



**Free Questions for 5V0-62.22 by dumpssheet**

**Shared by Obrien on 21-08-2023**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

## Question Type: MultipleChoice

---

A user reported that they were unable to see some of the expected applications and also did not receive the Wi-Fi profile. The profile status, application status, and device-related logging need to be seen to solve the problem:

Which console page should be used to see this information?

### Options:

---

- A- Resources > Profiles & Baselines > Profiled
- B- Groups & Settings > All Settings > Admin > Troubleshooting
- C- Devices > List View > Device Details View > More > Troubleshooting
- D- Monitor > Reports & Analytics > Events

### Answer:

---

C

### Explanation:

---

The console page that should be used to see this information is Devices > List View > Device Details View > More > Troubleshooting. This page allows the administrator to view various information about a specific device, such as profile status, application status, device-related logging, compliance status, commands history, and so on. This page can help troubleshoot issues related to device enrollment, configuration, management, and communication.

## Question 2

---

**Question Type:** MultipleChoice

---

The VMware Workspace ONE UEM administrator in an organization found that the Certificate Authority integration test connection failed recently. His organization uses on-premises Microsoft AD CS CA as their certificate authority, which resides on an internal-only Windows server. The VMware Workspace ONE UEM console resides in the cloud.

Why did this certificate authority integration test connection fail?

### Options:

---

- A-** Entrust PKI is disabled under the Certificate Authorities settings.
- B-** Symantec MPKI is disabled under the Certificate Authorities settings.

**C-** Fetching the root certificate from CA failed.

**D-** Credential in UEM is incorrect.

**Answer:**

---

C

**Explanation:**

---

The reason that this certificate authority integration test connection failed is that fetching the root certificate from CA failed. The root certificate from CA is a certificate that validates the identity and trustworthiness of the certificate authority (CA) that issues certificates for devices. Workspace ONE UEM needs to fetch the root certificate from CA to verify and manage certificates for devices. If fetching the root certificate from CA failed, it could indicate that there is a problem with CA configuration, connectivity, or availability. Workspace ONE UEM will not be able to connect to CA or issue certificates for devices, and the certificate authority integration test connection will fail.

## Question 3

---

**Question Type: MultipleChoice**

---

An administrator is getting reports that the profile status on multiple devices is not updating and need view the log which provides information about profile samples from the device. Which log should be viewed?

### Options:

---

- A- On the Console Server. \Logs\Services\Devicequeue.log
- B- On the Console Server \Logs\Services\QueuingService.log
- C- On the Device Services Server \Logs\Services\InterrogatorQueueService log
- D- On the Device Services Server \Logs\Services\Queuemanager\_log

### Answer:

---

C

### Explanation:

---

The log file that should be viewed is On the Device Services Server \Logs\Services\InterrogatorQueueService.log. InterrogatorQueueService.log is a log file that records the profile samples from devices and updates them in the Workspace ONE UEM console. Profile samples are data that show the status and details of profiles installed on devices. If profile status on multiple devices is not updating, it could indicate that there is a problem with InterrogatorQueueService configuration, connectivity, or performance. The administrator should view and analyze the InterrogatorQueueService.log file to identify and troubleshoot the issue.

## Question 4

---

**Question Type: MultipleChoice**

---

Refer to the exhibit.

The screenshot displays the configuration page for Secure Email Gateway settings in the VMware Workspace ONE UEM console. At the top, the 'Enable Secure Email Gateway Settings' toggle is turned ON (YES). Below this, several configuration fields are listed, each with an information icon (i) to its right:

- API Server URL \***: wsoapi.airwlab.com:443
- API Server Username \***: admin
- API Server Password \***: ..... (masked)
- Secure Email Gateway Hostname \***: seg01.airwlab.com
- MEM Config GUID \***: 01f336b3-b041-4a7c-b6af-7473473323fb
- Outbound Proxy Host**: (empty)
- Outbound Proxy Port**: (empty)
- Outbound Proxy Username**: (empty)
- Outbound Proxy Password**: (empty)

A VMware Workspace ONE administrator made changes to the Secure Email Gateway in the VMware Workspace ONE UEM console. When validating the new settings, the test connection fails.

Which statement describes the root cause of this issue?

### Options:

---

- A- The outbound proxy host, port, username, and password values are missing.
- B- The protocol https: // is missing in the Secure Email Gateway hostname value
- C- The Secure Email Gateway configuration does not have a valid SSL certificate.
- D- The protocol https: // is missing in the API server URL value.

### Answer:

---

B

### Explanation:

---

The statement that describes the root cause of this issue is that the protocol https:// is missing in the Secure Email Gateway hostname value. The Secure Email Gateway hostname value is the URL that Workspace ONE UEM uses to connect to the Secure Email Gateway edge service on UAG and perform email management tasks, such as quarantine, wipe, or block. The protocol https:// is required to indicate that the connection is secure and encrypted. If the protocol https:// is missing, Workspace ONE UEM will not be able to connect to the Secure Email Gateway edge service, and the test connection will fail. The administrator should add the protocol https:// to the Secure Email Gateway hostname value.

## Question 5

---

### Question Type: MultipleChoice

---

An organization wants to use the Content Gateway edge service of VMware Workspace ONE- UAG (Unified Access Gateway) so users of unmanaged Android and Apple iOS devices can access content on file servers on their internal network, using the VMware Workspace ONE Content application.

