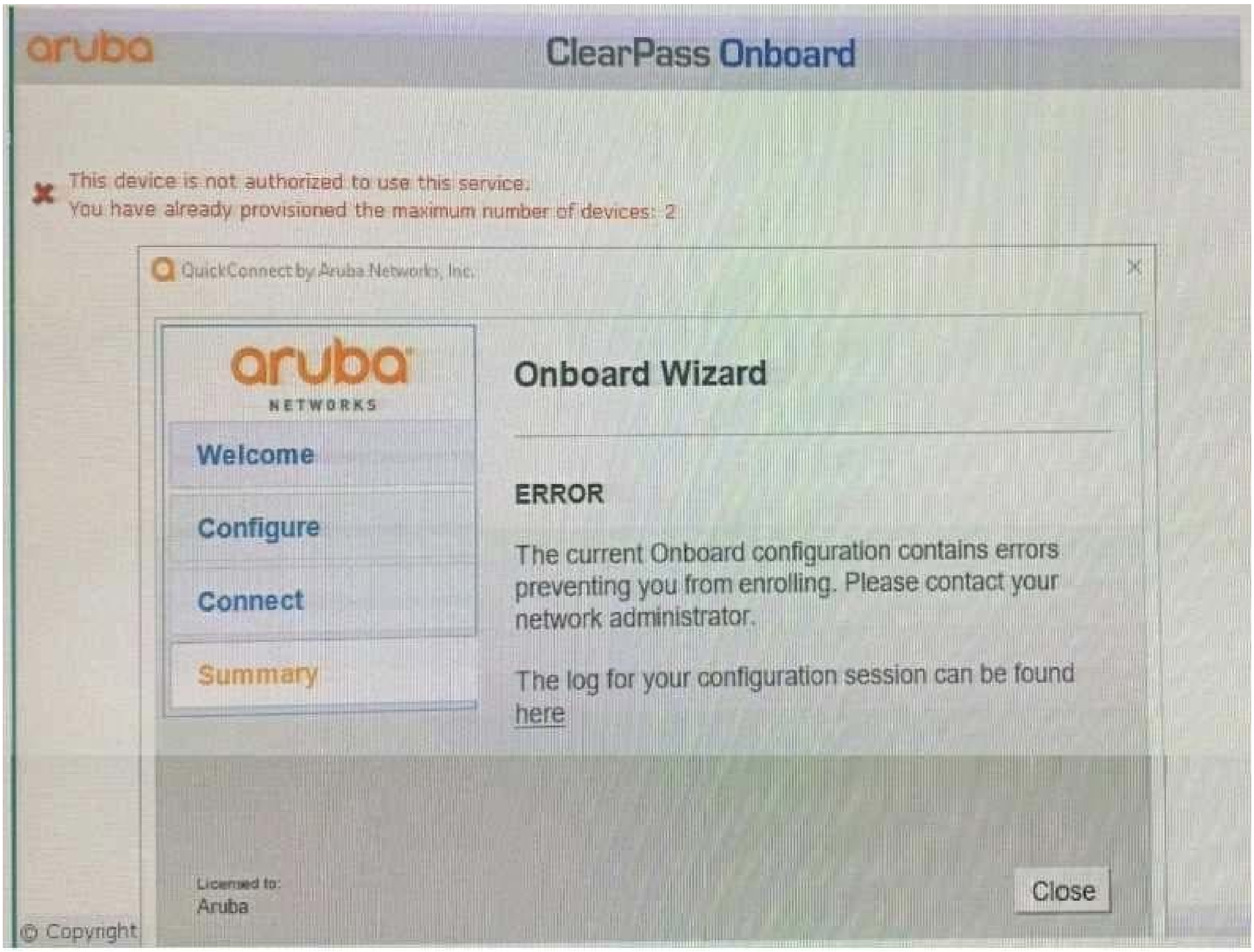
HPE6-A81 Q&As

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

QUESTION 1

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?



This device is not authorized to use this service.
You have already provisioned the maximum number of devices: 2

ERROR

The current Onboard configuration contains errors preventing you from enrolling. Please contact your network administrator.

The log for your configuration session can be found here

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 2

You are integrating a Postgres SQL server with the ClearPass Policy Manager. What steps will you follow to complete the integration process? (Select three)

A. Click on the default filter name with pre-defined filter queries and check box to enable as role.

B. Specify a new filter with filter queries to fetch authentication and authorization attributes.

C. Attribute Name under filter configuration must match one of the columns being requested from the database table.

D. Create a new Endpoint context server and add the SQL server IP, credentilas and the database name.

E. Alias Name under filter configuration must match one of the columns being requested from the database table.

F. Create a new authentication source and add the SQL server IP, credentials and the database name.

Correct Answer: BDF

QUESTION 3

A customer would like to allow only the AD users with the "Manager" title from the "HQ" location to

Onboard their personal devices. Any other AD users should not be authorized to pass beyond the initial

device provisioning page.

Which Onboard service will you use to implement this requirement?

