QUESTION 126
An engineer is testing Cisco ISE policies in a lab environment with no support for a deployment server. In order to push supplicant profiles to the workstations for testing, firewall ports will need to be opened. From which Cisco ISE persona should this traffic be originating?

A. monitoring
B. policy service
C. administration
D. authentication

Answer: D

QUESTION 127
What is an advantage of using EAP-TLS over EAP-MS-CHAPv2 for client authentication?

A. EAP-TLS uses a username and password for authentication to enhance security, while EAP-MS-CHAPv2 does not.
B. EAP-TLS secures the exchange of credentials, while EAP-MS-CHAPv2 does not.
C. EAP-TLS uses a device certificate for authentication to enhance security, while EAP-MS-CHAPv2 does not.
D. EAP-TLS uses multiple forms of authentication, while EAP-MS-CHAPv2 only uses one.

Answer: D

QUESTION 128
There are several devices on a network that are considered critical and need to be placed into the ISE database and a policy used for them. The organization does not want to use profiling. What must be done to accomplish this goal?

A. Enter the MAC address in the correct Endpoint Identity Group.
B. Enter the MAC address in the correct Logical Profile.
C. Enter the IP address in the correct Logical Profile.
D. Enter the IP address in the correct Endpoint Identity Group.

Answer: D

QUESTION 129
An engineer is tasked with placing a guest access anchor controller in the DMZ. Which two ports or port sets must be opened up on the firewall to accomplish this task? (Choose two.)

A. UDP port 1812 RADIUS
B. TCP port 161
C. TCP port 514
D. UDP port 79
E. UDP port 16666

Answer: BC

QUESTION 130
Which three conditions can be used for posture checking? (Choose three.)

A. certificate
B. operating system
C. file
D. application
E. services

Answer: CDE

QUESTION 131
What does MAB leverage a MAC address for?

A. Calling-Station-ID
B. password
C. cisco-av-pair
D. username

Answer: D

QUESTION 132
By default, which traffic does an 802.IX-enabled switch allow before authentication?

A. all traffic
B. no traffic
C. traffic permitted in the port dACL on Cisco ISE
D. traffic permitted in the default ACL on the switch

Answer: B

QUESTION 133
Which scenario does not support Cisco ISE guest services?

A. wired NAD with local WebAuth
B. wireless LAN controller with central WebAuth
C. wireless LAN controller with local WebAuth
D. wired NAD with central WebAuth

Answer: A

QUESTION 134
Which Cisco ISE node does not support automatic failover?

A. Inline Posture node
B. Monitoring node

C. Policy Services node
D. Admin node

Answer: C

QUESTION 135
In which scenario does Cisco ISE allocate an Advanced license?

A. guest services with dACL enforcement
B. endpoint authorization using SGA enforcement
C. dynamic device profiling
D. high availability Administrator nodes

Answer: B

QUESTION 136
Which statement is true?

A. A Cisco ISE Advanced license is perpetual in nature.
B. A Cisco ISE Advanced license can be installed on top of a Base and/or Wireless license.
C. A Cisco ISE Wireless license can be installed on top of a Base and/or Advanced license.
D. A Cisco ISE Advanced license can be used without any Base licenses.

Answer: B

QUESTION 137
What are the three default behaviors of Cisco ISE with respect to authentication, when a user connects to a switch that is configured for 802.1X, MAB, and WebAuth? (Choose three)

A. MAB traffic uses internal endpoints for retrieving identity.
B. Dot1X traffic uses a user-defined identity store for retrieving identity.
C. Unmatched traffic is allowed on the network.
D. Unmatched traffic is dropped because of the Reject/Reject/Drop action that is configured under Options.
E. Dot1x traffic uses internal users for retrieving identity.

Answer: ABD

QUESTION 138
Which types of design are required in the Cisco ISE ATP program?

A. schematic and detailed
B. preliminary and final
C. high-level and low-level designs
D. top down and bottom up

Answer: C

QUESTION 139
The profiling data from network access devices is sent to which Cisco ISE node?

A. Monitoring node
B. Administration node
C. Inline Posture node
D. Policy Service node

Answer: D

QUESTION 140
Which statement is not correct about the Cisco ISE Monitoring node?

A. The local collector agent collects logs locally from itself and from any NAD that is configured to send logs to the Policy Service node.
B. Cisco ISE supports distributed log collection across all nodes to optimize local data collection, aggregation, and centralized correlation and storage.
C. The local collector agent process runs only the Inline Posture node.
D. The local collector buffers transport the collected data to designated Cisco ISE Monitoring nodes as syslog; once Monitoring nodes are globally defined via Administration, ISE nodes automatically send logs to one or both of the configured Monitoring nodes.

Answer: C

QUESTION 141
What is the condition that a Cisco ISE authorization policy cannot match?

A. company contact
B. custom
C. time
D. device type
E. posture

Answer: A

QUESTION 142
What is the Cisco ISE default admin login name and password?

A. ISEAdmin/admin
B. admin/cisco
C. admin/no default password--the admin password is configured at setup
D. admin/admin

Answer: C

QUESTION 143
What does MAB stand for?

A. MAC Address Binding
B. MAC Authorization Binding
C. MAC Authorization Bypass
D. MAC Authentication Bypass

Answer: D

QUESTION 144
The default (standalone) Cisco ISE node configuration has which role or roles enabled by default?

A. Administration only
B. Inline Posture only
C. Administration and Pokey Service
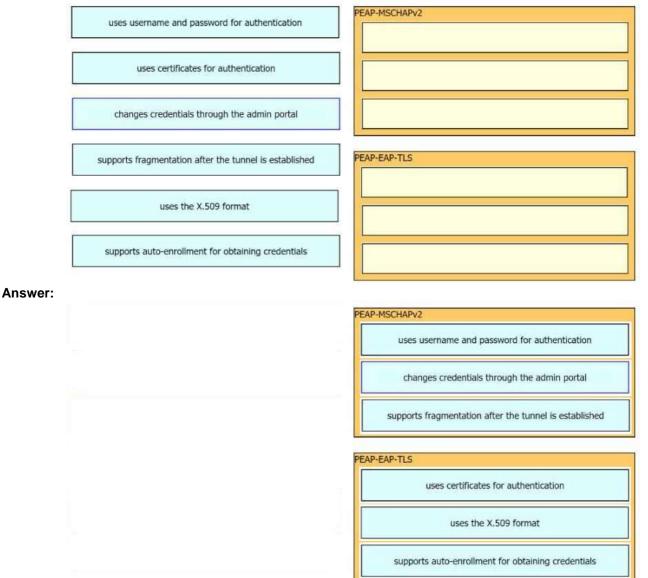D. Policy Service, Monitoring and Admin

Answer: D

QUESTION 145
Drag and Drop Question
An organization wants to implement 802.1X and is debating whether to use PEAP-MSCHAPv2 or PEAP-EAP-TLS for authentication. Drag the characteristics on the left to the corresponding protocol on the right.

Characteristics	PEAP-MSCHAPv2
uses username and password for authentication	
uses certificates for authentication	
changes credentials through the admin portal	
supports fragmentation after the tunnel is established	PEAP-EAP-TLS
uses the X.509 format	
supports auto-enrollment for obtaining credentials	

Answer:

PEAP-MSCHAPv2
- uses username and password for authentication
- changes credentials through the admin portal
- supports fragmentation after the tunnel is established

PEAP-EAP-TLS
- uses certificates for authentication
- uses the X.509 format
- supports auto-enrollment for obtaining credentials