	Final



Contents

1. Introduction 8
1.1 Updates 9
Version 2.5.0.0 9
Version 2.3.0.0 9
Version 2.2.0.0 9
1.2 Editions 11
1.2.1 Features 11
2. Estimated Deployment Times 12
3. Requirements 13
3.1 Operating System 13
3.2 Software 13
3.3 Azure 13
3.4 Network 13
3.5 Virtual Machines 14
3.6 Azure / Entra ID Permissions - Users 15
3.7 Microsoft Entra Permissions & Azure Permissions - Configuration 16
3.8 Microsoft Active Directory 17
3.9 Microsoft Entra ID 18
3.10 Microsoft Entra hybrid Join 19
4. Getting Started 21
4.1 Create AVD-Admins Group 21
4.2 Resource Groups & Roles 21
4.3 Azure Permissions 23
4.3.1 Virtual Machine Scale Set Resource Group (VMSS) 23
4.3.2 Azure Virtual Desktop Resource Group (AVD) 24
4.3.3 Master VMs, Snapshots and Images Resource Group (GOLD-VDA) 25
4.3.4 Network Resource Group (NETWORK) 27
4.3.5 Domain Controller / Entra Connect Resource Group (DOMAIN) 30
4.4 Entra ID Permissions 33
4.5 Check AVDManage Requirements 34

4.6 Install AVDManage 36
4.6.1 Silent Installation 36
4.6.2 Authentication 36
4.6.2.1 Older Windows Operating Systems 37
4.6.2.2 Manual Authentication 37
4.7 Configure AVDManage 38
4.8 Create Service Principals 39
4.8.1 Create AVD-Join (Application Registration) 39
4.8.2 Create AVDManage (User-Assigned Managed Identity) 40
4.9 Create Automation Account – AVD-Automate (Optional) 41
5. Create (Master) VM 43
5.1 Modify the Master VM 46
5.2 Snapshot the Master VM 48
5.3 Sysprep the Master VM 49
5.4 Create Image of the Master VM 50
6. Virtual Machine Scale Sets 51
6.1 Uniform vs Flexible 51
6.2 Create a Virtual Machine Scale Set 53
7. Image Updates 57
7.1 Recreate the Master VM 57
7.2 Modify the Master VM 58
7.3 Snapshot the Master VM 59
7.4 Sysprep the Master VM 60
7.5 Create Image of the Master VM 61
8. Update a Scale Set 62
8.1 Create Update Runbook 64
8.2 Create Update Automation Task 65
9. AVDManage Plus 67
9.1 Azure Permissions 67
9.2 Licensing 67
9.3 Additional Features 67
9.4 Install AVDManage 68
9.5 Overview 69
9.6 Create an Azure Compute Gallery 70
9.7 Create an Image Definition 71

9.7.1 Specialized Image Definition 71
9.7.2 Generalized Image Definition 72
9.8 Create (Master) VM 73
9.9 Create a Compute Gallery Image Version 75
9.9.1 Specialized Image 75
9.9.2 Generalized Image 76
9.10 Create a Virtual Machine Scale Set 77
9.10.1 Specialized Image 77
9.10.2 Generalized Image 78
9.11 Image Updates 79
10. AVD-Prep - Pre-Stage the Remote Desktop Infrastructure and Boot Loader Agents 81
11. Reference 82
11.1 Virtual Machines 82
11.1.1 Configuration 82
11.1.2 OS Disk Type: Persistent vs Ephemeral 82
11.1.3 Menu Actions 83
11.2 Virtual Machine Scale Sets 83
11.2.1 Windows Licensing 83
11.2.2 Orchestration Mode 84
11.2.3 Update Mode 84
11.2.4 Load Balancing 84
11.2.5 OS Disk Type: Persistent vs Ephemeral 84
11.2.6 Menu Actions 86
11.3 Service Principals 87
11.3.1 Menu Actions 88
11.4 AVD-Automate Automation Account 89
11.4.1 Menu Actions 89
11.5 Snapshots 90
11.5.1 Menu Actions 90
11.6 Images 90
11.6.1 Menu Actions 90
11.7 PowerShell 91
11.7.1 Module Installation for AVDManage 91
11.7.2 Verify Installed Modules 92
11.8 SysPrep Failure 93
12. Smart App Control 94

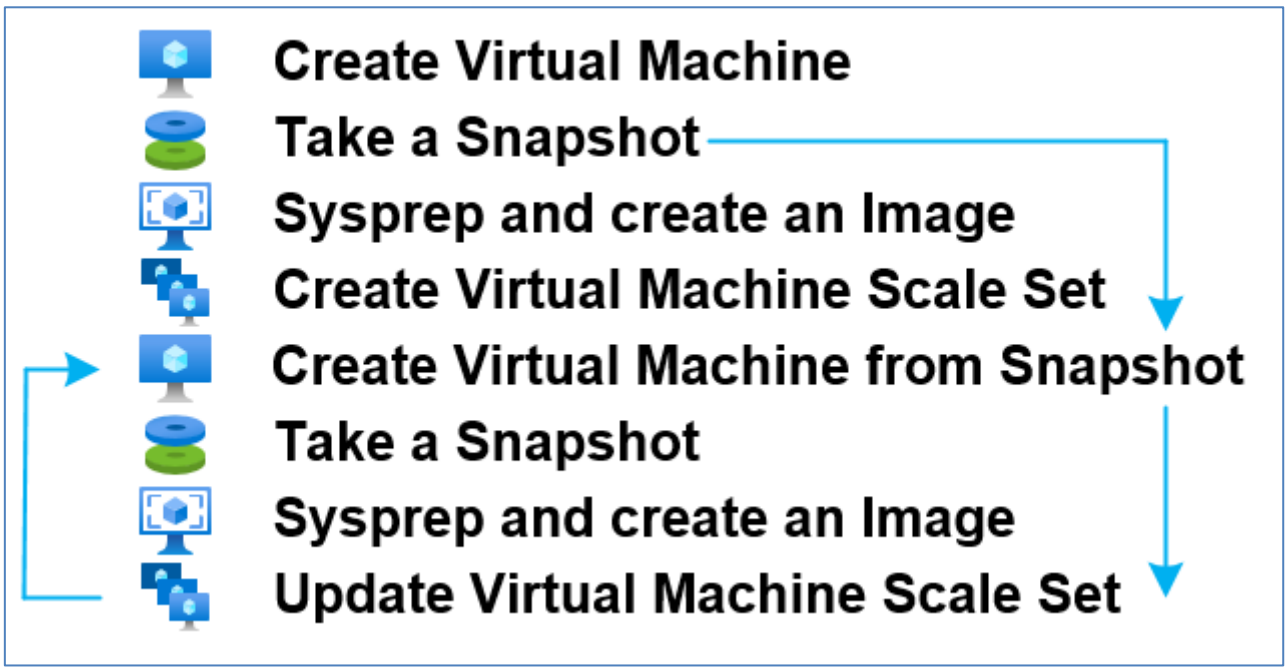
13. Login Issues 95
13.1 Internet Explorer Trust 95
13.2 Something went wrong 96
14. Installation Issues 97
14.1 SmartScreen prevents installation 97

Standardise and Simplify Azure Virtual Desktop Image Management

- Create Virtual Machines, Snapshots & Images
- Create Uniform and Flexible Virtual Machine Scale Sets
- Deploy Virtual Machines with Persistent or Ephemeral disks
- Deploy, Re-Deploy, Re-Image, Update & Rollback Virtual Machine Scale Sets using Managed Images, Azure Gallery Images or Compute Gallery Images
- Virtual Machine instances retain their identity when updating, re-imaging, re-deploying (AD, Entra ID, AVD Session Host)
- Scale Up / Down – Change VM Size
- Scale In / Out – Adjust Virtual Machine Scale Set VM instances
- Join Active Directory Domain during deployment / update
- Join Entra ID during deployment / update
- Delete AVD Session Host, Active Directory Computer objects and Entra ID Devices when deleting VM instances
- Supports native AVD Power Management Autoscaling (Flexible Scale Sets)
- **AVD-Turbo** – Join Entra ID or AD Domain & AVD Host Pool
- **AVD-Automate** – Schedule tasks for planned maintenance.

  E.g. Image Updates, Power Management, Scheduled Reboot

Consistent repeatable process for Image Continuity



1. Introduction

AVDManage leverages Microsoft Azure Virtual Machine Scale Sets to deploy, update and rollback Windows images to multiple uniform Virtual Machine instances.

Virtual Machine instances retain their machine identity when updating, re-imaging, re-deploying and rolling back. (Windows ComputerName, Active Directory ComputerName, AVD Session Host name, Entra Device ID)

Up to 1000 virtual machines may be deployed or updated from Azure Gallery Images and Compute Gallery Images or up to 600 virtual machines from Windows Managed Images subject to Azure subscription quota and limits.

AVD-Turbo leverages the Azure Custom Script Extension for Windows.

AVD-Turbo enables Generalized and Specialized Scale Set Virtual Machine instances to join an Active Directory domain or Entra ID, and an Azure Virtual Desktop host pool when deploying or updating Virtual Machine Scale Sets.

AVD-Automate leverages Azure Automation enabling tasks to be scheduled and assigned to Virtual Machine Scale Sets to Automate Tasks such as updating, restarting or power management.

AVDManage provides a simplified and consistent methodology and process for creating, deploying, and updating customised Windows images to Virtual Machine Scale Sets.

1. Create a Windows Master VM from an Azure Gallery Image
2. Configure the Master Image based on user desktop requirements
3. Create a Snapshot of the Master VM
4. Sysprep the Master VM
5. Create an Image from the sysprepped Master VM
6. Deploy the Image to a new or existing Virtual Machine Scale Set

The Master VM can be recreated from the Snapshot that was created in step 3 enabling future image control and consistency, and continuity of master image lifecycle.

VMs may be updated manually or scheduled to update during planned maintenance windows using Azure Automation and **AVD-Automate**.

AVDManage can provision Virtual Machine Scale Sets in Automatic update mode however this is unlikely to be appropriate for an AVD host pool as user sessions would be interrupted during unscheduled automatic updates. It is recommended that Virtual Machine Scale Sets are deployed in Manual mode and **AVD-Automate** is used to deploy out-of-hours updates.

AVDManage supports Azure Virtual Desktop environments however **AVD-Turbo** and **AVD-Automate** are optional features therefore AVDManage may be used to manage image deployment to Virtual Machine Scale Sets for almost any Windows based image.

1.1 Updates

Updates since the previous release.

Version 2.5.0.0

Improved Login Experience

- Login uses InterActiveBrowserCredential

Join Entra ID

- Virtual Machine Scale Sets may be configured to join Entra Id or Active Directory
- **AVD-Turbo** can now join VMs to Entra ID or Active Directory

AVD-Automate

- AVD Task scripts updated to handle Entra ID names

Virtual Machine Scale Set Creation

- Join Entra ID or Active Directory
- Syncs AD Connect after Active Directory Computer account creation / deletion
- WVD registration Token is pre-created when deploying / updating VMs
- Optionally disable AVD logons after VM deployment

Virtual Machine Scale Set Instance Deletion

- Entra ID Devices may be deleted when deleting Scale Set VM instances
- Active Directory Computer account and DNS record deletion

Virtual Machine Instances

- Reset AVD Agent if the VM 'NeedsAssistance'

Version 2.3.0.0

Virtual Machine Scale Set Creation

- Added support for Flexible Virtual Machine Scale Sets

Join AVD Host Pools

- **AVD-Join** has been retired
- **AVD-Turbo** is used to deploy both Generalized and Specialized Images

AVD-Automate

- Modified Task scripts for compatibility with Flexible Scale Sets
- Modified ReDeploy, Update and ReImage task scripts to generate a WVD token

Version 2.2.0.0

Digitally Signed

- The AVDManage installer and application files are digitally signed
- AVD-Joinx.ps1 and AVD-Turbox.ps1 deployment scripts are digitally signed

- AVD-Join and AVD-Turbo no longer require Az.Accounts and Az.DesktopVirtualization modules

Configuration

- Template Active Directory Domain information
- Automatic Job refresh

Virtual Machine Creation

- Enable Accelerated Networking
- NVMe Disks

Virtual Machine Scale Set Creation

- Enable Accelerated Networking
- NVMe Disks

Virtual Machine Scale Set Instance Deletion

- Deletes the Active Directory Computer object
- Deletes the Azure Virtual Desktop Session Host

Join AVD Host Pools

- **AVD-Join** and **AVD-Turbo** now use Secretless Authentication to authenticate to Azure when joining VM Scale Set Instances to an AVD-Host Pool

1.2 Editions

AVDManage is available in two editions, Free and Plus.

AVDManage Plus enables deployment of images from Azure Compute Galleries. This allows for deployment of generalized and specialized images.

VMs and scale sets created from specialized images can be up and running quicker, because they're created from a source that has already been through first boot. VMs created from specialized images boot faster and can contain a greater degree of local customisation as they have not been sysprepped.

AVDManage Plus requires a 30-day evaluation or annual license. (Fixed annual fee. Not based on number of users or devices.)

Please contact info@chawn.com for license enquiries.

1.2.1 Features

	Free	Plus
Create VMs from Snapshots	○	○
Create Virtual Machines & Scale Sets from Azure Gallery	○	○
Create Virtual Machines & Scale Sets from Managed Images	○	○
Create Virtual Machines & Scale Sets from Compute Galleries		○
Create Virtual Machines in any Resource Group in the base Location		○
Uniform and Flexible Orchestration Mode Virtual Machine Scale Sets	○	○
Deploy Generalized Windows Images	○	○
Deploy Specialized Windows Images		○
Persistent & Ephemeral Disks	○	○
Accelerated Networking	○	○
NVMe Disks	○	○
Create Trusted Launch Virtual Machines & Scale Sets		○
AVD-Automate	○	○
Supports native AVD Power Management Autoscaling (Flexible Scale Sets)	○	○
Delete AVD Session Hosts when deleting VM Scale Set Instance	○	○
Delete Entra ID Devices when deleting VM Scale Set Instance	○	○
Delete Active Directory Computer objects when deleting VM Scale Set Instance	○	○
AVD-Turbo – Join Domain, Join Entra ID, Join AVD Host Pool	○	○
AVD-Prep – Pre-stage the Remote Desktop Infrastructure and Boot Loader Agents	○	○

2. Estimated Deployment Times

Virtual Machine: Standard_DS3_v2 with Accelerated Networking and Trusted Launch

(Managed Images are deployed with Standard Security)

O/S: win11-25h2-avd-m365 (Windows 11 Enterprise Multi-Session with Office, Teams, OneDrive, FSLogix, Edge)

Storage: Premium LRS (127 GB)

Deployment times are based on deploying one Virtual Machine instance in a Scale Set.

Source	Image	Configuration	Total
Compute Gallery	Specialized	AVDPrep / AVDTurbo	3m – 5m
Compute Gallery	Generalized	AVDPrep / AVDTurbo	6m - 8m
Managed Image	Generalized	AVDPrep / AVDTurbo	7m - 9m
Azure Gallery	Deployed	AVDTurbo	6m - 8m

AVDPrep – Preinstalls the Remote Desktop Infrastructure and Boot Loader Agents in the master image reducing deployment time by about 45 seconds.

AVDTurbo –Joins Active Directory or Entra ID, Joins AVD Host Pool

Specialized Images deploy, boot up, rename the VM, Join Entra ID / Join AD, Join AVD Host Pool, reboot.

Generalized Images deploy, boot up, Join Entra ID / Join AD, Join AVD Host Pool, reboot.

Azure Gallery Images deploy, boot up, Join Entra ID / Join AD, Join AVD Host Pool, reboot.

Deployment times are not always consistent and can easily vary depending on the virtual machine size, storage type, Azure Region, or time of day.

3. Requirements

3.1 Operating System

- Microsoft Windows 10 build 1607 or higher

3.2 Software

- Microsoft .Net Framework 4.7.2 or higher
- Microsoft Windows PowerShell 5.1 or higher
- Microsoft Windows PowerShell Modules
  - Az.Accounts 5.3.3
  - Az.Compute 11.3.0
  - Az.DesktopVirtualization 5.4.1
  - Az.Resources 9.0.1
  - Az.Automation 1.11.2
  - Az.Network 7.25.0
  - Az.ManagedServiceIdentity 2.0.0
  - ActiveDirectory 1.0.1 (If *DeleteADComputer* is enabled)
  - Microsoft.Graph.Authentication 2.35.0 (If DeleteEntraDevice is enabled)
  - Microsoft.Graph.Identity.DirectoryManagement 2.35.0 (If DeleteEntraDevice is enabled)

3.3 Azure

- An Azure Tenant and Microsoft Entra Directory
- An Azure Subscription
- An Active Directory group for **AVD-Admins** (synced to Entra ID) or preferably an Entra ID group that can be assigned Entra Roles.
- Azure Resource Groups for:
  - Master VM, Snapshots, Images, Compute Gallery (AVDManage Plus)
  - Virtual Machine Scale Sets and Automation Account
  - AVD Host pools and Application Groups
- Azure Virtual Network and Subnet(s)
- Azure Virtual Desktop Provider, Workspace, Host Pool, Application Group
- Sufficient Azure quota to deploy the intended number of VMs
- All Azure Objects in the AVDManage configuration must be in the same Azure location

AVD Host Pools must NOT have a Session Host Configuration

3.4 Network

AVDManage requires access to Azure CLI Endpoints.

Endpoints used when installing the Azure CLI | Microsoft Learn

3.5 Virtual Machines

If Virtual Machines will be joined to an Active Directory Domain / Entra ID or an AVD Host Pool with **AVD-Turbo**, Virtual Machines require network access to:

- **AVD-Turbo5.ps1** PowerShell Script
  https://raw.githubusercontent.com/ChawnLimited/AVDManage/refs/heads/main/AVD-Turbo5.ps1

- **AVD-EntraReg.ps1** PowerShell Script
  https://raw.githubusercontent.com/ChawnLimited/AVDManage/refs/heads/main/AVD-EntraReg.ps1

- Installation media for the Microsoft Remote Desktop Service Infrastructure Agent and Boot Agent
  https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWrmXv
  https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWrxrH

PowerShell scripts and Microsoft Remote Desktop Agents source media are downloaded by Virtual Machines when deploying and updating.

- Required FQDNs and Endpoints for Azure Virtual Desktop
  Required FQDNs and endpoints for Azure Virtual Desktop | Microsoft Learn

Default outbound internet access for Azure VMs will be retired on 30th September 2025. Ensure that Virtual Machines have a valid route to required internet endpoints.

Azure Default Outbound Internet Access
Plan for inbound and outbound internet connectivity | Microsoft Learn

Flexible scale sets are secure by default. Any instances created via Flexible scale sets don't have the default outbound access IP associated with them, so an explicit outbound method is required. For more information, see Flexible orchestration mode for Virtual Machine Scale Sets.

Virtual Machines no longer require any additional Powershell Modules to join AVD Host Pools (AVDManage Version 2.2.11.0 / AVD-Turbo3.ps1)

3.6 Azure / Entra ID Permissions - Users

The following permissions are required by the **AVD-Admins** group.

(Broad Scope Permissions)

- Contributor permissions to all in-scope Resource Groups
- Network Contributor Permissions to the Virtual Network
- Entra ID Cloud Device Administrator if DeleteEntraDevice is required.

or

(Narrow Scope Permissions)

Resource	Permission
Scale Sets Resource Group	Automation Contributor Virtual Machine Contributor Managed Identity Operator
Virtual Machines Resource Group	Virtual Machine Contributor Disk Snapshot Contributor Microsoft.Compute/images/write Microsoft.Compute/images/read Microsoft.Compute/images/delete Compute Gallery Artifacts Publisher ☺
AVD Resource Group	Desktop Virtualization Contributor
Virtual Network Resource Group	Microsoft.Resources/subscriptions/resourceGroups/read Microsoft.Network/virtualNetworks/read Microsoft.Network/virtualNetworks/subnets/join
Domain Controller Resource Group	Microsoft.Compute/virtualMachines/read Microsoft.Compute/virtualMachines/runCommand/action Microsoft.Compute/virtualMachines/runCommands/write Microsoft.Compute/virtualMachines/runCommands/read
Entra ID	If DeleteEntraDevice is required, then users must be assigned the 'Cloud Device Administrator' role or a custom role with the 'microsoft.directory/devices/delete' permission.

☺ *AVDManage Plus* only

3.7 Microsoft Entra Permissions & Azure Permissions - Configuration

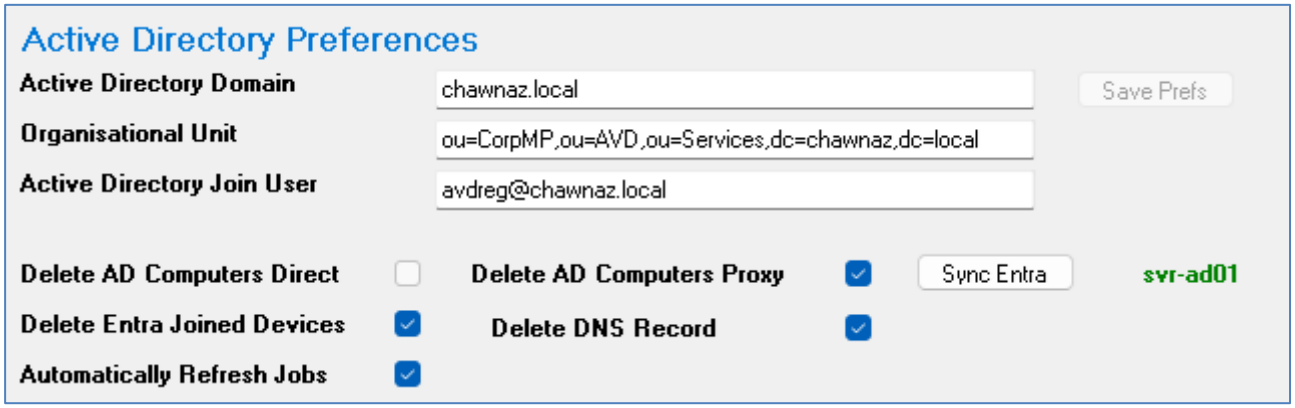
The following permissions are required to initially configure the AVDManage environment. They are not required by the **AVD-Admins** group.

Resource	Permission
Entra ID	Entra Global Administrator, Application Administrator, Application Developer or Cloud Application Administrator To create AVD-Join Application Registration Privileged Role Administrator To create 'Delete Entra Devices' custom role
AVD Resource Group	Owner, Role Based Access Control Administrator or User Access Administrator To assign RBAC roles to AVD-Join Application Registration To assign RBAC roles to the AVD-Admins group
Scale Sets Resource Group	Owner, Contributor or Managed Identity Contributor To create AVDManage User-Assigned Managed Identity Owner, Contributor or Automation Contributor To create AVD-Automate Automation Account Owner, Role Based Access Control Administrator or User Access Administrator To assign RBAC roles to AVD-Automate Automation Account To assign RBAC roles to the AVD-Admins group
Virtual Machines Resource Group	Owner, Role Based Access Control Administrator or User Access Administrator To assign RBAC roles to AVD-Automate Automation Account To assign RBAC roles to the AVD-Admins group
Virtual Network Resource Group	Owner, Role Based Access Control Administrator User Access Administrator To assign RBAC roles to the AVD-Admins group
Domain Controller Resource Group	Owner, Role Based Access Control Administrator User Access Administrator To assign RBAC roles to the AVD-Admins group

3.8 Microsoft Active Directory

- Active Directory Domain
- Dedicated Organisational Unit for Master VM
- Dedicated Organisational Units for each AVD Host Pool
- AD account (delegated Create Computer Object) to join VMs to the domain
- Delete Computer Object delegated to **AVD-Admins** for in-scope Organisational Units

A default domain, organisational unit and AD account can be configured as preferences, so that you do not have to type the same values when deploying VMs and Scale Sets.



Delete AD Computers Direct (DeleteADComputer)

If enabled, when Active Directory joined VM instances are deleted, the Active Directory computer accounts are deleted if the logged on user has sufficient permissions to the computers' Organizational Unit.

Direct connectivity to a domain controller is required and the **ActiveDirectory** Powershell module must be installed.

The **AVD-Admins** group must be delegated permissions to **Delete Computer Objects**, and the Active Directory Join User account must have been delegated permissions to **Create Computer Objects** on all required Active Directory Organisational Units to join VMs to the domain.

Delete AD Computers Proxy (DeleteADProxy)

If enabled, when Active Directory joined VM instances are deleted, the Active Directory computer accounts and DNS records are also deleted. Entra Connect Sync is triggered to remove the device from Entra ID.

When new Computers are added Entra Connect Sync is triggered to ensure prompt registration of Entra Hybrid joined devices.

AVDManage communicates directly with an Azure Virtual Machine running the Domain Controller and DNS roles, and Entra Connect.

The **AVD-Admins** group must be assigned an Azure role that enables them to execute VM Run Commands on the assigned Virtual Machine.

Automatically Refresh Jobs (AutoRefresh)

AVDManage will update the status of submitted jobs in the background.

User preferences are stored in the registry and may be edited according to your environment.

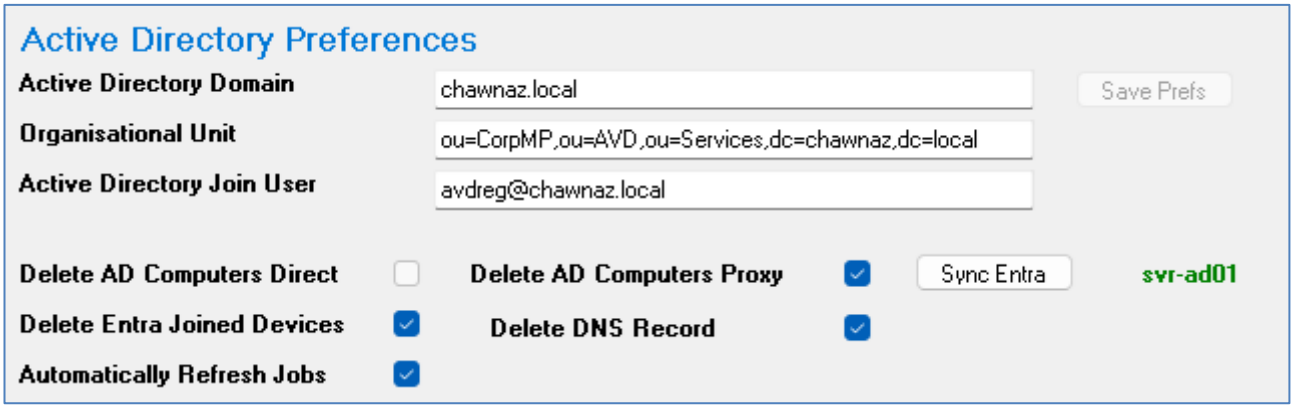
[HKEY_CURRENT_USER\SOFTWARE\Chawn\AVDManage\Config]

AutoRefresh = True
DefaultADAdmin = avdreg@domain.local
DefaultDomain = domain.local
DefaultOU = ou=AVD, ou=Services, dc=domain, dc=local
DeleteADComputer = True
DeleteADProxy = <Name of VM>
DeleteADDns = True
DefaultVM = Standard_DS3_v2

3.9 Microsoft Entra ID

Microsoft Entra join is required on Virtual Machines to enable SSO and Conditional Access.

