HPE6-A77 Q&As

Aruba Certified ClearPass Expert Written

Pass HP HPE6-A77 Exam with 100% Guarantee

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

https://www.geekcert.com/hpe6-a77.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

You are deploying ClearPass 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 customers guest solution? (Select two.)

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

B. Install the same public certificate on all Controllers with the common name "controller {company domain}"

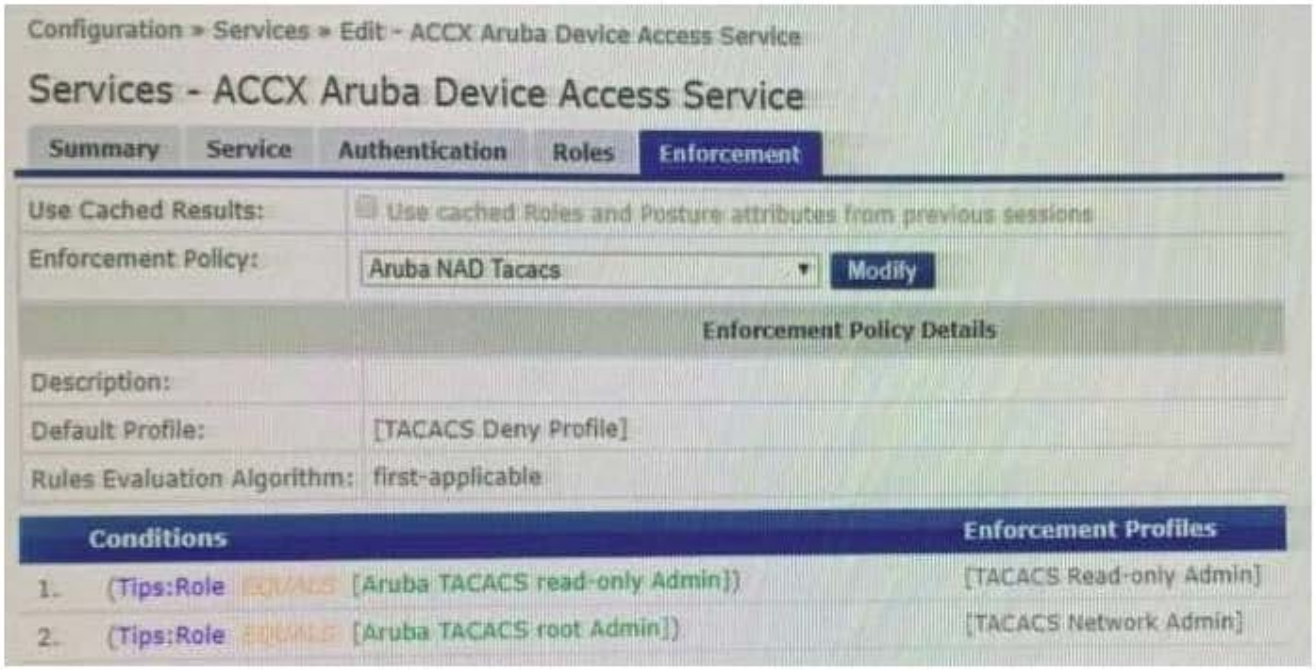
C. Build one Web Login page with vendor settings for controller {company domain)

