DUMPSBOSS.

# Aruba Certified ClearPass Expert Written Exam

## HP HPE6-A81

### Version Demo

**Total Demo Questions: 12**

**Total Premium Questions: 124**

**Buy Premium PDF**

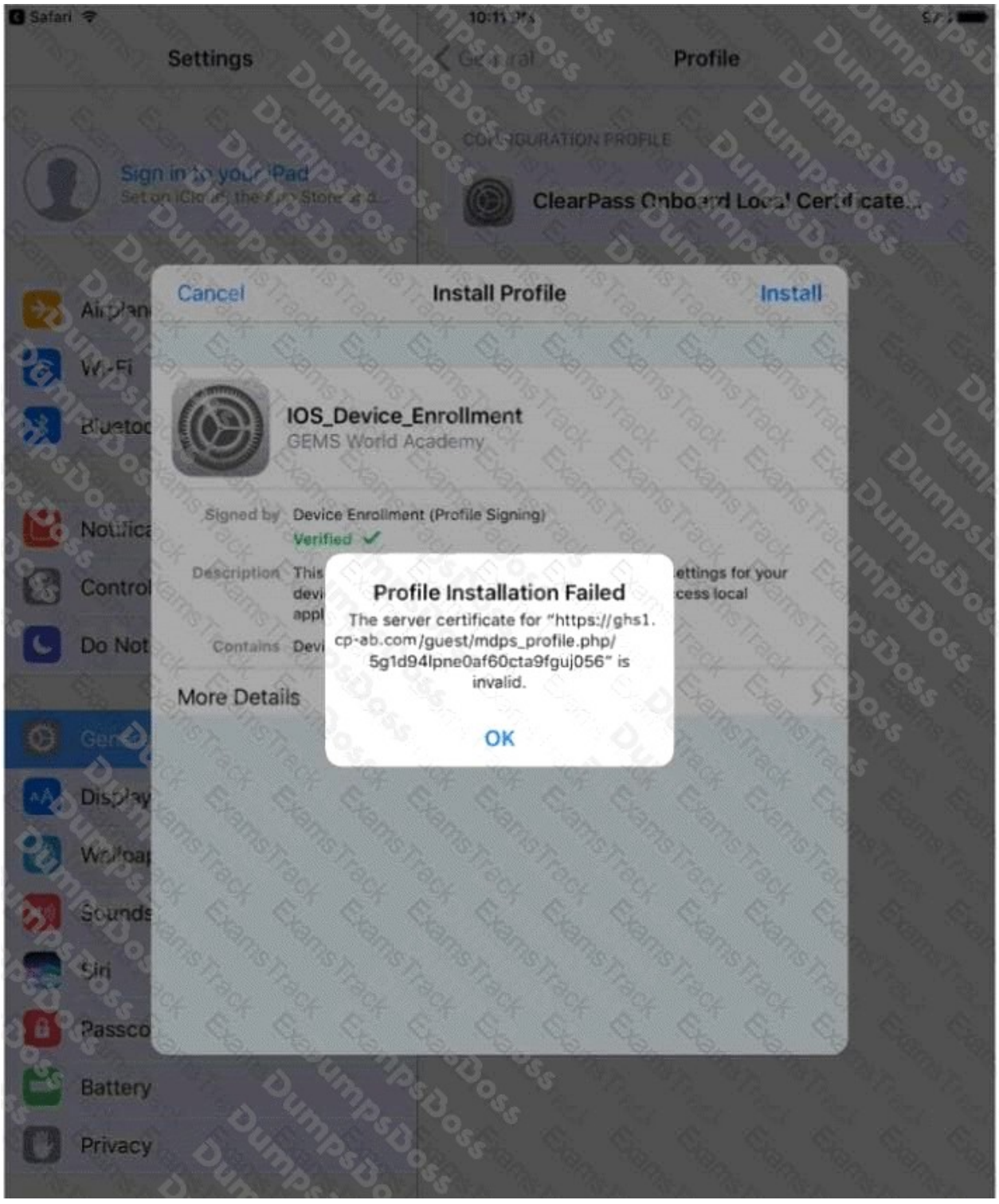
https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Refer to the exhibit.




A customer has configured Onboard in his lab ClearPass server and Windows devices work as expected but cannot get the Apple iOS devices to Onboard successfully Where would you look to troubleshoot the issue? {Select two)

**A.** Check if the customer installed the internal PKI Root certificate presented by the ClearPass during the provisioning process.