A. Onboard CP login service

B. Onboard Authorization service

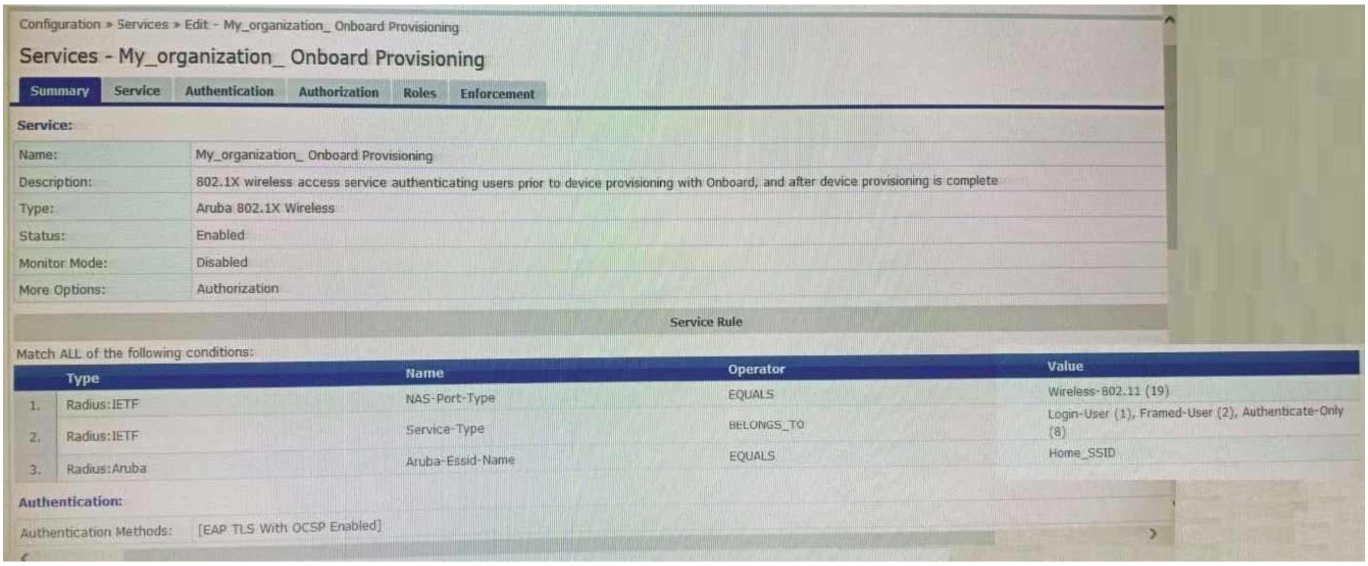
C. Onboard Provisioning service

D. Onboard Pre-Auth service

Correct Answer: A

QUESTION 4

Refer to the exhibit: A customer has configured a service with the Onboard Devices Repository as an Authentication Source and an Active Directory Domain Server as an Authorization Source. What will happen if the client certificate is still valid and the user account associated with the certificate is disabled in Active Directory?



Configuration » Services » Edit - My_organization_ Onboard Provisioning
Summary
Service
Authentication
Authorization
Roles
Enforcement

Services - My_organization_ Onboard Provisioning

Service:

Name:	My_organization_ 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

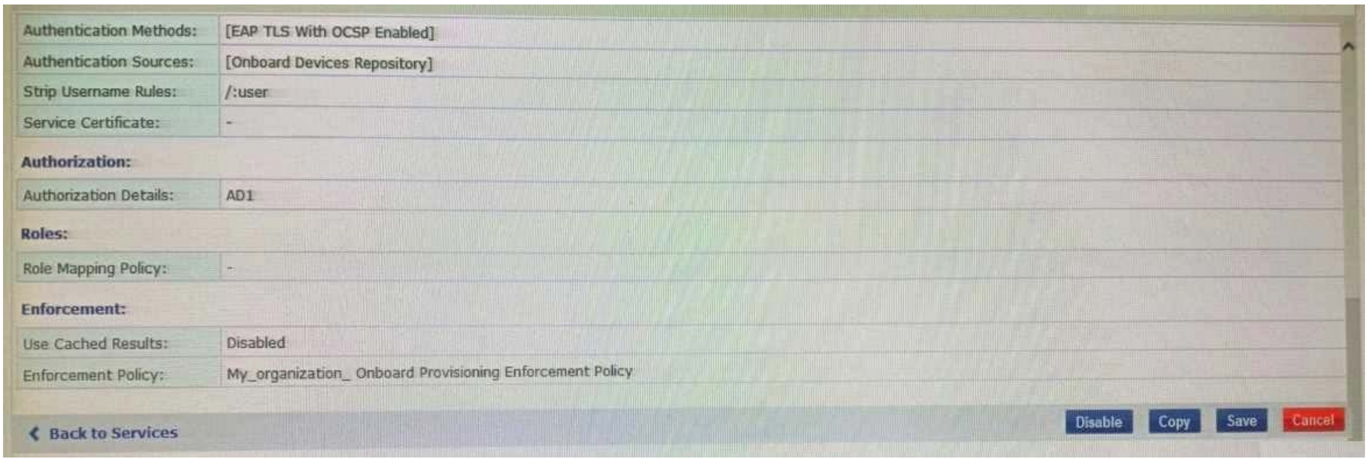
Service Rule

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	Home_SSID

Authentication:

Authentication Methods:	[EAP TLS With OCSP Enabled]



Authentication Methods:	[EAP TLS With OCSP Enabled]
Authentication Sources:	[Onboard Devices Repository]
Strip Username Rules:	/:user
Service Certificate:	-

Authorization:

Authorization Details:	AD1

Roles:

Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	My_organization_ Onboard Provisioning Enforcement Policy

A. ClearPass will not process the request

B. Enforcement will apply the [Deny Access Profile]

C. ClearPass will redirect the client to Onboard again

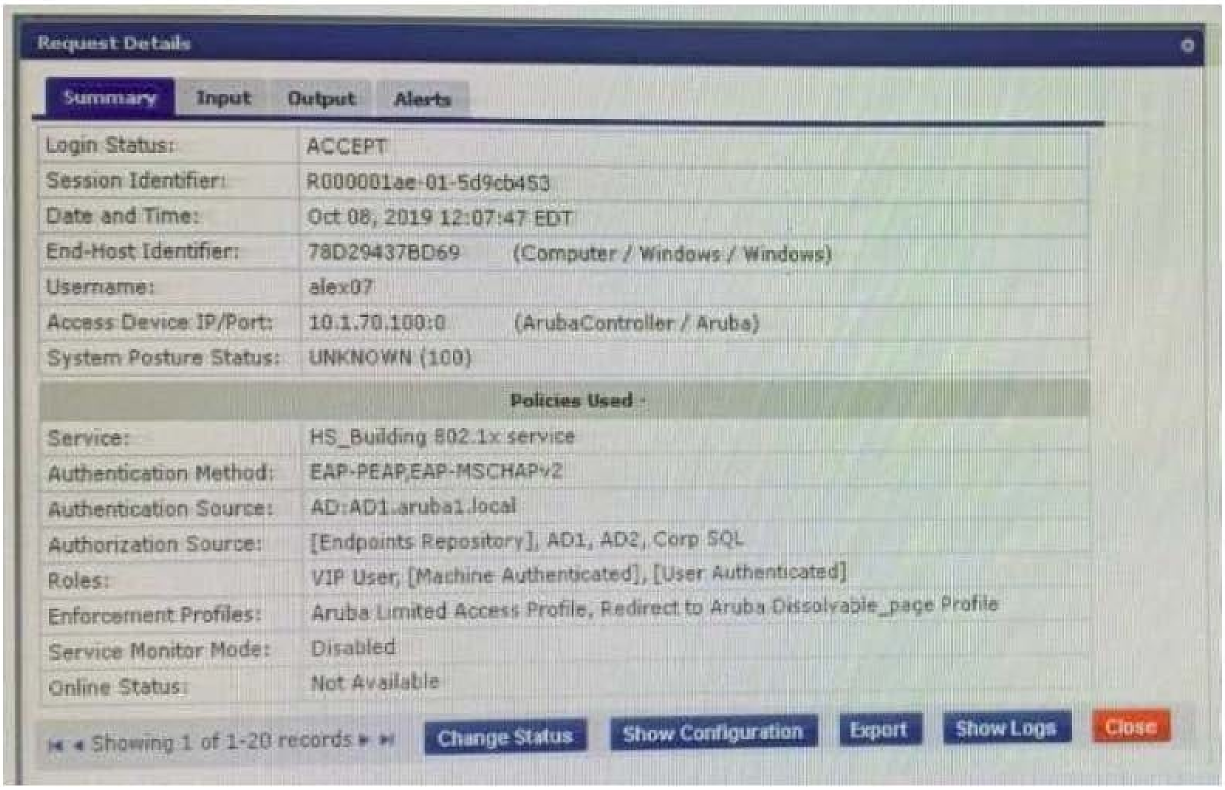
D. ClearPass will block network access to the device

