

AZ-140

Configuring and Operating Azure Virtual Desktop



AZ-140 Agenda

Learning Path 1

1. Azure Virtual Desktop Architecture
2. Design the Azure Virtual Desktop architecture
3. Design for user identities and profiles

Learning Path 2

4. Implement and manage networking for AVD
5. Implement and manage storage for AVD
6. Create and configure host pools and session hosts for AVD
7. Create and manage session host image for AVD

Learning Path 3

8. Manage access for AVD
9. Manage security for AVD ← CA Policies

Learning Path 4

10. Implement and manage FSLogix
11. Configure user experience settings
12. Install and configure apps on a session host

Learning Path 5

13. Plan for disaster recovery
14. Automate Azure Virtual Desktop management tasks
15. Monitor and manage performance and health

Manage security for Azure Virtual Desktop



Introduction

- 1 Plan and implement Conditional Access policies for connections to Azure Virtual Desktop
- 2 Understand Conditional Access policy components
- 3 Plan and implement MFA in Azure Virtual Desktop
- 4 Manage security by using Azure Security Center
- 5 Microsoft Defender Antivirus for session hosts

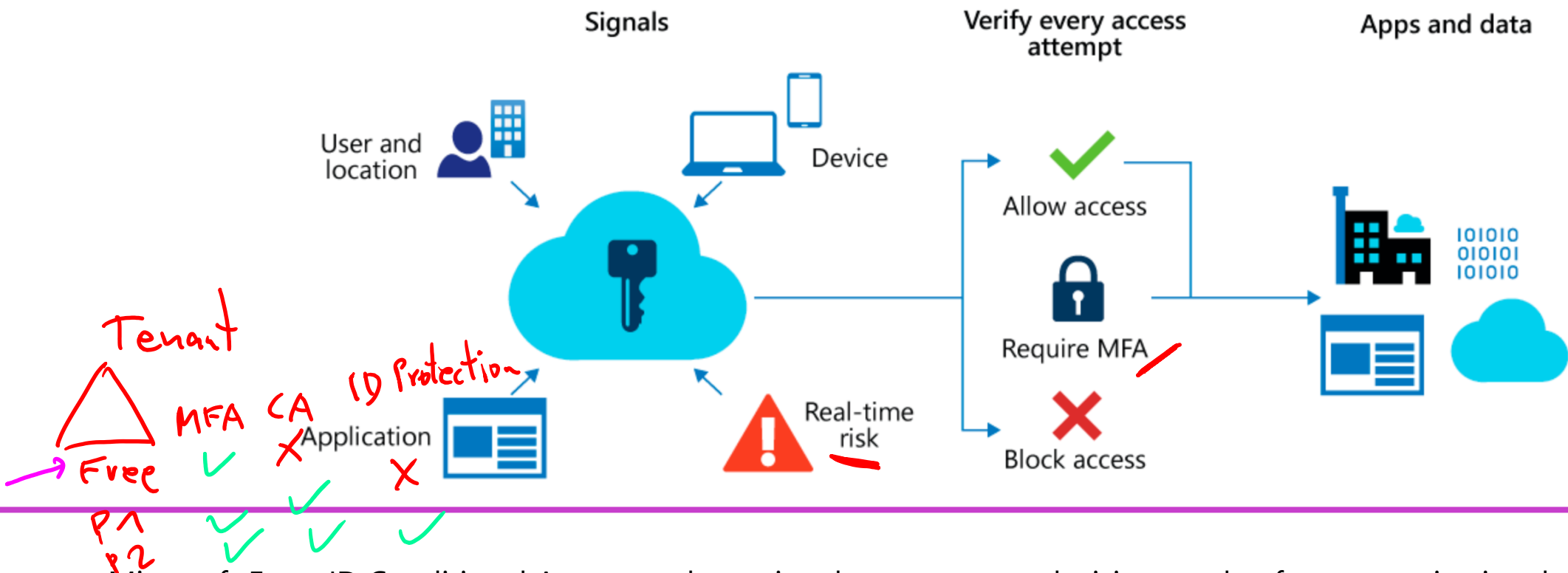
AZ-140: Manage access and security (10-15%)

Manage security

- Conceptual knowledge of Azure compute solutions
- Working experience with virtual machines, virtual networks, and app service

Plan and implement Conditional Access policies for connections to Azure Virtual Desktop





- Microsoft Entra ID Conditional Access analyses signals to automate decisions and enforce organizational access policies for resource.
- Conditional Access policies to apply access controls like multifactor authentication (MFA).
- Conditional Access policies allow you to prompt users for MFA when needed.

Plan and implement MFA in Azure Virtual Desktop



Plan MFA in Azure Virtual Desktop

When you first sign in, the client asks for your username, password, and Azure multifactor authentication.

- The next time you sign in, the client will remember your token from your Microsoft Entra Conditional Access Enterprise Application.
- When you select **Remember me** on the prompt for credentials for the session host, your users can sign in after restarting the client without needing to reenter their credentials.

Client apps ×

Control user access to target specific client applications not using modern authentication.

[Learn more](#)

Select the client apps this policy will apply to

Modern authentication clients

☐ Browser

☒ Mobile apps and desktop clients

Legacy authentication clients

☐ Exchange ActiveSync clients

☐ Other clients ⓘ

i Since this policy was created, the default client apps configuration has been updated.

