



#htmdcommunity

@htmdcommunity

HTMD Community Conference - 2024



Thank You Sponsors!



Speaker



Rajul OS

Senior Consultant, Microsoft ISD



www.linkedin.com/in/rajulros/

Azure Virtual Desktop

Image and Session Host Management

Image Management

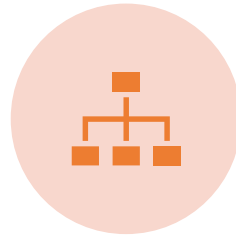
Managed Images



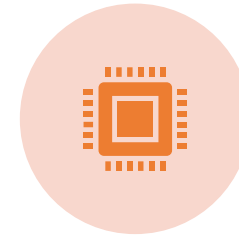
A SINGLE IMAGE OF A VM THAT INCLUDES THE OS DISK AND OPTIONALLY ANY ATTACHED DATA DISKS.



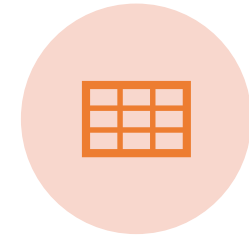
PRIMARILY USED FOR CREATING VM WITH A CONSISTENT CONFIGURATION. SUITABLE FOR SMALLER-SCALE DEPLOYMENTS.



SIMPLICITY: EASY TO CREATE AND MANAGE.



LIMITATIONS: LIMITED TO 20 SIMULTANEOUS VM DEPLOYMENTS FROM A SINGLE IMAGE.



REGION BOUND: MANAGED IMAGES ARE REGION-SPECIFIC AND CANNOT BE REPLICATED ACROSS REGIONS.

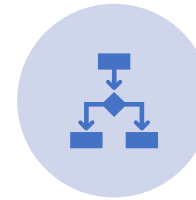
Azure Compute Gallery



Azure Compute Gallery (formerly Shared Image Gallery) is a service that helps you manage and share custom VM images and applications across your organization.



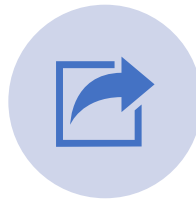
Global Replication: Allows you to replicate images across multiple regions, ensuring high availability and reducing latency.



Versioning: Supports multiple versions of an image, making it easier to manage updates and rollbacks.



Scalability: Enables large-scale deployments with resource replicas in each region.



Sharing: Images can be shared within your organization, across subscriptions, or even publicly through a community gallery.



High Availability: Utilizes Zone Redundant Storage (ZRS) for better resilience against zonal failures.

VM Image Definition

+ Add ▾ 🗑 Delete ↻ Refresh 👤 Give feedback

^ Essentials

[JSON View](#)