E. ClearPass will allow the device to access the network.

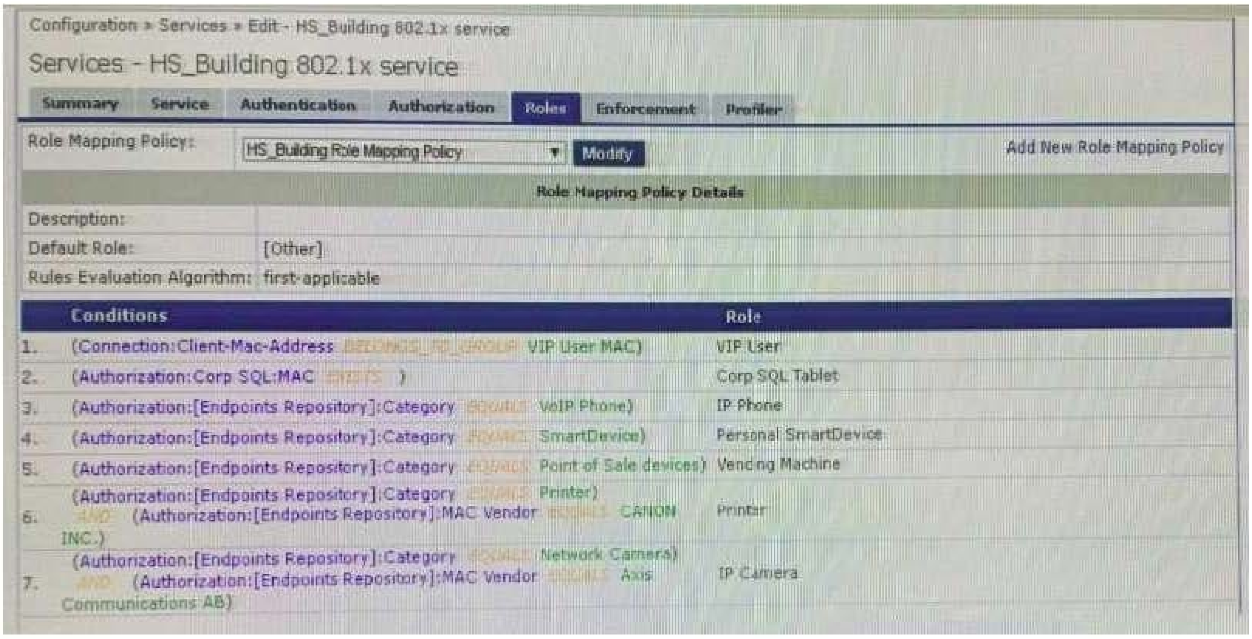
Correct Answer: D

QUESTION 5

Refer to the exhibit:



Login Status:	ACCEPT
Session Identifier:	R000001ae-01-5d9cb453
Date and Time:	Oct 08, 2019 12:07:47 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	HS_Building 802.1x service
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	[Endpoints Repository], AD1, AD2, Corp SQL
Roles:	VIP User, [Machine Authenticated], [User Authenticated]
Enforcement Profiles:	Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
Service Monitor Mode:	Disabled
Online Status:	Not Available


Configuration » Services » Edit - HS_Building 802.1x service
Summary
Service
Authentication
Authorization
Roles
Enforcement
Profiler
Modify
Add New Role Mapping Policy