Virtual Machine Scale Set instances may be configured to directly join Entra ID when deploying or updating.
Microsoft Entra joined devices may not be joined to an Active Directory Domain.
AVD-Turbo joins Virtual Machine Scale Set instances to Entra ID using the **AVDManage** User Assigned Managed Identity.



Delete Entra Joined Devices (DeleteEntraDevice)
When deleting Entra joined Virtual Machine Scale Set instances, the Entra Joined device may also be deleted.
Delete Entra Devices may only be enabled if the following Powershell modules are installed.

- Microsoft.Graph.Authentication
- Microsoft.Graph.Identity.DirectoryManagement

Members of **AVD-Admins** must be assigned the 'Cloud Device Administrator' role or a custom role with the 'microsoft.directory/devices/delete' permission.

User preferences are stored in the registry and may be edited according to your environment.

[HKEY_CURRENT_USER\SOFTWARE\Chawn\AVDManage\Config]

DeleteEntraDevice = True

3.10 Microsoft Entra hybrid Join

Microsoft Entra hybrid join is required on Virtual Machines to enable SSO and Conditional Access.

Configure Microsoft Entra hybrid join - Microsoft Entra ID | Microsoft Learn

Configuration requires:

- Microsoft Entra Connect
- Service Connection Point
- Group Policy Object linked to the dedicated organisational units for each AVD Host Pool

Computer Configuration\Policies\Administrative Templates

Windows Components/Device Registrations

Register domain joined computers as devices - Enabled

Windows Components/Internet Explorer/Internet Control Panel/Security Page

Site to Zone Assignment List

https://device.login.microsoftonline.com
https://autologon.microsoftazuread-sso.com
https://enterpriseregistration.windows.net
https://login.microsoftonline.com

Windows Components/Internet Explorer/Internet Control Panel/Security Page/Intranet Zone

Allow updates to status bar via script - Enabled

Preferences Registry

Hive HKEY_LOCAL_MACHINE
Key path SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD
Value name TenantID
Value type REG_SZ
Value data xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Hive HKEY_LOCAL_MACHINE
Key path SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD
Value name TenantName
Value type REG_SZ
Value data xxxxxxxx.onmicrosoft.com / domain.com

When devices join Active Directory, they will sync to Entra ID.

When redeployed, devices re-join Active Directory and will sync to Entra ID.

When devices are deleted from Active Directory, the deletion will sync to Entra ID.

The minimum sync cycle interval for Entra ID Connect is thirty minutes. When deploying, updating and deleting VMs, AVDManage can be configured to force synchronisation of Entra ID Connect. This reduces the time required for the Active Directory Computer Object to Hybrid Join Entra ID.

To configure AVDManage to force an Entra Connect sync when deploying, updating and deleting VMs, add the following registry setting.

HKEY_CURRENT_USER\Software\Chawn\AVDManage\Config
DeleteADProxy = *<Name of an Azure VM that is a writeable Domain Controller, DNS Server and hosts Entra Connect> (REG_SZ)*

You can add multiple domain controllers using a comma delimited string. AVDManage will connect to the first domain controller that is online.

Azure Permissions
Virtual Machine Contributor to the Resource Group containing the Domain Controller VM

Or

Create a custom role with the following permissions:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/runCommand/action
- Microsoft.Compute/virtualMachines/runCommands/write
- Microsoft.Compute/virtualMachines/runCommands/read

Assign the Role to **AVD-Admins**
Assign the Scope of the role to the Resource Group containing the Domain Controller VM.

AVD-Turbo
After AVD-Turbo has joined the VM to the Active Directory Domain, it creates a task to register the VM with Entra ID two minutes after the next reboot.

When the deployment is complete, AVDManage forces an Entra Connect sync allowing the device to register with Entra ID.

When deleting a VM instance, AVDManage will delete the Active Directory Computer object and associated DNS record. AVDManage then forces an Entra Connect sync which deletes the corresponding hybrid Entra ID device.

4. Getting Started

The user performing these tasks should be an **Azure Subscription Owner** and an **Entra ID Global Administrator** to create:

- Resource Groups
- Application Registration **AVD-Join** and assign the **Desktop Virtualization Contributor** role to the AVD Resource Group
- User-Assigned Managed Identity **AVDManage**
- Automation Account **AVD-Automate** and assign **Desktop Virtualization Contributor** role to the AVD Resource Group, and the **Virtual Machine Contributor** role to the VMSS Resource Group.

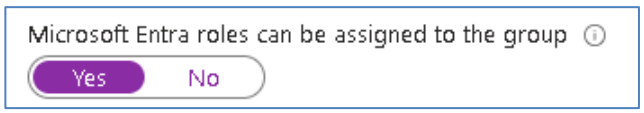
If you need help configuring AVDManage or have any questions, please email info@chawn.com.

4.1 Create AVD-Admins Group

The **AVD-Admins** group may be synced from an Active Directory Domain using Microsoft Entra Connect, or a Cloud Group may be manually created in Microsoft Entra.

It is recommended that a Cloud Group is used so that Microsoft Entra roles may be assigned to **AVD-Admins** as well as Azure permissions and roles.

When creating an Entra Cloud Group, ensure that you select 'Yes' so that Microsoft Entra roles may be assigned to the AVD-Admins group.



Add required members to the **AVD-Admins** group.

4.2 Resource Groups & Roles

Create the following Resource Groups and assign Roles to the **AVD-Admins** group.

Suggested Name	Purpose	AVD-Admins Roles
VMSS	Contains Virtual Machine Scale Sets and **AVD-Automate** Automation Account, and User-Assigned Managed Identity **AVDManage**	Virtual Machine Contributor Automation Contributor Managed Identity Operator
AVD	Contains AVD Host Pools, Application Groups and WorkSpaces	Desktop Virtualization Contributor
GOLD-VDA	Contains Master VMs, Snapshots and Images	Virtual Machine Contributor Disk Snapshot Contributor Image Contributor ☺ Compute Gallery Artifacts Publisher ☺

☺ *AVDManage Plus* only

☺ You will need to create a Custom Role named **Image Contributor** with the following permissions:

- Microsoft.Compute/images/write
- Microsoft.Compute/images/read
- Microsoft.Compute/images/delete

NETWORK

AVD-Admins require permissions to join VMs to a Virtual Subnet.

Create a Custom Role named **Network Joiner** with the following permissions.

- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Network/virtualNetworks/subnets/join/action

Assign the **Network Joiner** custom role to **AVD-Admins** on the Resource Group containing your Virtual Network(s).

Entra Connect

If using **DeleteADProxy**, **AVD-Admins** require permissions to run Azure VM Commands on a Virtual Machine hosting the Domain Controller, DNS Server and Entra Connect roles.

Create a Custom Role named **DeleteADProxy** with the following permissions.

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/runCommand/action
- Microsoft.Compute/virtualMachines/runCommands/write
- Microsoft.Compute/virtualMachines/runCommands/read

Assign the **DeleteADProxy** custom role to **AVD-Admins** on the Resource Group containing your Domain Controller(s).

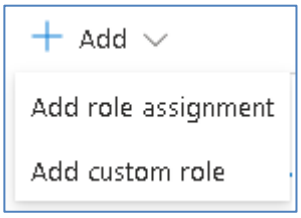
4.3 Azure Permissions

Configure Narrow Scope Permissions.

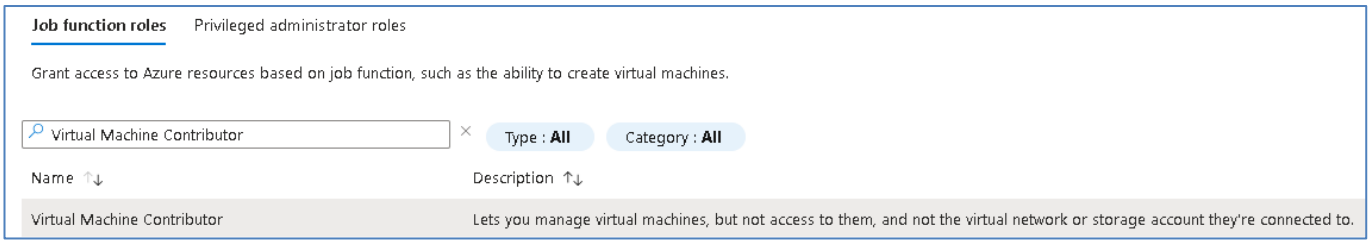
4.3.1 Virtual Machine Scale Set Resource Group (VMSS)

Assign Roles

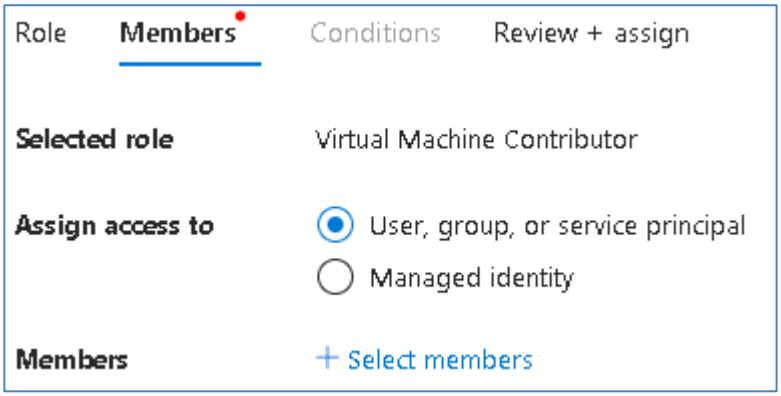
- Open the Azure Portal
- Locate the **VMSS** Resource Group
- Select Access Control (IAM)
- Select Role Assignments
- Click Add Role Assignment



- Select the **Virtual Machine Contributor** role and click Next.



- Click Select Members
- Search for **AVD-Admins** and click Select.



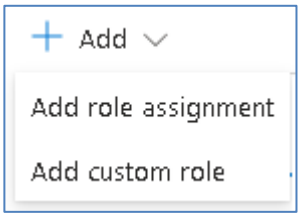
- Click Next
- Click Review and Assign

Repeat this process to assign the **Automation Contributor** and **Managed Identity Operator** roles.

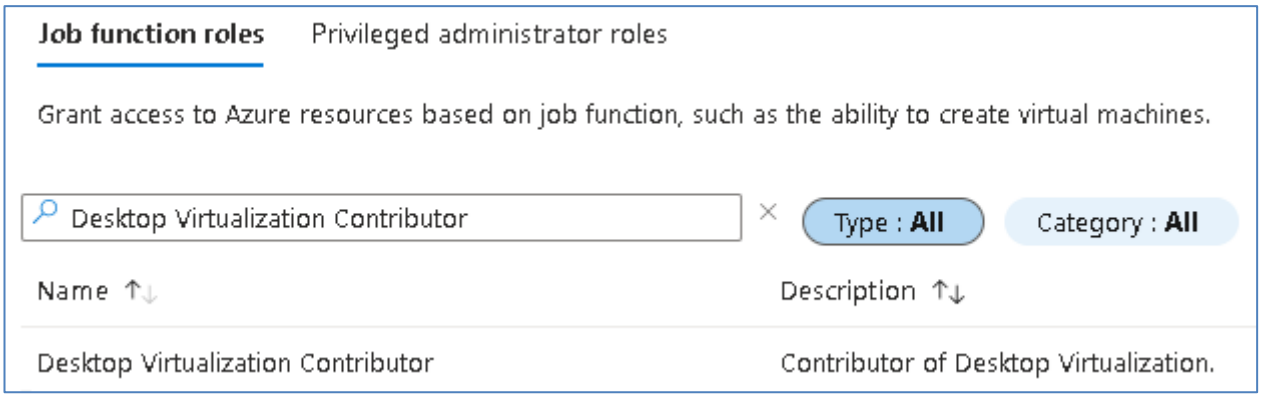
4.3.2 Azure Virtual Desktop Resource Group (AVD)

Assign Roles

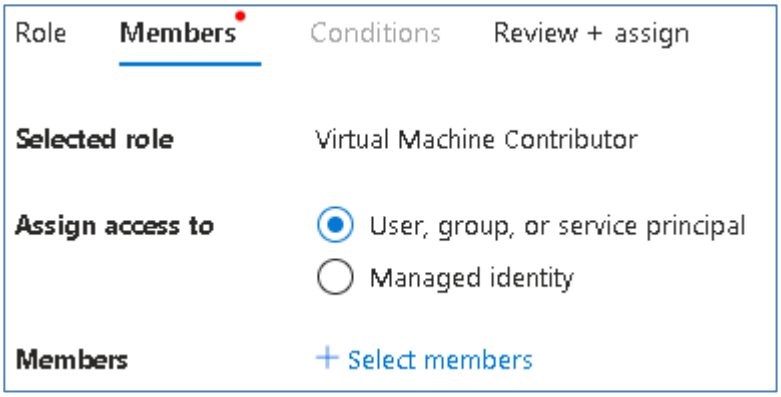
- Open the Azure Portal
- Locate the **AVD** Resource Group
- Select Access Control (IAM)
- Select Role Assignments
- Click Add Role Assignment



- Select the **Desktop Virtualization Contributor** role and click Next.



- Click Select Members
- Search for **AVD-Admins** and click Select.

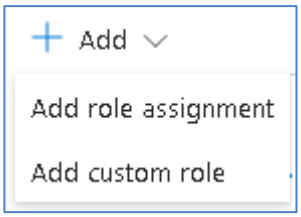


- Click Next
- Click Review and Assign

4.3.3 Master VMs, Snapshots and Images Resource Group (GOLD-VDA)

Create the **Image Contributor** Role

- Open the Azure Portal
- Locate the **GOLD-VDA** Resource Group
- Select Access Control (IAM)
- Select Role Assignments
- Click Add custom role



Basics

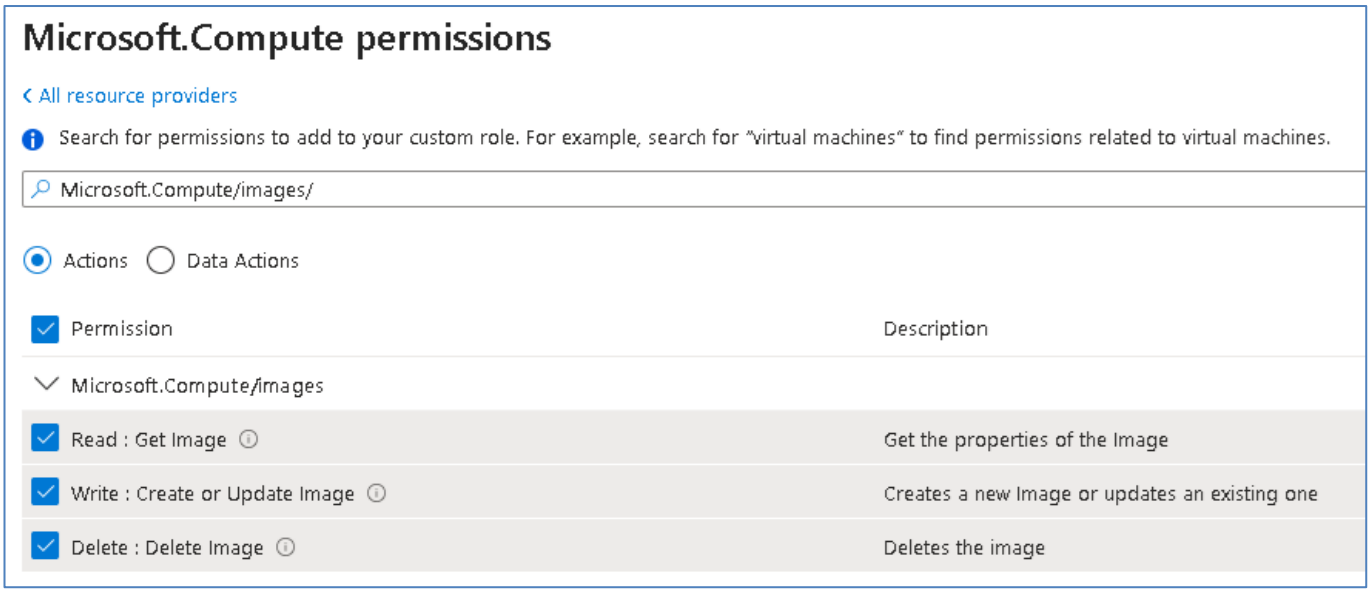
Custom Role Name: **Image Contributor**

Click Next.

Permissions

Click Add Permissions

Search for **Microsoft.Compute/images** and select the following permissions.



Click Add

Click Next

Assignable Scopes

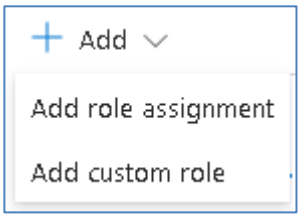
The **GOLD-VDA** Resource Group should already be selected.

Click Next to the end and click Create.

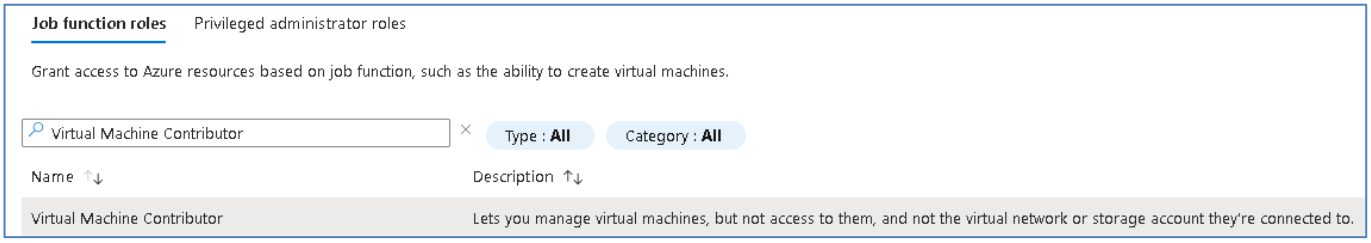
Assign Roles

- Open the Azure Portal
- Locate the **GOLD-VDA** Resource Group
- Select Access Control (IAM)

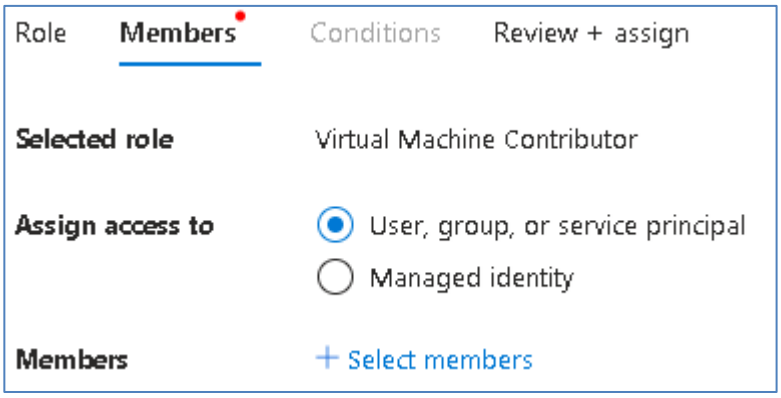
- Select Role Assignments
- Click Add Role Assignment



- Select the **Virtual Machine Contributor** role and click Next.



- Click Select Members
- Search for **AVD-Admins** and click Select.



- Click Next
- Click Review and Assign

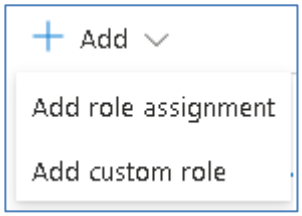
Repeat this process to assign the **Disk Snapshot Contributor** and **Image Contributor** roles.

If you have an AVDManage Plus license, repeat the process to assign the **Compute Gallery Artifacts Publisher** role.

4.3.4 Network Resource Group (NETWORK)

Create the **Network Joiner** Role

- Open the Azure Portal
- Locate the **NETWORK** Resource Group
- Select Access Control (IAM)
- Select Role Assignments
- Click Add custom role



Basics

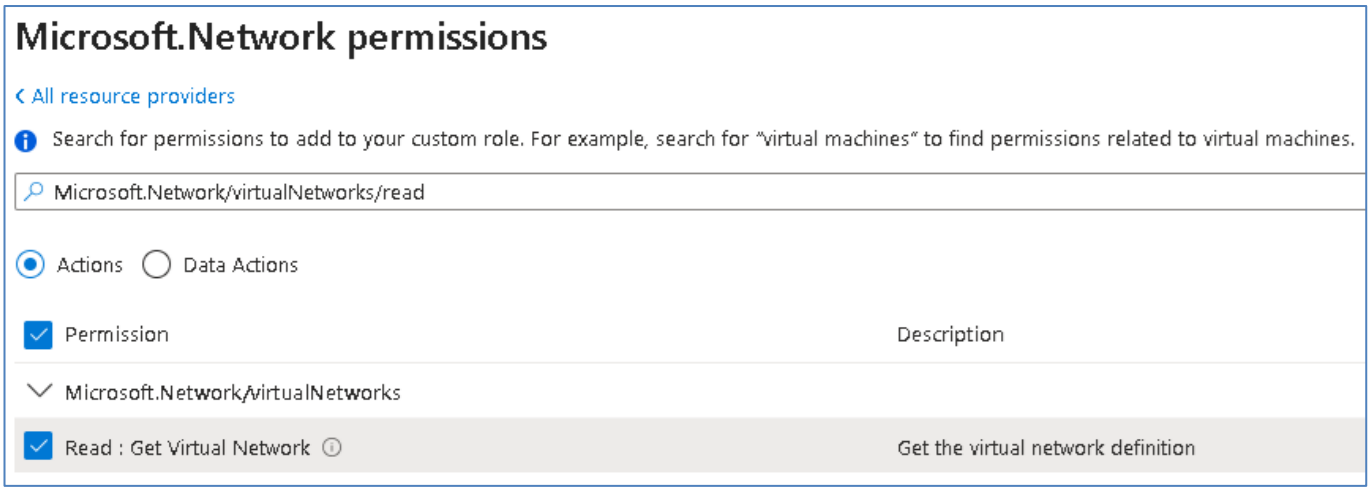
Custom Role Name: **Network Joiner**

Click Next.

Permissions

Click Add Permissions

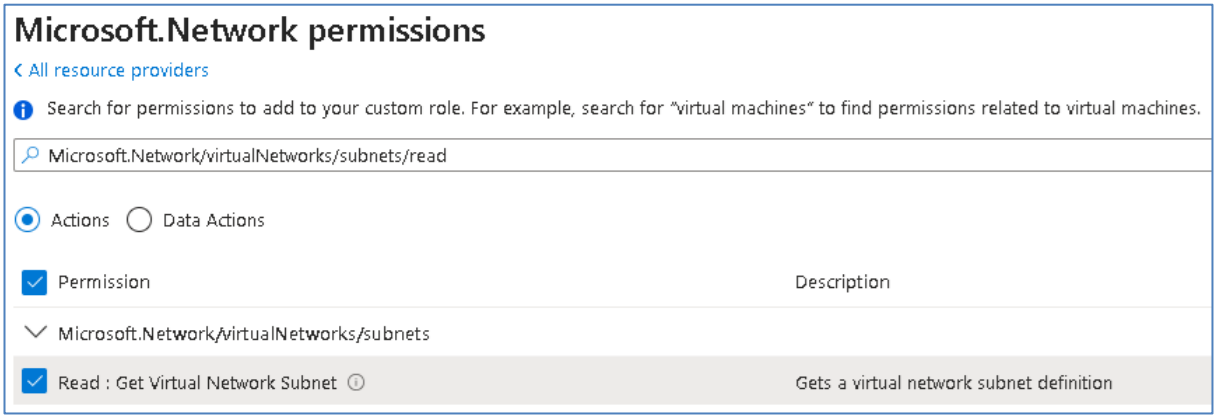
Search for **Microsoft.Network/virtualNetworks/read** and select the following permission.



Click Add

Click Add Permissions

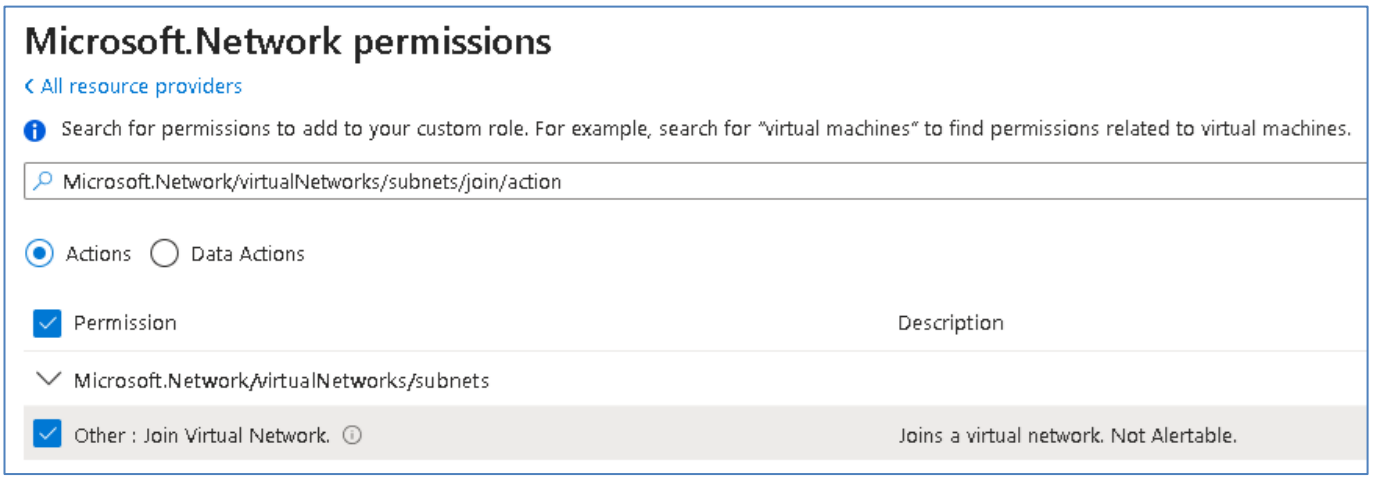
Search for **Microsoft.Network/virtualNetworks/subnets/read** and select the following permission.



Click Add

Click Add Permissions

Search for **Microsoft.Network/virtualNetworks/subnets/join/action** and select the following permission.



Click Add

Click Next

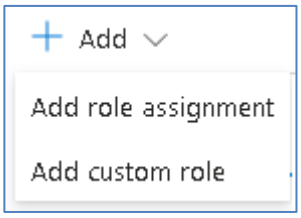
Assignable Scopes

The **NETWORK** Resource Group should already be selected.

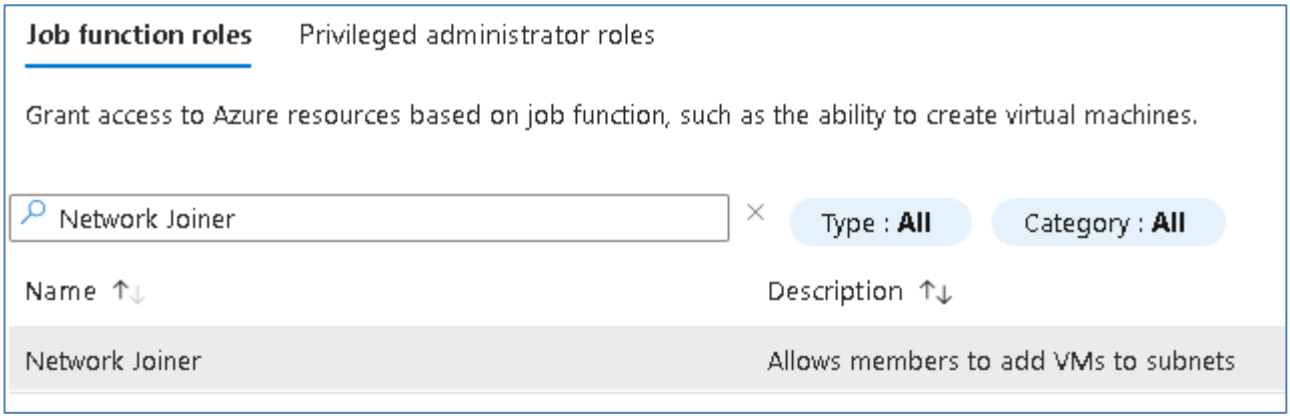
Click Next to the end and click Create.