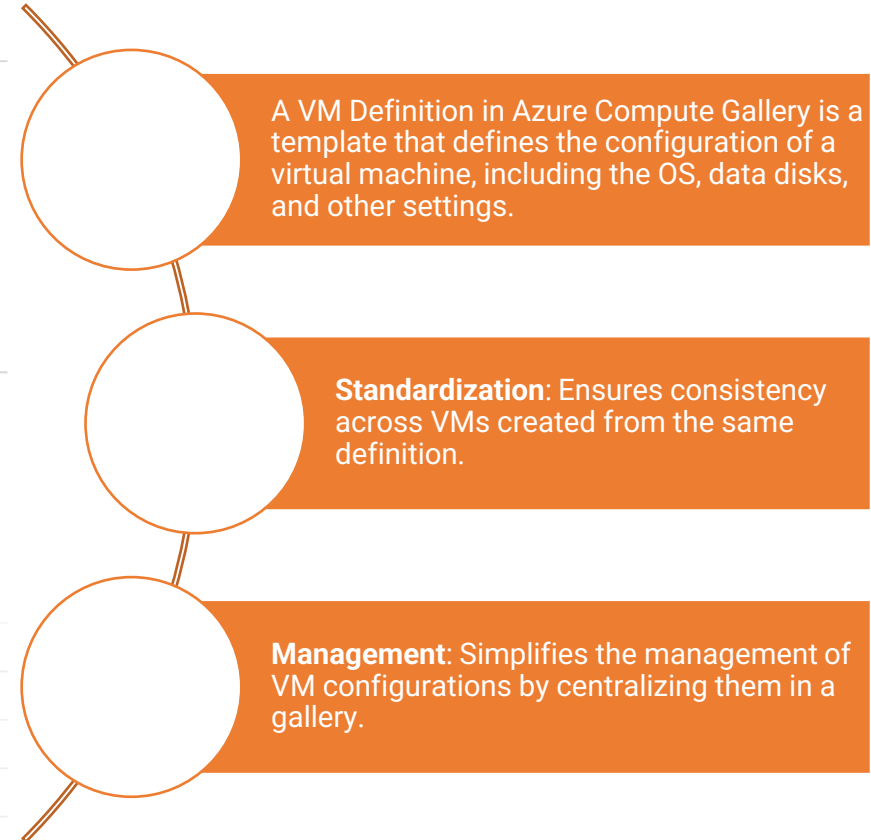
Resource group [\(move\)](#) : [rg-aztf-machine-images-dev](#)
Location [\(move\)](#) : Canada Central
Subscription [\(move\)](#) : [Visual Studio Enterprise Subscription](#)
Subscription ID : 93532d02-130f-4318-b508-9ac4fbf37f8d
Status : Succeeded
Tags [\(edit\)](#) : [Add tags](#)

Get started Definitions

▾ Showing 4 of 4 VM image definitions

Showing all 4 items

Name	Type	Provisioning State	OS type	OS state	VM generation	Location
ubuntu1804-baseline	VM image definition	Succeeded	Linux	Generalized	V2	canadacentral
W21H2_multisession	VM image definition	Succeeded	Windows	Generalized	V2	canadacentral
windows1123H2-multisession	VM image definition	Succeeded	Windows	Generalized	V2	canadacentral
windows21H2-multisession	VM image definition	Succeeded	Windows	Generalized	V2	canadacentral



VM Image Version

Home > Azure compute galleries > galaztfmachineimagesdev >

windows1123H2-multisession (galaztfmachineimagesdev/windows1123H2-multisession) ☆ ...

Search + Add version + Create VM + Create VMSS Delete Refresh Give feedback

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Automation
- Help

Essentials

Resource group (move) : rg-aztf-machine-images-dev Azure compute gallery : galaztfmachineimagesdev
Location (move) : Canada Central OS type : Windows
Subscription (move) : Visual Studio Enterprise Subscription OS state : Generalized
Subscription ID : 93532d02-130f-4318-b508-9ac4fbf37f8d Publisher :: Offer :: SKU : :: Windows-11 :: win11-23h2-avd
Status : Succeeded
Tags (edit) : Add tags

Properties Get started Versions

Filter by number... Showing 3 of 3 VM image versions Delete

Showing all 3 items

Name	Provisioning State	Published date	Target regions	Replication status	Create VM from version
2024.09.1	Succeeded	9/9/2024, 3:13:55 PM	Canada Central; East US	Completed	Create VM
2024.12.0	Succeeded	12/6/2024, 2:55:01 PM	Canada Central; East US	Completed	Create VM
2024.12.1 (latest version)	Succeeded	12/6/2024, 3:38:22 PM	Canada Central; East US	Completed	Create VM