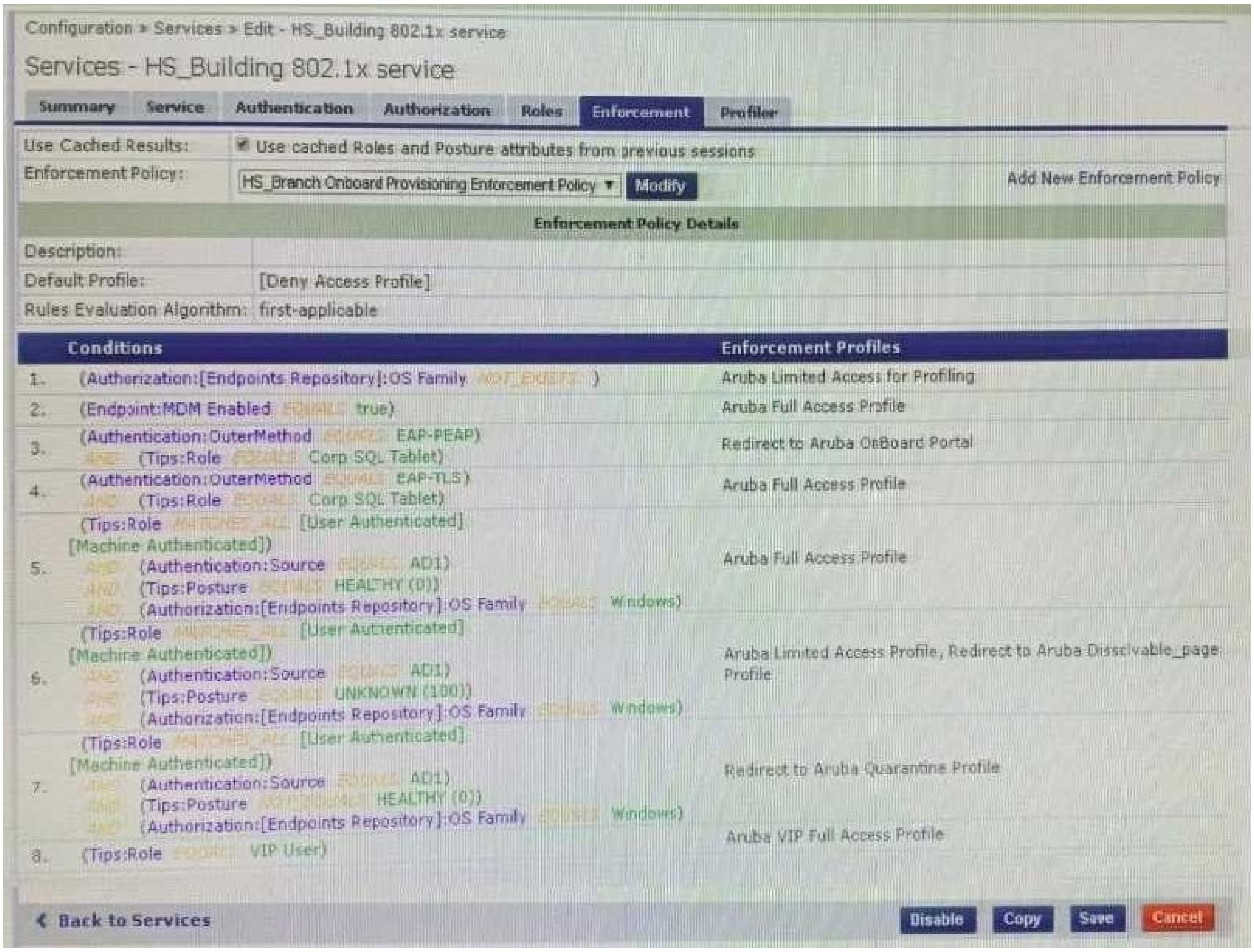
Services - HS_Building 802.1x service

Role Mapping Policy: HS_Building 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 802.1x service

Services - HS_Building 802.1x service

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

Enforcement Policy: HS_Branch Onboard Provisioning 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.	(Authorization:[Endpoints Repository]:OS Family NOT_EXISTS)	Aruba Limited Access for Profiling
2.	(Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
3.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS Corp SQL Tablet)	Redirect to Aruba OnBoard Portal
4.	(Authentication:OuterMethod EQUALS EAP-TLS) AND (Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
5.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Aruba Full Access Profile
6.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	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)) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows)	Redirect to Aruba Quarantine Profile
8.	(Tips:Role EQUALS VIP User)	Aruba VIP Full Access Profile

The customer created a new enforcement policy condition to allow VIP Users access without additional security compliance checks hut cannot gel it working. The customer has sent you the above screenshots. How would you resolve the issue?

A. Ask the VIP user to complete the one time web health check to get the VIP profile.

B. Set the Enforcement Policy rules evaluation algorithm to evaluate all.

C. Include VIP User role along with the Healthy posture enforcement condition.

D. Modify the Enforcement Policy and re-order the VIP user condition to the lop.

Correct Answer: C

QUESTION 6

You have configured a Guest SSID with Captive-portal Web Authentication and MAC authentication The MAC caching expiry time set to 12 hours and the Guest Account expiration time is set to 8 hours. What will happen if the guest were to disconnect from the SSID and re-connect 9 hours later?

A. The client will tail the MAC authentication and be denied access to the Guest SSID.

B. The client will successfully pass the mac authentication until the mac caching time expires.

C. The client will successfully pass the MAC authentication but still be redirected to captive portal page.

D. The client will fail the MAC authentication and will be redirected to the Captive-portal login page.

Correct Answer: C

QUESTION 7

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.

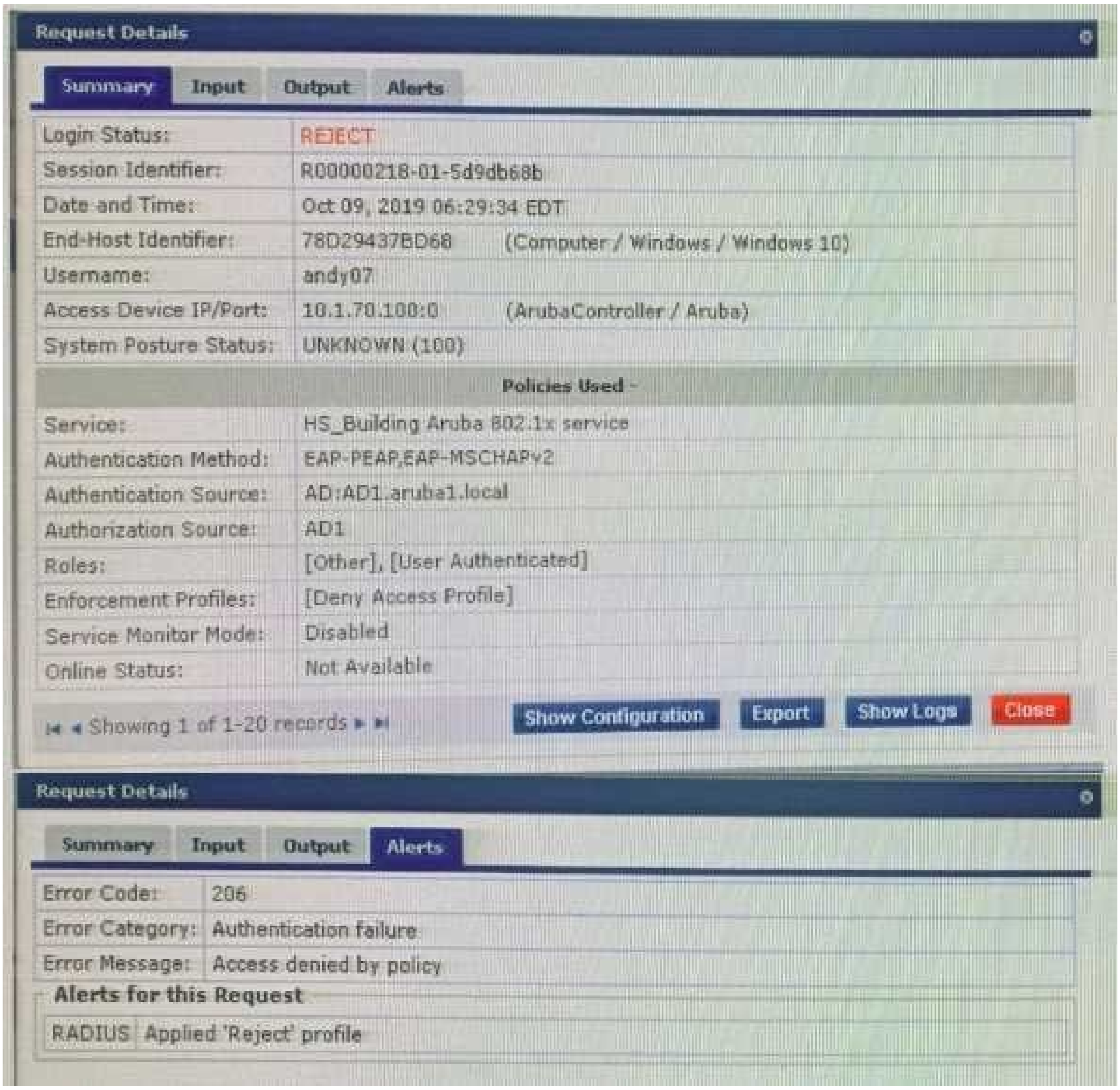
C. The primary authentication server Is not available to authenticate the users.