Assign Roles

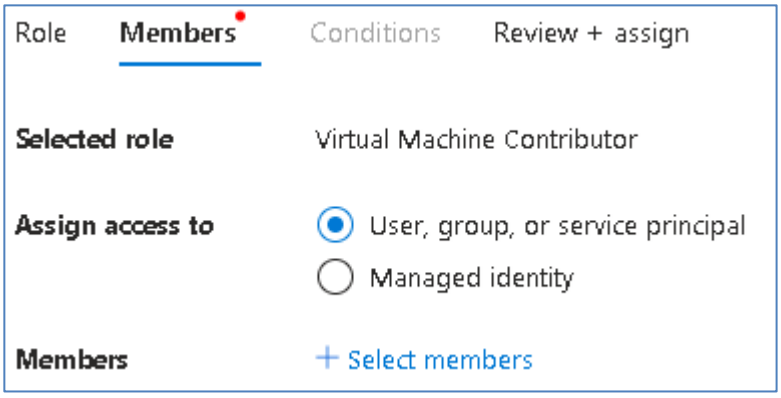
- Open the Azure Portal
- Locate the **NETWORK** Resource Group
- Select Access Control (IAM)
- Select Role Assignments
- Click Add Role Assignment



- Select the **Network Joiner** role and click Next.



- Click Select Members
- Search for **AVD-Admins** and click Select.

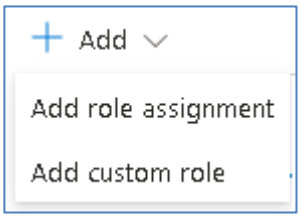


- Click Next
- Click Review and Assign

4.3.5 Domain Controller / Entra Connect Resource Group (DOMAIN)

Create the **DeleteADProxy** Role

- Open the Azure Portal
- Locate the **DOMAIN** Resource Group
- Select Access Control (IAM)
- Select Role Assignments
- Click Add custom role



Basics

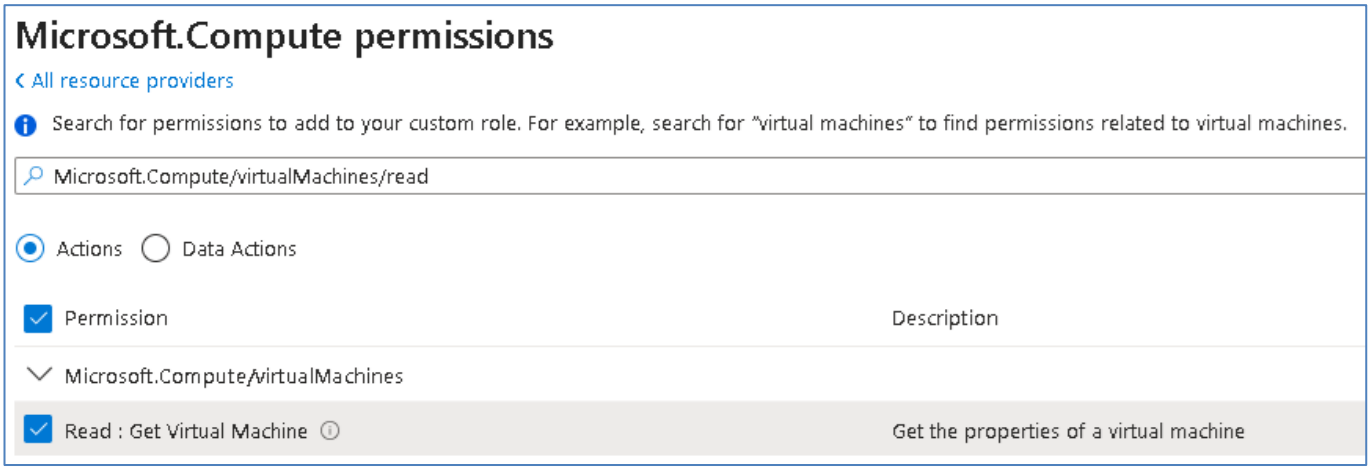
Custom Role Name: **DeleteADProxy**

Click Next.

Permissions

Click Add Permissions

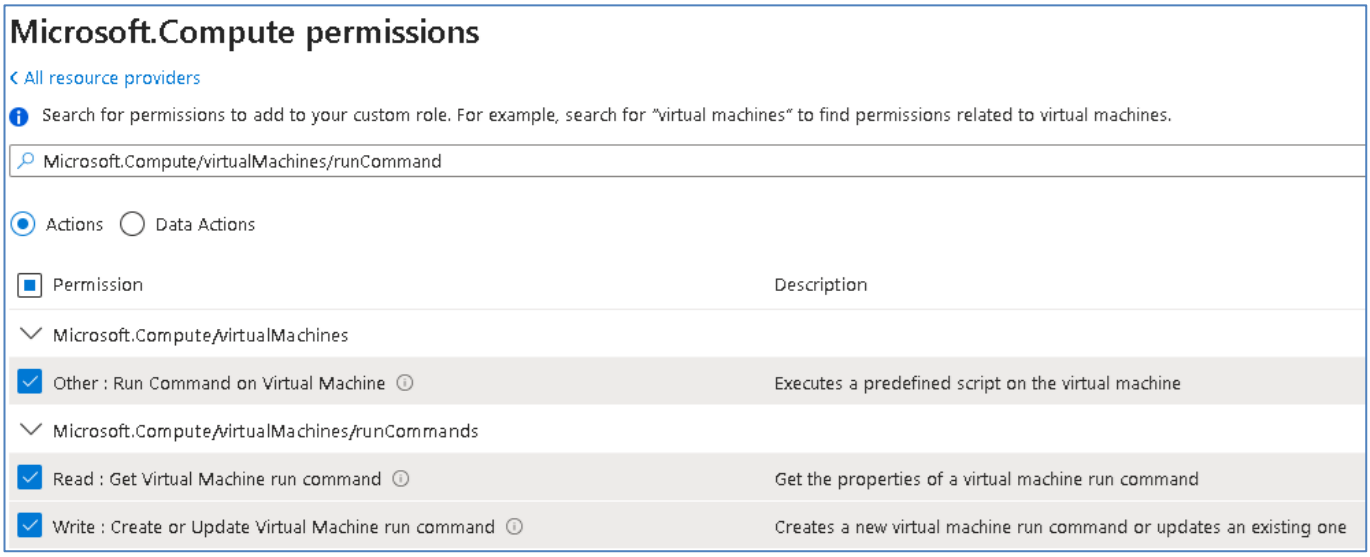
Search for **Microsoft.Compute/virtualMachines/read** and select the following permission.



Click Add

Click Add Permissions

Search for **Microsoft.Compute/virtualMachines/runCommand** and select the following permissions.



Click Add

Click Next

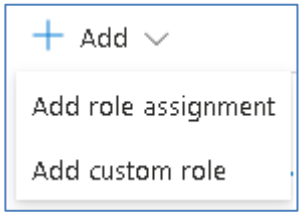
Assignable Scopes

The **DOMAIN** Resource Group should already be selected.

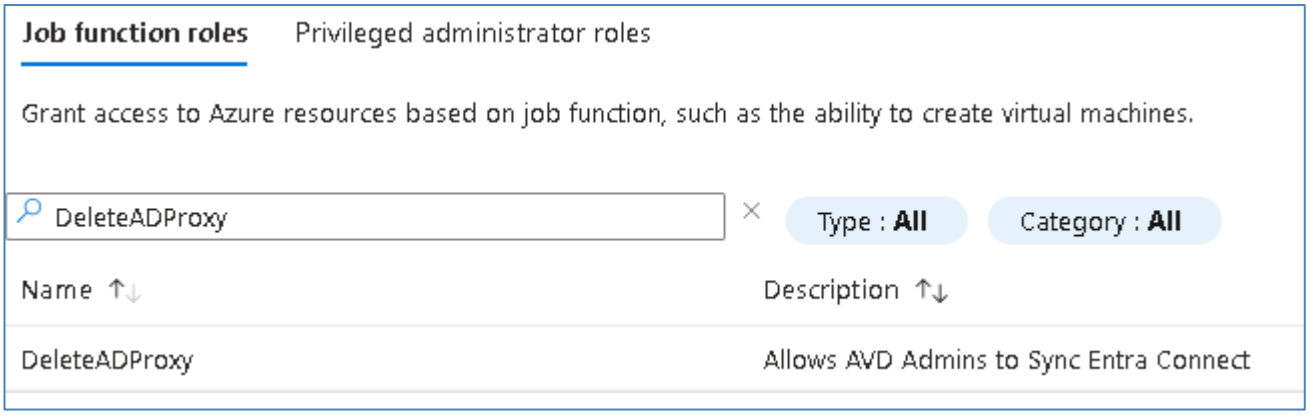
Click Next to the end and click Create.

Assign Roles

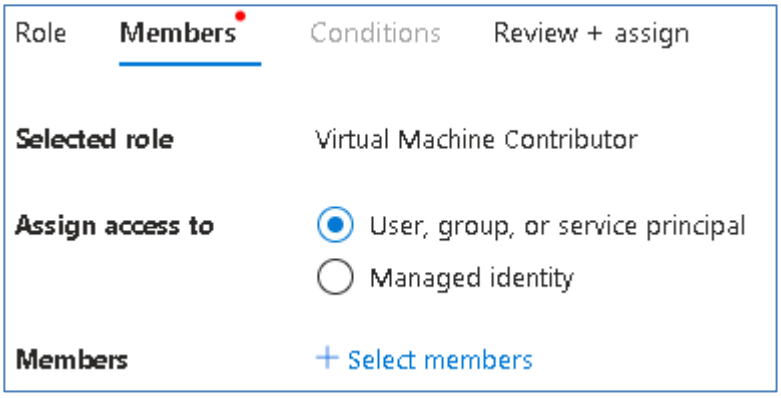
- Open the Azure Portal
- Locate the **Domain** Resource Group
- Select Access Control (IAM)
- Select Role Assignments
- Click Add Role Assignment



- Select the **DeleteADProxy** role and click Next.



- Click Select Members
- Search for **AVD-Admins** and click Select.



- Click Next
- Click Review and Assign

4.4 Entra ID Permissions

To delete Entra Joined devices when modifying or deleting a Scale Set, members of **AVD-Admins** must be assigned the ‘Cloud Device Administrator’ role or a custom role with the ‘microsoft.directory/devices/delete’ permission. Otherwise errors will be encountered when deleting Entra ID devices.

Broad Scope

- Open the Entra ID portal.
- Select the Roles and Administrators Blade
- Search for the ‘Cloud Device Administrator’ Role
- Click on the Role
- Click Add Assignment and select the **AVD-Admins** Group

Or

Narrow Scope

- Open the Entra ID portal.
- Select the Roles and Administrators Blade
- Click New Custom Role
- Name the Role (e.g. Delete Entra Devices)
- Select the ‘microsoft.directory/devices/delete’ permission
- Create the Custom Role
- Select the Roles and Administrators Blade
- Search for the new CustomRole
- Click on the Role
- Click Add Assignment and select the **AVD-Admins** Group

4.5 Check AVDManage Requirements

The user performing this task must be a Windows local administrator.

Open PowerShell as Administrator

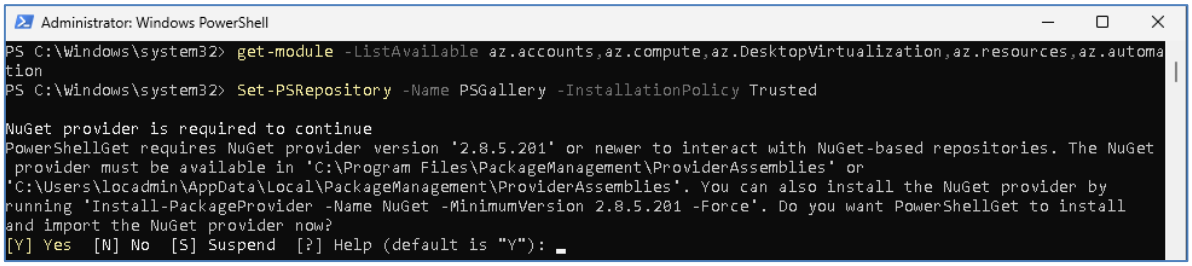
Run

```
get-module -ListAvailable Az.Accounts, Az.Compute, Az.DesktopVirtualization, Az.Resources, Az.Automation, Az.Network, Az.ManagedServiceIdentity
```

If no modules are returned then run

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
```

If prompted to install the the Nuget Provider, type Y



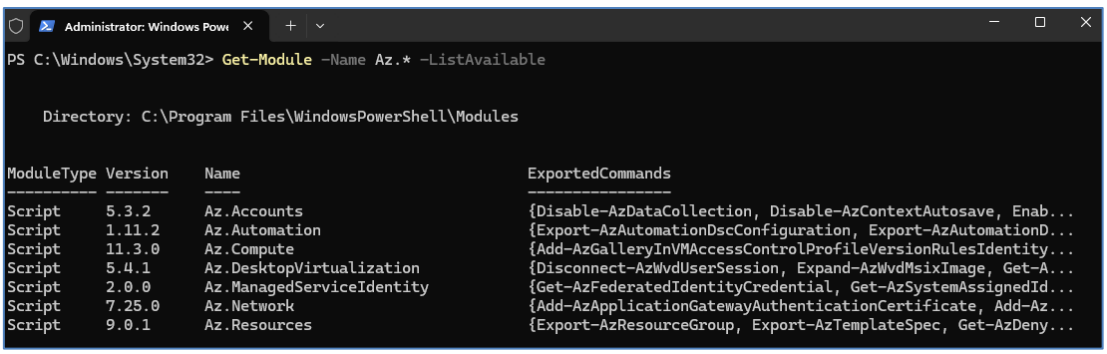
After NuGet is installed, run

```
Install-Module -Name Az.Accounts -RequiredVersion 5.3.3 -Scope AllUsers -Force
Install-Module -Name Az.Compute -RequiredVersion 11.3.0 -Scope AllUsers -Force
Install-Module -Name Az.DesktopVirtualization -RequiredVersion 5.4.1 -Scope AllUsers -Force
Install-Module -Name Az.Resources -RequiredVersion 9.0.1 -Scope AllUsers -Force
Install-Module -Name Az.Automation -RequiredVersion 1.11.2 -Scope AllUsers -Force
Install-Module -Name Az.Network -RequiredVersion 7.25.0 -Scope AllUsers -Force
Install-Module -Name Az.ManagedServiceIdentity -RequiredVersion 2.0.0 -Scope AllUsers -Force
```

Re-run

```
get-module -ListAvailable Az.Accounts, Az.Compute, Az.DesktopVirtualization, Az.Resources, Az.Automation, Az.Network, Az.ManagedServiceIdentity
```

You should see all required modules.

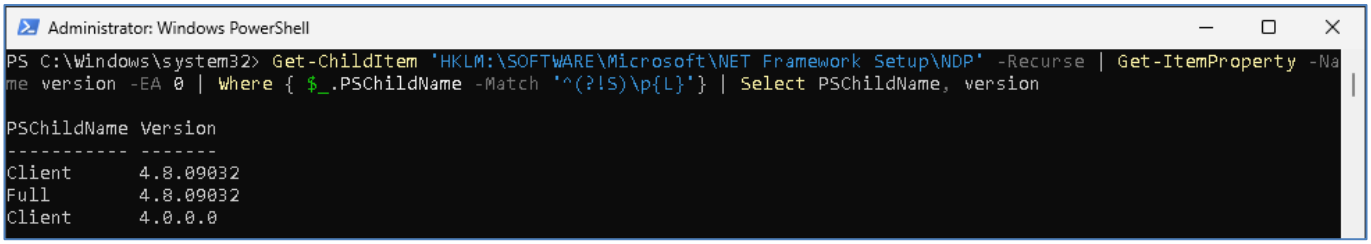


Check the .Net Framework Version

Run

```
Get-ChildItem 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP' -Recurse | Get-ItemProperty -Name version -EA 0 | Where { $_.PSChildName -Match '^(?!S)\p{L}'} | Select PSChildName, version
```

The output should be similar to below. Check that the .Net Framework Version is 4.72 or higher.



If you want to delete Active Directory Computer accounts when modifying or deleting a Scale Set, install the **ActiveDirectory** PowerShell Module.

Desktop O/S

```
Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools
```

Server OS

```
Add-WindowsFeature -Name RSAT-AD-PowerShell
```

If you want to delete Entra ID devices when modifying or deleting a Scale Set, install the **Microsoft.Graph.Identity.DirectoryManagement** PowerShell Module. This will automatically install the **Microsoft.Graph.Authentication** PowerShell Module.