JSON View

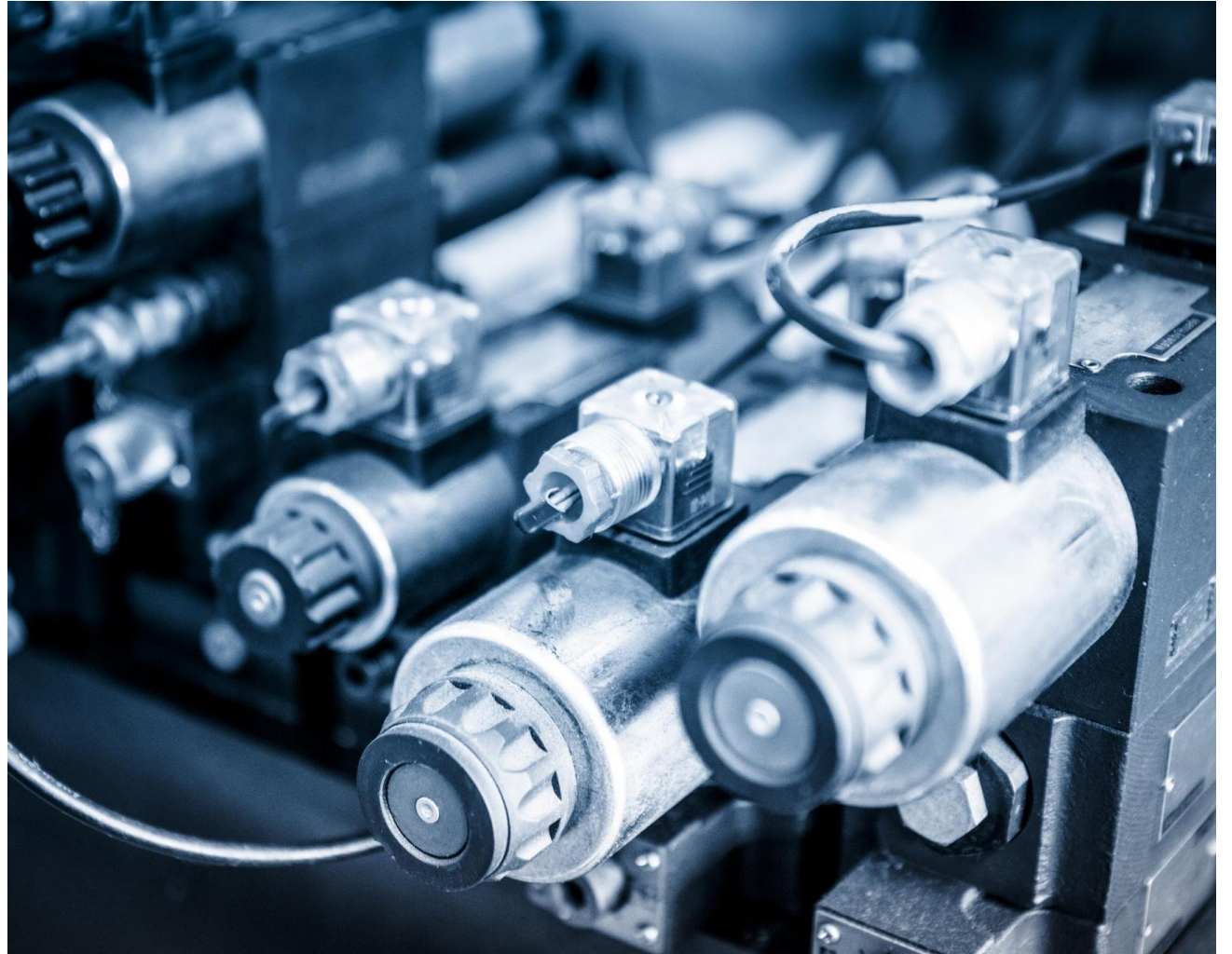
A versioned image stored in a gallery, which can include multiple versions of an image.

Versioning: Supports multiple versions of an image, allowing for better management and updates.

Scalability: Can handle large-scale deployments and supports features like ARM64, Trusted Launch, and Confidential VMs.

Packer

- Platform-agnostic: Supports multiple providers like Azure, AWS, VMware, etc.
- Highly customizable with scripts, plugins, and extensions.
- Build once, deploy anywhere approach.
- The workflow entails creating templates and executing build commands.
- Although it is a robust tool, Packer necessitates a certain level of expertise for optimal utilization.