D. The ClearPass server will be hosting captive portal pages for multiple FQDN entries

Correct Answer: A

QUESTION 8

Refer to the exhibit:

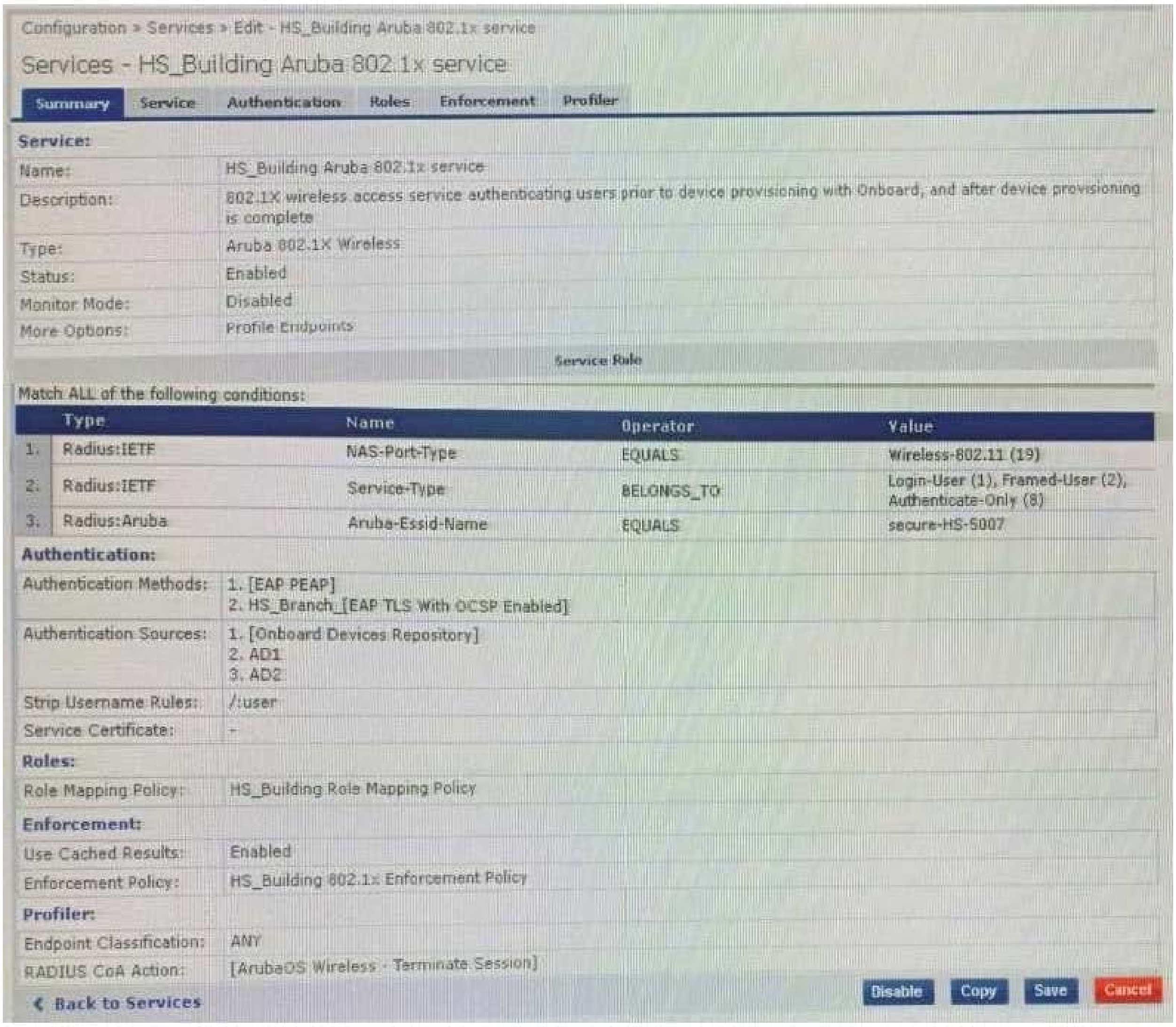


Login Status:	REJECT
Session Identifier:	R00000218-01-5d9db68b
Date and Time:	Oct 09, 2019 06:29:34 EDT
End-Host Identifier:	78D29437BD68 (Computer / Windows / Windows 10)
Username:	andy07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
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