**B.** Check if the customer has installed the same internal PKI signed RADIUS server certificate as the HTTPS server certificate.

**C.** Check if the customer has installed a custom HTTPS certificate for iOS and another internal PKI HTTPS certificate for other devices.

**D.** Check if a DNS entry is available for the ClearPass hostname in the certificate, resolvable from the DNS server assigned to the client.

**E.** Check if the ClearPass HTTPS server certificate installed in the server is issued by a trusted commercial certificate authority.

**ANSWER: D E**

**Explanation:**

Check if a DNS entry is available for the ClearPass hostname in the certificate, resolvable from the DNS server assigned to the client. During iOS Onboard enrollment, the device must connect to ClearPass by using the hostname advertised in the HTTPS certificate. That name must resolve from the network to which the device is currently connected, and it must match the certificate identity. A reachable, correctly resolved fully qualified domain name allows iOS to establish the HTTPS session required to download and install the provisioning profile.

Check if the ClearPass HTTPS server certificate installed in the server is issued by a trusted commercial certificate authority. iOS evaluates the HTTPS connection before the onboarding profile can deliver enterprise trust material or device credentials. A certificate chaining to a broadly trusted public commercial authority avoids an initial trust dependency and lets iOS validate ClearPass without requiring a preinstalled private PKI root certificate. The certificate should also be valid, unexpired, and include the ClearPass DNS name in its subject alternative name. Apple documents certificate trust and payload behavior in its certificate payload settings guide; ClearPass configuration concepts are covered in the ClearPass Policy Manager documentation.

**QUESTION NO: 2**

Under OnBoard Management and Control, which option will deny the user from re-enrolling one of his devices with Onboard?

View by Certificate >> Click on the device >> Delete certificate

**A.** Delete this client certificate View by Dev >> Click on the device

**B.** Manage Access >> Deny access to this device View by Certificate

**C.** Click on the device >> Revoke certificate >> Revoke this client certificate

**D.** View by Username >> Click on the user >> Delete Actions >> Delete all devices

**ANSWER: B**

**Explanation:**

**Manage Access >> Deny access to this device View by Certificate** is the appropriate action because Onboard Management and Control maintains a device-level access status in addition to the client certificate itself. Setting a device to denied blocks the user from using Onboard to enroll that particular device again. This is the intended administrative control when a device must be prevented from obtaining a replacement Onboard certificate, such as when it is no longer authorized, has been lost, or is no longer compliant with organizational policy.

ClearPass Onboard tracks devices and their issued credentials so that administrators can manage enrollment eligibility independently from routine certificate lifecycle actions. The deny-access control applies an explicit restriction to the managed device record, allowing the administrator to preserve a clear management decision and prevent a subsequent enrollment attempt for that device. This distinction is important in environments that use self-service provisioning, where users would otherwise be able to request a new certificate after removal of an existing credential.

For ClearPass Policy Manager and Onboard administrative guidance, see the Aruba ClearPass Policy Manager User Guide and the Aruba ClearPass Policy Manager product documentation.

## QUESTION NO: 3

Refer to the exhibit.

A customer has configured Onboard in a cluster. After the Primary server's failure, the BYOD devices fail to connect to the network. Which step below is the best starting point when troubleshooting'

**A.** Verify the CPPM hostname in OCSP URL under TLS authentication method is updated to localhost instead of primary server's hostname.

**B.** Reboot the active ClearPass server and reconnect the client to the SSID by selecting the correct certificate when prompted.

**C.** Check if a DNS entry is available for the ClearPass hostname in the certificate, resolvable from the DNS server assigned to the client.

**D.** Check EAP certificate on the secondary node is issued by the same common root Certificate Authority (CA).

## ANSWER: A

**Explanation:**

Verify the CPPM hostname in the OCSP URL under the TLS authentication method is updated to localhost instead of the primary server's hostname. ClearPass Onboard commonly uses client certificates for BYOD access, and ClearPass must be able to perform certificate-status checking as part of EAP-TLS processing. If the TLS authentication method on the remaining active cluster member is configured to reach an OCSP responder by using the failed primary server's hostname, certificate validation can be interrupted when that primary node is unavailable. This can prevent otherwise valid Onboard-issued client certificates from authenticating to the network.