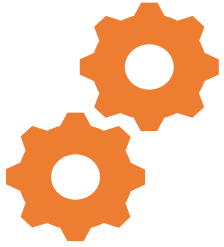




```
6 Author      : Microsoft Corporation
7 Help        : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/bash
8 =====
9 Generating script.
10 Formatted command: exec bash '/home/vsts/work/1/s/.azdo-pipelines/scripts/packer.sh'
11 ===== Starting Command Output =====
12 /usr/bin/bash /home/vsts/work/_temp/60c04042-8891-4c5a-9a9c-75791df495a9.sh
13 Packer Image Version:2024.12.1
14 Build Agent IP Address:4.188.240.102
15 Image Name:windows1123H2-multisession
16 Installed plugin github.com/hashicorp/azure v2.2.0 in "/home/vsts/.config/packer/plugins/github.com/hashicorp/azure/packer-plugin-azure_v2.2.0_x5.0_linux_amd64"
17 azure-arm.vm: output will be in this color.
18
19 ==> azure-arm.vm: Running builder ...
20     azure-arm.vm: Creating Azure Resource Manager (ARM) client ...
21     azure-arm.vm: ARM Client successfully created
22 ==> azure-arm.vm: Getting source image id for the deployment ...
23 ==> azure-arm.vm: -> SourceImageName: '/subscriptions/93532d02-130f-4318-b508-9ac4fbf37f8d/providers/Microsoft.Compute/locations/canadacentral/publishers/MicrosoftWindowsDesktop/ArtifactType
24 ==> azure-arm.vm: Using existing resource group ...
25 ==> azure-arm.vm: -> ResourceGroupName : 'rg-aztf-machine-images-dev'
26 ==> azure-arm.vm: -> Location           : 'canadacentral'
27 ==> azure-arm.vm: Validating deployment template ...
28 ==> azure-arm.vm: -> ResourceGroupName : 'rg-aztf-machine-images-dev'
29 ==> azure-arm.vm: -> DeploymentName   : 'kvpkrdp1nzmw44o0r'
30 ==> azure-arm.vm: Deploying deployment template ...
31 ==> azure-arm.vm: -> ResourceGroupName : 'rg-aztf-machine-images-dev'
32 ==> azure-arm.vm: -> DeploymentName   : 'kvpkrdp1nzmw44o0r'
33 ==> azure-arm.vm: Getting the certificate's URL ...
34 ==> azure-arm.vm: -> Key Vault Name      : 'pkrkvinzmw44o0r'
35 ==> azure-arm.vm: -> Key Vault Secret Name : 'packerKeyVaultSecret'
36 ==> azure-arm.vm: -> Certificate URL      : 'https://pkrkvinzmw44o0r.vault.azure.net/secrets/packerKeyVaultSecret/9f12a945914b4b2e84a221a9f2fad359'
37 ==> azure-arm.vm: Setting the certificate's URL ...
38 ==> azure-arm.vm: Validating deployment template ...
39 ==> azure-arm.vm: -> ResourceGroupName : 'rg-aztf-machine-images-dev'
40 ==> azure-arm.vm: -> DeploymentName   : 'pkrdp1nzmw44o0r'
41 ==> azure-arm.vm: Deploying deployment template ...
42 ==> azure-arm.vm: -> ResourceGroupName : 'rg-aztf-machine-images-dev'
43 ==> azure-arm.vm: -> DeploymentName   : 'pkrdp1nzmw44o0r'
44 ==> azure-arm.vm: Getting the VM's IP address ...
45 ==> azure-arm.vm: -> ResourceGroupName : 're-aztf-machine-images-dev'
```

```
1233 ==> azure-arm.vm: Querying the machine's properties ...
1234 ==> azure-arm.vm: -> ResourceGroupName : 'rg-aztf-machine-images-dev'
1235 ==> azure-arm.vm: -> ComputeName       : 'packertempvm'
1236 ==> azure-arm.vm: -> Managed OS Disk   : '/subscriptions/93532d02-130f-4318-b508-9ac4fbf37f8d/resourceGroups/rg-aztf-machine-images-dev/providers/Microsoft.Compute/disks/pkros1nzmw44o0r'