```
Install-Module -Name Microsoft.Graph.Identity.DirectoryManagement -RequiredVersion 2.35.0 -Scope AllUsers
```

4.6 Install AVDManage

- Download AVDManage from www.chawn.com/downloads/AVDManage2.zip
- Extract the MSI installer from the zip file.
- Install AVDManage.msi as an Administrator

If the installation is blocked by SmartScreen, please see SmartScreen prevents installation.

4.6.1 Silent Installation

AVDManage may be installed silently using the following command.

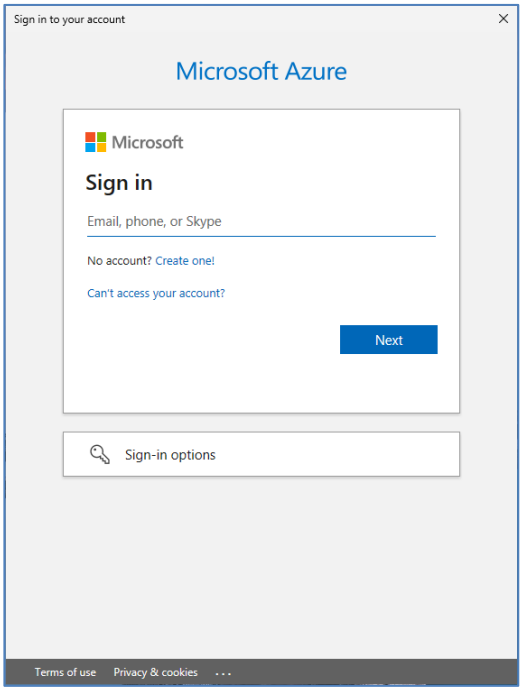
msiexec /i AVDManage.msi COMPANYNAME="Company Name" /qb

4.6.2 Authentication

Authentication to Microsoft Azure is handled by the **InteractiveBrowserControl**.

InteractiveBrowserControl supports

- Interactive Authentication
- Conditional Access / MFA
- Continuous Access Evaluation
- Access Token Acquisition
- Brokered authentication through Windows Authentication Authority (WAM)

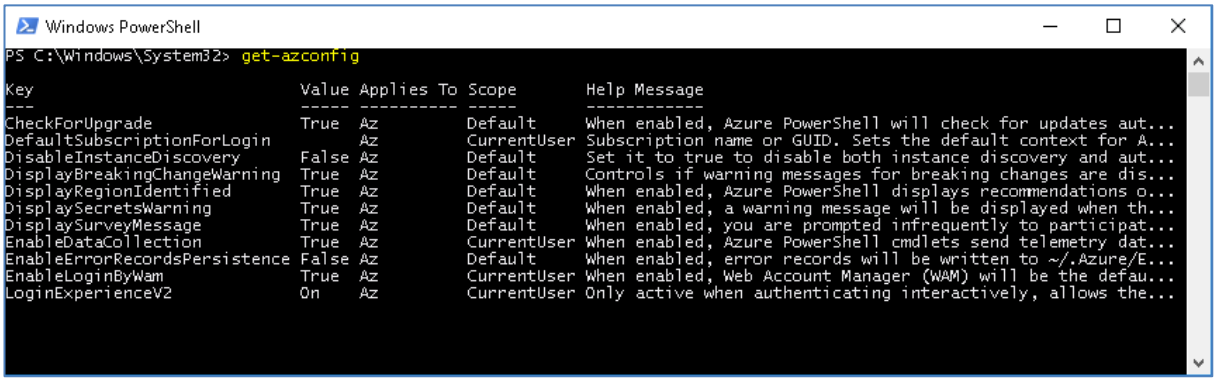


It is recommended that Web Account Manager (WAM) is enabled.

Web Account Manager (WAM) **must** be enabled to delete Entra ID Devices.

Validate that WAM is enabled by running

Get-AZConfig



If WAM is not enabled, run

Set-AzConfig -EnableLoginByWam $True

4.6.2.1 Older Windows Operating Systems

To prevent security warnings due to 'Internet Explorer Enhanced Security Configuration', older operating systems may need to be configured to trust the following sites:

Windows Components/Internet Explorer/Internet Control Panel/Security Page

Site to Zone Assignment List

- https://login.microsoftonline.com
- https://aadcdn.msauth.net

4.6.2.2 Manual Authentication

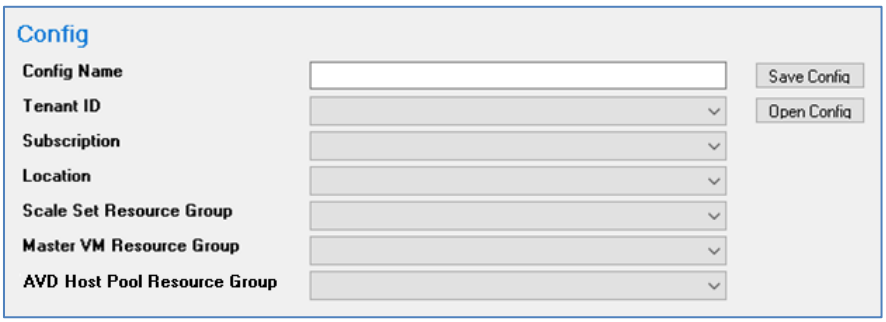
If you wish to authenticate manually, run **connect-azaccount**

Then launch AVDManage with the **bypassauth** parameter.

e.g. "C:\Program Files\Chawn\AVDManage\AVDManage.exe" bypassauth

4.7 Configure AVDManage

Authenticate to Azure as an Azure Subscription Owner and an Entra Global Administrator

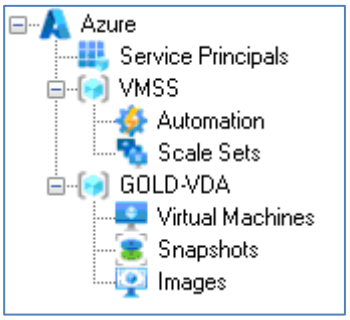


Configure AVDManage

- Provide a Config Name
- Select the target Azure Tenant
- Select the target Azure Subscription
- Select the target Azure Location
- Select the Resource Group for Virtual Machine Scale Sets and the Automation Account
- Select the Resource Group for the Master VM(s), Snapshots and Images
- Select the Resource Group that contains your AVD host pools – If you do not wish to use **AVD-Join**, just select the Master VM Resource Group

Save the configuration file.

AVDManage will open and display the following items.



Service Principals - This is a container for Service Principals which enable VMs to join Entra Id and AVD Host Pools

AVD-Join – Application Registration

AVDManage – User-Assigned Managed Identity

<ResourceGroupName> - VMSS - Resource Group containing:

Automation - A container for the Automation account.

Scale Sets - A container for the Virtual Machine Scale Sets.

<ResourceGroupName> - GOLD-VDA - Resource Group containing:

Virtual Machines - A container for Master VM Virtual Machines

Snapshots - A container for Master VM snapshots

Images - A containers for Master VM images.

Compute Galleries, **Image Definitions**, **Image Versions**

4.8 Create Service Principals

To enable Virtual Machine Scale Set Instances to join AVD Host Pools, two Service Principals are required.

- **AVD-Join** – Application Registration
- **AVDManage** – User-Assigned Managed Identity

AVD-Join is assigned Azure RBAC permissions to join VM instances to AVD Host Pools.

AVD-Join is assigned the ***Desktop Virtualization Host Pool Contributor*** role to the Resource Group containing AVD Host Pools. This enables **AVD-Join** to join and remove Session Hosts from the AVD Host Pools when deploying or updating Virtual Machine Scale Sets.

AVDManage is not assigned any RBAC permissions. **AVDManage** is assigned to all Virtual Machine Scale Sets that are configured to join Entra ID or an AVD Host Pool.

A Federated Credential is created on the **AVD-Join** Application Registration creating an Application Trust with **AVDManage**. This allows **AVDManage** to join VM instances to AVD Host Pools using Secretless Authentication.

4.8.1 Create AVD-Join (Application Registration)

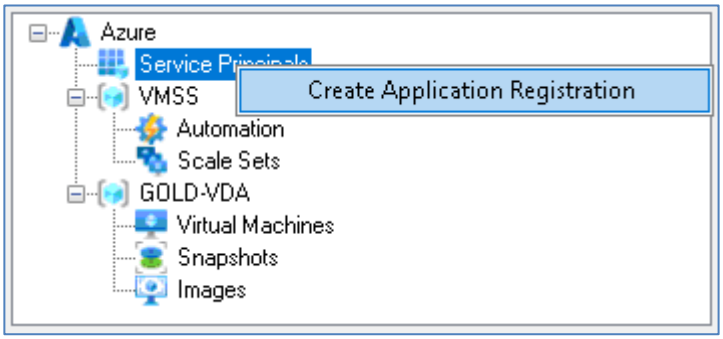
The user performing this task should have one to the following Entra roles to create an Application Registration.

- ***Entra Global Administrator***
- ***Application Administrator***
- ***Application Developer***
- ***Cloud Application Administrator*** role.

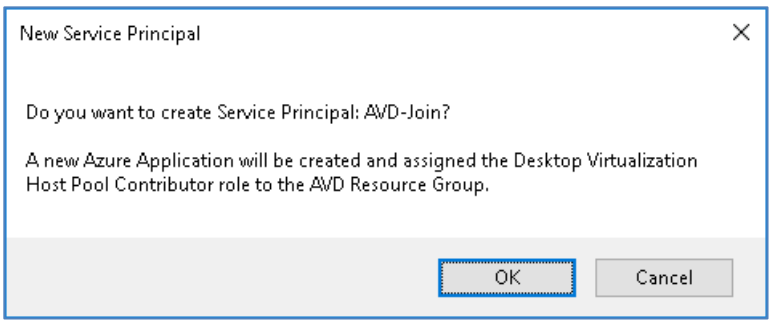
The user performing this task should also have one of the following roles to the Azure Virtual Desktop Resource Group to assign the ***Desktop Virtualization Host Pool Contributor*** role to **AVD-Join**.

- ***Owner***
- ***Role Based Access Control Administrator***
- ***User Access Administrator***

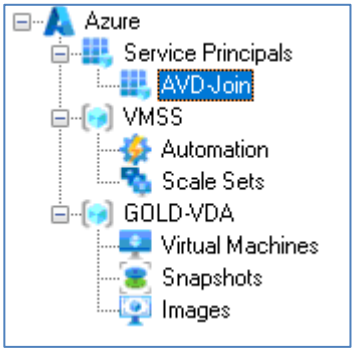
Right click the Service Principals node and select **Create Application Registration.**



Confirm that you want to create **AVD-Join**



AVD-Join is created.



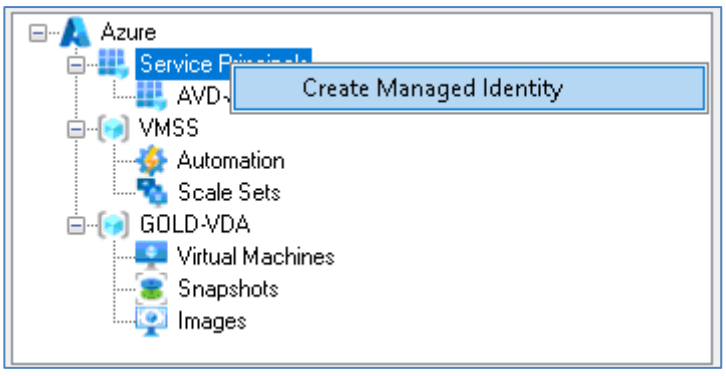
4.8.2 Create AVDManage (User-Assigned Managed Identity)

The **AVDManage** User Assigned Managed Identity is assigned to Scale Sets enabling VM instances to join Entra ID and AVD Host Pools.

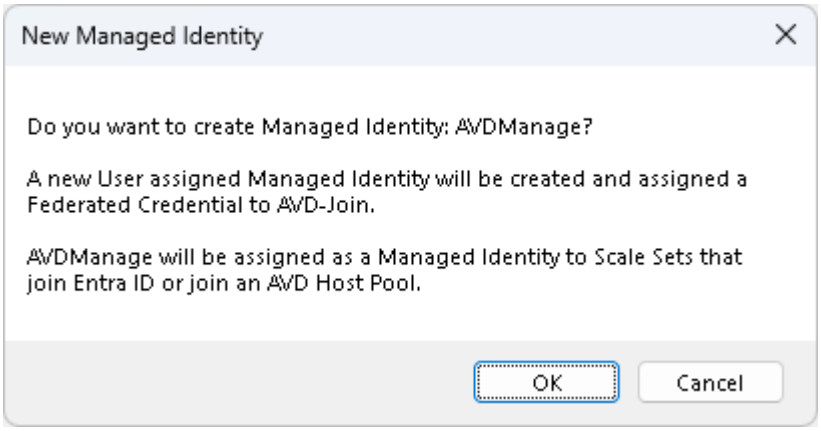
The user performing this task should have one of the following roles to the Virtual machine Scale Set Resource Group to create a user-assigned managed identity.

- ***Owner***
- ***Contributor***
- ***Managed Identity Contributor***

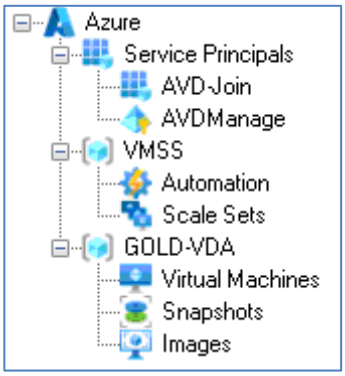
Right click the Service Principals node and select **Create Managed Identity.**



Confirm that you want to create **AVDManage**



AVDManage is created.



4.9 Create Automation Account – AVD-Automate (Optional)

An Automation Account may be used to run PowerShell scripts at specific times to Automate Tasks such as updating, restarting or power management of Virtual Machine Scale Sets.

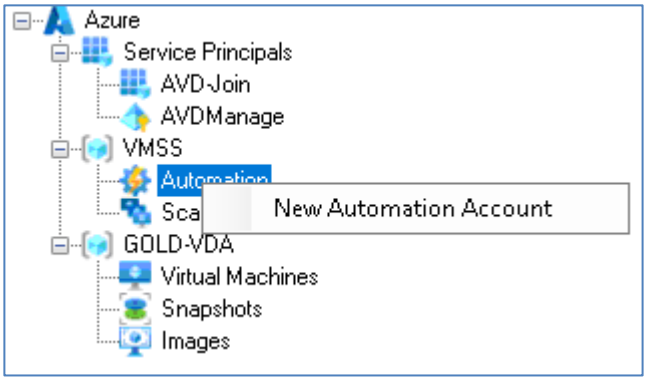
The user performing this task should have one of the following roles to the Virtual machine Scale Set Resource Group to create an Automation Account.

- **Owner**
- **Contributor**
- **Automation Contributor**

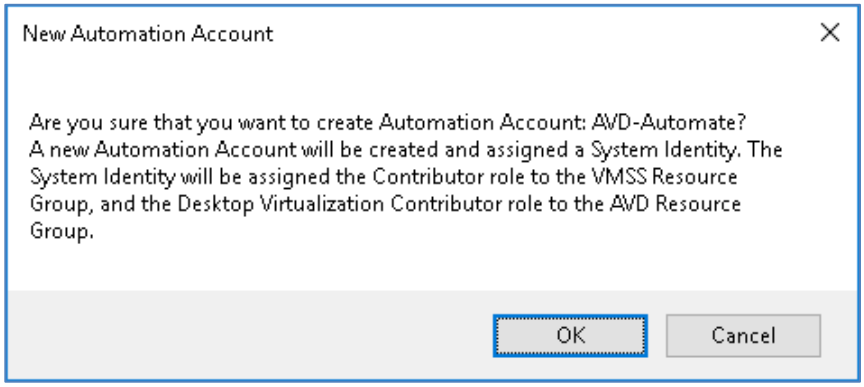
The user performing this task should also have one of the following roles to the Virtual machine Scale Set Resource Group to assign the ***Virtual Machine Contributor*** role to **AVD-Automate**, and the Azure Virtual Desktop Resource Group to assign the ***Desktop Virtualization Contributor*** role to **AVD-Automate**.

- ***Owner***
- ***Role Based Access Control Administrator***
- ***User Access Administrator***

Right Click Automation and select New Automation Account.

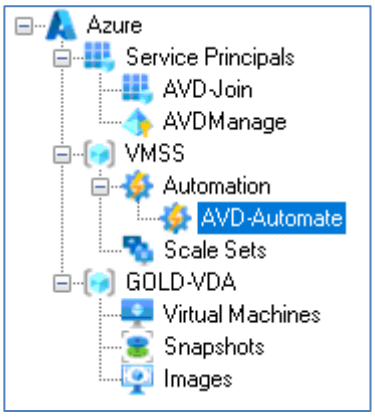


You will be asked to confirm that you want to create an Automation Account named AVD-Automate.



The AVD-Automate Automation Account will be created and assigned a System Identity.

The System Identity will be assigned the *Virtual Machine Contributor* role to the Resource Group containing Virtual Machine Scale Sets, and the *Desktop Virtualization Contributor* role to the Resource Group containing AVD Host Pools.



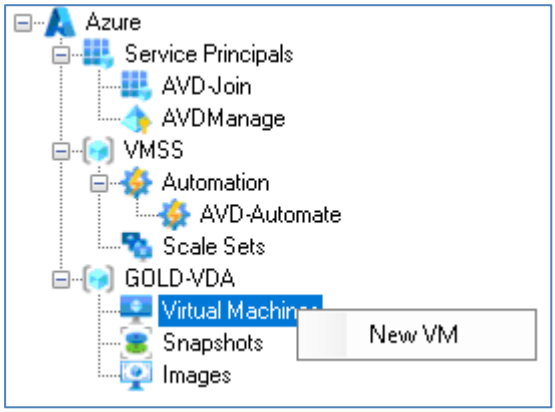
Configuration Complete. **AVD-Admins** can now use all features of AVDManage.

You can distribute the config file to **AVD-Admins**, or they can create their own config file using identical parameters.

5. Create (Master) VM

The user performing these tasks should be a member of **AVD-Admins**.

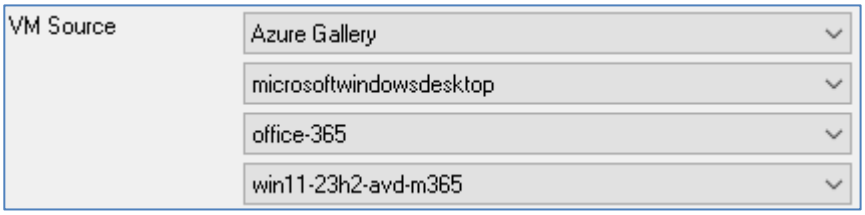
Right click Virtual Machines and select New VM.



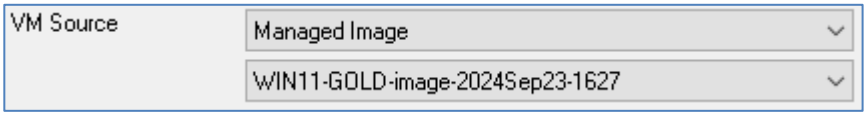
Supply parameters for the following properties.

VM Source

This can be either an Azure Gallery Image,



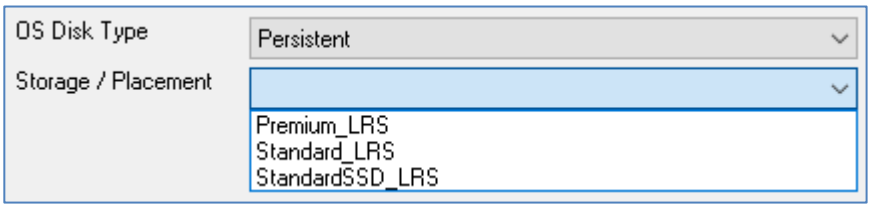
or a Managed Image.



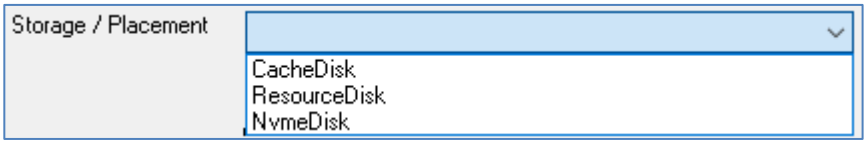
It is recommended that the Master VM is created from an Azure Gallery Image as Microsoft does not recommend deploying a Master VM from a managed image that has been previously sysprepped.

OS Disk Type

This can either be Persistent



or Ephemeral.

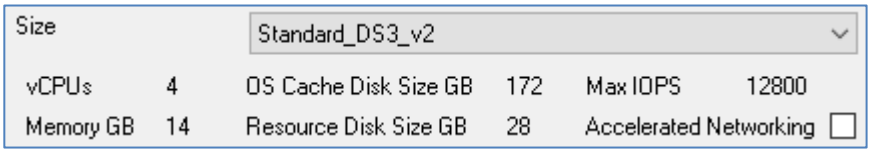


The Master VM must be created using a Persistent OS Disk as VMs with Ephemeral OS Disks cannot be shutdown, sysprepped or used to create Images.

(VM) Size

The Size of the VM is filtered based on the OS Disk Type.

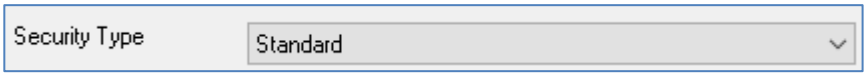
If supported, you can enable Accelerated Networking however this is not recommended for Master VMs.



Security Type

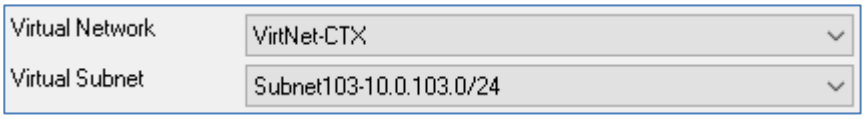
AVDManage (Free) – Security Type is always Standard as Managed Images do not support Trusted Launch.

AVDManage (Plus) – You can choose Trusted Launch however Standard Security is recommended for Master VMs.



Virtual Network / Virtual Subnet

Select a Virtual Network and Virtual Subnet.



VM Name

Maximum length: 15 characters

VM names can only contain alphanumeric characters and hyphens.

Local Administrator

The name of the Local Administrator Account.

Maximum length: 20 characters

(Local Administrator) Password

Maximum length: 123 characters

The Local Administrator password must contain characters from at least three of the following categories. One upper case letter, one lower case letter, a number, one special character.

Make a note of the Local Administrator name and password. When the VM is recreated in the future from a snapshot, you will need the same credentials to logon.

Join Active Directory Domain (Optional)

Domain Name: The name of the target Active Directory Domain

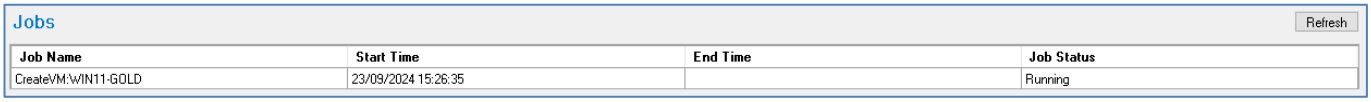
Org Unit: The name of the target AD Organizational Unit in LDAP format

AD User: The userPrincipalName of a user with sufficient privileges to join the VM to the Domain

Password: Password of the AD User

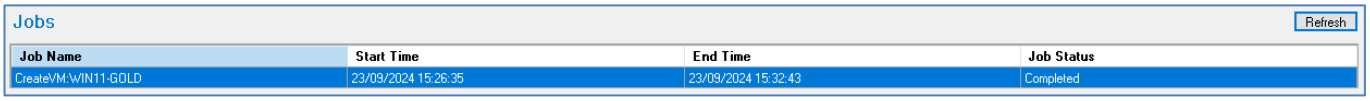
It is not necessary to join an Active Directory Domain however it may simplify access to application resources while building the Master VM. It is recommended that the Master VM is removed from the Active Directory Domain before running sysprep on the Master VM.

A new job will be created to deploy the Virtual Machine



You can click Refresh to update the status of the job and right click the job to view its details.

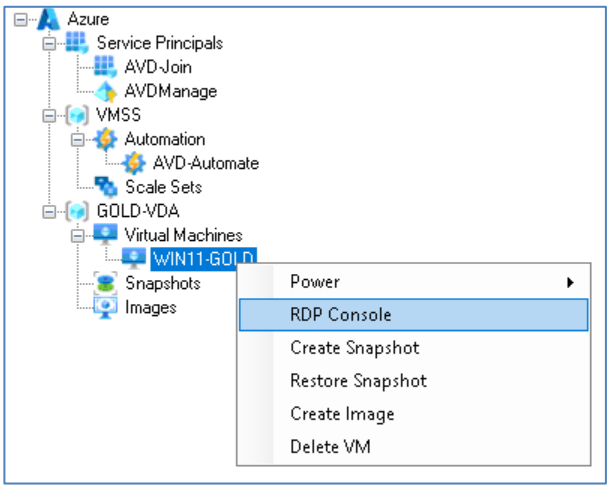
When the job is complete, the Job Status will change to Completed.



Estimated time to complete: 6 mins

5.1 Modify the Master VM

If you have a private network connection to Azure, you can RDP to the new VM.



Don't install the Remote Desktop Service Infrastructure Agent or Boot Agent. These will be deployed later with **AVD-Turbo** when deploying a Virtual Machine Scale Set.

Standard modifications:

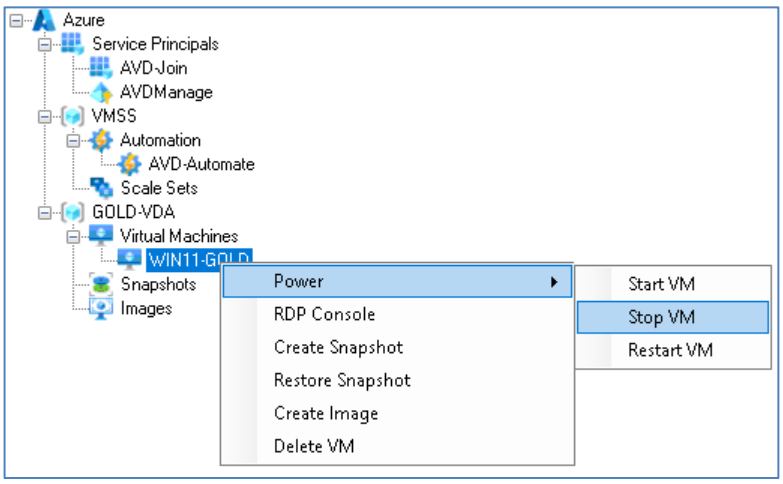
- Disable BitLocker
- Add / Remove required Applications and Features
- Remove unwanted Microsoft Store Apps
- Install required Language Packs
- Install all available Windows and Application updates
- Install required Printer Drivers
- Configure the Default User Profile
- Configure Regional Settings – Apply to current and new users
- Configure Time Zone
- Configure Location
- Modify the All Users Start Menu
- Disable unnecessary Scheduled Tasks
- Disable unnecessary Services
- Enable required Services (Windows Search)
- Enable Firewall Rules (Domain Profile)
- Delete Temporary Files and Source Media on the OS Disk
- Apply known optimizations

AVD-Update may be used to update Windows and primary software.

AVD-Optimise may be used to optimise the system.

AVD-Prep may be used to pre-stage the Microsoft Remote Desktop Service Infrastructure Agent and Boot Agent.

When you have made all required changes to the Master VM, shut the VM down using AVDManage so that the VM status is deallocated.



[Create an Azure Virtual Desktop golden image | Microsoft Learn]

[Prepare and customize a VHD image of Azure Virtual Desktop - Azure | Microsoft Learn]

[Recommended configuration for VDI desktops | Microsoft Learn]

[Prepare a Windows VHD to upload to Azure - Azure Virtual Machines | Microsoft Learn]

[(Azure) Virtual Desktop Optimization Tool now available - Microsoft Community Hub]

[Optimizing Windows configuration for VDI desktops | Microsoft Learn]

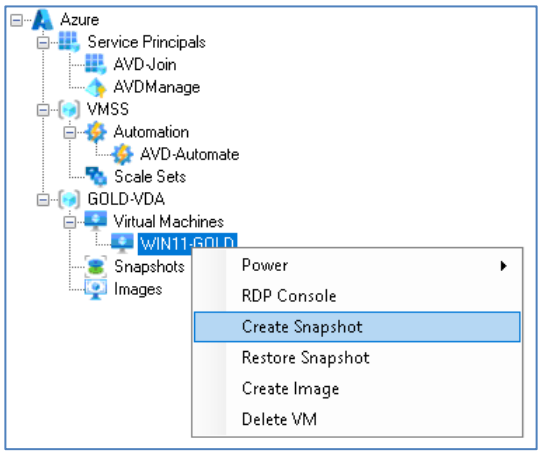
5.2 Snapshot the Master VM

A snapshot is required so that the Master VM can be recreated in the future in the same state as its last update.

After the snapshot has been created, the next step is to sysprep the Master VM which will render the Master VM unusable. The snapshot allows for the original VM to be recreated in the future.

Check the VM status is Deallocated.

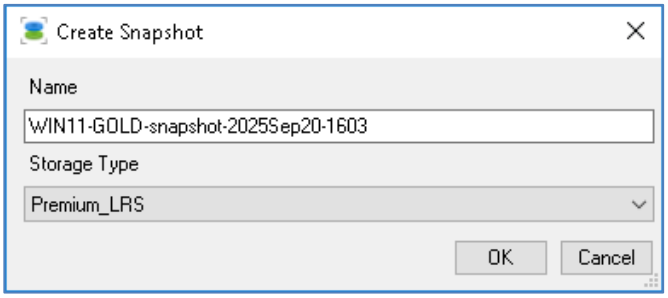
Right click the VM and select Create Snapshot



Name

Maximum length: 80 characters

The name is auto-generated based on the name of the VM and the current date / time. It may be modified. Snapshot names can only contain Alphanumeric characters, hyphens and underscores.

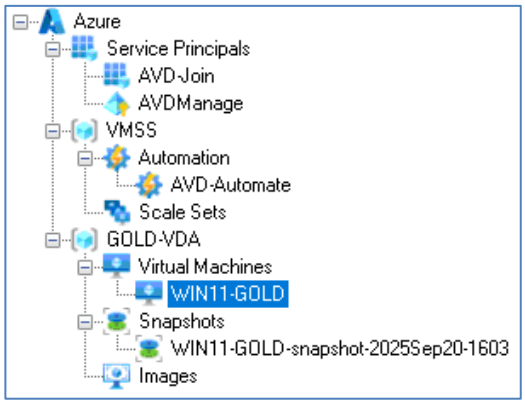


Storage

Select from

- Standard_LRS
- Premium_LRS
- Standard_ZRS

The new Snapshot is displayed under the Snapshots node.



Estimated time to complete: 10-20 seconds

5.3 Sysprep the Master VM

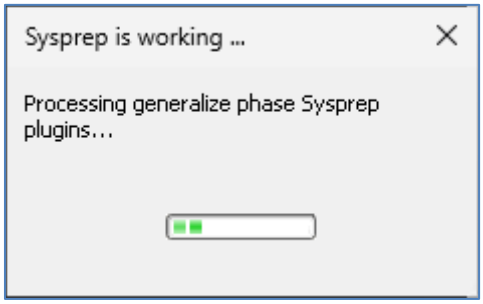
Start the VM.

When the VM is running, connect using RDP to the new VM.

If the VM is joined to an Active Directory Domain, remove the VM from the Domain and restart.

Open a command prompt as Administrator and run:

C:\Windows\System32\Sysprep\sysprep.exe /oobe /generalize /shutdown



After several minutes the VM will shut down.

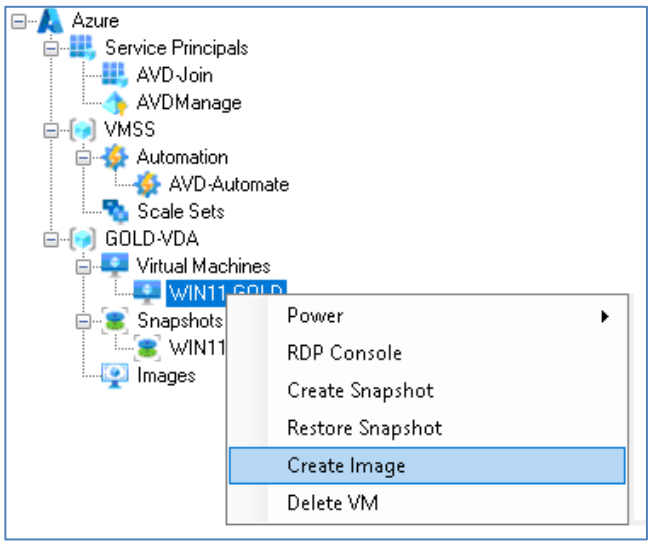
It is recommended that a ***Seal Script*** is used to shut down and sysprep the VM. A seal script can perform tasks that affect the state of the VM.

AVD-Seal may be used as a seal script to prepare the master image and run Sysprep.

5.4 Create Image of the Master VM

Check the VM status is Stopped or Deallocated.

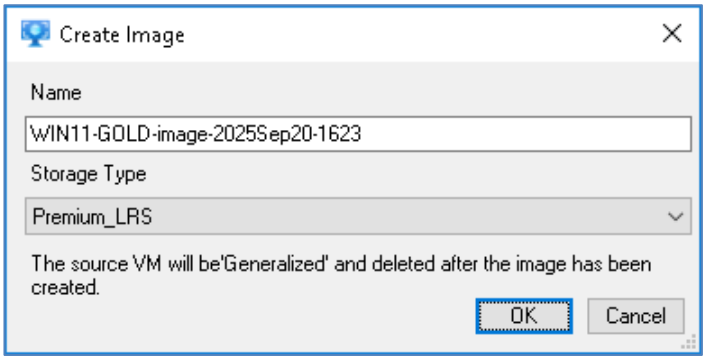
Right click the VM and select Create Image



Name

Maximum length: 80 characters

The name is auto-generated based on the name of the VM and the current date / time. It may be modified. Image names can only contain Alphanumeric characters, hyphens and underscores.



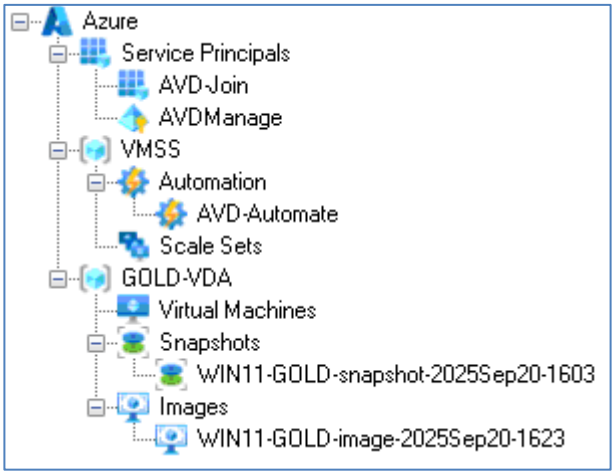
Storage

Select from

- Standard_LRS
- Premium_LRS

The VM will be marked as generalized before an Image is created and the VM is deleted.

The new Image is displayed under the Images node.



Estimated time to complete: 60 seconds

6. Virtual Machine Scale Sets

Virtual Machine Scale Sets define a common Virtual Machine profile which is applied to all Virtual Machine Scale Set instances. The Virtual Machine profile includes:

- Vm Size
- Os Disk Type
- Image Reference
- Network Configuration
- Virtual Machine Extensions

Before creating a Virtual Machine Scale Set, you must choose which Orchestration Mode to use, Uniform or Flexible.

6.1 Uniform vs Flexible

A Virtual Machine Scale Set in **Uniform** Orchestration mode is a single object in Azure. The Virtual Machine instances are discreet properties of the Scale Set, and may only be managed using Virtual Machine Scale Set VM API commands.

A Virtual Machine Scale Set in **Flexible** Orchestration mode is a single object in Azure however each Virtual Machine instances are explicit Virtual Machine with a disk and network card, and may be managed using Virtual Machine VM API commands. This allows for integration with services that rely on a Virtual Machine object. (E.g. AVD Power management autoscaling)

Orchestration modes for Virtual Machine Scale Sets in Azure - Azure Virtual Machine Scale Sets | Microsoft Learn

All **AVDManage** operations and Task scripts are compatible with both Uniform and Flexible Orchestration Modes.

Uniform Scale Sets	Flexible Scale Sets
No Virtual Machine objects in Azure	Virtual Machine objects exist in Azure
VM instances do **not** report PowerState and Location to the AVD Host Pool	VM instances do report PowerState and Location to the AVD Host Pool
Do **not** support AVD Power management autoscaling	Do support AVD Power management autoscaling when using persistent O/S disk
Do **not** support AVD Dynamic autoscaling	Do **not** support AVD Dynamic autoscaling
Managed with Virtual Machine Scale Set VM API commands only	Managed with Virtual Machine Scale Set VM API commands and Virtual Machine VM API commands
Support non-private subnets (Internet access enabled by default)	Require Default Outbound Internet Access (Requires explicit method to enable Internet access)

Orchestration modes for Virtual Machine Scale Sets in Azure - Azure Virtual Machine Scale Sets | Microsoft Learn

> **Important**
>
> After March 31, 2026, new virtual networks will default to using private subnets, meaning that an explicit outbound method must be enabled in order to reach public endpoints on the internet and within Microsoft. For more information, see the official announcement. We recommend that you use one of the explicit forms of connectivity discussed in the following section. For other questions, see the "FAQs: Default Behavior Change to Private Subnets" section.

Power management and scaling tasks may be configured using **AVD-Automate** for both Uniform and Flexible Scale Sets.

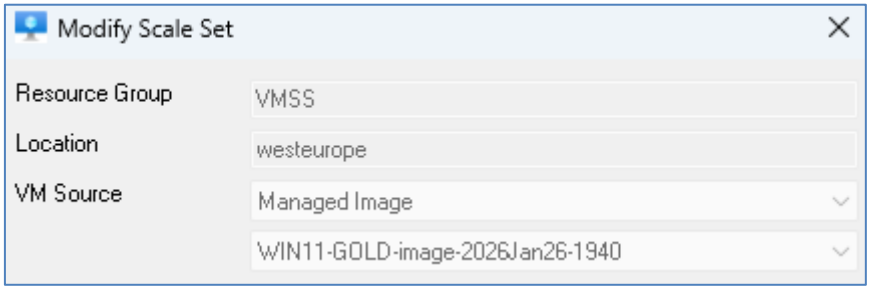
Virtual Machine Scale Sets with Ephemeral O/S disks do not support AVD Power management autoscaling because they cannot be powered off.

Further Differences

Flexible Scale Set VM instances take slightly longer to create and may not be immediately visible after creating a Scale Set or increasing Scale Set capacity.

When updating, re-deploying or re-imaging a Flexible Scale Set or Flexible Scale Set VM instance, jobs will report as 'Completed' before the operation has entirely completed. This may cause confusion as the AVD-Status of the VM may vary between 'Shutdown', 'Not Available' or 'Provisioning Failed'. When the operation is entirely complete, the AVD-Status will change to 'Available'.

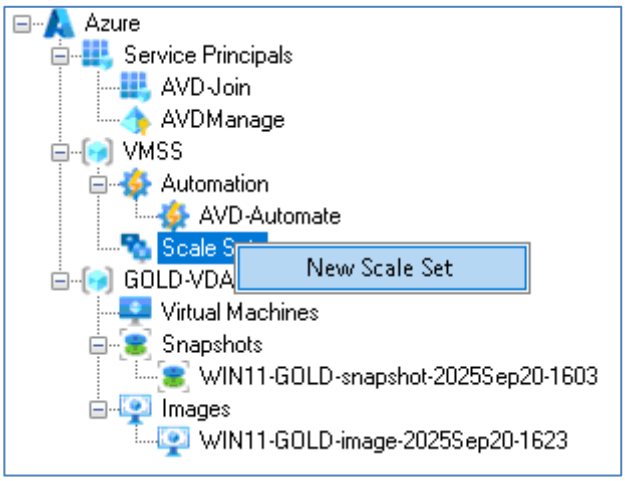
It is not possible to modify the image reference for a Flexible Scale Set when deploying from a Managed Image. You can create a Flexible Scale Set with a Managed Image, however AVDManage does not permit modifying the assigned Manage Image.



Orchestration Mode	Flexible	Uniform
Image Source	**Image Update Supported**	
Managed Image	No	Yes
Azure Gallery Image	Yes	Yes
Compute Gallery Image	Yes	Yes

6.2 Create a Virtual Machine Scale Set

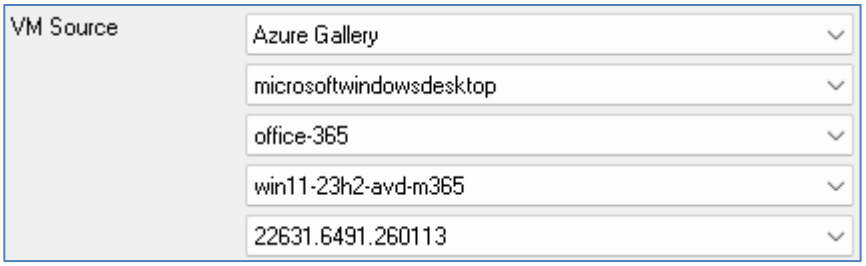
Right Click Scale Sets and select New Scale Set



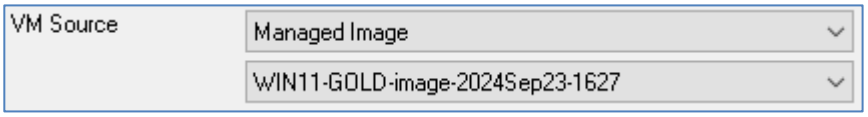
Supply parameters for the following properties.

VM Source

This can be either an Azure Gallery Image,

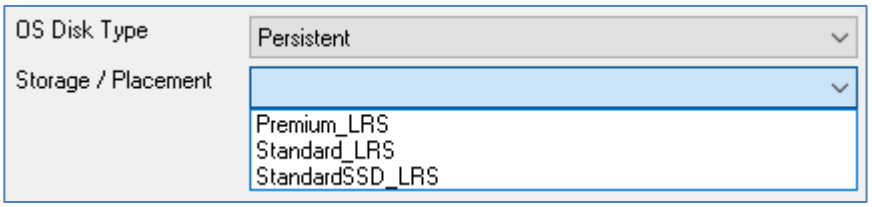


or a Managed Image.

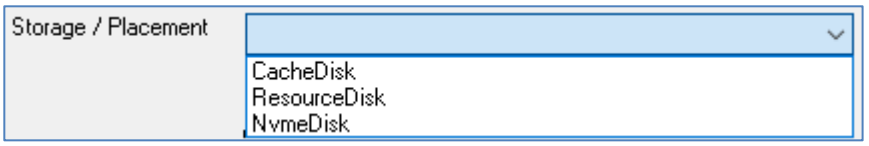


OS Disk Type

This can either be Persistent



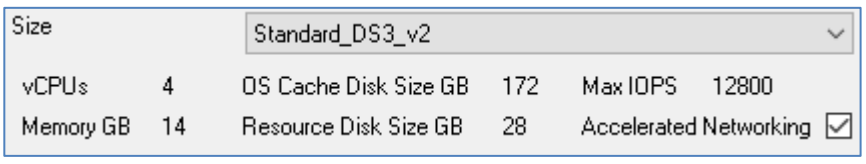
or Ephemeral.



(VM) Size

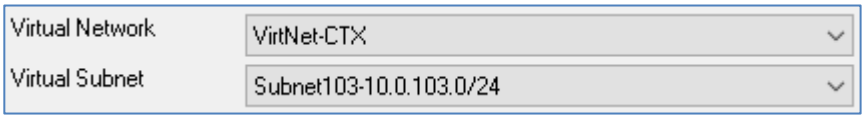
The Size of the VM is filtered based on the OS Disk Type.

If supported by the VM, you can enable Accelerated Networking.



Virtual Network / Virtual Subnet

Select a Virtual Network and Virtual Subnet.



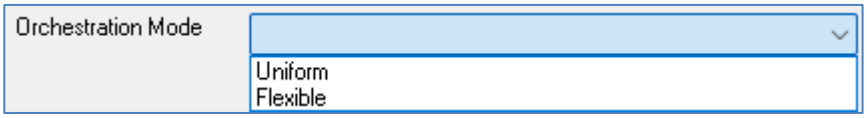
Scale Set Name

Maximum length: 15 characters

