



HPE6-A81^{Q&As}

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/hpe6-a81.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

A customer is planning to implement machine and user authentication on infrastructure with one Aruba Controller and a single ClearPass Server.

What should the customer consider while designing this solution? (Select three.)

- A. The Windows User must log off, restart or disconnect their machine to initiate a machine authentication before the cache expires.
- B. The machine authentication status is written in the Multi-master cache on the ClearPass Server for 24 hrs.
- C. Onboard must be used to install the Certificates on the personal devices to do the user and machine authentication.
- D. The Customer should enable Multi-Master Cache Survivability as the Aruba Controller will not cache the machine state.
- E. Machine Authentication only uses EAP TLS, as such a PKI infrastructure should be in place for machine authentication.
- F. The customer does not need to worry about Multi-Master Cache Survivability because the Controller will also cache the machine state.

Correct Answer: BCE

QUESTION 2

When is it recommended to use a certificate with multiple entries on the Subject Alternative Name?

- A. The ClearPass servers are placed in different OnGuard zones to allow the client agent to send SHV updates.
- B. Using the same certificate to Onboard clients and the Guest Captive Portal on a single ClearPass server.
- C. The primary authentication server is not available to authenticate the users.
- D. The ClearPass server will be hosting captive portal pages for multiple FQDN entries

Correct Answer: A

QUESTION 3

What is used to validate the EAP Certificate? (Select three.)

- A. Common Name
- B. Date
- C. Key usage
- D. Server Identity



E. SAN entries

F. Trust chain

Correct Answer: ACF

QUESTION 4

While configuring a guest solution, the customer is requesting that guest user receive access for four hours from their first login. Which Guest Account Expiration would you select?

A. expire_after

B. do_expire

C. expire_time

D. expire_postlogin

Correct Answer: A

QUESTION 5

Refer to the exhibit:



Monitoring > Live Monitoring > Access Tracker

Access Tracker Oct 02, 2019 03:43:03 EDT Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] p50-t07-cp1 (10.1.79.1) Last 1 day before Today Edit

Filter: Login Status contains acc Go Clear Filter Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:02:13
2.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:02:07
3.	10.1.79.1	RADIUS	mike07	HS_Branch Onboard Provisioning	ACCEPT	2019/10/02 03:00:55

aruba ClearPass Onboard

Menu

Guest Onboard

- Start Here
- Certificate Authorities
- Management and Control
 - Start Here
 - View by Device
 - View by Username
 - View by Certificate
 - Usage
- Configuration
 - Start Here
 - Network Settings
 - iOS Settings
 - Windows Applications
- Deployment and Provisioning
 - Start Here
 - Configuration Profiles
 - Provisioning Settings
- Self-Service Portal

Common Name	Certificate Authority	Serial Number	Type	Valid From	Valid To	Device Type
mike07	HS_Branch	8	tls-client	2019-10-02 02:45:47-04:00	2020-10-01 03:15:47-04:00	Windows

View certificate: Trust Chain Export certificate Delete certificate

Certificate Information

Certificate Details
Details about the certificate and its owner.

Issued To: mike07

Revoked At: Wednesday, 02 October 2019, 3:01 AM

Revoked: This certificate has been revoked.

Valid From: Wednesday, 02 October 2019, 2:45 AM

Valid To: Thursday, 01 October 2020, 3:15 AM

Country US
Locality Sunnyvale
Organization Aruba
Common Name mike07
State California

Subject: mdpUsername mike07
mdpDeviceName Windows 10
mdpDeviceType Windows



Certificate Authorities Create new

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
p50-t07-cp1: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.
p50-t07-cp2: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS devices.

How do I fix this problem?

Use this list to manage certificate authorities.

Name	Mode	Status	Expiry	OCSP URL
HS_Branch	root	Valid	2029-09-25T03:19:47-04:00	http://p50-t07-cp1/guest/mdps_ocsp.php/2
Local Certificate Authority <small>This is the default certificate authority.</small>	root	Valid	2029-06-25T21:25:44-04:00	http://p50-t07-cp1/guest/mdps_ocsp.php/1

Refresh 1

Configuration » Services » Edit - HS_Branch Onboard Provisioning

Services - HS_Branch Onboard Provisioning

- Summary
- Service
- Authentication
- Authorization
- Roles
- Enforcement

Service:

Name: HS_Branch Onboard Provisioning

Description: 802.1X wireless access service authenticating users prior to device provisioning with Onboard, and after device provisioning is complete

Type: Aruba 802.1X Wireless

Status: Enabled

Monitor Mode: Disabled

More Options: Authorization

Service Rule:

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3. Radius:Aruba	Aruba-Essid-Name	EQUALS	secure-HS-5007

Authentication:

Authentication Methods: 1. [EAP PEAP]
2. [EAP TLS]

Authentication Sources: 1. [Onboard Devices Repository]
2. AD1
3. AD2

Strip Username Rules: /user

Service Certificate: -

Authorization:

Authorization Details: 1. AD1
2. AD2

After the helpdesk revoked the certificate of a device reported to be lost by an employee, the lost device was seen as connected successfully to the secure network. Further testing has shown that device revocation is not working.

What steps should you follow to make device revocations work?

A. Copy the default [EAP-TLS with OSCP Enabled] authentication method and set The Verify certificate using OSCP option as required then update the correct OSCP URL link of the OnBoard CA. Remove EAP-TLS and map the custom



created method to the OnBoard Authorization Service.

B. copy the default [EAP-TLS with OSCP Enabled] authentication method and set the verify certificate using OSCP: option as "required" then configure the correct OSCF URL link for the OnBoard CA. Remove EAP-TLS and map the new [EAP-TLS with OSCP Enabled] method to the 802 1X Radius Service.

C. Remove the EAP-TLS authentication method configuration changes are required and add "EAP-TLS with OSCP Enabled" authentication method in the OnBoard Provisioning service. No other configuration changes are required.

D. Edit the default [EAP-TLS with OSCP Enabled] authentication method and set the Verify certificate using OSCP option as required then update the correct OSCP URL link of the OnBoard CA Remove EAP-TLS and map the new [EAP-TLS with OSCP Enabled] method to the OnBoard Provisioning Service.

Correct Answer: C

[HPE6-A81 VCE Dumps](#)

[HPE6-A81 Practice Test](#)

[HPE6-A81 Braindumps](#)