1237 ==> azure-arm.vm: Querying the machine's additional disks properties ...
1238 ==> azure-arm.vm: -> ResourceGroupName : 'rg-aztf-machine-images-dev'
1239 ==> azure-arm.vm: -> ComputeName       : 'packertempvm'
1240 ==> azure-arm.vm: Powering off machine ...
1241 ==> azure-arm.vm: -> ResourceGroupName : 'rg-aztf-machine-images-dev'
1242 ==> azure-arm.vm: -> ComputeName       : 'packertempvm'
1243 ==> azure-arm.vm: -> Compute ResourceGroupName : 'rg-aztf-machine-images-dev'
1244 ==> azure-arm.vm: -> Compute Name          : 'packertempvm'
1245 ==> azure-arm.vm: -> Compute Location       : 'canadacentral'
1246 ==> azure-arm.vm: Generalizing machine ...
1247 ==> azure-arm.vm: Publishing to Shared Image Gallery ...
1248 ==> azure-arm.vm: -> Source ID used for SIG publish : '/subscriptions/93532d02-130f-4318-b508-9ac4fbf37f8d/resourceGroups/rg-aztf-machine-images-dev/providers/Microsoft.Compute/virtualMachines'
1249 ==> azure-arm.vm: -> SIG publish resource group      : 'rg-aztf-machine-images-dev'
1250 ==> azure-arm.vm: -> SIG gallery name                : 'galaztfmachineimagesdev'
1251 ==> azure-arm.vm: -> SIG image name                  : 'windows1123H2-multisession'
1252 ==> azure-arm.vm: -> SIG image version               : '2024.12.1'
1253 ==> azure-arm.vm: -> SIG target regions              : '["canadacentral eastus']'
1254 ==> azure-arm.vm: -> SIG storage account type        : 'Standard_IRS'
1255 ==> azure-arm.vm: -> SIG image version endoflife date : '2025-03-06T09:48:52Z'
1256 ==> azure-arm.vm: -> SIG image version exclude from latest : 'false'
1257 ==> azure-arm.vm: -> Shared Gallery Image Version ID : '/subscriptions/93532d02-130f-4318-b508-9ac4fbf37f8d/resourceGroups/rg-aztf-machine-images-dev/providers/Microsoft.Compute/galleries'
1258 ==> azure-arm.vm:
1259 ==> azure-arm.vm: Deleting Virtual Machine deployment and its attached resources...
1260 ==> azure-arm.vm: Deleted -> packertempvm : 'Microsoft.Compute/virtualMachines'
1261 ==> azure-arm.vm: Deleted -> pkrm1nzmw44o0r : 'Microsoft.Network/networkInterfaces'
1262 ==> azure-arm.vm: Deleted -> packertempvm/extension-customscript : 'Microsoft.Compute/virtualMachines/extensions'
1263 ==> azure-arm.vm: Deleted -> pkrip1nzmw44o0r : 'Microsoft.Network/publicIPAddresses'
1264 ==> azure-arm.vm: Deleted -> Microsoft.Compute/disks : '/subscriptions/93532d02-130f-4318-b508-9ac4fbf37f8d/resourceGroups/rg-aztf-machine-images-dev/providers/Microsoft.Compute/disks/pkros1nzmw44o0r'
1265 ==> azure-arm.vm: Removing the created Deployment object: 'pkrdp1nzmw44o0r'
1266 ==> azure-arm.vm:
1267 ==> azure-arm.vm: Deleting KeyVault created during build
1268 ==> azure-arm.vm: Deleted -> pkrkvinzmw44o0r : 'Microsoft.KeyVault/vaults'
1269 ==> azure-arm.vm: Removing the created Deployment object: 'kvpkrdp1nzmw44o0r'
1270 ==> azure-arm.vm:
1271 ==> azure-arm.vm: The resource group was not created by Packer, not deleting ...
1272 Build 'azure-arm.vm' finished after 31 minutes 20 seconds.
```