An administrator for the organization deployed a UAG appliance onto Microsoft Hyper-V for testing. In the UAG administrative web interface, the "Health Check" indicator for the Content Gateway edge service is red.

What is the most likely cause of this issue?

### Options:

---

- A- The user's devices must be managed by VMware Workspace ONE UEM to utilize Content Gateway
- B- The organization's Workspace ONE license does not include Content Gateway.
- C- The UAG appliance must be deployed to VMware vSphere.
- D- The Content Gateway certificate on the organization's UAG is invalid

### Answer:

---

D



### **Explanation:**

---

The Content Gateway certificate on the organization's UAG is invalid. The Content Gateway certificate is a certificate that allows UAG (Unified Access Gateway) to communicate with Workspace ONE UEM and provide secure access to content on file servers on the internal network. If the Content Gateway certificate is invalid, expired, or mismatched, UAG will not be able to establish a secure connection with Workspace ONE UEM, and the Content Gateway edge service will show a red health check indicator. The administrator should check and renew the Content Gateway certificate if needed.

## **Question 6**

---

**Question Type:** MultipleChoice

---

Refer to the exhibit.

Enable Secure Email Gateway Settings  YES ⓘ

API Server URL \*  ⓘ

API Server Username \*  ⓘ

API Server Password \*  ⓘ

Secure Email Gateway Hostname \*  ⓘ

MEM Config GUID \*  ⓘ

Outbound Proxy Host  ⓘ

Outbound Proxy Port  ⓘ

Outbound Proxy Username  ⓘ

Outbound Proxy Password  ⓘ

A VMware Workspace ONE administrator made changes to the Secure Email Gateway in the VMware Workspace ONE UEM console. When validating the new settings, the test connection fails.

Which statement describes the root cause of this issue?

**Options:**

---

- A- The outbound proxy host, port, username, and password values are missing.
- B- The protocol https: // is missing in the Secure Email Gateway hostname value
- C- The Secure Email Gateway configuration does not have a valid SSL certificate.
- D- The protocol https: // is missing in the API server URL value.

**Answer:**

---

B

**Explanation:**

---

The statement that describes the root cause of this issue is that the protocol https:// is missing in the Secure Email Gateway hostname value. The Secure Email Gateway hostname value is the URL that Workspace ONE UEM uses to connect to the Secure Email Gateway edge service on UAG and perform email management tasks, such as quarantine, wipe, or block. The protocol https:// is required to indicate that the connection is secure and encrypted. If the protocol https:// is missing, Workspace ONE UEM will not be able to connect to the Secure Email Gateway edge service, and the test connection will fail. The administrator should add the protocol https:// to the Secure Email Gateway hostname value.

## Question 7

---

**Question Type:** MultipleChoice

---

An administrator is getting reports that the profile status on multiple devices is not updating and need view the log which provides information about profile samples from the device. Which log should be viewed?

**Options:**

---

- A- On the Console Server. \Logs\Services\Devicequeue.log
- B- On the Console Server \Logs\Services\QueuingService.log
- C- On the Device Services Server \Logs\Services\InterrogatorQueueService log
- D- On the Device Services Server \Logs\Services\Queuemanager\_log

**Answer:**

---

C

**Explanation:**

---

The log file that should be viewed is On the Device Services Server \Logs\Services\InterrogatorQueueService.log. InterrogatorQueueService.log is a log file that records the profile samples from devices and updates them in the Workspace ONE UEM console. Profile samples are data that show the status and details of profiles installed on devices. If profile status on multiple devices is not updating, it could indicate that there is a problem with InterrogatorQueueService configuration, connectivity, or performance. The administrator should view and analyze the InterrogatorQueueService.log file to identify and troubleshoot the issue.

## Question 8

---

### Question Type: MultipleChoice

---

An organization wants to use the Content Gateway edge service of VMware Workspace ONE - UAG (Unified Access Gateway) so users of unmanaged Android and Apple iOS devices can access content on file servers on their internal network, using the VMware Workspace ONE Content application.

An administrator for the organization deployed a UAG appliance onto Microsoft Hyper-V for testing. In the UAG administrative web interface, the "Health Check" indicator for the Content Gateway edge service is red.

What is the most likely cause of this issue?

### Options:

---

- A- The user's devices must be managed by VMware Workspace ONE UEM to utilize Content Gateway
- B- The organization's Workspace ONE license does not include Content Gateway.
- C- The UAG appliance must be deployed to VMware vSphere.
- D- The Content Gateway certificate on the organization's UAG is invalid

**Answer:**

---

D

**Explanation:**

---

The Content Gateway certificate on the organization's UAG is invalid. The Content Gateway certificate is a certificate that allows UAG (Unified Access Gateway) to communicate with Workspace ONE UEM and provide secure access to content on file servers on the internal network. If the Content Gateway certificate is invalid, expired, or mismatched, UAG will not be able to establish a secure connection with Workspace ONE UEM, and the Content Gateway edge service will show a red health check indicator. The administrator should check and renew the Content Gateway certificate if needed.

**To Get Premium Files for 5V0-62.22 Visit**

<https://www.p2pexams.com/products/5v0-62.22>

**For More Free Questions Visit**

<https://www.p2pexams.com/vmware/pdf/5v0-62.22>