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

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

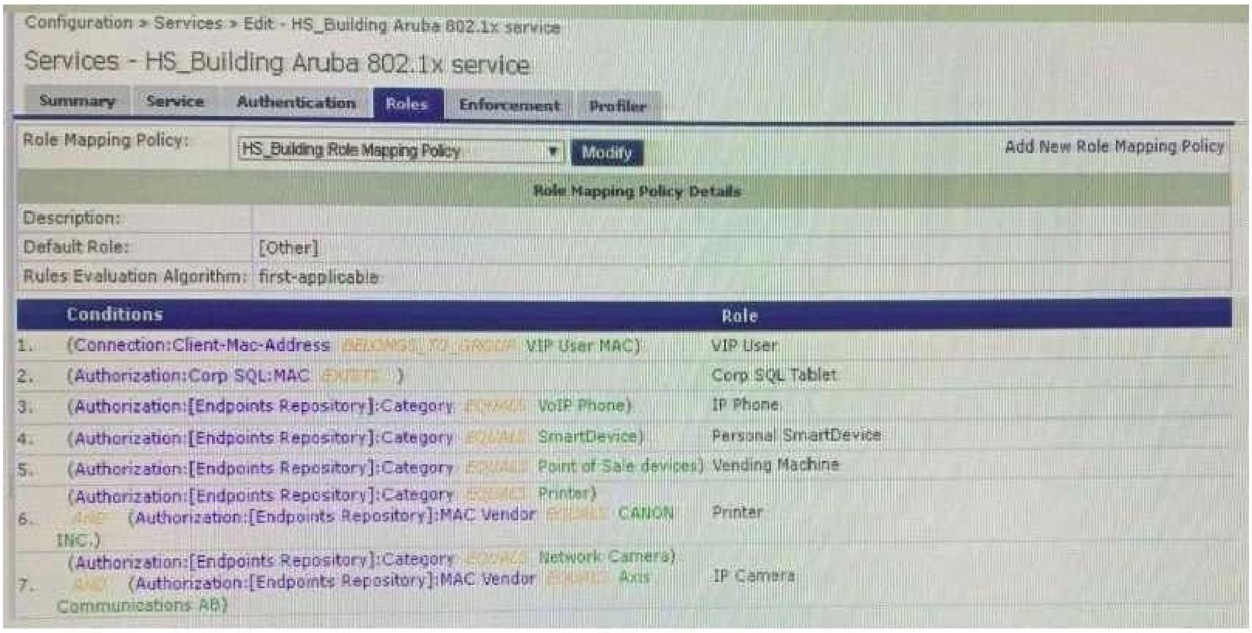
Enforcement:

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



Configuration » Services » Edit - HS_Building Aruba 802.1x service

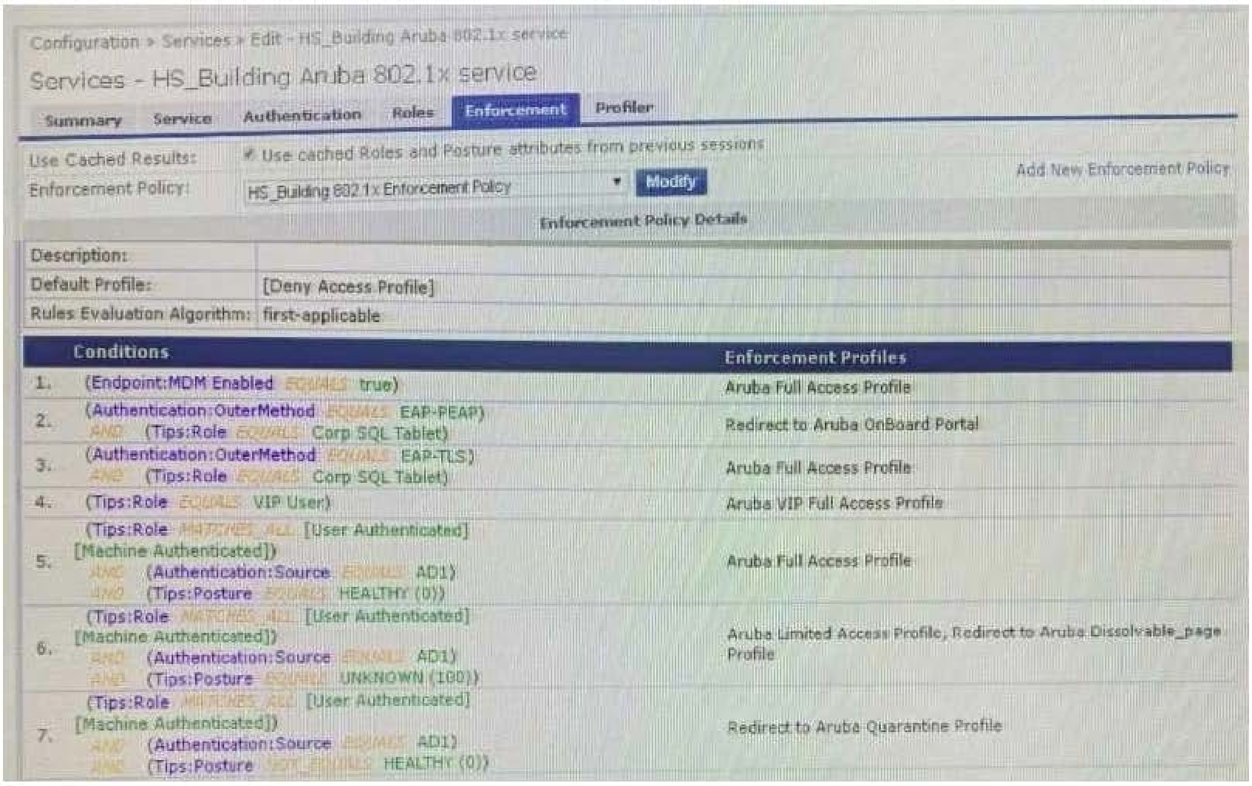
Services - HS_Building Aruba 802.1x service

Role Mapping Policy: HS_Building 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

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

Enforcement Policy: HS_Building 802.1x 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.