Using `localhost` for the locally hosted OCSP responder makes the certificate-status request independent of which ClearPass node is currently processing authentication. Each Policy Manager node checks the responder on itself rather than relying on the availability or name resolution of a specific primary appliance. Therefore, this setting is an appropriate first troubleshooting check immediately after a primary-node failure in an Onboard cluster. Aruba's ClearPass documentation

describes the cluster architecture and high-availability behavior in the ClearPass cluster overview, and its certificate-validation configuration is covered in the EAP-TLS configuration documentation.

## QUESTION NO: 4

The customer would like to add a default common self-registration sponsor email under the initial value on all the ten self-registration pages created for different locations except for the guest registration page created for Sunnyvale location to use a different sponsor email in initial value. Under self-registration form fields, you have "Edit" and "Edit Base Field"

Which edit options will you choose to make minimal configuration changes to implement the customer's requirement? (Select two)

**A.** Update the common sponsor email by clicking the "Edit" option of the sponsor email form field on the one of the self-registration register form page

**B.** Update the sponsor email by clicking on both "Edit" and "Edit Base Field" options of the sponsor_email filed on the Sunnyvale register page

**C.** Update the specific sponsor email by clicking on "Edit Base Field" option of the sponsor_email form filed on the Sunnyvale location register form page

**D.** Update the common sponsor email by clicking the "Edit Base Field" option of the sponsor_email form field on the one of the self-registration form page

**E.** Update the specific sponsor email by clicking on the "Edit" option of the sponsor_email form filed on the Sunnyvale self-registration register form page

## ANSWER: D E

**Explanation:**

The correct approach is to update the shared sponsor-email field through *"Edit Base Field"* on any one of the self-registration forms, then update the Sunnyvale-specific sponsor email through *"Edit"* on the Sunnyvale self-registration form. ClearPass Guest form fields can inherit their configuration from a base field. Editing that base field changes the common field definition, including its configured initial value, wherever that base field is used. This provides the required default sponsor email across the ten location forms without repeating the same update on each page.

After the common base value is configured, using *"Edit"* on the Sunnyvale form creates or maintains a form-specific field configuration for that page. The Sunnyvale page can therefore retain a distinct initial sponsor-email value while the other forms continue to use the inherited common value. This is the minimal-change design because it uses one shared base-field update for the standard behavior and one local override only where an exception is required. Aruba ClearPass Guest documentation describes the use of form fields and their reusable base-field configuration in the Guest administration workflow. See the Aruba ClearPass Guest documentation and the ClearPass Guest configuration guide.

## QUESTION NO: 5

Refer to the exhibit.

A customer is doing a new ClearPass installation and is setting up clustering between two ClearPass servers running a 6.8.6 version. The ClearPass server failed to add the subscriber node. The customer was able to login to the console of the ClearPass server with the same CLI password used during the cluster setup. The customer has sent you the screenshots seeking your support Why did an attempt to add a subscriber node failed showing that error?