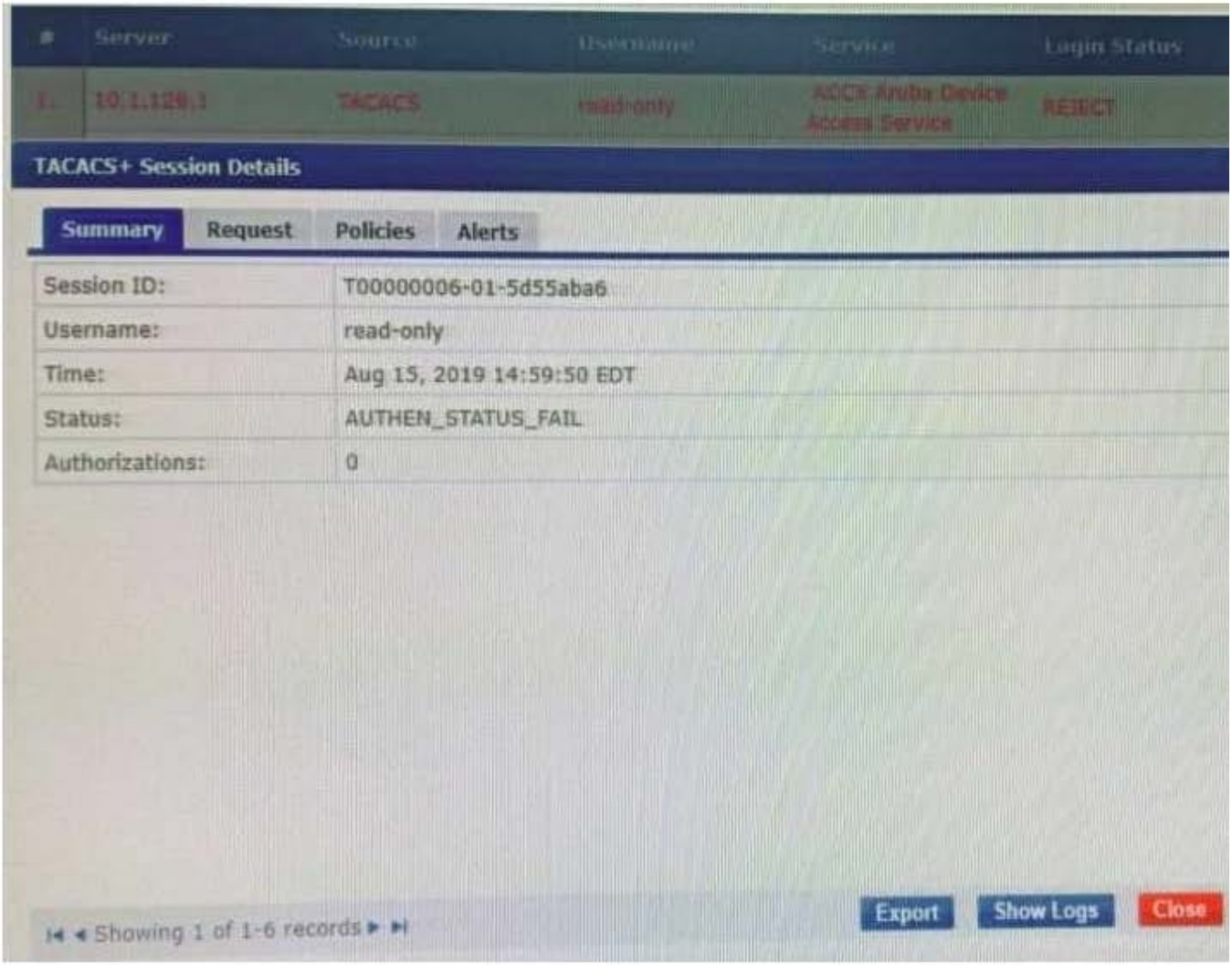
D. Install multiple public certificates with a different Common Name on each controller