Understand Conditional Access policy components



Common questions about assignments, access controls, and session controls:


- **Users and Groups:** Which users and groups will be included in or excluded from the policy? Does this policy include all users, specific group of users, directory roles, or external users?
- **Cloud apps or actions:** What application(s) will the policy apply to? What user actions will be subject to this policy?
- **Session controls:** Do you want to control access to cloud apps by implementing requirements such as app enforced permissions or Conditional Access App Control?
- **Conditions:** Which device platforms will be included in or excluded from the policy? What are the organization's trusted locations?
- **Access controls:** Do you want to grant access to resources by implementing requirements such as MFA, devices marked as compliant, or hybrid Azure AD joined devices?




Manage security by using Microsoft Defender for Cloud (ASC)




Security requisites the customer is responsible for in an Azure Virtual Desktop deployment:

Enable Microsoft Defender for Cloud for:

- Subscriptions 
- Virtual machines
- Key vaults
- Storage accounts

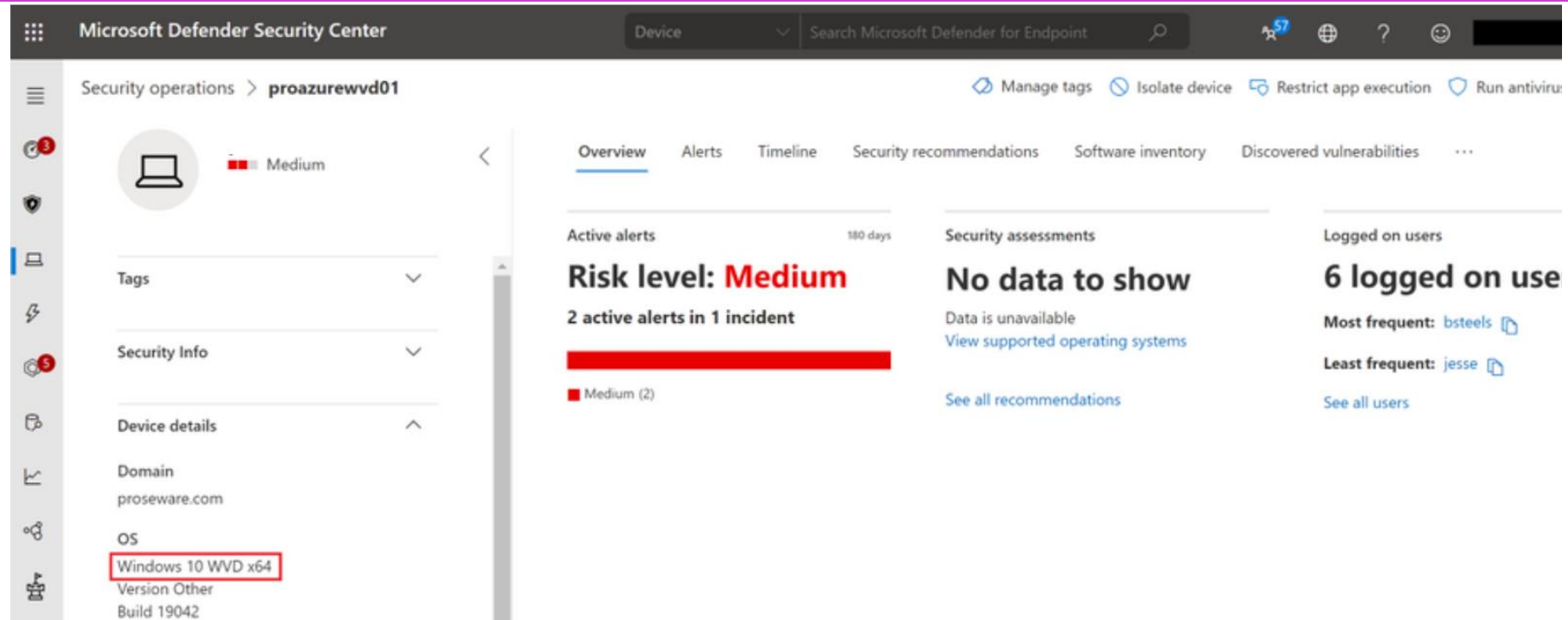
Security	Customer responsibility
Identity 	Yes
User devices (mobile and PC)	Yes
App security	Yes
Session host OS 	Yes
Deployment configuration	Yes
Network controls	Yes
Virtualization control plane	No
Physical hosts	No
Physical network	No
Physical datacenter	No 



Microsoft Defender Antivirus for session hosts



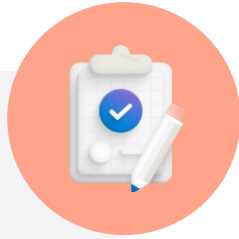
Microsoft Defender Antivirus for session hosts



- Works with virtual desktops running in Azure Virtual Desktop in Azure or on a physical Windows 10 Endpoint.
- Supports Azure Virtual Desktop with up to 50 concurrent user connections for Windows 10 Enterprise multi-session.
- Single session scenarios on Windows 10 Enterprise is supported for onboarding Azure Virtual Desktop machines into Defender for Endpoint.

Knowledge check and Summary

Check your knowledge



What you learned:

- Plan and implement Conditional Access policies for connections to Azure Virtual Desktop.
- Plan and implement multifactor authentication (MFA) in Azure Virtual Desktop.
- Understand Conditional Access policy components.
- Manage security by using Microsoft Defender for Cloud.
- Understand Microsoft Defender Antivirus for session hosts.

End of presentation