**A.** The data and time in the subscriber was not synchronized with the NTP server

**B.** The subscriber server is running with a default self -signed HTTPS certificate

**C.** The default database certificate used in the publisher server is not a valid certificate

**D.** The subscriber server is running with a public signed and trusted HTTPS certificate

## ANSWER: B

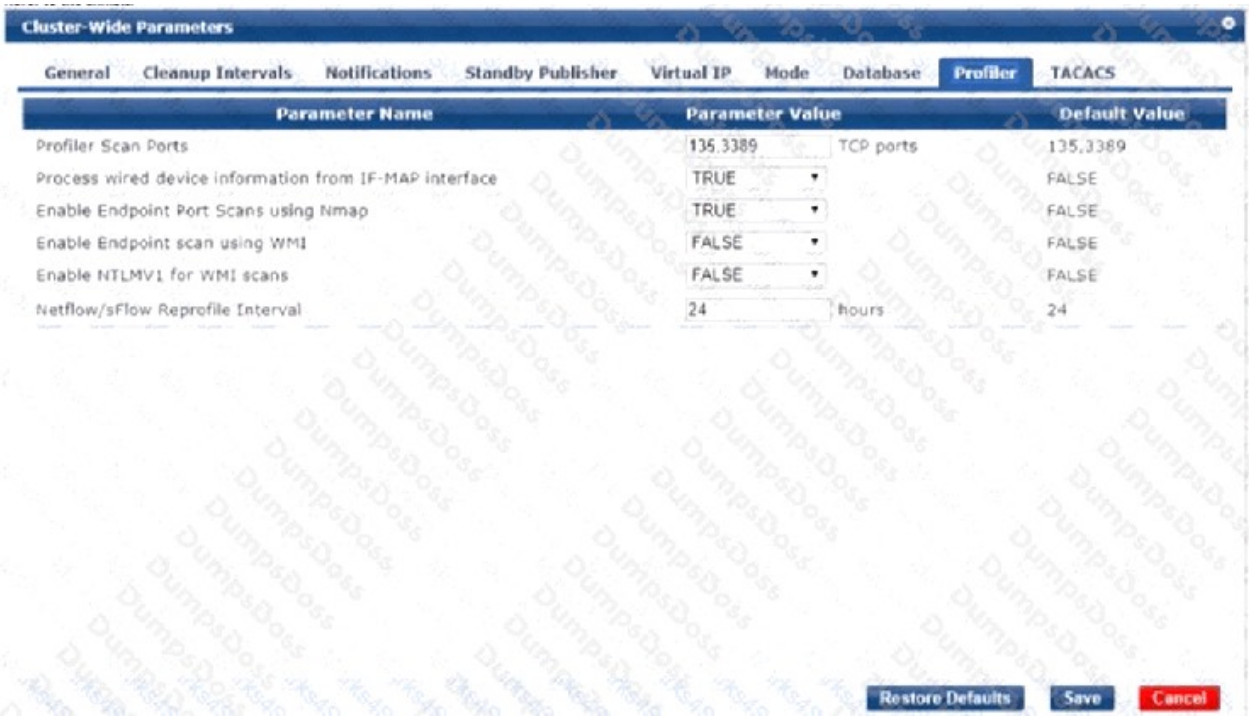
**Explanation:**

The subscriber server is running with a default self -signed HTTPS certificate. When a ClearPass node is added to a cluster, the publisher must establish a secure HTTPS connection to the prospective subscriber and validate the certificate presented by that node. A default self-signed HTTPS certificate is not inherently trusted by the other ClearPass appliance because it is not issued by a trusted certificate authority and its issuing certificate is not already in the peer's trust store. As a result, the secure connection required to complete cluster formation cannot be validated, even when the CLI credentials are correct and console login succeeds.

Before joining the node, install an HTTPS server certificate on the subscriber that is issued by a CA trusted by the publisher, including any required intermediate CA certificates. Alternatively, import the applicable issuing/self-signed certificate into the publisher's trust list when that deployment method is appropriate for the organization. ClearPass documentation describes cluster administration and the certificate requirements for secure inter-node communication in its ClearPass 6.8 cluster documentation and provides certificate-management guidance in the ClearPass server certificates documentation.

## QUESTION NO: 6

Refer to the exhibit.




A customer has incomplete information for endpoints in the Endpoint Repository. In order to make accurate decisions about what types of devices are connecting to the network. ClearPass is enabled to process the device information from IF-MAP interface, but no updates are received. What can the customer do to update those endpoints using IF-MAP?

**A.** Configure ClearPass Management IP in the DHCP Helper address

**B.** Configure IF-MAP on all networking devices to send additional information to ClearPass

**C.** Configure IF-MAP only on Aruba Mobility Controller, providing ClearPass username and password

**D.** Configure the authentication service to Audit the endpoints using, the embedded Nmap Server

## ANSWER: A

**Explanation:**

Configuring the ClearPass Management IP in the DHCP helper address causes DHCP relay devices to forward DHCP client exchanges to ClearPass in addition to the normal DHCP server. ClearPass can then inspect the forwarded DHCP data,

including attributes such as the client MAC address, requested options, vendor class, and host information. This data is used to create or enrich Endpoint Repository records and supports more reliable endpoint profiling and policy decisions. DHCP information is particularly useful because it is normally observed as a device first joins the network or renews its lease, providing ClearPass with fresh endpoint context without requiring a separate authentication event. The ClearPass management address must be reachable from the relay-capable network device, and the forwarding configuration should preserve delivery to the organization's production DHCP service as well. Once DHCP traffic reaches ClearPass, the endpoint information can be correlated with the identity and contextual information available through the enabled integrations, allowing endpoint records to be updated. Aruba documents endpoint profiling and repository behavior in the ClearPass Policy Manager documentation. Additional Aruba ClearPass technical documentation is available through the Aruba ClearPass TechDocs portal.

## QUESTION NO: 7

You art deploying Cleat Pass Policy Manager with Guest functionality for a customer with multiple Aruba Networks Mobility Controllers. The customer wants to avoid SSL errors during guest access but due to company security policy cannot use a wildcard certificate on

ClearPass or the Controllers.

