Question 1

A Workspace ONE UEM administrator is concerned about the security of their organization's mobile devices. The concern is with jail-broken or rooted devices accessing company resources or navigating within the company network. The company's CIO wants a no-tolerance policy for devices in this state, requesting that they be removed immediately if detected.

How can the administrator enforce the policy using Workspace ONE UEM?

Options:

A- Configure a compliance policy to check for Compromised Status = Compromised. Configure the compliance action to send an email to the user asking them to unenroll.

B- Configure an application blacklist policy for one of the apps that is used to jail-break or root devices.

C- Configure a compliance policy to check for Compromised Status = Compromised. Configure the compliance action to enterprise wipe the device immediately.

D- Configure a daily report checking for compromised devices. Manually send enterprise wipe commands to each device based on the devices listed in the report.

Answer:

C

Explanation:

To enforce a no-tolerance policy for jailbroken or rooted devices, an administrator should configure a compliance policy in Workspace ONE UEM that checks for a compromised status. If a device is compromised, the configured action should be to enterprise wipe the device immediately. Reference: VMware Workspace ONE UEM documentation on compliance policies.

Question 2

Question Type: **MultipleChoice**

Which three are benefits of a Workspace ONE Content productivity application? (Choose three.)

Options:

A- Promote Content Disaster Recovery.

B- Secure Document distribution and mobile access.

C- Secure application distribution and mobile access.

D- Protect sensitive content in a corporate container.

E- Protect certificate keychain from third party access.

F- Promote secure collaboration.

Answer:

B, D, F

Explanation:

Workspace ONE Content offers benefits such as secure document distribution and mobile access, protecting sensitive content within a corporate container, and promoting secure collaboration among users. These features enhance both security and productivity.

Reference: VMware Workspace ONE Content documentation.

Question 3

Question Type: **Hotspot**

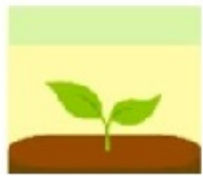# Add Application

Search 🔍

Editor's Choice | New

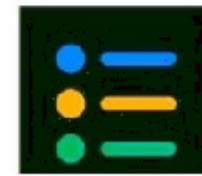|					
Forest: Focus for Seekrtech ⭐⭐⭐⭐⭐	Minimalist Promod Goodtime ⭐⭐⭐⭐	Google Keep – No Google LLC ⭐⭐⭐⭐	MemoMeister – Do Freiraum GmbH ⭐⭐⭐⭐⭐	Taskiee: To-Do List Faith Tirek ⭐⭐⭐⭐	Productive – Habit Apalon Apps ⭐⭐⭐⭐
Todoist: to do list Doist Inc. ⭐⭐⭐⭐	Google Tasks Google LLC ⭐⭐⭐⭐	Notion – notes, Notion Labs, Inc ⭐⭐⭐⭐	Google Calendar Google LLC ⭐⭐⭐⭐	Focus To-Do Pomodoro Timer & ⭐⭐⭐⭐⭐	Evernote – Note Evernote Corporation ⭐⭐⭐⭐

Refer to the Exhibit.

Where would an administrator click in the Managed Play Store to add Private Apps that are developed for their organization? Mark your answer by clicking on the image.

Answer:

Question 4

Question Type: **MultipleChoice**

Which security solution can be integrated with the Workspace ONE Intelligent Hub?

Options:

A- Advanced Threat Prevention

B- Carbon Black

C- Symantec Endpoint Protection Mobile

D- Mobile Threat Defense

Answer:

B

Explanation:

Carbon Black, a comprehensive security solution, can be integrated with the Workspace ONE Intelligent Hub. This integration provides advanced threat detection and response capabilities to protect mobile devices managed by Workspace ONE. Reference: VMware Workspace ONE and Carbon Black integration documentation.

Question 5

Question Type: MultipleChoice

Which two are prerequisites to activate Hub Services? (Choose two.)

Options:

A- Workspace ONE Access admin credential

B- Workspace ONE Intelligence URL

C- Workspace ONE Access tenant URL

D- Workspace ONE UEM DS URL

E- Workspace ONE UEM enrollment user credential

Answer:

A, C

Explanation:

To activate Hub Services, you need the Workspace ONE Access admin credentials for authentication and the Workspace ONE Access tenant URL to connect to the correct Access environment. These are essential for setting up and configuring Hub Services. Reference: VMware documentation on Workspace ONE Hub Services activation.

Question 6

Question Type: DragDrop

Key terms		Definitions
Service Provider	0	A system or service that manages and maintains user identities and credentials.
Identity Provider	0	An XML document containing information about a user's identity and authentication status.
Assertion	0	A protocol used for exchanging authentication and authorization data between parties.
Single Sign-On (SSO))	0	A software application or platform that provides access to a specific service or application.
SAML 2.0	0	A process that enables users to authenticate once and access multiple applications or services without having to log in again.

Match the terms related to Workspace ONE Access SAML 2.0 authentication on the left with their corresponding definitions on the right.

Answer:

Question 7

Question Type: Hotspot

Refer to the Exhibit.

Distribution

- ✅ Restrictions
- ✅ Tunnel
- ✅ Application Configuration
- ✅ Components Profile Configuration

Distribution

Name *

Description

Assignment Groups *

To whom do you want to assign this app?

Deployment Begins *

02/28/2023 12:00 AM ∨ (GMT–05:00) Eastern Time (US & Canada)

App Delivery Method * ● Auto   ○ On Demand

Where would an administrator click to add and send configuration settings as part of the Application Assignment? Mark your answer by clicking on it in the image.

Answer:

Question 8

Match each Content Gateway error message to its potential resolution.

Error Message		Potential Resolution
Failed to create process		Check user account permissions
Cannot establish trust relationship		Check user account permissions
Impersonation Failed		Update the Java keystore
Unable to access SharePoint files		Install missing dependencies on the UAG