Scale Set names can only contain Alphanumeric characters and hyphens.

Orchestration Mode

Select Uniform or Flexible.



VM Instances

Up to 1000 VMs may be created from an Azure Gallery Image.

Up to 600 VMs may be created from a Managed Image.

(Subject to Azure Subscription limits & quotas)

Update Mode

Manual mode is preferred for AVD Scale Sets so that updates and maintenance can be scheduled for appropriate times using an Automation Account.

Automatic mode is available however the scale set makes no guarantees about the order of virtual machines being brought down. The scale set might take down all virtual machines at the same time to perform upgrades.

VM Name Prefix

Maximum length: 9 characters

VM names can only contain alphanumeric characters and hyphens.

Local Administrator

The name of the Local Administrator Account.

Maximum length: 20 characters

(Local Administrator) Password

Maximum length: 123 characters

The Local Administrator password must contain characters from at least three of the following categories. One upper case letter, one lower case letter, a number, one special character.

Join Active Directory Domain (Optional)

Domain Name: The name of the target Active Directory Domain

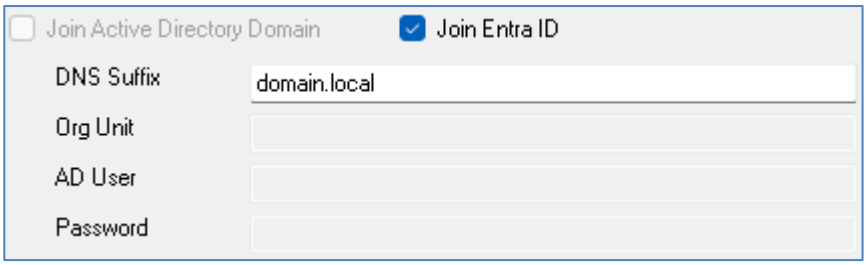
Org Unit: The name of the target AD Organizational Unit in LDAP format

AD User: The userPrincipalName of a user with sufficient privileges to join the VM to the Domain

Password: Password of the AD User

Or

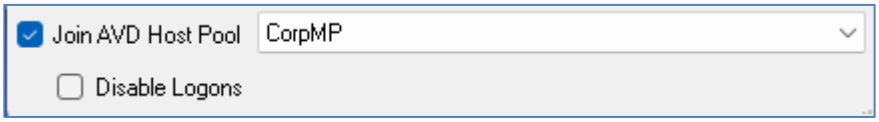
Join Entra ID



The device will join your Entra ID Tenant.

You may optionally specify a primary DNS Suffix.

Join AVD Host Pool



Host Pool: Select a Host Pool name. Optionally choose to Disable AVD logons after deployment.

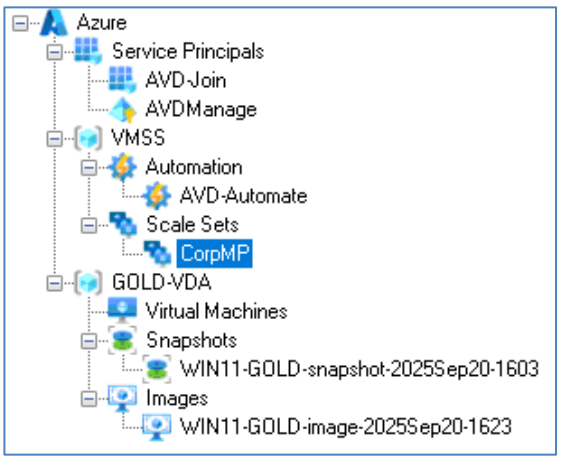
You must have created the Application Registration **AVD-Join**, and User-Assigned System Identity **AVDManage**.

You must have created an AVD Host Pool in the AVD Resource Group.

You must enable and configure **Join Active Directory Domain** or **Join Entra** to enable this option.

The time to create the Scale Set can vary depending on how many VMs are created and the VM Size.

When the Scale Set has been created, a new node will appear under Scale Sets.



Estimated time to complete: ~8 minutes (5 VM instances)

Don't forget to configure Windows Licensing

7. Image Updates

The user performing these tasks should be a member of **AVD-Admins**.

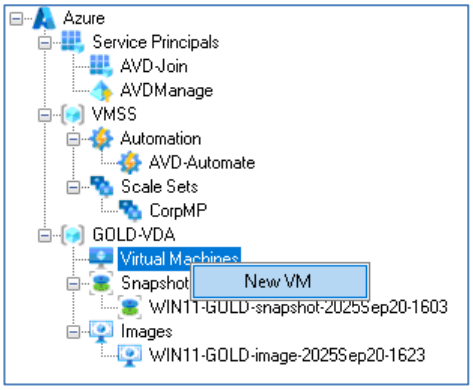
Managed Images will require updating at least once per month.

Updates may include:

- Windows Updates
- Application Updates
- Add / Remove Applications
- Fixes to discovered issues

7.1 Recreate the Master VM

Right click Virtual Machines and select New VM.



VM Source

Select Snapshot then select the last known good snapshot.

Storage / Placement

The OS Disk Type is Persistent. Select a storage tier.

(VM) Size

Select a virtual machine size.

Security Type

This is inherited from the Snapshot and may not be modified.

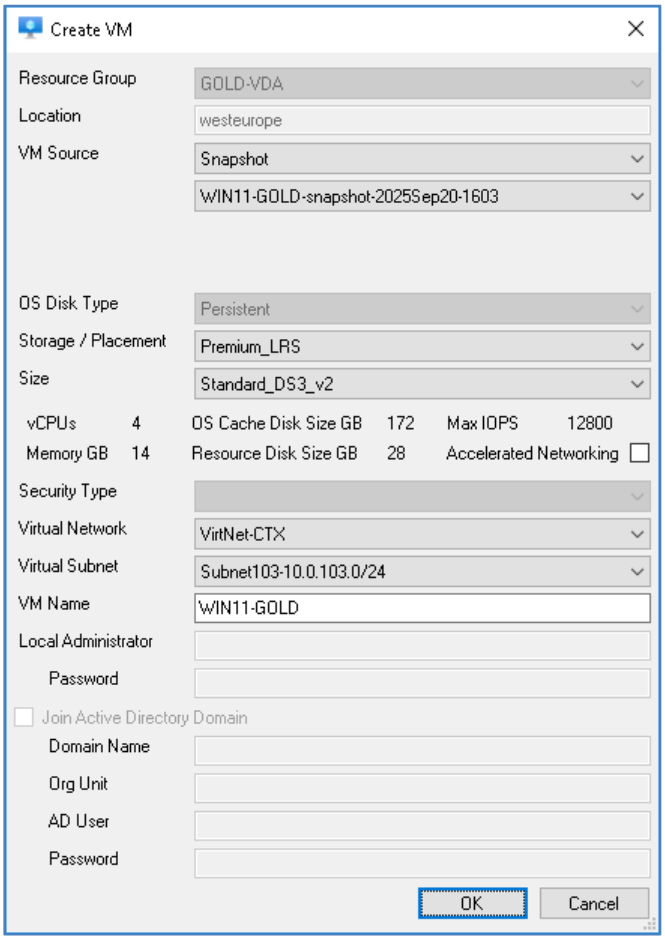
Virtual Network / Virtual Subnet

Select a Virtual Network and Virtual Subnet.

VM Name

The Master VM will have the same Windows ComputerName as before so it is recommended to name the VM accordingly.

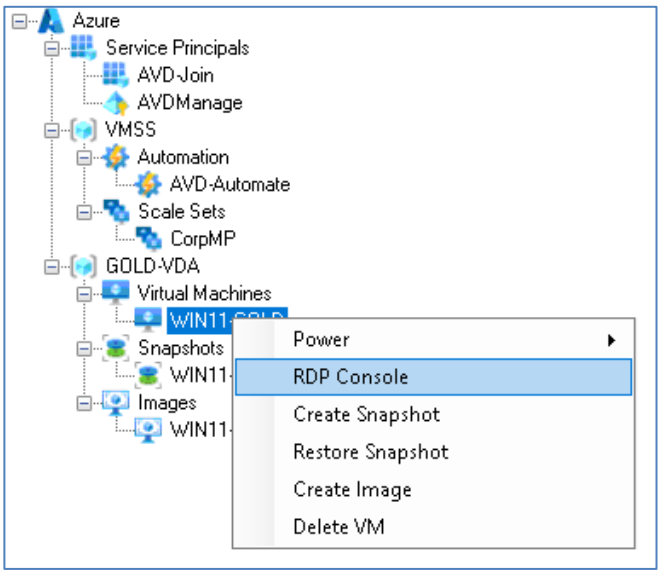
If the Master VM was previously domain joined when the snapshot was created, it will still be domain joined after creation.



Estimated time to complete: 2 minutes

7.2 Modify the Master VM

If you have a private network connection to Azure, you can RDP to the new VM.

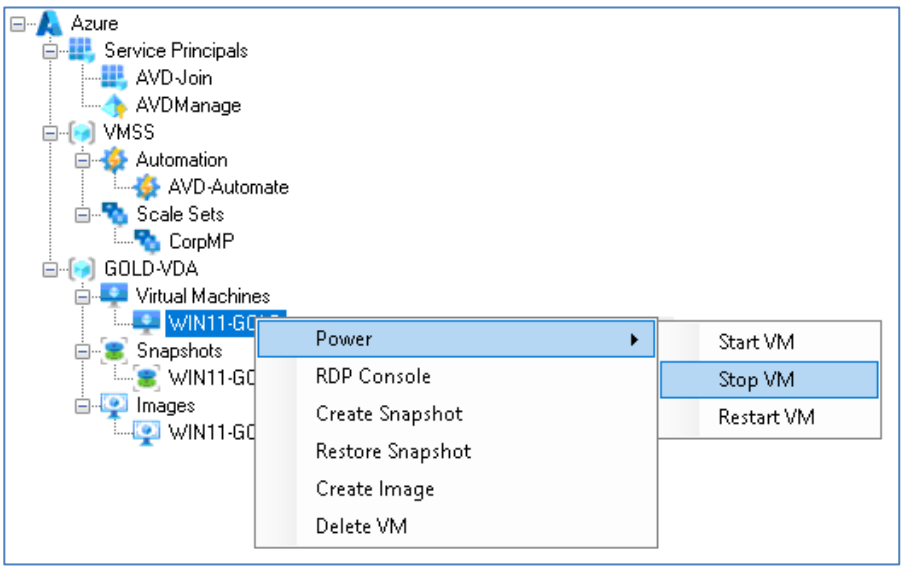


Updates may include:

- Windows Updates
- Application Updates
- Add / Remove Applications
- Fixes to discovered issues

When applying Windows Updates and rebooting, the VM may not be contactable for several minutes.

When you have made all required changes to the Master VM, shut the VM down.



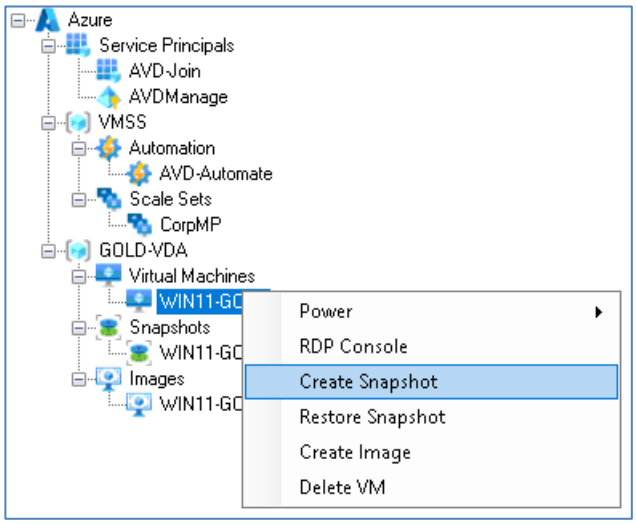
7.3 Snapshot the Master VM

A snapshot is required so that the Master VM can be recreated in the future in the same state as its last update.

After the snapshot has been created, the next step is to sysprep the Master VM which will render the Master VM unusable. The snapshot allows for the original VM to be recreated in the future.

Check the VM status is Deallocated.

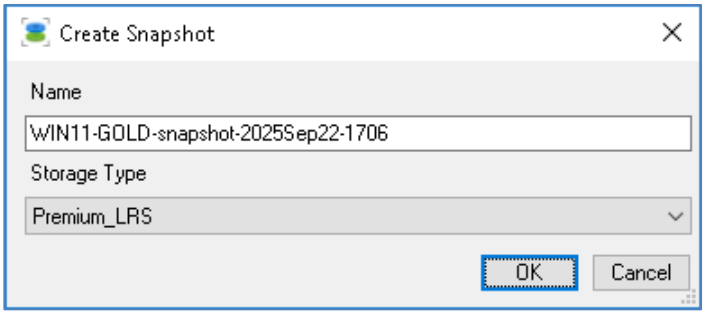
Right click the VM and select Create Snapshot



Name

Maximum length: 80 characters

The name is auto-generated based on the name of the VM and the current date / time. It may be modified. Snapshot names can only contain Alphanumeric characters, hyphens and underscores.

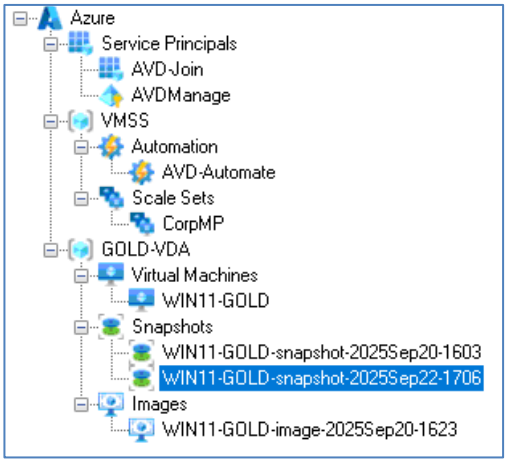


Storage

Select from

- Standard_LRS
- Premium_LRS
- Standard_ZRS

The new Snapshot is displayed under the Snapshots node.



Estimated time to complete: 10-20 seconds

7.4 Sysprep the Master VM

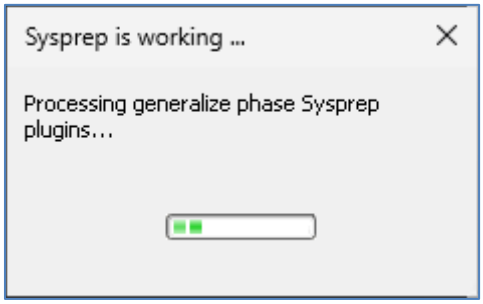
Start the VM.

When the VM is running, RDP to the new VM.

If the VM is joined to an Active Directory Domain, remove the VM from the Domain and restart.

Open a command prompt as Administrator and run a seal script or:

C:\Windows\System32\Sysprep\sysprep.exe /oobe /generalize /shutdown



After several minutes the VM will shut down.

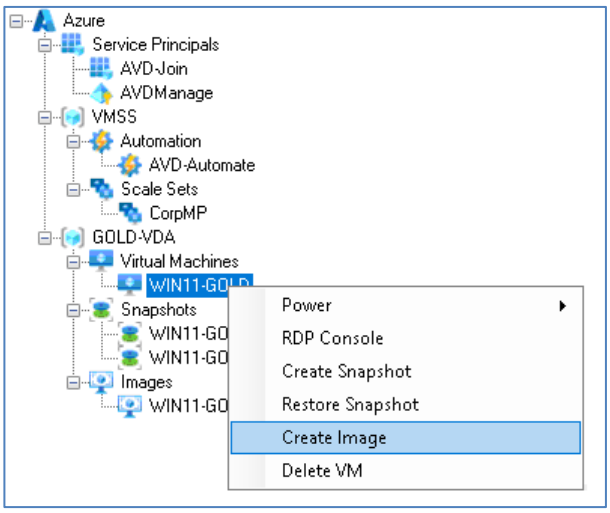
It is recommended that a ***Seal Script*** is used to shut down and sysprep the VM. A seal script can perform tasks that affect the state of the VM.

AVD-Seal may be used as a seal script to prepare the master image and run Sysprep.

7.5 Create Image of the Master VM

Check the VM status is Stopped or Deallocated.

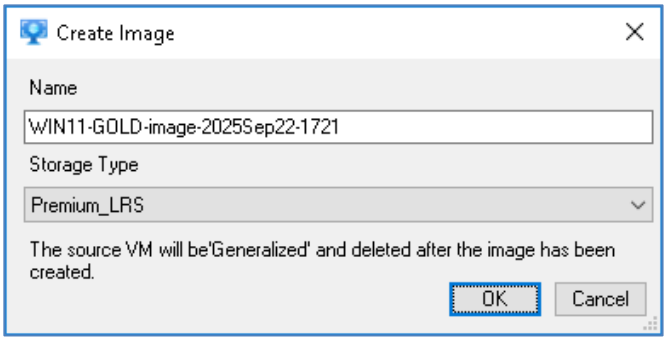
Right click the VM and select Create Image



Name

Maximum length: 80 characters

The name is auto-generated based on the name of the VM and the current date / time. It may be modified. Image names can only contain Alphanumeric characters, hyphens and underscores.



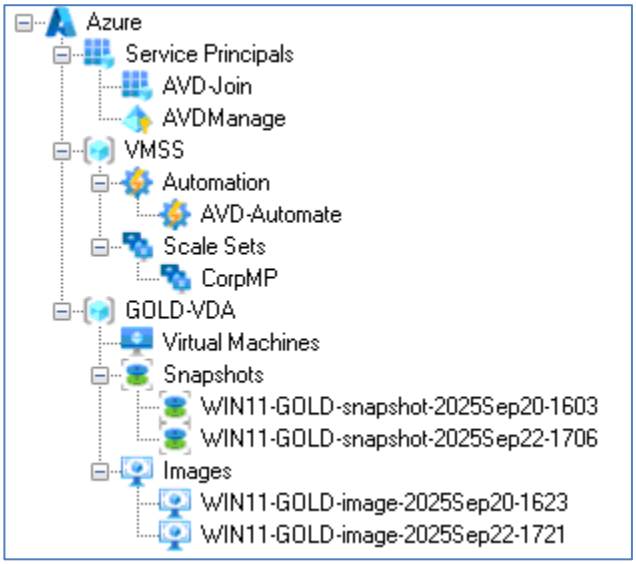
Storage

Select from

- Standard_LRS
- Premium_LRS

The VM will be marked as generalized before an Image is created and the VM is deleted.

The new Image is displayed under the Images node.



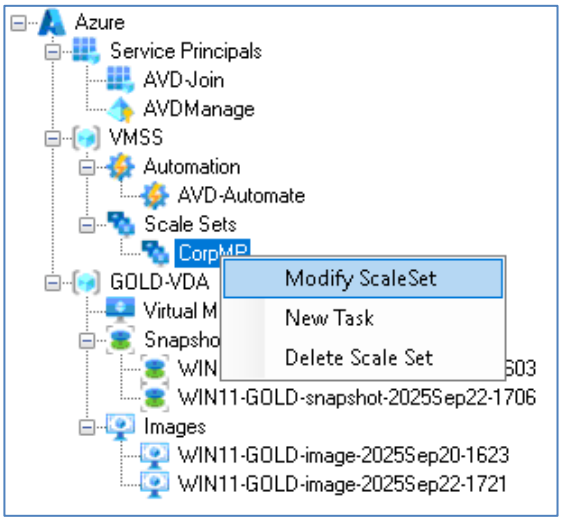
Estimate time to complete: 60 seconds

8. Update a Scale Set

The user performing these tasks should be a member of **AVD-Admins**.

When a new image has been prepared, the Scale Set configuration may be updated.

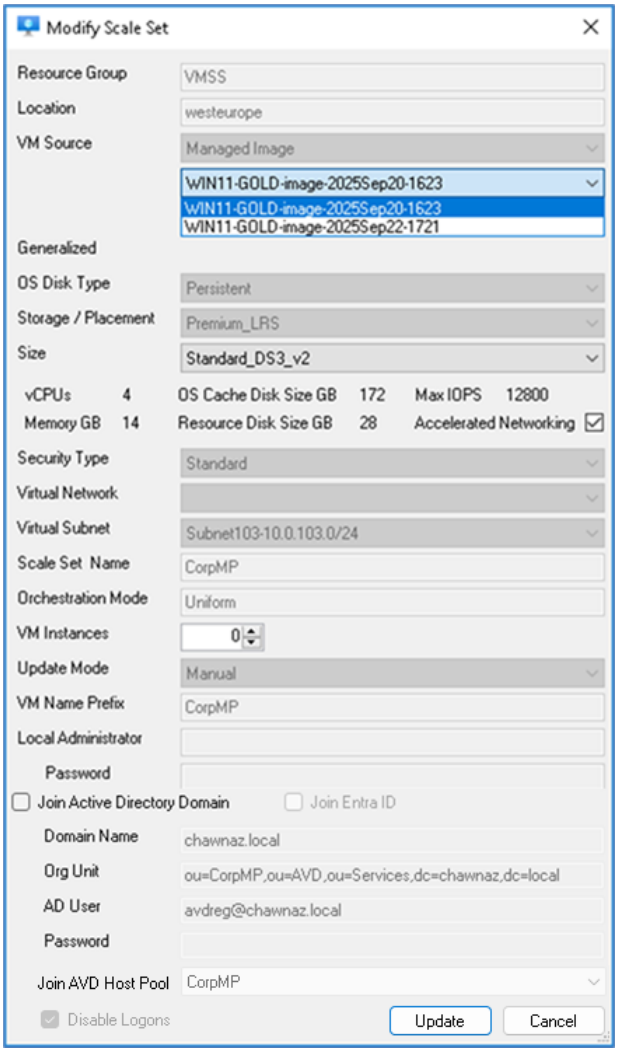
Right click the Scale Set and select Modify Scale Set.



You can modify the:

- **VM Source**
- **(VM) Size – Scale Up**
- **(VM Instances) – Scale Out**

In this instance, the VM Source is being updated to the newer Managed Image.

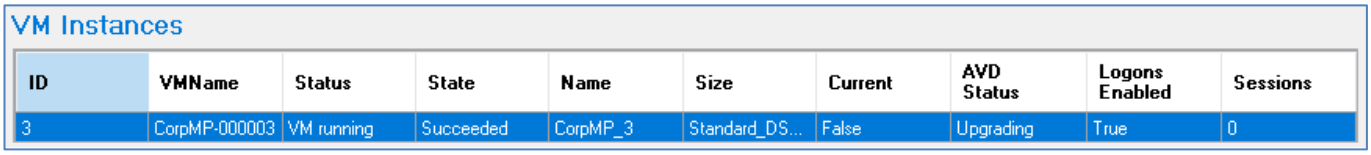


If the Scale Set is configured to Join Active Directory, you can update the AD User and Password.

If you do not select the checkbox, the Active Directory configuration remains the same.

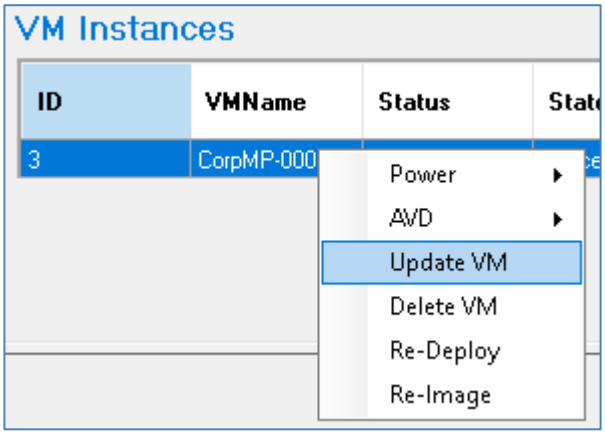
The Join AVD configuration remains the same.

The **Current** status of the VM Instances will change from True to False. They are still running the old image, and do not have the latest Scale Set configuration.



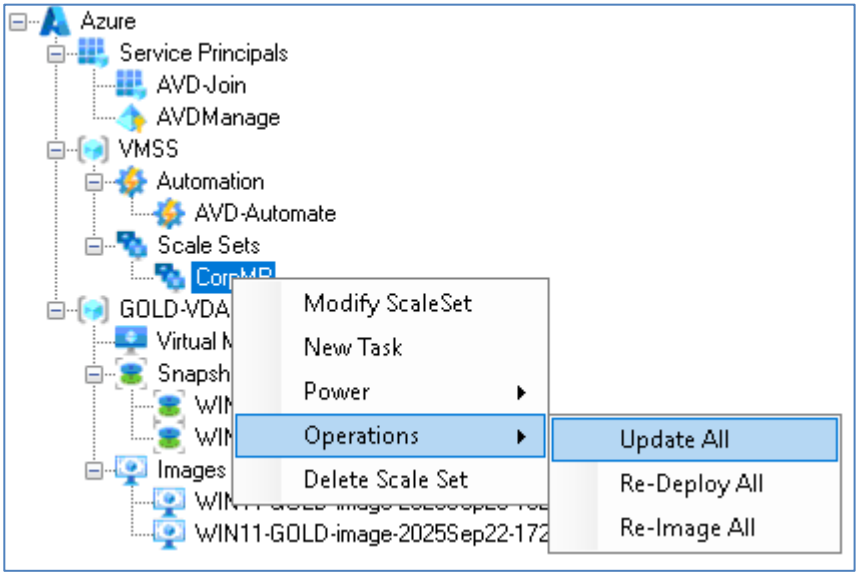
A single VM instance may be updated by right clicking the VM and selecting update.

The VM will shut down and be unavailable while updating.



All VM instances in the Scale Set may be updated by right clicking the Scale Set and selecting Update All.

All VMs will shut down and be unavailable while updating.



When updating Ephemeral and Persistent Virtual Machine instances, they will retain their VMName, VM Instance name, Windows ComputerName Active Directory ComputerName, and Entra Device ID.

Immediate updating of VMs is unlikely to be appropriate if the VMs are hosting AVD sessions.

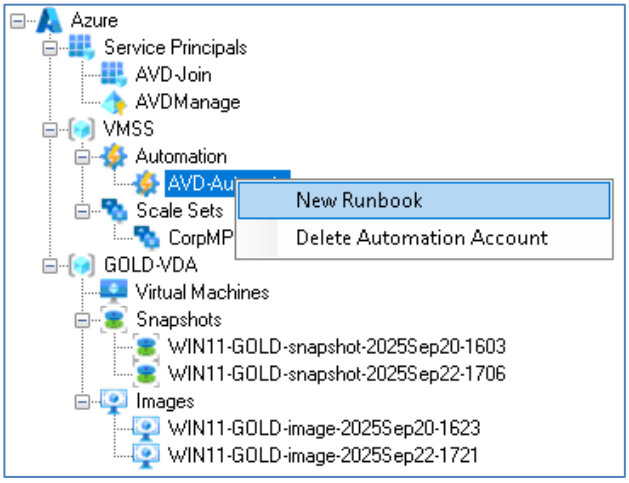
It is recommended that Scale Set updates are scheduled during a planned maintenance window using Azure Automation and ***AVD-Automate***.

8.1 Create Update Runbook

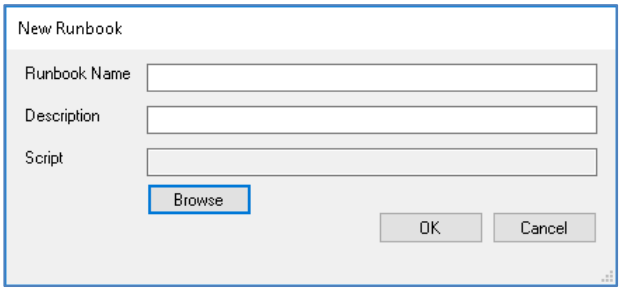
AVD-Automate can schedule an update of the Virtual Machine instances.

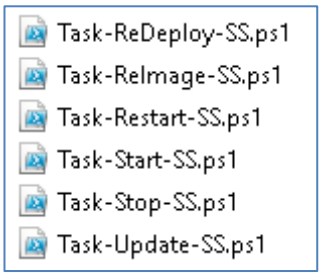
Task-Update-SS.ps1 is used to create an Automation Task that updates all the VM Instances at the same time during a planned maintenance window. The VMs will be re-deployed with the new Scale Set configuration such as an updated Image.

Right Click AVD-Automate and select New Runbook.



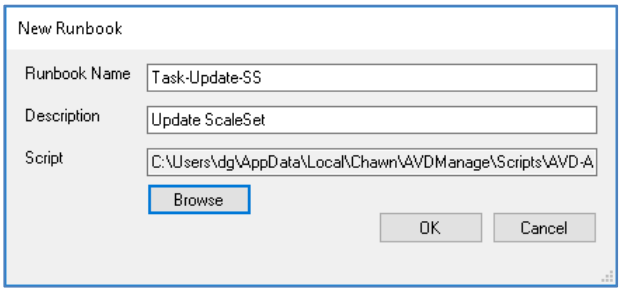
Click Browse and select a Runbook script.



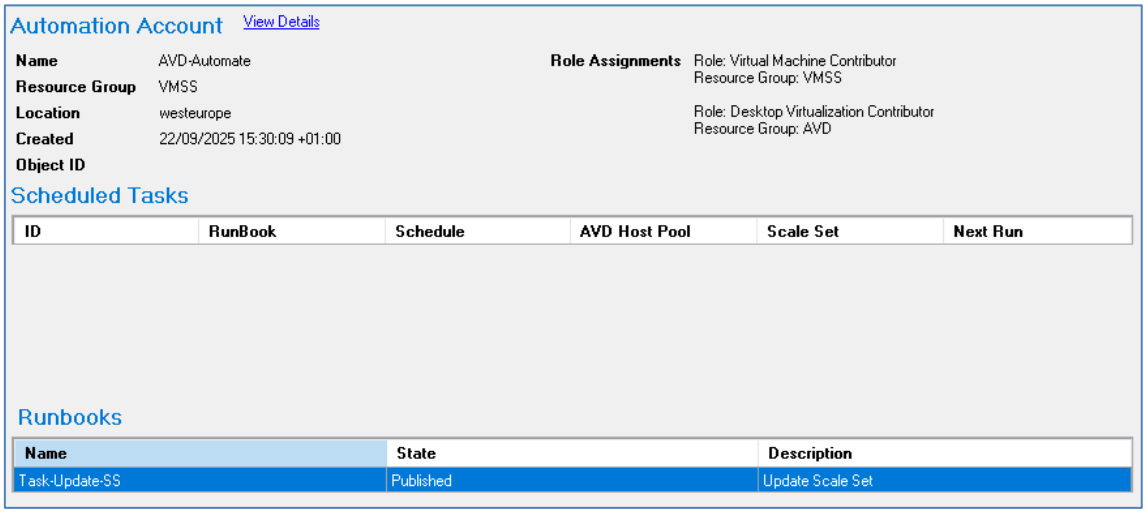


The Runbook name and Description are auto-completed but may be edited.

Click OK.



The new Runbook is visible when clicking on the AVD-Automate node.



A single runbook can be applied to multiple Scale Sets.

Runbook scripts are stored in **%LOCALAPPDATA%\Chawn\AVDManage\Scripts\AVD-Automate**.

Additional Task Scripts will be made available at https://github.com/ChawnLimited/AVDManage.

Runbook Script	Purpose
Task-DisableLogons-SSAVD.ps1	Disable AVD logons for Scale Set VM instances
Task-EnableLogons-SSAVD.ps1	Enable AVD logons for Scale Set VM instances
Task-LogOffSessions-SSAVD.ps1	Logoff all AVD sessions on Scale Set VM instances
Task-ReDeploy-SS.ps1	Re-Deploy all Scale Set VM instances
Task-ReImage-SS.ps1	Re-Image all Scale Set VM instances
Task-Restart-SS.ps1	Restart all Scale Set VM instances
Task-Start-SS.ps1	Start all Scale Set VM instances
Task-Stop-SS.ps1	Stop all Scale Set VM instances
Task-Update-SS.ps1	Update all Scale Set VM instances

8.2 Create Update Automation Task

A Task is required to associate a Scale Set with a Runbook. The Runbook will execute at the time specified in the Task schedule.

Runbook: Task-Update-SS

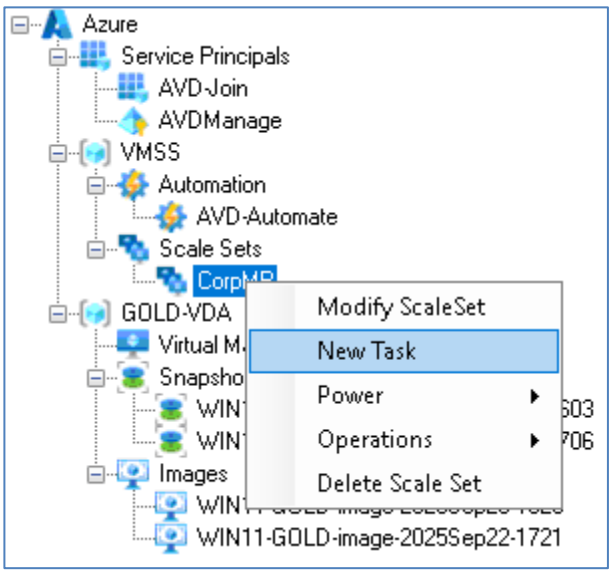
Parameters:

Target Scale Set Name: FlexS

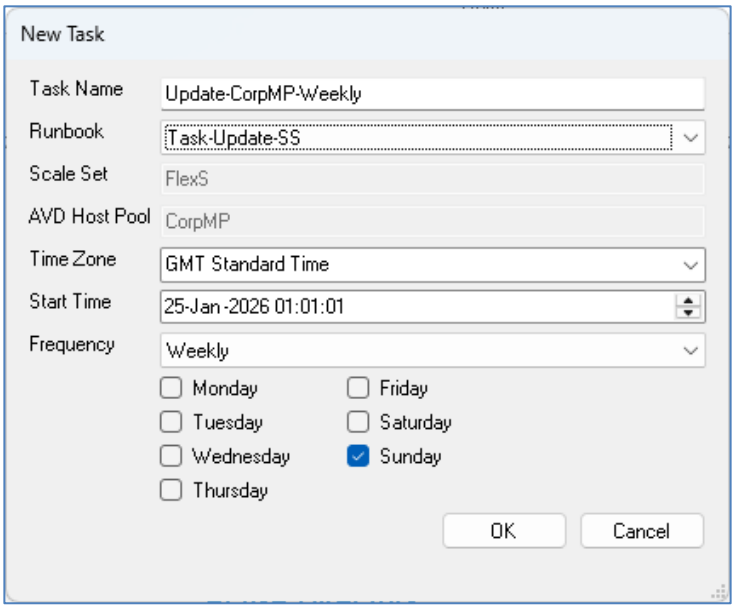
Target AVD Host Pool: CorpMP

Schedule: Weekly. Every Sunday at 1am

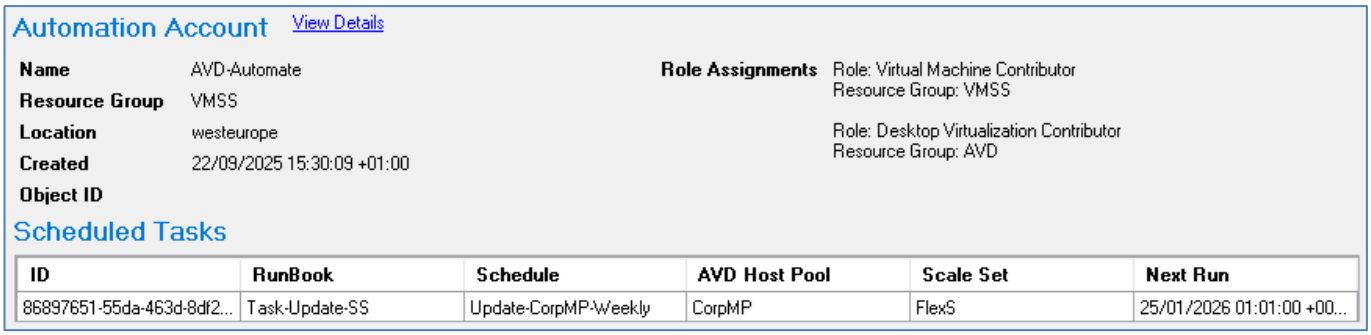
Right Click a Scale Set and select New Task.



- Enter a Task Name
- Select a Runbook
- The Scale Set and AVD Host Pool values are pre-filled.
- Adjust the Time Zone if necessary
- Specify a Start Time and Frequency.
- Click OK



The new task is visible when clicking on the AVD-Automate node.



You can right click the task to delete it or view further schedule details.

If scheduling multiple tasks, allow sufficient time between tasks for the first task to complete before the second task executes.

Managed Identity logon issues can occur if the jobs overlap.

9. AVDManage Plus

AVDManage Plus has the same configuration requirements as AVDManage Free as described in Getting Started.

9.1 Azure Permissions

As noted in Resource Groups & Roles, the **AVD-Admins** group requires the ***Compute Gallery Artifacts Publisher*** role to the Virtual Machines Resource Group.

Compute Galleries, Image Definitions and Image versions are located in the Virtual Machines Resource Group.

9.2 Licensing

AVDManage Plus is enabled with a 30-day evaluation license or a full annual license. (Fixed annual fee. Not based on number of users or devices.)

To request a 30-day evaluation license, email info@chawn.com stating:

- Contact Name
- Contact Details
- Company Name

You will receive a 30 days evaluation license file and registration code.

The license file may then be copied to the installation folder (C:\Program Files\Chawn\AVDManage).

Users will be prompted for a registration code at the next launch.

9.3 Additional Features

AVDManage Plus leverages Azure Compute Galleries to provide the following features:

- Create Virtual Machines & Scale Sets from Compute Galleries
- Deploy Specialized Windows Images
- Create Trusted Launch Virtual Machines & Scale Sets
- AVDTurbo (for Specialized Virtual Machines & Scale Sets)

> Generalizing or deprovisioning a VM is not necessary for creating an image in an Azure Compute Gallery unless you specifically want to create an image that has no machine specific information, like user accounts. Generalizing is still required when creating a managed image outside of a gallery.
>
> Generalizing removes machine specific information so the image can be used to create multiple VMs. Once the VM has been generalized or deprovisioned, you need to let the platform know so that the boot sequence can be set correctly.

Deprovision or generalize a VM before creating an image - Azure Virtual Machines | Microsoft Learn

> **Important**
>
> When you create a new VM from a specialized image, the new VM retains the computer name of the original VM. Other computer-specific information, like the CMID, is also kept. This duplicate information can cause issues. When copying a VM, be aware of what types of computer-specific information your applications rely on.

Create a VM from a specialized image version - Azure Virtual Machines | Microsoft Learn

There are two operating system states supported by Azure Compute Gallery. Typically images require that the VM used to create the image has been generalized before taking the image. Generalizing is a process that removes machine and user specific information from the VM. For Linux, you can use waagent `-deprovision` or `-deprovision+user` parameters. For Windows, the Sysprep tool is used.

Specialized VMs haven't been through a process to remove machine specific information and accounts. Also, VMs created from specialized images don't have an `osProfile` associated with them. This means that specialized images will have some limitations in addition to some benefits.

- VMs and scale sets created from specialized images can be up and running quicker. Because they're created from a source that has already been through first boot, VMs created from these images boot faster.
- Accounts that could be used to log into the VM can also be used on any VM created using the specialized image that is created from that VM.
- VMs will have the **Computer name** of the VM the image was taken from. You should change the computer name to avoid collisions.
- The `osProfile` is how some sensitive information is passed to the VM, using `secrets`. This may cause issues using KeyVault, WinRM and other functionality that uses `secrets` in the `osProfile`. In some cases, you can use managed service identities (MSI) to work around these limitations.

Generalized and Specialized Images - Azure Virtual Machines | Microsoft Learn

When deploying specialized images, **AVDTurbo**;

- Renames the Computer to match the VM Name
- Optionally joins an Active Directory Domain or Entra ID
- Optionally joins an Azure Virtual Desktop Host Pool

9.4 Install AVDManage

Run the following command to install AVDManage with a Registration code.

msiexec /i AVDManage.msi COMPANYNAME="Company Name" SERIALBODYTEXT="1234567890" /qb

This prevents users being prompted to enter licensing information.

Copy the license file to **C:\Program Files\Chawn\AVDManage**

9.5 Overview

AVDManage *Free* can deploy VMs and Scale Sets from Managed Images only. Managed Images must be Generalized. Managed Images do not support:

- Specialized Images
- TrustedLaunch security

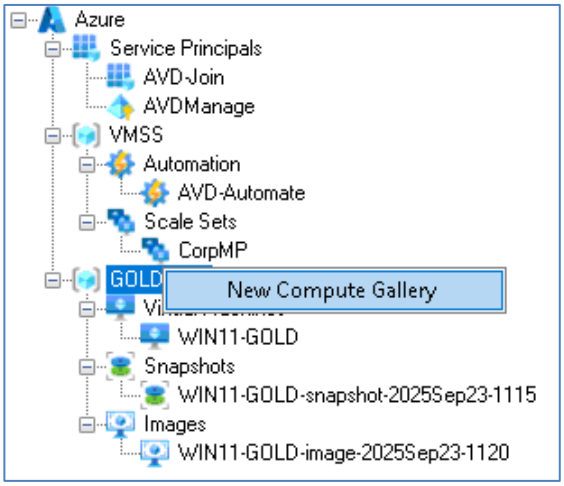
AVDManage *Plus* can deploy VMs and Scale Sets from Managed Images and Azure Compute Galleries. Azure Compute Galleries support Generalized and Specialized Images and TrustedLaunch security.

1 - Create an Azure Compute Gallery		
2 - Create an Image Definition (Generalized or Specialized)		
3- Create a Master VM		
	Generalized	**Specialized**
4	Shutdown the VM and take a Snapshot	Run AVD-Seal-Special.ps1. **VM will shutdown**
5	Power on the VM and run AVD-Seal.ps1 or Sysprep. **VM will shutdown**	Snapshot the VM
6	Create a Generalized Compute Gallery Image Version	Create a Specialized Compute Gallery Image Version
7 - Create a Virtual Machine Scale Set using the Image Version		

9.6 Create an Azure Compute Gallery

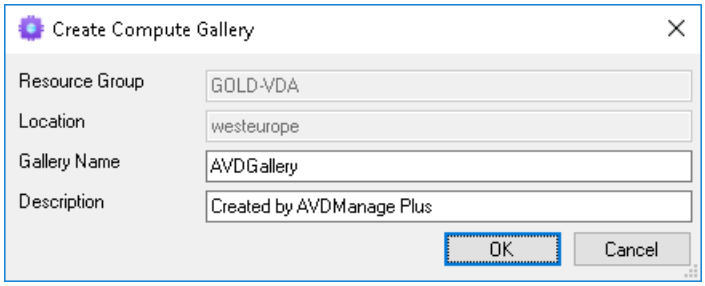
The user performing these tasks should be a member of **AVD-Admins**.

Right click the Master Resource Group and select New Compute Gallery.



Name the Gallery and optionally provide a description.

Click OK.



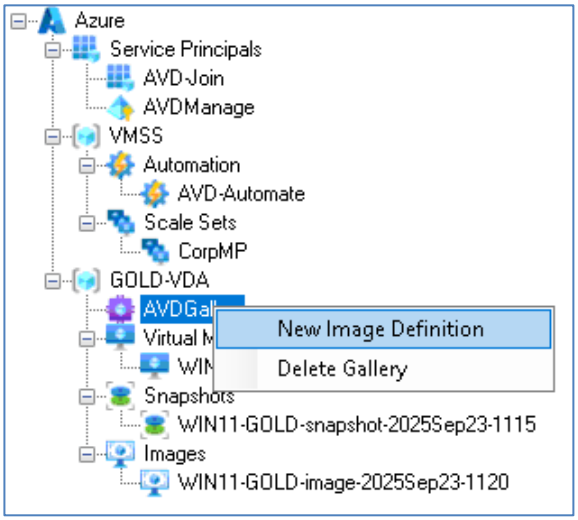
Estimated time to complete: 60 seconds

9.7 Create an Image Definition

The user performing these tasks should be a member of **AVD-Admins**.

9.7.1 Specialized Image Definition

Right Click the Compute Gallery and select New Image Definition.

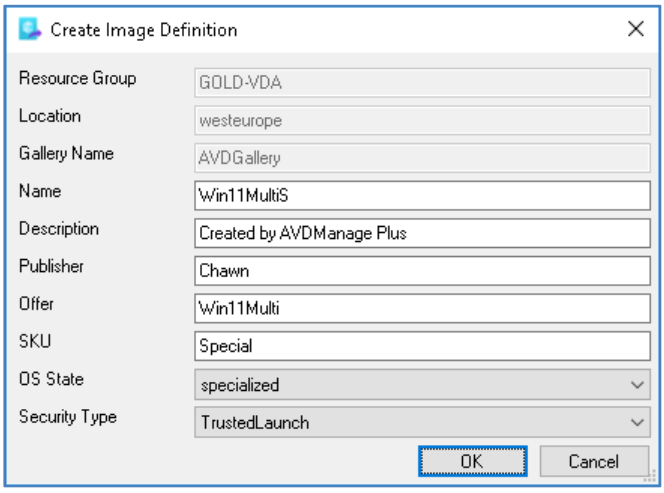


Enter a name and optionally provide a description.

Enter a Publisher, Offer and SKU.

Specify the intended OS State.

Specify the Security Type for VMs deployed from this Image Definition.

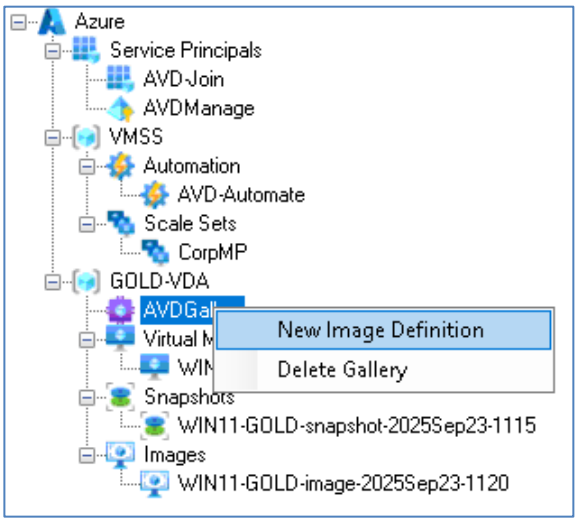


When creating Image Definitions, the Publisher, Offer and SKU combination cannot be the same as any other Image Definition in the Gallery.

Estimated time to complete: 60 seconds

9.7.2 Generalized Image Definition

Right Click the Compute Gallery and select New Image Definition.

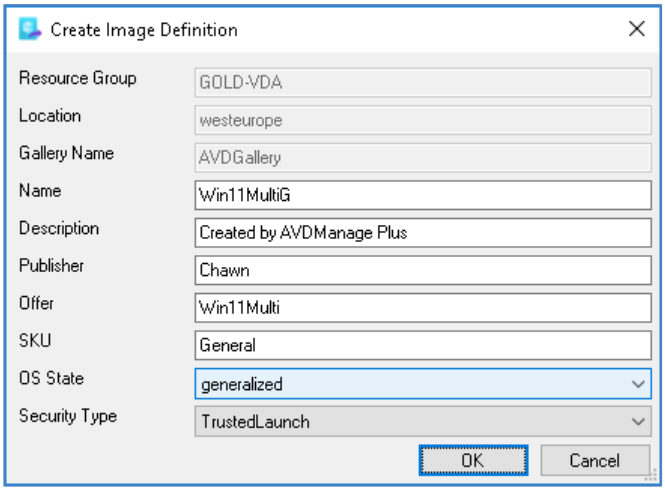


Enter a name and optionally provide a description.

Enter a Publisher, Offer and SKU.

Specify the intended OS State.

Specify the Security Type for VMs deployed from this Image Definition.



When creating Image Definitions, the Publisher, Offer and SKU combination cannot be the same as any other Image Definition in the Gallery.

Estimated time to complete: 60 seconds

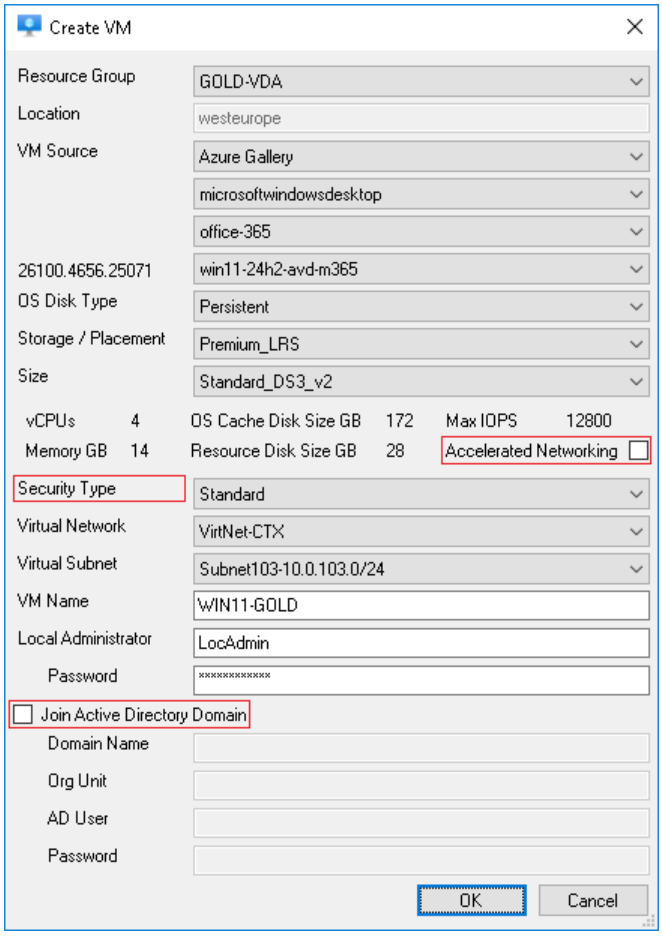
9.8 Create (Master) VM

The user performing these tasks should be a member of **AVD-Admins**.

Recommendations:

- Record the local administrator password. It will be required when recreating the Master VM from snapshots and if deploying Specialized images.
- Use the same VM Size that will be used by the Virtual Machine Scale Set.
- The OS Disk Type must be Persistent.
- Do **not** join an Active Directory Domain
- Do **not** enable Accelerated Networking. This can be enabled when creating a Virtual Machine Scale Set. If Accelerated Networking is enabled in the Master VM, all Scale Set VM instances will have a ghost Mellanox network adapter.
- Don't enable TrustedLaunch security.
    - A Standard security VM may be added to a Compute Gallery Image Definition with Standard or TrustedLaunch security however a TrustedLaunch security VM cannot be added to Compute Gallery Image Definition with Standard security
    - TrustedLaunch can be enabled when creating a Virtual Machine Scale Set
    - Windows 11 24H2 now enables Bitlocker by default. This is not required in a Master VM and prevents Sysprep from completing

Create a VM from the Azure Gallery.



Estimated time to complete: 6 mins

Modify the VM as described in Modify the Master VM

Depending on your imaging and deployment strategy, either Generalize the Master VM by running Sysprep (AVD-Seal) or shut down the Master VM for a specialized image (AVD-Seal-Special).

It is important that the Windows Azure Agent is neutralised when creating a specialized image. A new Virtual Machine configuration file is created at the next startup which includes the Virtual Machine name. **AVDTurbo** uses the latest configuration file to set the ComputerName correctly.

Whether generalizing or specializing the Master VM, AVD-Seal.ps1 and AVD-Seal-Special.ps1 contain the following commands to remove previous Azure Guest Agent configuration files.