Azure Image Builder



Azure Image Builder is a managed service that simplifies the creation, customization, and management of VM images in Azure.



Key Features:

Customization: Allows you to create custom images by specifying configurations and customizations using existing scripts and tools.

Integration: Works with Azure DevOps, Azure Compute Gallery, and other Azure services for seamless image management.

Scalability: Supports large-scale image building and distribution across multiple regions.

Security: Ensures images are secure by integrating with Azure security services and maintaining compliance.

Efficiency: Reduces the complexity and time required to build and manage VM images

Custom Image Template in AVD

Key Features

1. Specifically optimized for AVD settings.
2. May incorporate applications, policies, and user preferences tailored for AVD.
3. Expands upon pre-set base images.

The image you select will become the source image used to generate a custom image.

Source type * ⓘ

Select image * ⓘ

Generation

Platform image (marketplace) ▼

Platform image (marketplace)

Managed image

Azure Compute Gallery

Select built-in scripts

Operating system specific scripts

- ☐ Install languages ⓘ
- ☐ Set default OS language ⓘ
- ☐ Time zone redirection ⓘ
- ☐ Disable Storage Sense ⓘ

Azure Virtual Desktop scripts

- ☐ Install FSLogix and enable profile containers ⓘ
- ☐ Enable Kerberos and Azure AD ⓘ
- ☐ Configure RDP Shortpath for managed networks ⓘ
- ☐ Enable screen capture protection ⓘ
- ☐ Configure session timeouts ⓘ
- ☐ Install multimedia redirection ⓘ
- ☐ Configure Windows Optimizations ⓘ

MSIX App Attach

- ☐ Disable Auto updates for MSIX App Attach Applications. ⓘ

Application scripts

- ☐ Remove Appx packages ⓘ
- ☐ Add Microsoft Office applications ⓘ
- ☐ Remove Microsoft Office applications ⓘ

Other scripts

- ☐ Apply Windows Updates ⓘ

Comparison

Aspect	Azure Image Builder	Packer	Custom Image Templates(AVD)
Ease of Use	Medium	Medium	High
Customizability	Moderate	High	Low
Automation	High	High	Low
AVD Optimization	High	High	High
Cross-platform	No	Yes	No
Dependency on Azure	Yes	No	Yes
Scalability	High	High	Low
Expertise Required	Medium	High	Medium

Best Practices for Image Building in Azure

Using Automation

Implementing automation tools can streamline the image building process, reducing manual errors and saving time.

Maintaining Version Control

Version control is crucial for tracking changes and managing updates, ensuring the integrity and consistency of images.

Regular Updates

Regularly updating images is essential for security and performance, allowing for the integration of the latest features and fixes.



Session Host Management Using Intune

Prerequisites - Multisession



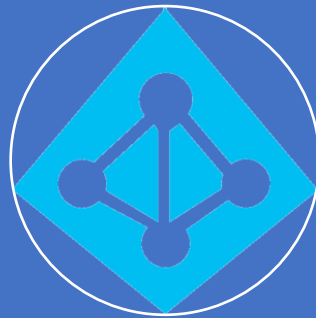
Supported OS

Windows 10 multi-session (version 1903 or later) or Windows 11 multi-session



Deployment

Set up as remote desktops in pooled host pools deployed through Azure Resource Manager



Tenant

Must be under the same tenant as Intune



AVD Agent

Running Azure Virtual Desktop agent version 1.0.2944.1400 or later



Licensing

Requires appropriate Azure Virtual Desktop and Microsoft Intune licenses



Enrollment

- **Hybrid Join:**
 - Enrolled in Intune using Active Directory group policy
 - Configuration Manager co-management policy
- **Entra AD Join:** Enrolled in Intune by enabling "Enroll the VM with Intune" in the Azure portal.

