

VMware Workspace ONE for macOS Skills

VMware 5V0-63-21

Version Demo

Total Demo Questions: 5

Total Premium Questions: 59

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, macOS Architecture and Technologies	1
Topic 2, VMware Workspace ONE UEM for macOS Deployment and Configuration	13
Topic 3, VMware Workspace ONE UEM for macOS Device Enrollment and Provisioning	5
Topic 4, VMware Workspace ONE UEM for macOS Application Management	6
Topic 5, VMware Workspace ONE UEM for macOS Security and Compliance	12
Topic 6, VMware Workspace ONE UEM for macOS Management and Troubleshooting	8
Topic 7, Mix Questions	14
Total	59

QUESTION NO: 1

A customer has decided to use VMware Workspace ONE as their primary SAAS solution for endpoint management. The customer's security team requires all infrastructure to support High Availability (HA).

Which two components of Workspace ONE will need to be maintained by the customer? (Choose two.)

- A. AirWatch Cloud Connector
- B. Workspace ONE Database
- C. Console Services Servers
- D. Unified Access Gateway
- E. Device Services Server

ANSWER: A D

Explanation:

In a Workspace ONE UEM SaaS deployment, the customer is responsible for maintaining the on-premises or customer-hosted components that extend the cloud service into its internal environment. **AirWatch Cloud Connector** is customer-managed because it provides a secure outbound connection between Workspace ONE UEM and internal enterprise resources, such as Active Directory, certificate authorities, and email infrastructure. To meet a high-availability requirement, customers deploy and maintain multiple Cloud Connector instances, generally configured in a load-balanced or redundant design.

Unified Access Gateway is also customer-maintained infrastructure. It is deployed at the customer edge to provide secure, remote access to Workspace ONE services and protected internal resources without exposing those resources directly to the internet. Availability of this access path is the customer's responsibility, commonly achieved by deploying multiple Unified Access Gateway appliances behind a load balancer. VMware/Omnissa hosts and operates the core Workspace ONE UEM SaaS service, while these connectivity and edge components remain part of the customer-managed environment. See the [AirWatch Cloud Connector requirements documentation](#) and the [Workspace ONE UEM and Unified Access Gateway deployment guide](#).

QUESTION NO: 2

An administrator must deploy macOS payloads that require User Approved MDM enrollment.

Which two enrollment methods result in User Approved MDM status? (Choose two.)

- A. Enroll the Mac through Automated Device Enrollment.
- B. Have the user approve the MDM enrollment in macOS System Settings.
- C. Install Intelligent Hub from a public download site.
- D. Send the user an enrollment invitation by email.
- E. Assign the Mac to a smart group.

ANSWER: A B

Explanation:

Automated Device Enrollment provides User Approved MDM status because the organization-owned Mac is enrolled through the Apple Business Manager enrollment workflow during Setup Assistant. For a manually enrolled Mac, the user can establish User Approved MDM by approving the MDM enrollment in macOS System Settings. Simply installing Intelligent Hub, receiving an enrollment email, or assigning a profile does not independently establish User Approved MDM status.

QUESTION NO: 3

Which VMware Horizon client application supports biometric authentication?

- A. macOS
- B. Linux
- C. Chrome
- D. Windows

ANSWER: A

Explanation:

macOS is correct because VMware Horizon Client for Mac integrates with Apple's Touch ID capability to provide biometric authentication. When the Mac hardware supports Touch ID and it has been configured in macOS, Horizon Client can use the user's fingerprint as part of the authentication experience rather than requiring repeated manual entry of credentials. This capability is especially useful for securely reconnecting to entitled Horizon desktops and applications while maintaining a convenient sign-in workflow for the end user.

Biometric support in this context depends on the native macOS security framework and the presence of compatible Touch ID hardware. Administrators must also ensure that the Horizon environment and applicable authentication configuration permit the desired client authentication flow. VMware's Horizon Client for Mac documentation describes the client's platform-specific features and authentication behavior, including use of macOS capabilities. See the [VMware Horizon Client for Mac documentation](#). Apple provides additional information about configuring and using Touch ID on a Mac in its [Touch ID on Mac guide](#).

QUESTION NO: 4

Which is required to deliver a Check In, Check Out experience on an Android Device?

- A. Block open enrollment into Workspace ONE UEM.
- B. Enable VMware Workspace ONE Intelligence.
- C. Deliver Launcher profile to the end-user.
- D. Use a basic user as a staging account.

ANSWER: C

Explanation:

Deliver Launcher profile to the end-user is required because Workspace ONE Launcher provides the shared-device interface that supports the Android Check In, Check Out workflow. In this model, a device is prepared for shared use and Launcher presents a controlled sign-in experience so that the person using the device can check in, receive the apps and settings intended for that session, and later check out for the next user. The Launcher profile is the UEM configuration mechanism that applies and manages this Launcher behavior on the Android device. Its delivery ensures the device enters the intended shared-device experience rather than operating as a conventionally assigned, single-user device. This configuration is especially important where devices are passed between shift workers, frontline staff, students, or other temporary users and the organization needs a consistent, managed handoff process. VMware's Workspace ONE Boxer documentation identifies support for Check In, Check Out on Android and describes the associated configuration considerations: [Workspace ONE Boxer Administration Guide](#). Additional Workspace ONE UEM product documentation is available from the [Workspace ONE UEM documentation portal](#).

QUESTION NO: 5 - (DRAG DROP)

Drag and drop the device operating system on the left into the box associated with its third party messaging solution.

iOS		APNS
Android		WNS
Windows		FCM

ANSWER:

Answer:

iOS	iOS	APNS
Android	Windows	WNS
Windows	Android	FCM

Answer:

Explanation:

iOS	APNS
Windows	WNS
Android	FCM

Table Description automatically generated

Explanation:

Workspace ONE UEM relies on each device platform's native third-party push-notification infrastructure to communicate efficiently with enrolled devices. The correct mapping is iOS to APNS, Windows to WNS, and Android to FCM. APNS, short for Apple Push Notification service, is Apple's push service for iPhone and iPad devices. Workspace ONE uses the APNS certificate and connection to notify managed Apple devices that they should contact the UEM service for pending commands or updated management information. Apple documents this service at [Setting up a remote notification server](#).

Windows devices use WNS, the Windows Notification Service. This is Microsoft's notification infrastructure for Windows applications and devices, and it provides the platform-specific notification channel needed for management communication. Microsoft describes this service in its [Windows Push Notification Services overview](#).

Android maps to FCM, Firebase Cloud Messaging. FCM is Google's cross-platform messaging service and is the supported notification mechanism used to wake or notify Android devices so they can retrieve queued Workspace ONE UEM actions. Google's [Firebase Cloud Messaging documentation](#) identifies FCM as the service for reliably sending messages to client applications. The completed answer places each operating system beside its corresponding native notification service, so the submitted mapping is correct.