What is the most efficient way to configure the customer's guest solution? (Select two.)

**A.** Install the same public certificate on all Controllers with the common name "controller.{company domain)

**B.** Build multiple Web Login pages with vendor settings configured for each controller.

**C.** Build one Web Login page with vendor settings for captiveportal-controller.companydomain.

**D.** Install multiple public certificates with a different Common Name on each controller

## ANSWER: A C

**Explanation:**

Installing the same publicly trusted certificate on every controller with the common name *controller.companydomain* provides a single certificate identity that guest clients can validate consistently, without using a wildcard certificate. The DNS name must resolve appropriately to the controller that is servicing the guest client, and the certificate must include the full hostname used in the captive-portal redirect. Using a certificate issued by a publicly trusted certification authority is important because unmanaged guest devices generally do not have an enterprise private CA certificate installed.

Building one Web Login page with vendor settings for *captiveportal-controller.companydomain* complements that approach by standardizing the controller hostname referenced by the ClearPass Guest portal workflow. A common, certificate-matching captive-portal hostname avoids maintaining separate guest pages and separate controller-specific certificate identities, while still allowing the deployment to scale across multiple Mobility Controllers. This design reduces operational overhead and ensures that the HTTPS name a guest sees is aligned with the installed certificate's subject identity. Aruba's guest-access documentation describes configuring external captive portals and their controller integration, while public CA guidance explains the hostname-validation requirement for TLS certificates. See Aruba ClearPass Guest documentation and RFC 9525: Service Identity in TLS.

## QUESTION NO: 8

A customer is deploying EAP-TLS for corporate wireless access. The supplicants must validate the identity and trustworthiness of the ClearPass EAP server before presenting a client certificate.

Which certificate-validation checks should be configured on the supplicants? (Select three.)

**A.** Validate the trusted CA chain of the EAP server certificate.

**B.** Validate the validity dates of the EAP server certificate.

**C.** Validate the configured server identity against the certificate identity.

**D.** Accept any server certificate if the client certificate is issued by a trusted CA.

**E.** Disable server-certificate validation when using a private enterprise CA.

**ANSWER: A B C**

**Explanation:**

Supplicants should be configured to validate the issuing CA chain for the ClearPass server certificate, validate that the certificate is within its validity period, and validate the expected server identity against the certificate identity. These checks help prevent a client from sending credentials or a client certificate to an untrusted RADIUS server.

The ClearPass EAP server certificate must also be appropriate for TLS server authentication and include an identity that matches the name configured by the client. In current certificate processing, the Subject Alternative Name extension is used for hostname identity matching. See the RFC 5280 certificate profile and the ClearPass certificate documentation.

## QUESTION NO: 9

What configuration steps should you follow to add terms and conditions page on Guest self-registration for CPPM? (Select two).

**A.** Edit the creetoraccepiterms form field in register page and change HTML section by pointing the hyperlink to the HTML file uploaded

**B.** Edit the accept_terms form field in receipt page and change HTML section by pointing the hyper link to the HTML file uploaded m Guest Manager

**C.** Create an HTML page with custom terms and condition and upload it to public files under Clearpass Guest -> configuration -> content manager

**D.** Edit the create_or_accept_terms form field in receipt page and change the HTML section by pointing the hyperlink to the uploaded HTML file

**E.** Create an HTML page with custom terms and condition and upload it to private files under Clearpass Guest -> configuration -> content manager

**ANSWER: C D**

**Explanation:**

To present custom terms and conditions during ClearPass Guest self-registration, first create the terms content as an HTML page and upload it through ClearPass Guest's Content Manager under *Public Files*. Public files are appropriate because an unauthenticated visitor must be able to retrieve the linked document while completing registration. After the file is available, customize the self-registration receipt page's `create_or_accept_terms` form field and update its HTML to link to the uploaded terms-and-conditions file. This field is used to present the acceptance workflow associated with creating or accepting guest access terms, so linking the hosted document there makes the terms available at the relevant point in the guest journey. Aruba's ClearPass Guest documentation describes Content Manager as the location for managing files used by guest pages and explains how page and form-field customization supports HTML-based guest workflow changes. See the ClearPass Guest Content Manager documentation and the ClearPass Guest forms reference.

## QUESTION NO: 10

A customer uses Active Directory attributes and ClearPass role-mapping policies to classify authenticated users before enforcement is evaluated.

Which statements are true about ClearPass role mapping? (Select three.)