```
# Neutralise the WindowsAzure Agent
Get-Service -Name RDAgent | stop-service
Get-Service -Name WindowsAzureGuestAgent | stop-service
Get-ChildItem -Path C:\WindowsAzure\config -Filter *.*  | Remove-Item -Force -Recurse
Get-ChildItem -Path C:\WindowsAzure\logs -Filter *.*  | Remove-Item -Force -Recurse
$certs=Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.Subject -match 'DC=Windows Azure CRP Certificate Generator' };foreach ($c in $certs) {Remove-Item $c.PSPath -Force}
$certs=Get-ChildItem "Cert:\LocalMachine\Windows Azure Environment";foreach ($c in $certs) {Remove-Item $c.PSPath -Force}
$certs=Get-ChildItem "Cert:\LocalMachine\Remote Desktop";foreach ($c in $certs) {Remove-Item $c.PSPath -Force}
$store=Get-Item "Cert:\LocalMachine\Runtime_Transport_Store_*" | select name
$store='Cert:\LocalMachine\'+ $store.Name
$certs=Get-ChildItem $store;foreach ($c in $certs) {Remove-Item $c.PSPath -Force}
Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\GuestAgent" -Recurse -Force -ErrorAction SilentlyContinue
Remove-Item -Path "HKLM:SOFTWARE\Microsoft\Windows Azure\HandlerState" -Recurse -Force -ErrorAction SilentlyContinue
Remove-Item -Path "HKLM:SOFTWARE\Microsoft\Windows Azure\ScriptHandler" -Recurse -Force -ErrorAction SilentlyContinue
```

Generalized Image	Specialized Image
Shutdown the VM and **take a Snapshot**	Run AVD-Seal-Special.ps1. **VM will shutdown**
Power on the VM and run AVD-Seal.ps1 or Sysprep. **VM will shutdown**	**Take a Snapshot**
Create a Generalized Compute Gallery Image Version	Create a Specialized Compute Gallery Image Version

9.9 Create a Compute Gallery Image Version

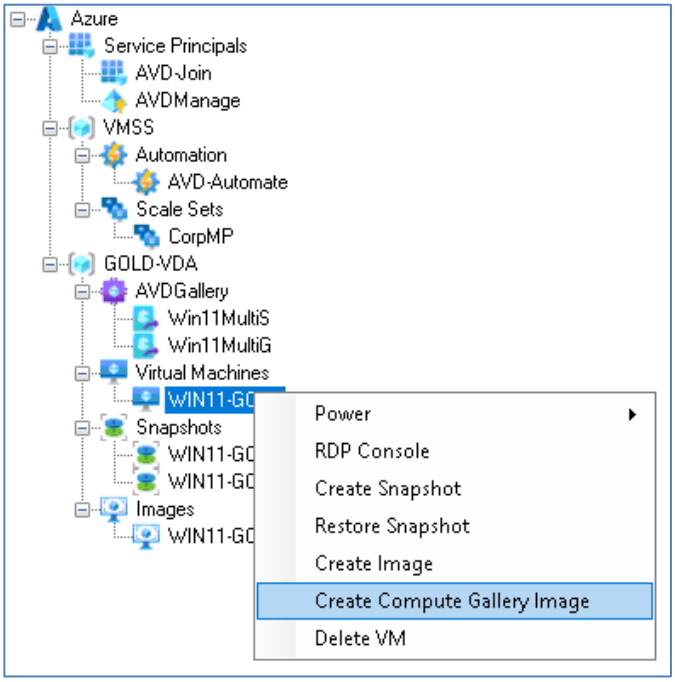
The user performing these tasks should be a member of **AVD-Admins**.

Before creating an Image Version or deleting the Master VM, ensure that you have taken a snapshot.

9.9.1 Specialized Image

Before creating the Image Version, ensure that you have run AVD-Seal-Special.ps1 and the VM has shutdown.

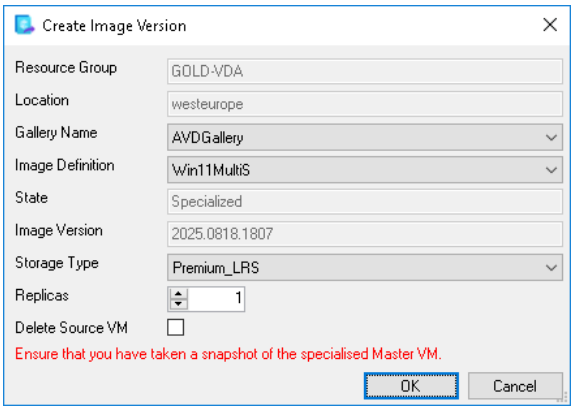
Right click the Master VM and select Create Compute Gallery Image.



Select the Compute Gallery.

Select the Image Definition. The image definition will indicate if it is intended for Specialized or Generalized deployments.

The Name is automatically created based on **yyyy.MMdd.HHmm**.



Select the Storage Type.

Microsoft recommends that you have 1 replica for every 20 VMs that you intend to deploy.
E.g. 100 VMs would require 5 replicas.

Choose whether to delete the Source VM.

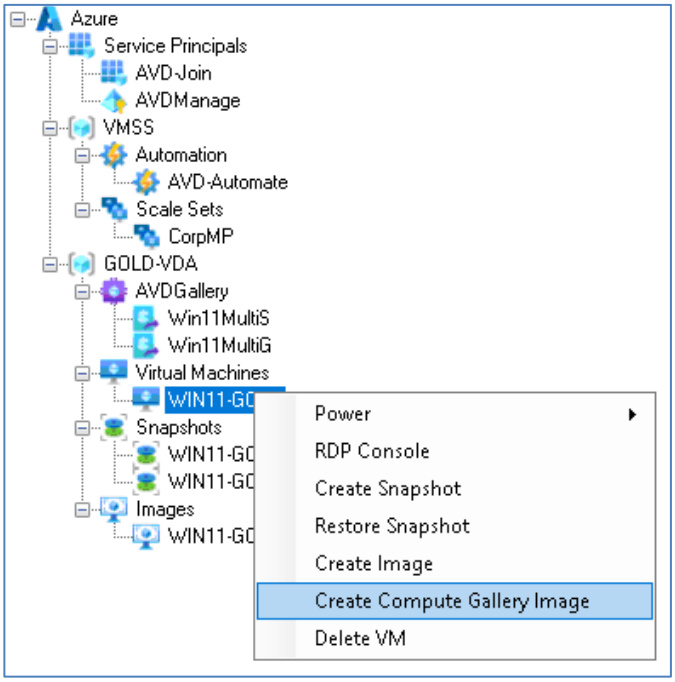
Click OK.

Estimated time to complete: 15 Minutes (Depending on the number of replicas)

9.9.2 Generalized Image

Before creating the Image Version, ensure that you have taken a snapshot, ensure that you have Generalized the Master VM by running Sysprep or AVD-Seal.ps1 and the VM has shutdown.

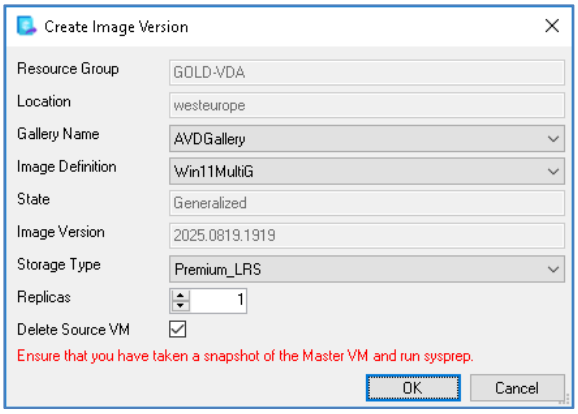
Right click the Master VM and select Create Compute Gallery Image.



Select the Compute Gallery.

Select the Image Definition. The image definition will indicate if it is intended for Specialized or Generalized deployments.

The Name is automatically created based on **yyyy.MMdd.HHmm**.



Select the Storage Type.

Microsoft recommends that you have 1 replica for every 20 VMs that you intend to deploy.

E.g. 100 VMs would require 5 replicas.

Choose whether to delete the Source VM.

Click OK.

When creating a Generalized Image, the Master VM is marked as ‘Generalized’ and therefore cannot be started afterwards.

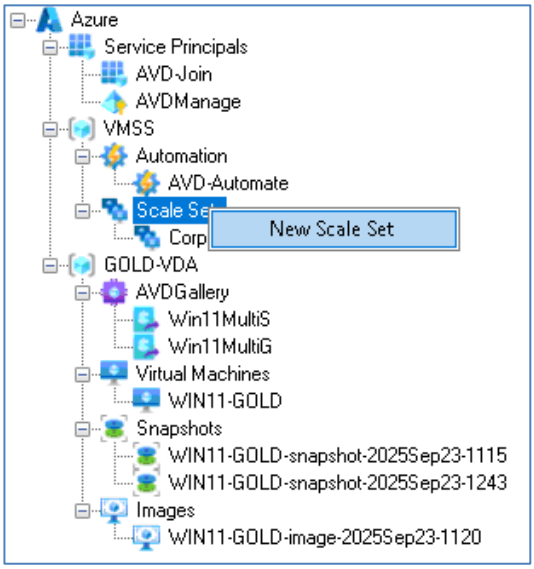
Estimated time to complete: 15 Minutes (Depending on the number of replicas)

9.10 Create a Virtual Machine Scale Set

The user performing these tasks should be a member of **AVD-Admins**.

9.10.1 Specialized Image

Right click the Scale Sets node and select New Scale Set.



Select Compute Gallery as the source.

Select your Azure Compute Gallery, Image Definition, and Image Version.

Select OS Disk Type, Storage / Placement and VM Size.

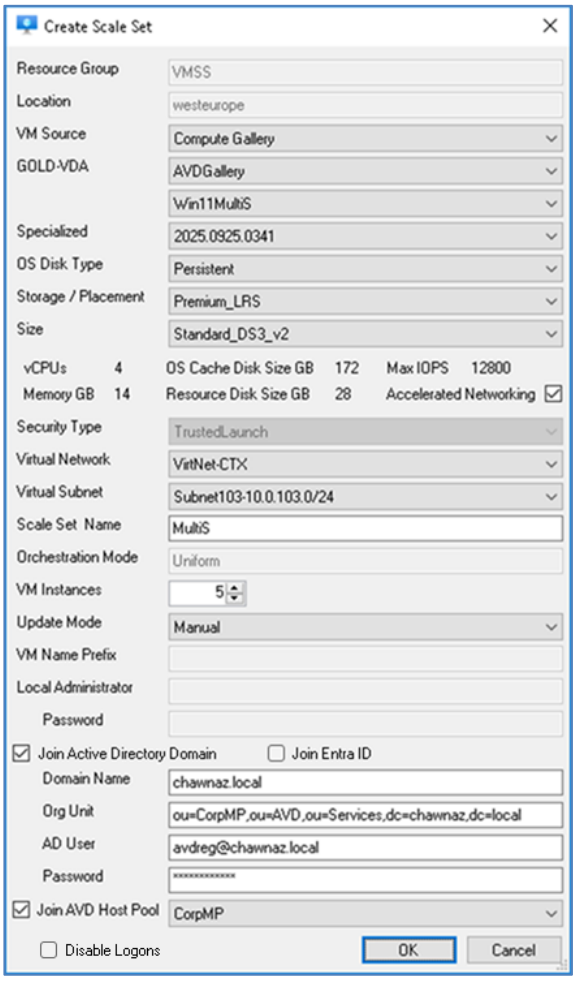
Security Type is inherited from the Image Definition.

Select the number of required VMs.

Update Mode is set to Manual by default but may be changed to Automatic.

VM Name Prefix is not configurable for a Specialized Image. The VM Name Prefix is based on the Scale Set name. The Scale Set name is limited to 11 characters.

For more available VM Names, use a shorter Scale Set Name.

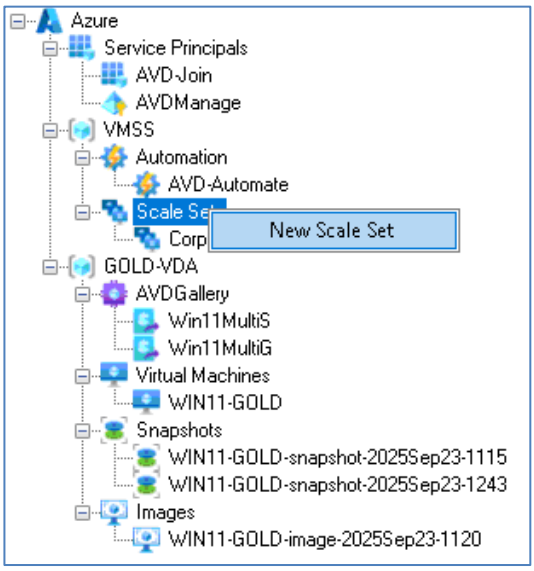


Estimated time to complete: ~5 Minutes (5 VM instances)

Don't forget to configure Windows Licensing

9.10.2 Generalized Image

Right click the Scale Sets node and select New Scale Set.



Select Compute Gallery as the source.

Select your Azure Compute Gallery, Image Definition, and Image Version.

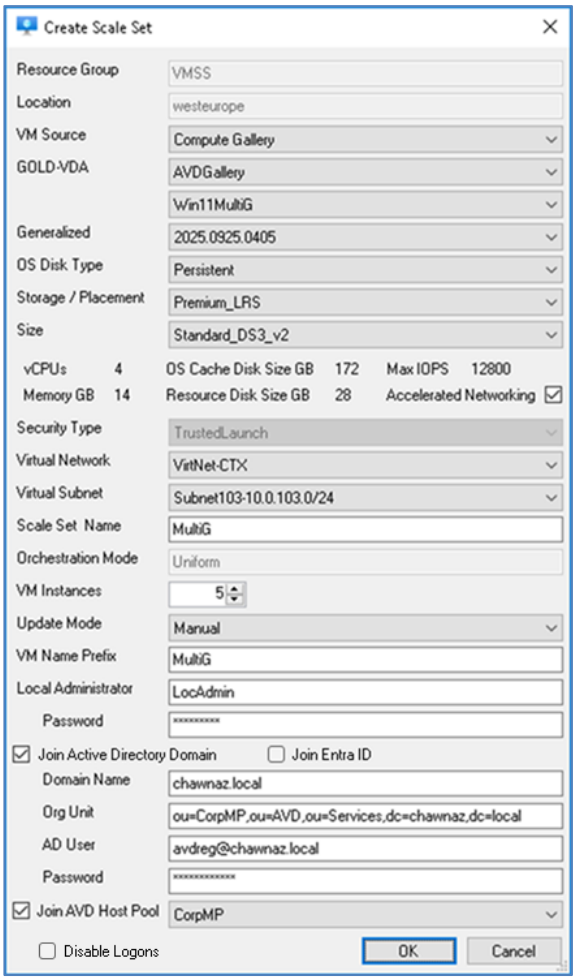
Select OS Disk Type, Storage / Placement and VM Size.

Security Type is inherited from the Image Definition.

Select the number of required VMs.

Update Mode is set to Manual by default but may be changed to Automatic.

VM Name Prefix is limited to 9 characters.



Estimated time to complete: ~7 Minutes (5 VM instances)

Don't forget to configure Windows Licensing

9.11 Image Updates

The user performing these tasks should be a member of **AVD-Admins**.

Images require updating at least once per month.

Recreate the Master VM as described in Recreate the Master VM.

Modify the Master VM.

Updates may include:

- Windows Updates
- Application Updates
- Add / Remove Applications
- Fixes to discovered issues

Depending on your image strategy

Generalized Image	Specialized Image
Shutdown the VM and **take a Snapshot**	Run AVD-Seal-Special.ps1. **VM will shutdown**
Power on the VM and run AVD-Seal.ps1 or Sysprep. **VM will shutdown**	**Take a Snapshot**
Create a Generalized Compute Gallery Image Version	Create a Specialized Compute Gallery Image Version

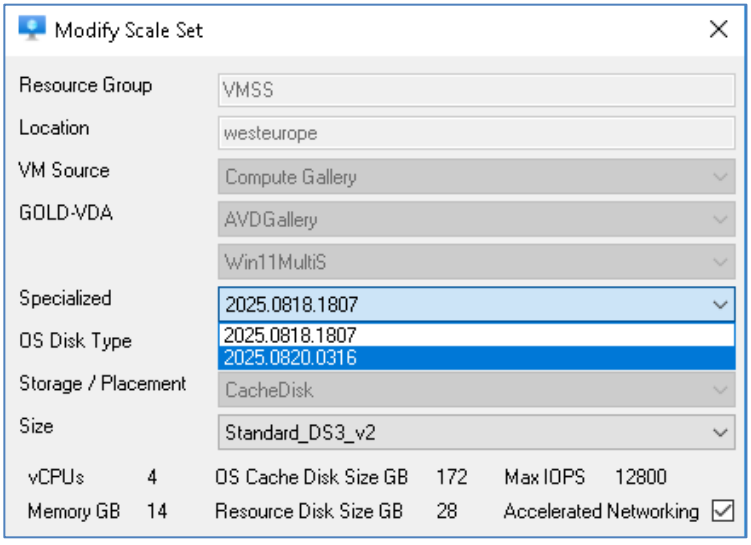
Update a Scale Set

Right Click a Scale Set and select **Modify Scale Set**.

The new Image Version may be selected to update the Scale Set.

The VM Size, Accelerated Networking and VM instances may be modified if required.

The password for the Active Directory user may be updated.



The Current status of the VM instances will change from True to False. They are still running the old image, and do not have the latest Scale Set configuration.

A specific VM instance may be updated by right clicking the VM and selecting update.

The VM will shut down and be unavailable while updating.

All VM instances in the Scale Set may be updated by right clicking the Scale Set and selecting Update All.

All VMs will shut down and be unavailable while updating.

When updating Ephemeral and Persistent Virtual Machine instances, they will retain their VMName, VM Instance name, Windows ComputerName and Active Directory ComputerName.

Immediate updating of VMs is unlikely to be appropriate if the VMs are hosting AVD sessions.

It is recommended that Scale Set updates are scheduled during a planned maintenance window using Azure Automation and **AVD-Automate**.

10. AVD-Prep - Pre-Stage the Remote Desktop Infrastructure and Boot Loader Agents

A typical deployment time for AVD-Turbo is around 1 minute 15 seconds.

This includes 40 seconds while installing the Remote Desktop Infrastructure and Boot Loader Agents.

By pre-staging the Agents on the Master VM, the deployment time can be reduced accordingly.

The Agents may be pre-staged on a Generalized or Specialized Image.

Re-Create the Master VM from a snapshot.

Logon and download AVD-Prep.ps1

Open Powershell as Administrator and run AVD-Prep.ps1.

The script will:

- Download the Remote Desktop Infrastructure and Boot Agents to C:\Source
- Install the Remote Desktop Infrastructure Agent with an **INVALIDTOKEN**
- Install the Remote Desktop Boot Loader Agent
- Stop and Disable the Remote Desktop Boot Loader Agent Service
- Delete HKLM:\SOFTWARE\Microsoft\RDInfraAgent
- Create HKLM:\SOFTWARE\Microsoft\RDInfraAgent\RegistrationToken ="AVDTurbo"
- Create HKLM:\SOFTWARE\Microsoft\RDInfraAgent\HostPoolType = "Default"
- Create HKLM:\SOFTWARE\Microsoft\RDInfraAgent\IsRegistered= 0

Complete the Image update process.

	Generalized	**Specialized**
	Shutdown the VM and take a Snapshot	Run AVD-Seal-Special.ps1. **VM will shutdown**
	Power on the VM and run AVD-Seal.ps1 or Sysprep. **VM will shutdown**	Snapshot the VM
	Create a Generalized Compute Gallery Image Version	Create a Specialized Compute Gallery Image Version

When **AVD-Turbo** runs, it checks for HKLM:\SOFTWARE\Microsoft\RDInfraAgent\RegistrationToken ="AVDTurbo".

If it is present, the script immediately passes the WVDRegistration token into the VM's registry and starts the Remote Desktop Boot Loader Agent.

The WinSXS Network and Geneva Agents will then be downloaded and installed.

If pre-staging the Remote Desktop Infrastructure and Boot Loader Agents ensure that you run AVD-Prep.ps1 during every update so that the latest versions of the Agents are present in the Master Image.

11. Reference

11.1 Virtual Machines

Only Microsoft Windows Virtual Machines may be created.

Virtual Machines may be created from:

- Azure Gallery Images
- Compute Gallery Images (AVDManage Plus)
- Managed Images
- Snapshots

11.1.1 Configuration

All Virtual Machines have the following configuration when deployed from a snapshot or Managed Image. When deploying from a Compute Gallery Image, SecurityType may be set to TrustedLaunch.

PublicIP	None
BootDiagnostics.Enabled	False
HyperVGeneration	V2
NetworkSecurityGroups	None
ProvisionVMAgent	True
PatchMode	AutomaticByOS
SecurityType	Standard

The following events may be logged due to the SecurityType as vTPM and SecureBoot are not enabled. These events may be ignored.

Log: System	Source: TPM-WMI	Event ID: 1796
The Secure Boot update failed to update a Secure Boot variable with error Secure Boot is not enabled on this machine.. For more information, please see https://go.microsoft.com/fwlink/?linkid=2169931		

Log: System	Source: Wininit	Event ID: 15
Credential Guard and/or VBS Key Isolation are configured but the secure kernel is not running; continuing without them.		

11.1.2 OS Disk Type: Persistent vs Ephemeral

Most VMs will be created with a Persistent disk however VMs with Ephemeral disks may be created for short term testing.

VMs with Ephemeral disks may not be used to create snapshots or images.

11.1.3 Menu Actions

Power - Start VM	Starts the VM. (Persistent only)
Power - Restart VM	Restarts the VM.
Power - Stop VM	Stops and De-Allocates the VM. (Persistent only)
RDP Console	Attempts to connect via RDP using the VM IP Address.
Create Snapshot	Creates a Snapshot. The VM must be in a deallocated state. (Persistent only)
Restore Snapshot	Reverts the VM to the previous Snapshot State. The VM must be in a deallocated state. (Persistent only)
Create Image	Creates an Image of the VM. The VM should have been sysprepped. The VM must be in a stopped or deallocated state. (Persistent only)
Create Compute Gallery Image	**AVDManage Plus** Creates a Compute Gallery Image Version. The VM may be generalized or specialized. The VM must be in a stopped or deallocated state. (Persistent only)
Delete VM	Deletes the VM, Disk and NIC

11.2 Virtual Machine Scale Sets

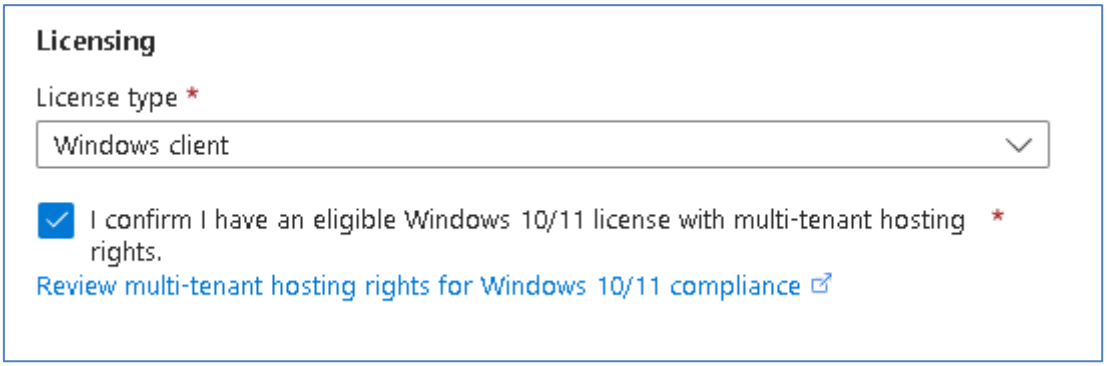
Only Microsoft Windows Virtual Machines can be created.

Virtual Machine Scale Sets may be created from:

- Azure Gallery Images
- Compute Gallery Images (AVDManage Plus)
- Managed Images

11.2.1 Windows Licensing

After creating a Scale Set, if you have Eligible licenses to use Azure Virtual Desktop then you can modify the properties of the Scale Set in the Azure portal on the **Operating System** blade to reduce the price of VM instances.



11.2.2 Orchestration Mode

You can choose between Uniform or Flexible modes.

Uniform: Single Virtual Machine Scale Set Azure Object

Flexible: Virtual Machine Scale Set Azure Object and Virtual Machine, disk and network card objects for each Virtual Machine

Uniform vs Flexible

Orchestration modes for Virtual Machine Scale Sets in Azure - Azure Virtual Machine Scale Sets | Microsoft Learn

11.2.3 Update Mode

You can choose between Manual and Automatic modes.

Manual: You choose when to update the scale set instances. Nothing happens automatically to the existing virtual machines when changes occur to the scale set model. New instances added to the scale set use the most update-to-date model available.

Automatic: The scale set makes no guarantees about the order of virtual machines being brought down. The scale set might take down all virtual machines at the same time to perform upgrades

Manual update is preferred for Scale Sets hosting AVD sessions. **AVD-Automate** can be used to update VM instances during planned maintenance windows.

Rolling update mode is not supported by AVDManage.

Upgrade policies for Virtual Machine Scale Sets (preview) - Azure Virtual Machine Scale Sets | Microsoft Learn

11.2.4 Load Balancing

Virtual Machine Scale Sets are frequently created with an Azure Load Balancer to spread traffic across multiple VMs, such as a web server farm.

AVDManage does not create any Load Balancers when creating Virtual Machine Scale Sets however you are free to configure your own Load Balancer in the Azure portal after VMSS creation.

11.2.5 OS Disk Type: Persistent vs Ephemeral

Ephemeral OS disks are created on the local virtual machine (VM) storage and not saved to the remote Azure Storage. Ephemeral OS disks work well for stateless workloads, where applications are tolerant of individual VM failures but are more affected by VM deployment time or reimaging of individual VM instances. With Ephemeral OS disk, you get lower read/write latency to the OS disk and faster VM reimage.

The key features of ephemeral disks are:

- Ideal for stateless applications.
- Supported by Marketplace, custom images, and by Azure Compute Gallery (formerly known as Shared Image Gallery).
- Ability to fast reset or reimage VMs and scale set instances to the original boot state.

- Lower latency, similar to a temporary disk.
- Ephemeral OS disks are free, you incur no storage cost for OS disks.
- Available in all Azure regions.

	Persistent	Ephemeral
Size	All VM Sizes	Restricted by Cachedisk or ResourceDisk size
Persistence	OS disk data written to OS disk are stored in Azure Storage	Data written to OS disk is stored on local VM storage and isn't persisted to Azure Storage.
Stop/Start	Supported	Not supported. Always running. Cannot be deallocated.
ReDeploy	OS Disk is preserved	VM is re-deployed
Disk Storage Costs	Yes	No

As stated above, Ephemeral disks are ‘Ideal for stateless applications’.

However as AVDManage can redeploy Persistent and Ephemeral VM instances both Persistent and Ephemeral disks can be considered as ‘stateless’.

VMs with Ephemeral disks can be slightly more complicated to manage.

Imagine you have a Scale Set with 10 VM instances all joined to an AVD Host Pool.

The Session Hosts are only required between 6am and 9pm therefore you can reduce PAYG costs by powering off the VM instances at 9pm and powering on at 5.30am.

This is not an issue for Persistent VMs. They can be powered off and will start with the same machine identity and ComputerName at 5.30am.

Ephemeral VMs cannot be powered off so you would have to delete all VM instances at 9pm and recreate them at 5.30pm.

In both cases the AVD Host Pool would be operational however the Ephemeral VMs will have new machine identities and OS ComputerNames.

If you wish to run Ephemeral VMs 24h/24h, they will maintain their identities when updating, re-imaging and re-deploying.

11.2.6 Menu Actions

New Scale Set	Create a new Scale Set
Power – Start All	Start all VM instances (Persistent only)
Power – Restart All	Restart all VM instances
Power - Stop All	Stop all VM instances (Persistent only)
Modify Scale Set	Modify and update the Scale Set configuration. • VMImageSource • VMSize • VMInstances • AVD-Turbo
New Task	Create and schedule a new automation task
Operations – Update All	Update all VM instances with the latest Scale Set configuration If a new image is available, all VM instances will rebuild
Operations – Re-Deploy All	Deploy all VM instances to a new Azure host with the existing VM instance configuration
Operations – Re-Image All	Rebuild all VM instances with the existing VM Instance configuration
AVD – Enable Logons	Disables logons on all VM instances
AVD – Disable Logons	Enables logons on all VM instances
AVD – Reset Agent	If the session host 'Needs Assistance', you can reset the AVD agents to resolve the issue.
Delete Scale Set	Delete the Scale Set and all VM instances

When deleting a Scale Set or Scale Set VM instances, the Azure Virtual Session Desktop Session Host instance is also deleted.

If **DeleteAD** is enabled and the **ActiveDirectory** Powershell module is installed, the Active Directory Computer object will also be deleted.

Azure Virtual Desktop – New Token button
Clicking New Token will generate a new WVD token which is used by AVD-Turbo to join new Session Hosts to the Host Pool.
When deploying multiple VM instances, it is recommended to generate a new WVD token. If AVD-Turbo is running at the same time on multiple machines, it is possible that 2 or more machines may generate a new token at the same time. The last token generated is the valid token so the joining the Host Pool may fail for one or more instances.
If a valid token exists and is valid for more than one hour, AVD-Turbo will use the existing token.

11.3 Service Principals

AVD-Join is an Entra Service Principal. It can be viewed as an App Registration and Enterprise Application in the Azure portal.

AVDManage is a User-Assigned Managed Identity. It is assigned to all Scales Sets configured to join an AVD Host Pool. A Federated Credential is created on the **AVD-Join** Application Registration creating an Application Trust with **AVDManage**.

When creating a Scale Set, **AVD-Turbo** can be configured to join an Active Directory Domain or Entra ID, and an AVD Host Pool.

The following parameters are included:

AVD-Turbo
• AD Domain • AD Organisational Unit • AD Admin User • AD Admin Password • AVD Host Pool to join • EntraJoin • Entra Tenant ID • Secretless Authentication

All parameters are created in ProtectedSettings. Protected settings are encrypted through a key known only to Azure and the VM.

After a Generalized VM has started up, **AVD-Turbo** will download
https://raw.githubusercontent.com/ChawnLimited/AVDManage/refs/heads/main/AVD-Turbo5.ps1

- Joins Active Directory or Entra ID
- Checks that the Microsoft RDS Infrastructure Agent is not already installed
- Downloads the Remote Desktop Services Infrastructure Agent & Boot Loader
- Authenticates to Azure as AVD-Join
- Removes the existing VM from the AVDHostPool (if it exists)
- Generates a new AVD Registration Token if it has expired
- Joins the AVDHostPool using the AVD Token
- Waits for the Windows SXS Network and Geneva Health agents to install
- Disconnects from Azure
- Reboots

AVD-Turbo5.log and installation log files are located in
C:\Packages\Plugins\Microsoft.Compute.CustomScriptExtension\x.x.x\Downloads\x

After a Specialized VM has started up, **AVD-Turbo** will download
https://raw.githubusercontent.com/ChawnLimited/AVDManage/refs/heads/main/AVD-Turbo5.ps1

- Renames the Computer
- Joins Active Directory or Entra ID
- Checks that the Microsoft RDS Infrastructure Agent is not already installed
- Downloads the Remote Desktop Services Infrastructure Agent & Boot Loader

- Authenticates to Azure as AVD-Join
- Removes the existing VM from the AVDHostPool (if it exists)
- Generates a new AVD Registration Token if it has expired
- Joins the AVDHostPool using the AVD Token
- Waits for the Windows SXS Network and Geneva Health agents to install
- Disconnects from Azure
- Reboots

If the Scale Set is configured to join Active Directory, **AVD-EntraReg.ps1** is also downloaded. **AVD-Turbo** creates a Scheduled Task that runs after startup to perform an Entra Hybrid Join. The output log file is named **AVD-EntraReg.log**.

If the Scale Set is configured to join Entra ID, **AVD-Turbo** will perform an Entra Direct Join. The output log file is named **AVD-EntraJoin.log**.

All log files and installation log files are located in
C:\Packages\Plugins\Microsoft.Compute.CustomScriptExtension\x.x.x\Downloads\x

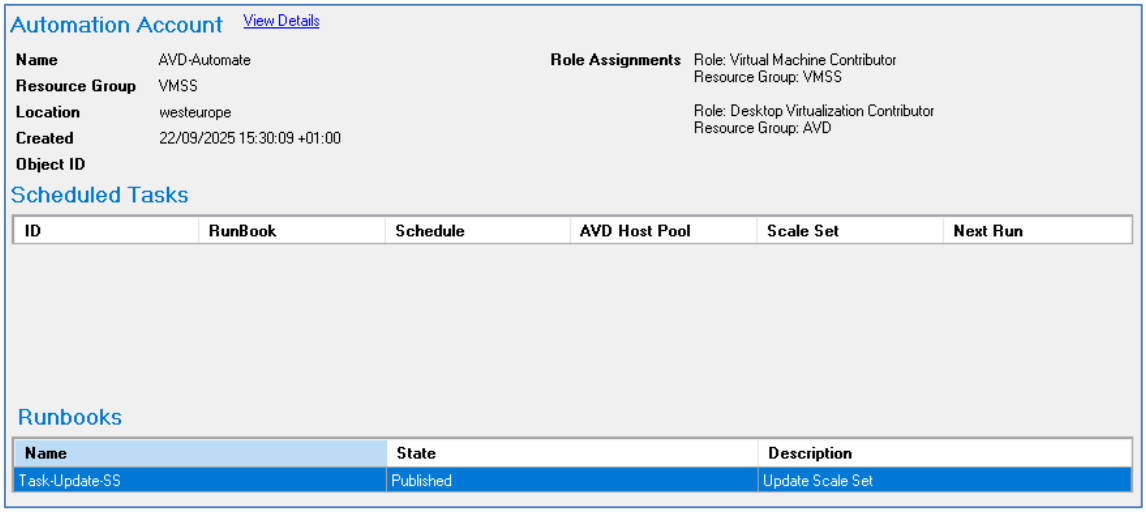
CustomScriptExtension logs are located in

C:\WindowsAzure\Logs\Plugins\Microsoft.Compute.CustomScriptExtension\x.x.x

11.3.1 Menu Actions

New Application Registration	Creates a new Entra Application Registration named **AVD-Join** and assigns the ***Virtualization Host Pool Contributor*** role to the Resource Group containing AVD Host Pools Menu action is disabled after creation
New Managed Identity	Creates a new User-Assigned Managed Identity named **AVDManage** in the Virtual Machine Scale Set Resource Group and creates a Federated Credential on the **AVD-Join** Application Registration creating an Application Trust with **AVDManage**. Menu action is disabled after creation
Delete AVD-Join	Delete AVD-Join and removes the Role assignments.
Delete AVDManage	Deletes AVDManage and removes the Federated Credential from the **AVD-Join** Application Registration.

11.4 AVD-Automate Automation Account



AVD-Automate is an Automation Account and can invoke Automation Runbooks at scheduled times.

An Automation Runbook is a PowerShell script that is executed with parameters

AVD-Automate is a Managed Identity. A managed identity from Microsoft Entra ID allows your runbook to easily access other Microsoft Entra protected resources. The identity is managed by the Azure platform and doesn't require you to provision or rotate any secrets.

AVD-Automate is assigned Roles that allow AVD-Automate to perform tasks against Virtual Machine Scale Sets and AVD Host Pools such as updating, restarting, power on / off.

Scripts are located in %LOCALAPPDATA%\Chawn\AVDManage\Scripts\AVD-Automate

Scripts are available to download from https://github.com/ChawnLimited/AVDManage

Tasks may be scheduled to run One Time, Daily, or Weekly on specific days.

11.4.1 Menu Actions

New Automation Account	Creates a new Automation Account named AVD-Automate and assigns the Virtual Machine Contributor role to the Resource Group containing Virtual Machine Scale Sets, and the Desktop Virtualization Contributor role to the Resource Group containing AVD Host Pools Menu action is disabled after creation
Delete Automation Account	Deletes the AVD-Automate Automation Account and removes the Role assignments

11.5 Snapshots

Snapshots will accumulate over time and incur storage costs.

It is recommended that the last three good snapshots are retained for rollback purposes.

11.5.1 Menu Actions

Delete Snapshot	Deletes the Snapshot

11.6 Images

Images will accumulate over time and incur storage costs.

It is recommended that the last three good Images are retained for rollback purposes.

Do not delete Images that are still in use by a Scale Set or Virtual Machine instances that have not yet updated.

Use Premium storage for faster deployments particularly when using VMs with Ephemeral Disks.

11.6.1 Menu Actions

Delete Image	Deletes the Image

11.7 PowerShell

Minimum PowerShell Version: 5.1

11.7.1 Module Installation for AVDManage

Install minimal PowerShell Modules for AVDManage.

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
```