This screenshot shows the 'Enable automatic MDM enrollment using default Azure AD credentials' window. It has tabs for 'Previous Setting' and 'Next Setting'. The 'Enabled' radio button is selected. The 'Comment' field is empty. The 'Supported on' dropdown is set to 'At least Windows 10'. Under 'Options', 'Select Credential Type to Use' is set to 'Device Credential'. The 'MDM Application ID' field contains '0000000a-0000-0000-c000-000000000000'. A help section on the right explains that this policy setting specifies whether to automatically enroll the device to the Mobile Device Management (MDM) service configured in Azure Active Directory (Azure AD). It also notes that if the enrollment is successful, the device will be remotely managed by the MDM service. Important notes state that the device must be registered in Azure AD for enrollment to succeed, and that enabling this policy setting creates a task to initiate enrollment of the device to the MDM service specified in the Azure AD. Disabling this policy setting will unenroll the device.

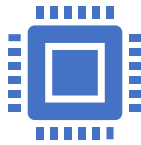
This screenshot shows the 'CoMgmtSettingsProd Properties' window. It has tabs for 'Cloud attach', 'Configure upload', 'Enablement', 'Workloads', and 'Staging'. The 'Enablement' tab is selected. The text indicates that workloads are for only clients in the Pilot group (specified later in this wizard). If you are not ready to move workloads to Intune, select Configuration Manager. A 'Learn more' link is provided. Below, there are sliders for 'Compliance policies', 'Device configuration', 'Endpoint Protection', and 'Resource access policies', each with a house icon. At the bottom, there are sliders for 'Client apps', 'Office Click-to-Run apps', and 'Windows Update policies', each with a house icon. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

This screenshot shows the 'Domain to join' dialog box. It has a dropdown menu for 'Select which directory you would like to join' set to 'Microsoft Entra ID'. Below, there are radio buttons for 'Enroll VM with Intune', with 'Yes' selected. There is also a 'No' option.

Policy



Use the Settings catalog in Intune to create and deploy configuration profiles



Device Context: Policies can be applied to devices for system-wide settings



User Context: Policies can be applied to users for user-specific settings



Compliance & Conditional Access Policy



Administrative Templates
ADMX-backed and ADMX-
Ingested policies

Edit profile - AVD M365 Policies ...

Settings catalog

1 Configuration settings

2 Review + save

+ Add settings ⓘ

Microsoft Office 2016 (Machine)

Remove category

OneDrive

Remove category

77 of 86 settings in this category are not configured

Exclude specific kinds of files from being uploaded ☒ Enabled ⓘ

Keywords: (Device)

Delete Sort Import Export

<input type="checkbox"/>	msedge.exe
<input type="checkbox"/>	Microsoft Teams.Ink
<input type="checkbox"/>	Microsoft Edge.Ink
<input type="checkbox"/>	

Prompt users when they delete multiple OneDrive files on their local computer ☒ Enabled ⓘ

Number of files: (Device) * 20

Require users to confirm large delete operations ☒ Enabled ⓘ

Silently move Windows known folders to ☒ Enabled ⓘ

Review + save

Cancel

Settings picker

Use commas "," among search terms to lookup settings by their keywords

Search for a setting

Search

+ Add filter

Add filter

Choose filter type for resources

Key OS Edition

Operator ==

Value Enterprise m...

- ☐ Holographic For Business
- ☐ IoT Enterprise
- ☐ Windows Education
- ☐ Windows Enterprise
- ☐ Windows Home
- ☒ Enterprise multi-session
- ☐ Windows Professional

Settings picker

Use commas "," among search terms to lookup settings by their keywords

Edge Search

Scenario == Enterprise multi-session Scope == Device Add filter

Browse by category

Administrative Templates\MSS (Legacy)
Administrative Templates\System\Internet Communication Management\Internet Communication settings
Administrative Templates\Windows Components\Internet Explorer
Administrative Templates\Windows Components\Tablet PC\Input Panel
Browser
Microsoft Edge
Microsoft Edge - Default Settings (users can override)
Microsoft Edge - Default Settings (users can override)\ Extensions
Microsoft Edge - Default Settings (users can override)\ Identity and sign-in
Microsoft Edge - Default Settings (users can override)\ Typosquatting Checker settings
Microsoft Edge - Default Settings (users can override)\Content settings

