

## Version: 9.0

### Question: 1

Which connecting endpoints are evaluated against all enabled device profiling rules?

- A. All hosts, each time they connect
- B. Rogues devices, only when they connect for the first time
- C. Known trusted devices each time they change location
- D. Rogues devices, each time they connect

**Answer: C**

<https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-design-endpoint-attributes>

### Question: 2

Which agent is used only as part of a login script?

- A. Mobile
- B. Passive
- C. Persistent
- D. Dissolvable

**Answer: C**

[https://www.websense.com/content/support/library/deployctr/v76/init\\_setup\\_creating\\_and\\_running\\_logon\\_agent\\_script\\_deployment\\_tasks.aspx](https://www.websense.com/content/support/library/deployctr/v76/init_setup_creating_and_running_logon_agent_script_deployment_tasks.aspx)

### Question: 3

What agent is required in order to detect an added USB drive?

- A. Persistent
- B. Dissolvable
- C. Mobile
- D. Passive

**Answer: A**

### Question: 4

What would occur if both an unknown (rogue) device and a known (trusted) device simultaneously appeared on a port that is a member of the Forced Registration port group?

- A. The port would be provisioned for the normal state host, and both hosts would have access to that VLAN.
- B. The port would not be managed, and an event would be generated.
- C. The port would be provisioned to the registration network, and both hosts would be isolated.
- D. The port would be administratively shut down.

**Answer: B**

### Question: 5

Which two agents can validate endpoint compliance transparently to the end user? (Choose two.)

- A. Passive
- B. Dissolvable
- C. Mobile
- D. Persistent

**Answer: C,D**

[https://www.websense.com/content/support/library/deployctr/v76/init\\_setup\\_creating\\_and\\_running\\_logon\\_agent\\_script\\_deployment\\_tasks.aspx](https://www.websense.com/content/support/library/deployctr/v76/init_setup_creating_and_running_logon_agent_script_deployment_tasks.aspx)

### Question: 6

Which three communication methods are used by the FortiNAC to gather information from, and control, infrastructure devices? (Choose three)

- A. RADIUS
- B. FTP
- C. OSNMP
- D. DCLI
- E. SMTP

**Answer: B,D,E**

<https://www.fortinet.com/products/network-access-control>

<https://docs.oracle.com/en/engineered-systems/exadata-database-machine/sagug/exadata-storage-server-dcli.html#GUID-472C6AA1-BF36-4885-825D-281FC2CEFBC3>

## Question: 7

Refer to the exhibit.

General			
User Name	<input type="text" value="admin"/>	Password	<input type="password" value="*****"/>
Enable Password	<input type="text"/>		
Protocol			
Type	<input type="text" value="SSH 2"/>		
VLAN ID			
Default	<input type="text" value="2"/>	Dead End	<input type="text" value="112"/>
Registration	<input type="text"/>	Quarantine	<input type="text" value="111"/>
Authentication	<input type="text"/>	Voice	<input type="text"/>
CLI Configurations			
Type:	<input checked="" type="radio"/> None <input type="radio"/> Port Based <input type="radio"/> Host Based		
		<input type="button" value="Apply"/>	<input type="button" value="Reset"/>

If you are forcing the registration of unknown (rogue) hosts, and an unknown (rogue) host connects to a port on the switch, what will occur?

- A. No VLAN change is performed
- B. The host is moved to a default isolation VLAN.
- C. The host is disabled.
- D. The host is moved to VLAN 111.

**Answer: C**