If prompted to install the the Nuget Provider, type Y

```
Uninstall-module -name Az.Accounts -AllVersions
Uninstall-module -name Az.Compute -AllVersions
Uninstall-module -name Az.DesktopVirtualization -AllVersions
Uninstall-module -name Az.Resources -AllVersions
Uninstall-module -name Az.Automation -AllVersions
Uninstall-module -name Az.Network –AllVersions
Uninstall-module -name Az.ManagedServiceIdentity –AllVersions

Install-Module -Name Az.Accounts -RequiredVersion 5.3.3 -Scope AllUsers -Force
Install-Module -Name Az.Compute -RequiredVersion 11.3.0 -Scope AllUsers -Force
Install-Module -Name Az.DesktopVirtualization -RequiredVersion 5.4.1 -Scope AllUsers -Force
Install-Module -Name Az.Resources -RequiredVersion 9.0.1 -Scope AllUsers -Force
Install-Module -Name Az.Automation -RequiredVersion 1.11.2 -Scope AllUsers -Force
Install-Module -Name Az.Network -RequiredVersion 7.25.0 -Scope AllUsers -Force
Install-Module -Name Az.ManagedServiceIdentity -RequiredVersion 2.0.0 -Scope AllUsers -Force
```

If you want to delete Active Directory Computer accounts when modifying or deleting a Scale Set, install the ActiveDirectory PowerShell Module.