**A.** Role-mapping rules can evaluate attributes returned by an Active Directory authorization source.

**B.** A user can be assigned more than one ClearPass role when multiple role-mapping rules match.

**C.** Enforcement-policy rules can use ClearPass roles as conditions.

**D.** Role mapping returns an Aruba controller user role directly without an enforcement profile.

**E.** Role mapping is evaluated only after an enforcement profile has been returned.

**ANSWER: A B C**

**Explanation:**

Role-mapping policies evaluate authorization attributes returned by configured authorization sources, such as Active Directory. A rule can assign one or more ClearPass roles when its conditions are met. These roles are then available to the enforcement policy, which can use them with other request and authorization attributes to select the correct enforcement profile.

ClearPass roles are internal policy roles and are distinct from the Aruba-User-Role attribute that might be returned to an Aruba network access device as an enforcement result. This separation allows ClearPass to use multiple sources of context before choosing the final access-control action. See the ClearPass Role Mapping documentation.

## QUESTION NO: 11

Refer to the exhibit.

A customer has just configured a Posture Policy and the T 2 -Health check Service. Next they installed the OnGuard Agent on a test client connected to the Secure_Employee SSID. When they check Access Tracker they see many WEBAUTH requests are being triggered What could be the reason'

**A.** The OnGuard Agent trigger the events based on changing the Health Status.

**B.** The OnGuard Agent is connecting to the Data Port interface on ClearPass.

**C.** TCP port 6658 is not allowed between the client and the ClearPass server.

**D.** OnGuard Web-Based Health Check interval has been configured to three minutes.

**ANSWER: D**

**Explanation:**

**OnGuard Web-Based Health Check interval has been configured to three minutes.** is correct because the Web-Based Health Check service initiates periodic web-authentication transactions to obtain and evaluate the endpoint's posture status. When its interval is set to three minutes, a client associated with the Secure_Employee SSID will generate a new WEBAUTH request approximately every three minutes. Therefore, multiple recurring WEBAUTH entries in Access Tracker are an expected result of that service configuration rather than necessarily indicating a connectivity or authentication failure.

ClearPass uses Web-Based Health Check as part of its OnGuard posture workflow to collect health information and apply the configured posture policy. The interval setting determines how frequently this health-check process runs. In a test environment, especially with a short interval, Access Tracker can quickly accumulate many requests from the same endpoint. Administrators should account for this expected request frequency when validating the service and when selecting an interval appropriate to the organization's endpoint count and desired posture re-evaluation cadence. Aruba's ClearPass documentation describes OnGuard posture assessment and Web-Based Health Check configuration in the ClearPass Policy Manager OnGuard documentation and related ClearPass technical documentation.

## QUESTION NO: 12

Which statement is true about Radius IETF attributes Called-Stat ion-Id and Calling-

Station-Id?

**A.** Called-Station-Id contains the mac address of the supplicant while Calling-Station-Id contains the mac address of the authenticator.

**B.** Called-Station-Id contains the mac address of the supplicant and SSID name while Calling-Station-Id contains the mac address of the authenticator.

**C.** Called-Station-Id contains the mac address of the authenticator while Calling-Station-Id contains the mac address of the supplicant.

**D.** Called-Station-Id contains the mac address of the authenticator while Calling-Station-Id contains the mac address of the supplicant and SSID name.

**E.** Called-Station-Id contains the MAC address of the authenticator and SSID name, while Calling-Station-Id contains the MAC address of the supplicant.

**ANSWER: E**

**Explanation:**

The accurate statement is that **Called-Station-Id** identifies the station being called—normally the wireless authenticator/access point—and, for IEEE 802.11 access, is commonly formatted as the AP radio MAC address followed by a colon and the SSID. **Calling-Station-Id** identifies the station initiating the connection, which is the supplicant/client, and is normally its MAC address. This distinction is important in ClearPass policy design because Called-Station-Id can be used to make decisions based on the AP and WLAN/SSID through which authentication arrived, while Calling-Station-Id identifies the endpoint attempting access. RFC 2865 defines Called-Station-Id as the identifier for the called station and Calling-Station-Id as the identifier for the calling station. RFC 3580 provides the IEEE 802.1X wireless usage guidance, including the recommended AP-MAC:SSID representation for Called-Station-Id and the client MAC representation for Calling-Station-Id. See RFC 2865, Called-Station-Id and RFC 3580, IEEE 802.1X RADIUS usage.