492 results in the "Microsoft Edge" category

Select all these settings

Setting name

- ✓ ☐ Ads setting for sites with intrusive ads ⓘ
 - ☐ Ads setting for sites with intrusive ads (Device)
- ✓ ☐ Allow access to sensors on specific sites ⓘ
 - ☐ Allow access to sensors on specific sites (Device)
- ☐ Allow access to the Enterprise Mode Site List Manager tool ⓘ
- ☐ Allow certificates signed using SHA-1 when issued by local trust anchors (deprecated) ⓘ
- ✓ ☐ Allow clipboard use on specific sites ⓘ
 - ☐ Allow clipboard use on specific sites (Device)
- ☐ Allow default search provider context menu search access ⓘ
- ✓ ☐ Allow download restrictions ⓘ

Settings picker

Use commas "," among search terms to lookup settings by their keywords

USB Search

Scenario == Enterprise multi-session Scope == User Add filter

Browse by category

Administrative Templates\Control Panel\Printers
Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone
Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone
Google Google Chrome Content settings
Microsoft Edge\Content settings
Microsoft Project 2016\Project Options\View\Show

10 results in the "Content settings" subcategory

Select all these settings

Setting name

- ✓ ☐ Allow WebUSB on these sites (User) ⓘ
 - ☐ Allow WebUSB on these sites (User)
- ✓ ☐ Automatically grant permission to sites to connect to USB serial devices. (User) ⓘ
 - ☐ Automatically grant permission to sites to connect to USB serial devices. (User)
- ✓ ☐ Automatically grant permission to these sites to connect to USB devices with the given vendor and product IDs. (User) ⓘ
 - ☐ Automatically grant permission to these sites to connect to USB devices with the given vendor and product IDs. (User)
- ✓ ☐ Block WebUSB on these sites (User) ⓘ
 - ☐ Block WebUSB on these sites (User)
- ✓ ☐ Control use of the WebUSB API (User) ⓘ
 - ☐ Control use of the WebUSB API (User)

Application Deployment for Windows 10/11 Enterprise Multi-Session

01

System Context: All apps must be installed in the system/device context and targeted to devices.

02

User Context: Web apps are applied in the user context by default and won't apply to multi-session VMs.

03

Assignment Intent: Only "Required" or "Uninstall" app assignment intents are supported. "Available" apps deployment intent is not supported.

04

Dependencies: Win32 apps with dependencies or supersedence relationships in the user context won't be installed. Ensure all dependencies are configured for the system context.

Script Deployment and Windows Update for Business



Script Deployment:

System Context: Supported on Windows 10/11 Enterprise multi-session. Assignment target should be device group

User Context: Supported on Windows 10/11 Enterprise multi-session. Assignment target should be user group



Windows Update for Business:

Management: Use the settings catalog to manage Windows Update settings for quality updates.

Limitations on Multi-Session Desktop

- Intune does not support using a cloned image of a computer that is already enrolled
- If you're joining session hosts to Microsoft Entra Domain Services, you can't manage them using Intune
- Device-based configuration cannot be assigned to users and user-based configuration cannot be assigned to devices.
- Configuration and compliance policies for BitLocker, Secure Boot, and features leveraging vTPM (Virtual Trusted Platform Module) are not supported at this time for Azure Virtual Desktop VMs
- User-targeted compliance configurations aren't supported
- Security Baselines are not supported on
- Only below configuration profile templates are supported
 - Trusted Certificate (Device)
 - SCEP Certificate (Device)
 - PKCS Certificate (Device)
 - VPN (Device Tunnel)
- Remote Actions not supported are below
 - Autopilot Reset
 - Bitlocker Key Rotation
 - Fresh Start
 - Remote Lock
 - Reset Password
 - Wipe

Questions?