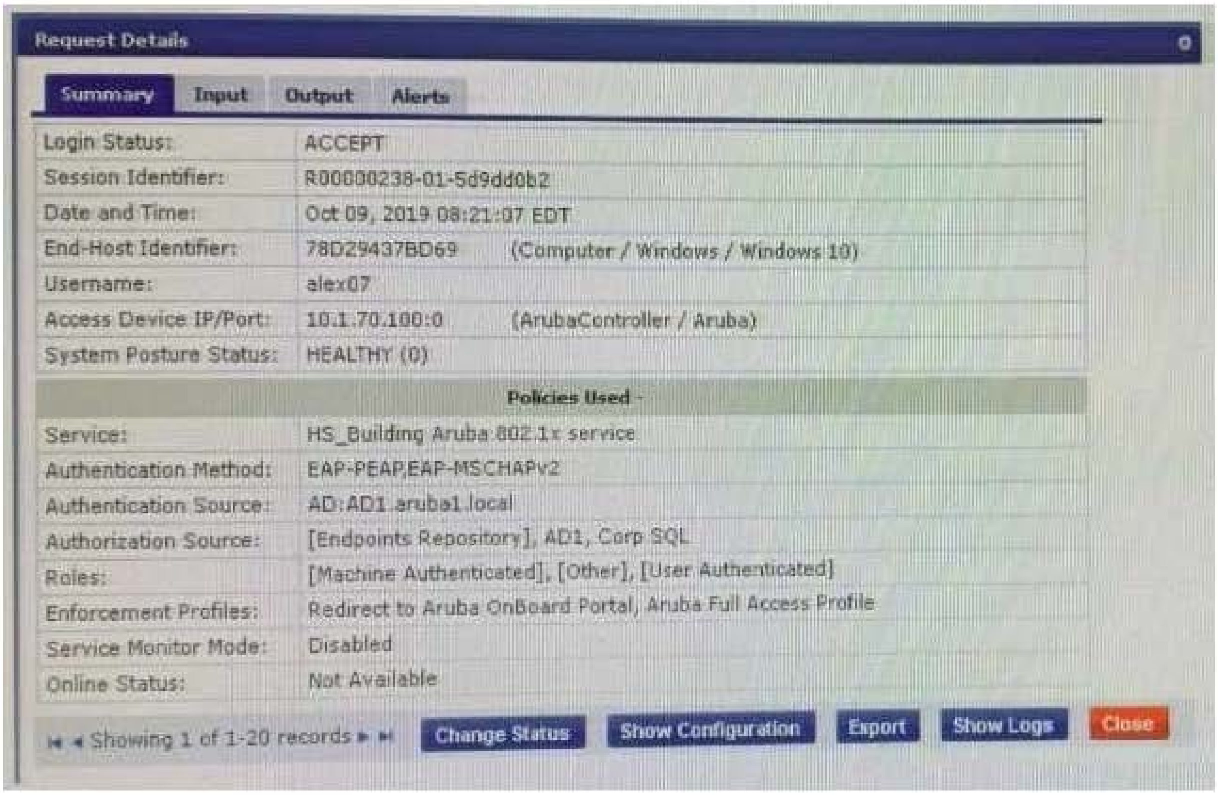
C. Add the SQL server as an authentication source and map .t under the authentication tab in the service.

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

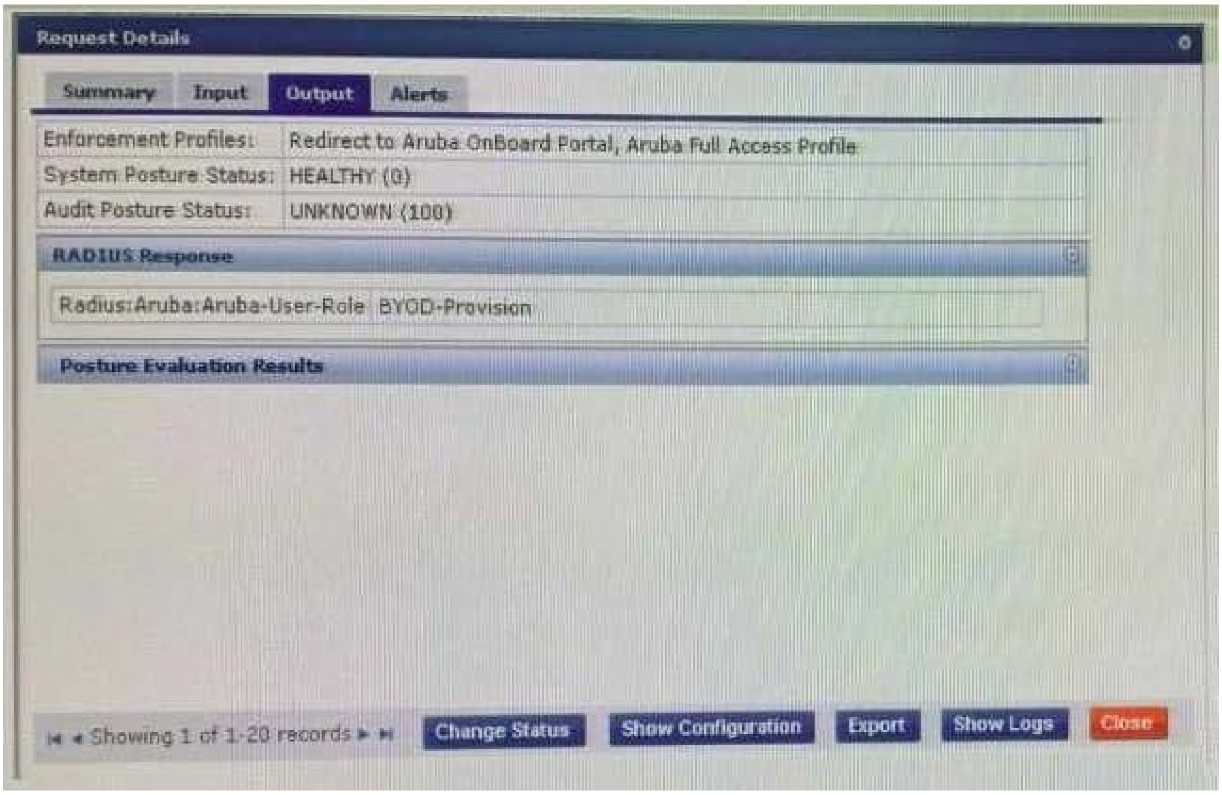
Correct Answer: B

QUESTION 9

Refer to the exhibit:



Login Status:	ACCEPT
Session Identifier:	R00000238-01-5d9dd0b2
Date and Time:	Oct 09, 2019 08:21:07 EDT
End-Host Identifier:	78D29437BD69 (Computer / Windows / Windows 10)
Username:	alex07
Access Device IP/Port:	10.1.70.100:0 (ArubaController / Aruba)
System Posture Status:	HEALTHY (0)
Policies Used -	
Service:	HS_Building Aruba 802.1x service
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:AD1.aruba1.local
Authorization Source:	[Endpoints Repository], AD1, Corp SQL
Roles:	[Machine Authenticated], [Other], [User Authenticated]
Enforcement Profiles:	Redirect to Aruba OnBoard Portal, Aruba Full Access Profile
Service Monitor Mode:	Disabled
Online Status:	Not Available

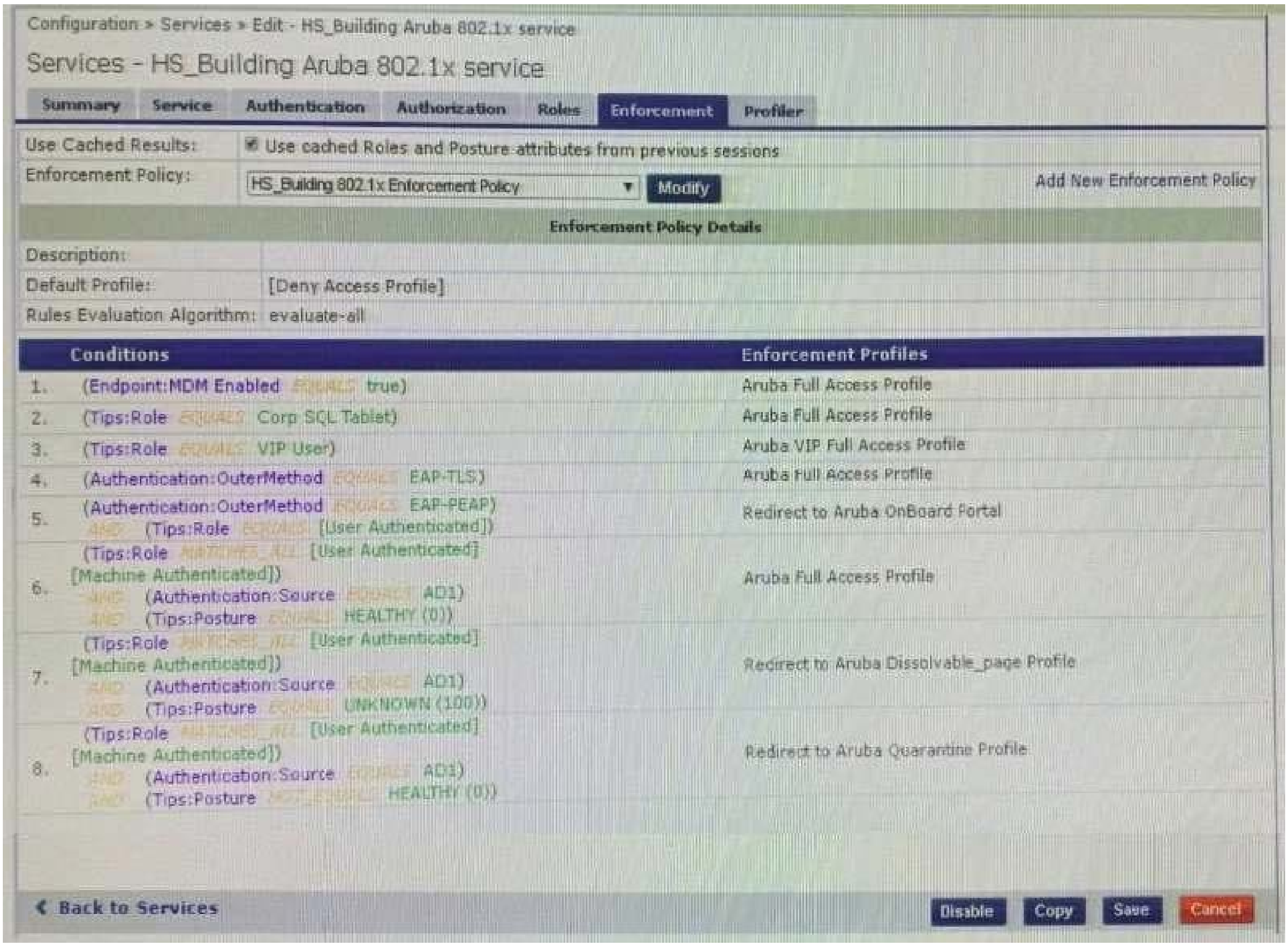


Enforcement Profiles:	Redirect to Aruba OnBoard Portal, Aruba Full Access Profile
System Posture Status:	HEALTHY (0)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role	BYOD-Provision

Posture Evaluation Results



Services - HS_Building Aruba 802.1x service

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

Enforcement Policy: HS_Building 802.1x Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	evaluate-all

	Conditions	Enforcement Profiles
1.	(Endpoint:MDM Enabled EQUALS true)	Aruba Full Access Profile
2.	(Tips:Role EQUALS Corp SQL Tablet)	Aruba Full Access Profile
3.	(Tips:Role EQUALS VIP User)	Aruba VIP Full Access Profile
4.	(Authentication:OuterMethod EQUALS EAP-TLS)	Aruba Full Access Profile
5.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS [User Authenticated])	Redirect to Aruba OnBoard Portal
6.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0))	Aruba Full Access Profile
7.	(Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100))	Redirect to Aruba Dissolvable_page Profile
8.	(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

The customer configured an 802.1x service with different enforcement actions for personal and corporate laptops. The corporate laptops are always being redirected to the BYOD Portal. The customer has sent you the above screenshots.

How would you resolve the issue? (Select two)

A. Modify the enforcement policy and change the rule evaluation algorithm to select first match

B. Modify the enforcement policy and re-order the condition with posture not_equals to healthy as the sixth condition

C. Modify the enforcement policy and re-order the EAP-PEAP with [user authenticated] rule to the last condition.

D. Modify the enforcement policy and re-order the condition with Posture - Unknown as the fifth condition

E. Remove the EAP-PEAP with [user authenticated] condition for Onboard and create another service

Correct Answer: CD

QUESTION 10

Under Onboard management and control, which option will deny the user from re-provisioning the device a second time?

A. Revoke and Delete certificate

B. Delete user

C. Revoke certificate

D. Delete certificate

Correct Answer: D