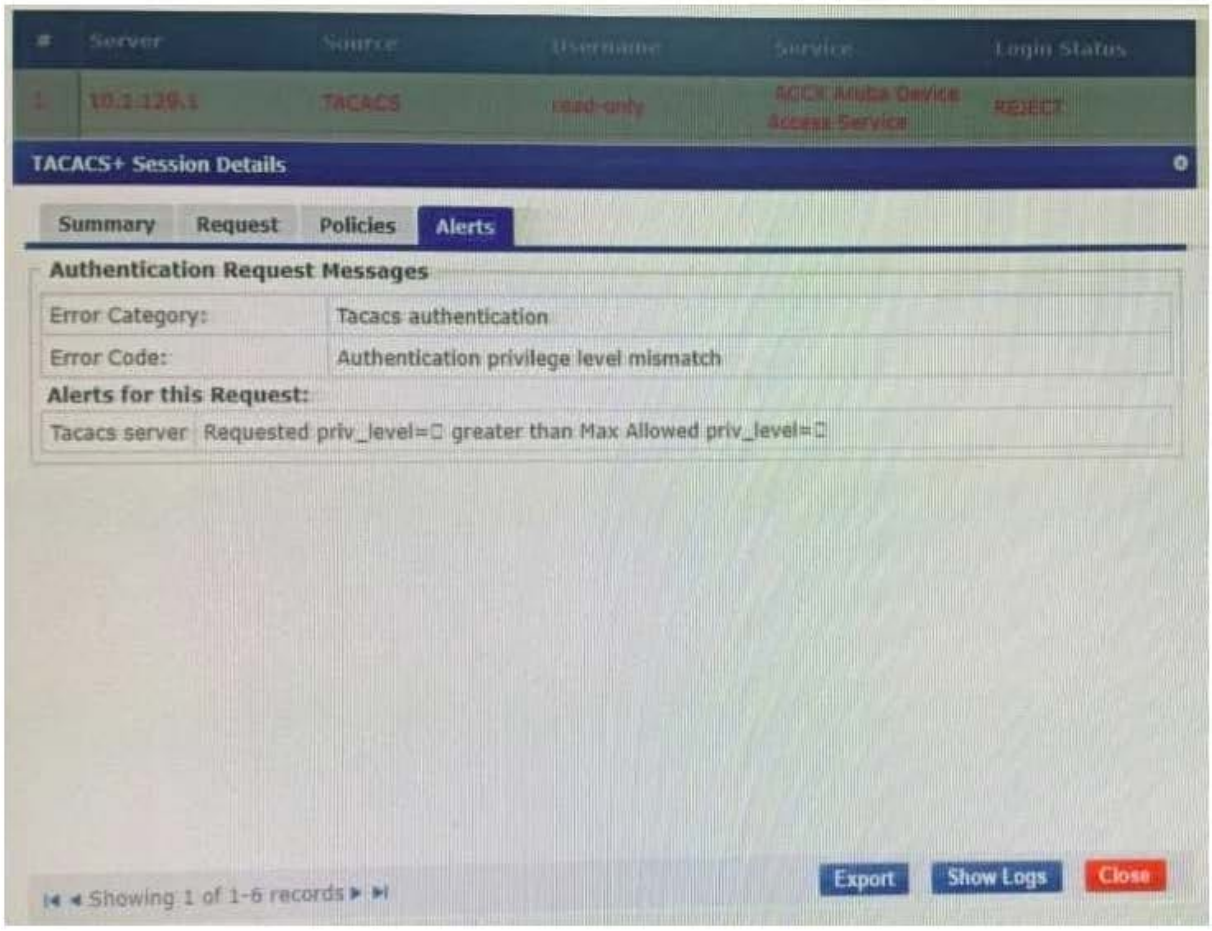
Correct Answer: AB

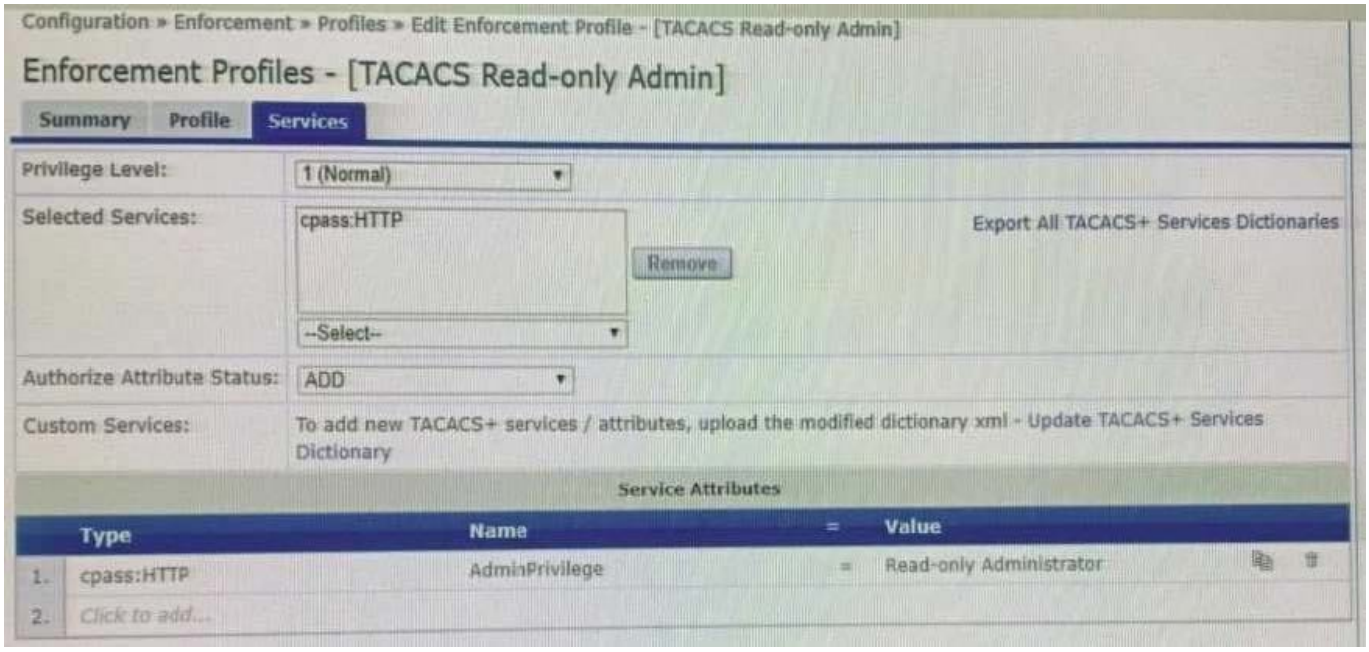
QUESTION 2

Refer to the exhibit:


Configuration » Services » Edit - ACCX Aruba Device Access Service
Services - ACCX Aruba Device Access Service
Summary
Service
Authentication
Roles
Enforcement
Use Cached Results:
Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:
Aruba NAD Tacacs
Modify
Enforcement Policy Details
Description:
Default Profile:
[TACACS Deny Profile]
Rules Evaluation Algorithm:
first-applicable
Conditions
Enforcement Profiles
1. (Tips:Role [Aruba TACACS read-only Admin])
[TACACS Read-only Admin]
2. (Tips:Role [Aruba TACACS root Admin])
[TACACS Network Admin]


Server
Source
Username
Service
Login Status
TACACS
read-only
REJECT
TACACS+ Session Details
Summary
Request
Policies
Alerts
Session ID:
T00000006-01-5d55aba6
Username:
read-only
Time:
Aug 15, 2019 14:59:50 EDT
Status:
AUTHEN_STATUS_FAIL
Authorizations:
0
Showing 1 of 1-6 records
Export
Show Logs
Close


Server
Source
Username
Service
Login Status
TACACS
read-only
REJECT
TACACS+ Session Details
Summary
Request
Policies
Alerts
Authentication Request Messages
Error Category:
Tacacs authentication
Error Code:
Authentication privilege level mismatch
Alerts for this Request:
Tacacs server
Requested priv_level=□ greater than Max Allowed priv_level=□
Showing 1 of 1-6 records
Export
Show Logs
Close



A customer is trying to configure a TACACS Authentication Service for administrative access to the Aruba Controller, During testing the authentication is not successful.

Given the screen shot what could be the reason for the Login status REJECT?