Desktop O/S

```
Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools
```

Server OS

```
Add-WindowsFeature -Name RSAT-AD-PowerShell
```

If you want to delete Entra ID devices when modifying or deleting a Scale Set, install the **Microsoft.Graph.Identity.DirectoryManagement** PowerShell Module. This will automatically install the **Microsoft.Graph.Authentication** PowerShell Module.

```
Uninstall-module -name Microsoft.Graph.Identity.DirectoryManagement –AllVersions
Uninstall-module -name Microsoft.Graph.Authentication  –AllVersions

Install-Module -Name Microsoft.Graph.Identity.DirectoryManagement -RequiredVersion 2.35.0 -Scope AllUsers -Force
```

11.7.2 Verify Installed Modules

```
Get-Module -Name Az.Accounts,Az.Compute,Az.DesktopVirtualization,Az.Resources,Az.Automation,Az.Network, Az.ManagedServiceIdentity -ListAvailable | select name,version
```

```
Get-Module -Name Microsoft.Graph.Authentication, Microsoft.Graph.Identity.DirectoryManagement -ListAvailable | select name,version
```

11.8 SysPrep Failure

Error:

> Sysprep was not able to validate your Windows installation. Review the log file at %WINDIR%\System32\Sysprep\Panther\setupact.log for details. After resolving the issue, use Sysprep to validate your installation again.

%WINDIR%\System32\Sysprep\Panther\setupact.log

> ActionPlatform::LaunchModule: Failure occurred while executing 'ValidateBitLockerState' from C:\Windows\System32\BdeSysprep.dll

Bitlocker is enabled on the Master VM. Sysprep cannot run on an encrypted drive.

Run

> **Manage-bde –off C:**

It will take a few minutes for the volume to decrypt. You can check the status of decryption by running

> **Manage-Bde -Status**

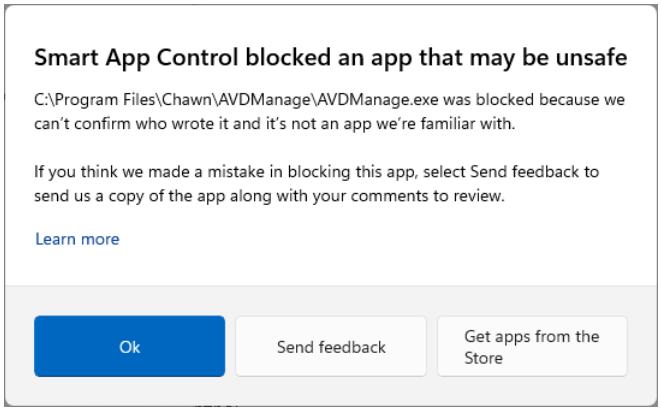
When the Drive is fully decrypted, run Sysprep again.

BitLocker overview | Microsoft Learn

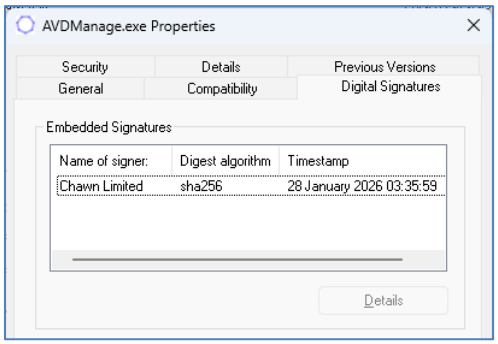
12. Smart App Control

27th January 2026 Smart App Control blocks AVDManage

When launching AVDManage on Windows 11 with Smart Access Control Enabled, you may receive the following message and AVDManage is blocked from launching.



Sectigo Support has confirmed that AVDManage correctly is signed with a valid code signing certificate.

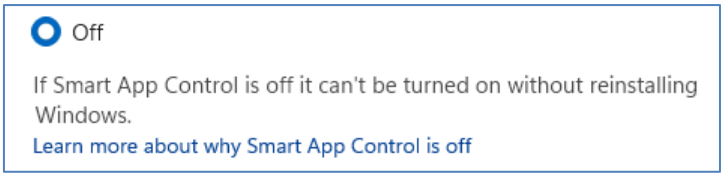


Resolved 30th January 2026

Workaround:

Windows 11 build 26220.7070 will contain a toggle to Enable / Disable Smart App Control.
Announcing Windows 11 Insider Preview Build 26220.7070 (Dev & Beta Channels) | Windows Insider Blog

Previously Microsoft have advised that if Smart App Control is disabled, it cannot be re-enabled without reinstalling Windows.



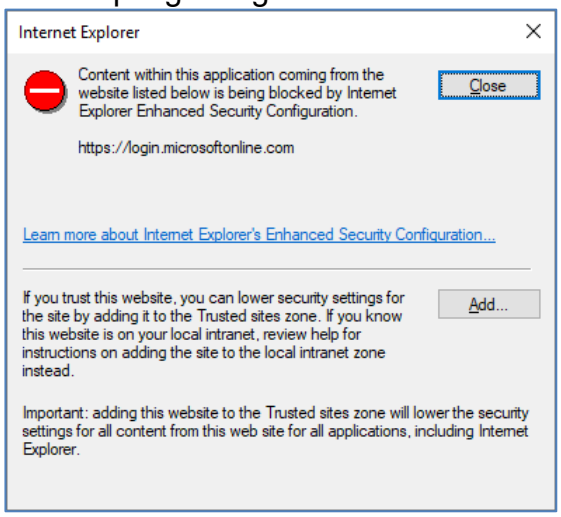
However you can toggle the following registry setting to Enable / Disable Smart App Control and reboot to implement the change.

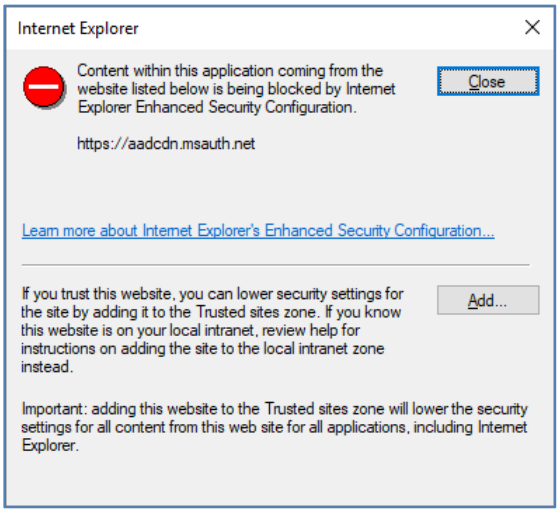
Key: HKLM\SYSTEM\CurrentControlSet\Control\CI\Policy
DWord: VerifiedAndReputablePolicyState
Value: 0 = Disabled 1 = Enabled

13. Login Issues

13.1 Internet Explorer Trust

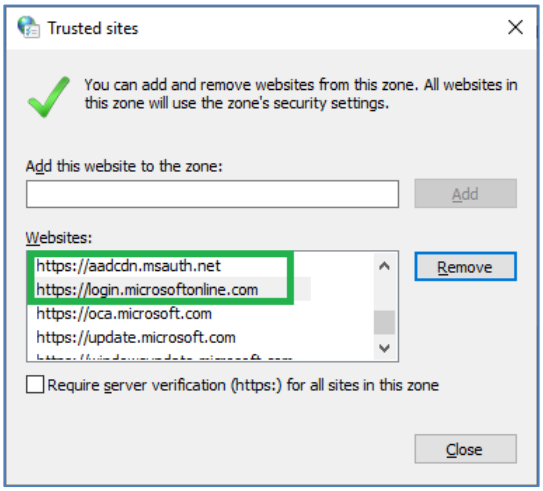
If running an older Windows Operating System, you may encounter the following warnings when attempting to logon.



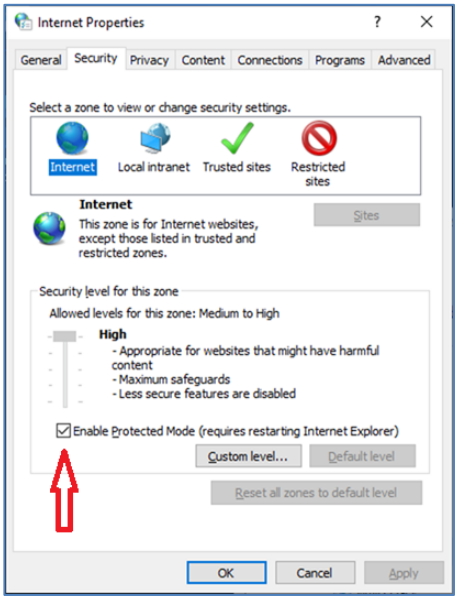


Solution 1
Add the following URLs to Internet Explorer Trusted Sites Zone

- https://login.microsoftonline.com
- https://aadcdn.msauth.net



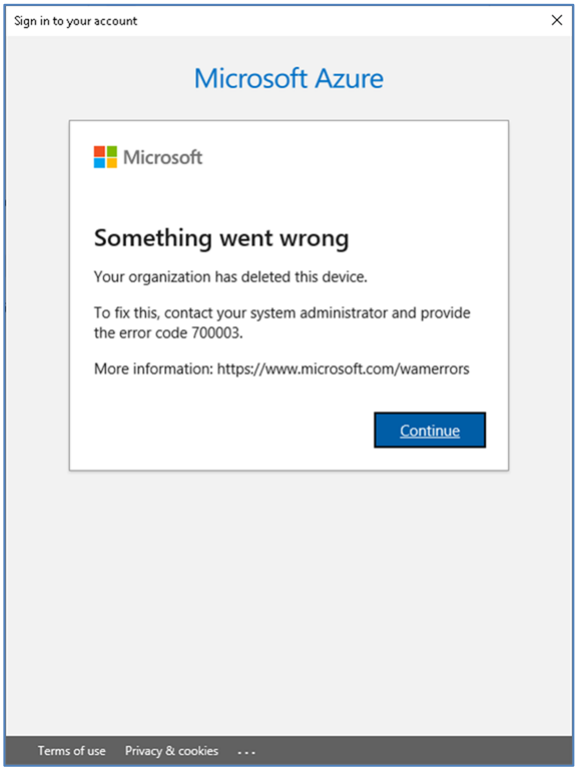
Solution 2
Disable Internet Explorer Protected Mode.



13.2 Something went wrong

After authenticating, the following message is displayed.

Click **Continue**, authentication will complete successfully.

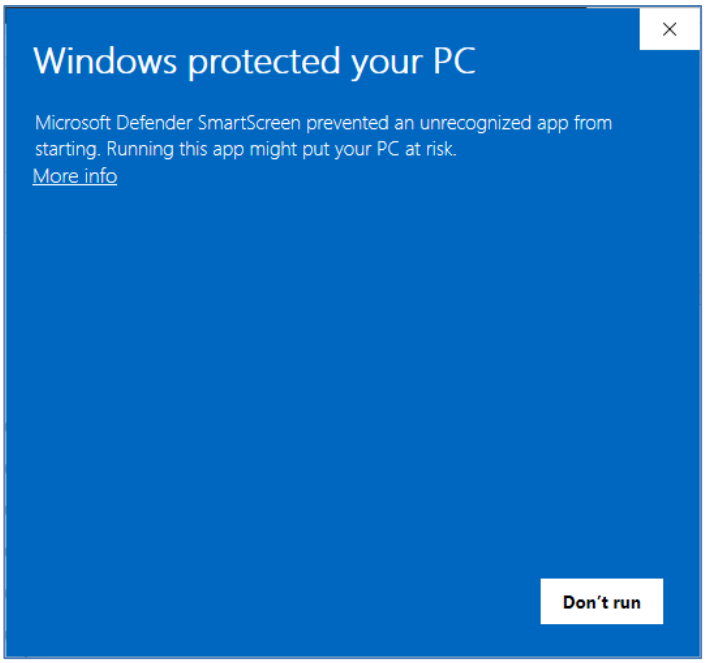


This behaviour has been seen when running AVDManage on an Active Directory Domain Controller.

14. Installation Issues

14.1 SmartScreen prevents installation

When running AVDManage.msi the following warning is displayed.



Solution
Right click AVDManage and select Properties.

Tick **Unblock** to remove the 'Mark of the Web'

Click Apply.

Rerun AVDManage.msi