A. The password used by the administrative user, user is wrong.

B. The Enforcement profile is not designed to be used on Aruba Controller.

C. The Read-only Administrator role does not exist on the Controller.

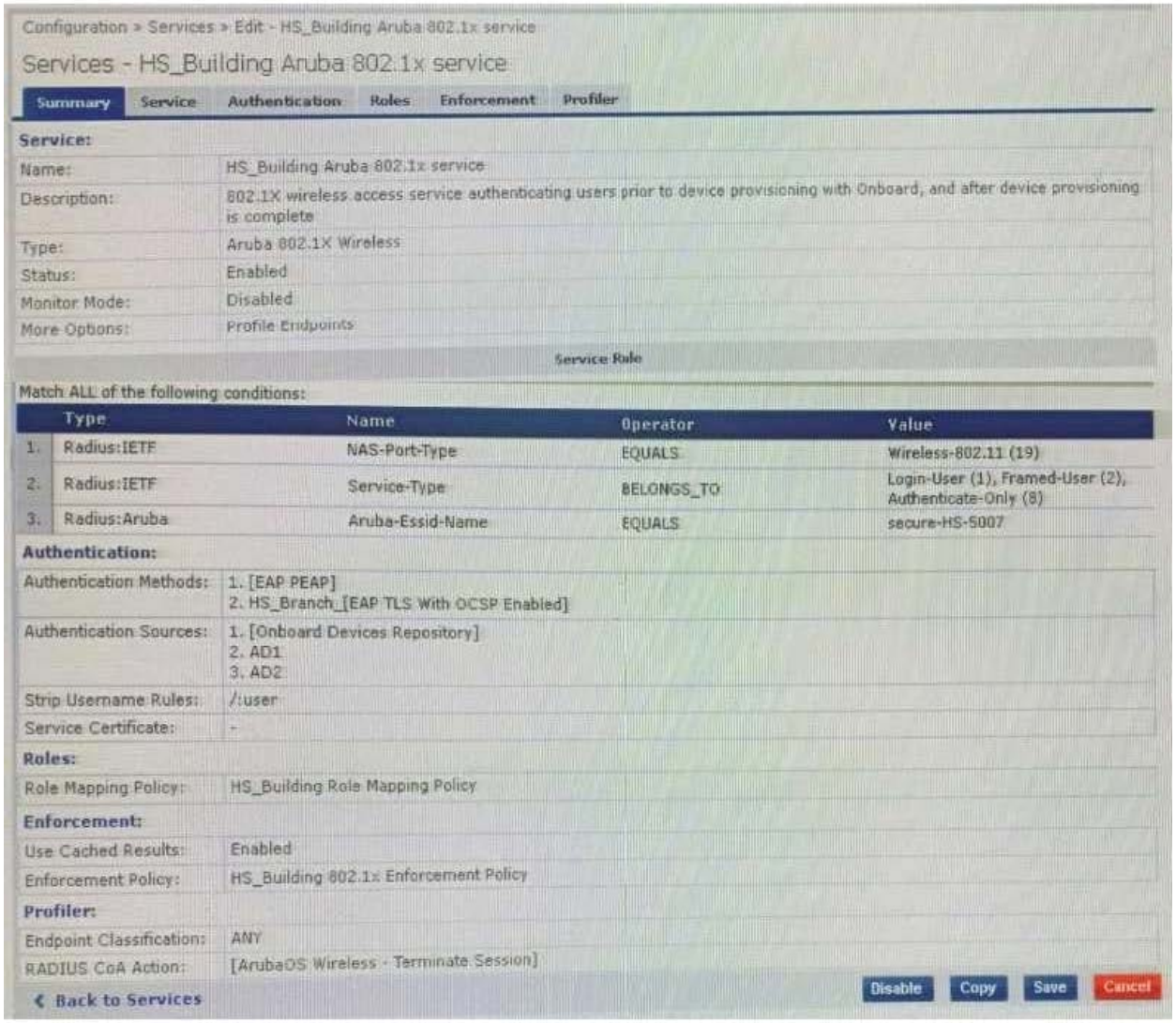
D. The Enforcement profile used is not a TACACS profile.

Correct Answer: A

QUESTION 3

Refer to the exhibit:


Request Details
Summary
Input
Output
Alerts
Login Status: REJECT
Session Identifier: R00000218-01-5d9db68b
Date and Time: Oct 09, 2019 06:29:34 EDT
End-Host Identifier: 78D29437BD68 (Computer / Windows / Windows 10)
Username: andy07
Access Device IP/Port: 10.1.70.100:0 (ArubaController / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: HS_Building Aruba 802.1x service
Authentication Method: EAP-PEAP,EAP-MSCHAPv2
Authentication Source: AD:AD1.aruba1.local
Authorization Source: AD1
Roles: [Other], [User Authenticated]
Enforcement Profiles: [Deny Access Profile]
Service Monitor Mode: Disabled
Online Status: Not Available
Showing 1 of 1-20 records
Show Configuration
Export
Show Logs
Close
Request Details
Summary
Input
Output
Alerts
Error Code: 206
Error Category: Authentication failure
Error Message: Access denied by policy
Alerts for this Request
RADIUS Applied 'Reject' profile



Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary | Service | Authentication | Roles | Enforcement | Profiler

Service:

Name:	HS_Building Aruba 802.1x service
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:	Profile Endpoints

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. HS_Branch_[EAP TLS With OCSP Enabled]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2
Strip Username Rules:	/:user
Service Certificate:	-

Roles:

Role Mapping Policy:	HS_Building Role Mapping Policy

Enforcement:

Use Cached Results:	Enabled
Enforcement Policy:	HS_Building 802.1x Enforcement Policy

Profiler:

Endpoint Classification:	ANY
RADIUS CoA Action:	[ArubaOS Wireless - Terminate Session]

« Back to Services

Disable | Copy | Save | Cancel


Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary | Service | Authentication | Roles | Enforcement | Profiler

Role Mapping Policy: HS_Building Role Mapping Policy | Modify | Add New Role Mapping Policy

Role Mapping Policy Details

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
1.	(Connection:Client-Mac-Address BELONGS_TO_GROUP VIP User MAC)	VIP User
2.	(Authorization:Corp SQL:MAC EXISTS)	Corp SQL Tablet
3.	(Authorization:[Endpoints Repository]:Category EQUALS VoIP Phone)	IP Phone
4.	(Authorization:[Endpoints Repository]:Category EQUALS SmartDevice)	Personal SmartDevice
5.	(Authorization:[Endpoints Repository]:Category EQUALS Point of Sale devices)	Vending Machine
6.	(Authorization:[Endpoints Repository]:Category EQUALS Printer) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS CANON INC.)	Printer
7.	(Authorization:[Endpoints Repository]:Category EQUALS Network Camera) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS Axis Communications AB)	IP Camera


Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary | Service | Authentication | Roles | Enforcement | Profiler

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: HS_Building 802.1x Enforcement Policy | Modify | Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
2.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
3.	(Authentication:OuterMethod EQUALS EAP-TLS) AND (Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
4.	(Tips:Role EQUALS VIP User)	Aruba VIP Full Access Profile
5.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0))	Aruba Full Access Profile
6.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100))	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture NOT_EQUALS HEALTHY (0))	Redirect to Aruba Quarantine Profile

Your company has a postgres SQL database with the MAC addresses of the company-owned tablets You have configured a role mapping condition to tag the SQL devices. When one of the tablets connects to the network, it does not get the correct role and receives a deny access profile.

How would you resolve the issue?

A. Remove SQL condition from role mapping policy and add it under the enforcement policy conditions.

B. Edit the SQL authentication source niter attributes and modify the SQL server filter query.

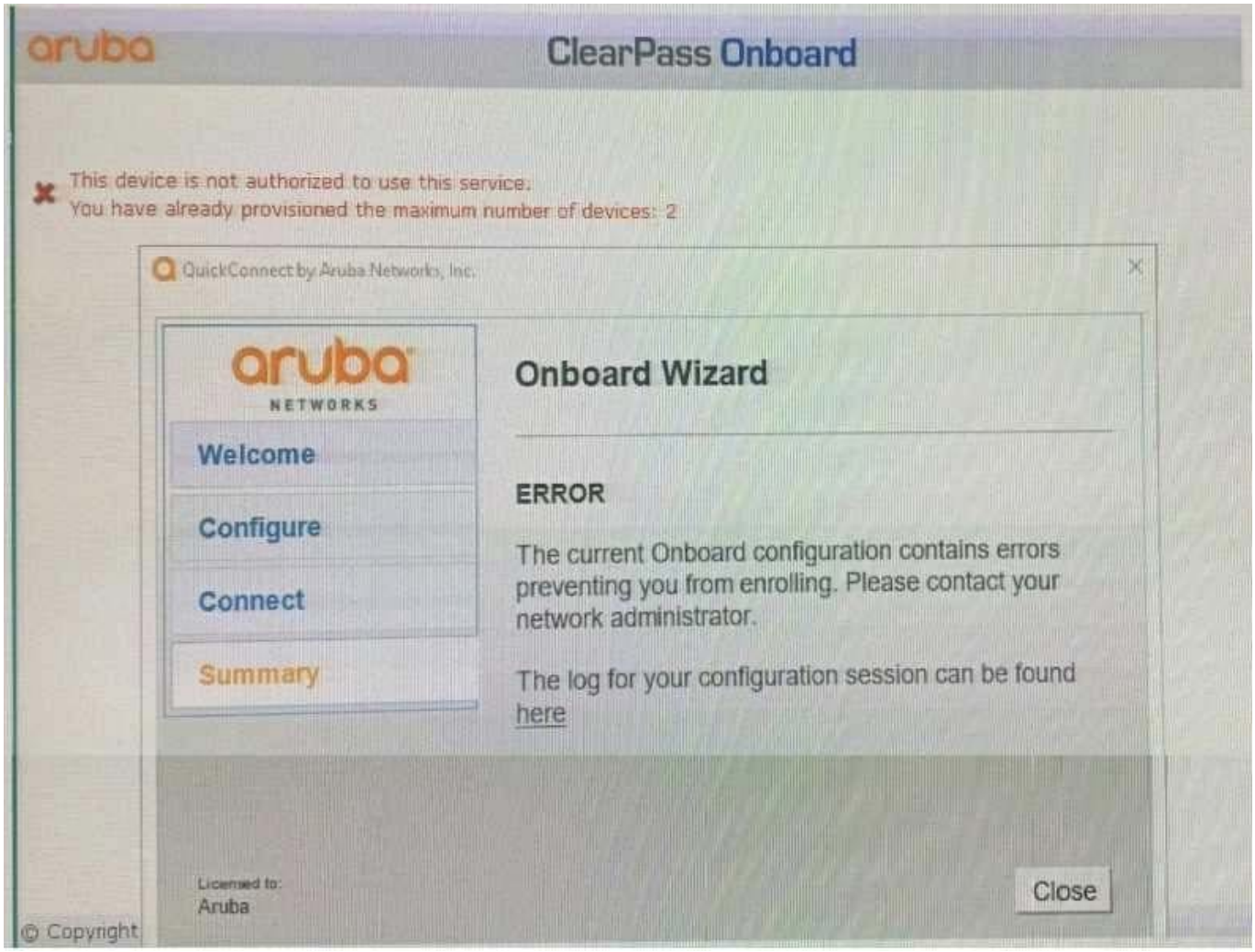
C. Add the SQL server as an authentication source and map .t under the authentication tab in the service.

D. Enable authorization tab in the service and add the SQL server as an authorization source.

Correct Answer: B

QUESTION 4

Refer to the exhibit: You have configured Onboard but me customer could not onboard one of his devices and has sent you the above screenshots. How could you resolve the issue?



A. Instruct the user to delete the profile on one of their other BYOD devices.

B. Instruct the user to run the Quick connect application in Sponsor Mode.

C. Increase the maximum number of devices allowed by the individual user account.

D. Increase the maximum number of devices that all users can provision to 3.

Correct Answer: D

QUESTION 5

A Customer has these requirements:

*

2.000 loT endpoints that use MAC authentication

*

6,000 endpoints using a mix of username/password and certificate (Corporate/BYOD) based authentication

*

1,000 guest endpoints at peak usage that use guest self-registration

*

1500 BYOD devices estimated as 3 devices per User (500 users)

*

2,500 endpoints that have OnGuard installed and connect on a daily basis

What licenses should be installed to meet customer requirements?

A. 11,500 Access, 500 Onboard, 2,500 Onguard

B. 13.000 Access, 1.500 Onboard, 2,500 Onguard

C. 11,500 Access, 1,500 Onboard, 2.500 Onguard

D. 9,000 Access, 500 Onboard. 2.500 Onguard

Correct Answer: C