ISLEVER

500-254

Implementing and Configuring Cisco Identity Service Engine - SISE

DEMO

https://www.islever.com/500-254.html

https://www.islever.com/cisco.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

QUESTION NO: 1

Which two elements must you configure on a Cisco Wireless LAN Controller to allow Cisco ISE to authenticate wireless users? (Choose two.)

A. Configure Cisco ISE as a RADIUS authentication server and enter a shared secret.
B. Configure Cisco ISE as a RADIUS accounting server and enter a shared secret.
C. Configure all attached LWAPs to use the configured Cisco ISE node.
D. Configure RADIUS attributes for each SSID.
E. Configure each WLAN to use the configured Cisco ISE node.
F. Configure the Cisco Wireless LAN Controller to join a Microsoft Active Directory domain.

Answer: A,E
Explanation:

QUESTION NO: 2

Which three Cisco TrustSec enforcement modes are used to help protect network operations when securing the network? (Choose three.)

A. logging mode
B. monitor mode
C. semi-passive mode
D. low-impact mode
E. closed mode

Answer: B,D,E
Explanation:

QUESTION NO: 3

Which statement is correct about Change of Authorization?

A. Change of Authorization is a fundamental component of Cisco TrustSec and Cisco ISE.
B. Change of Authorization can be triggered dynamically based on a matched condition in a policy, and manually by being invoked by an administrator operation.
C. It is possible to trigger Change of Authorization manually from the ISE interface.
D. Authentication is the supported Change of Authorization action type.

Answer: D

Explanation:

QUESTION NO: 4

The default Cisco ISE node configuration has which role or roles enabled by default?

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

Answer: D
Explanation:

QUESTION NO: 5

Inline Posture nodes support which enforcement mechanisms?

A. VLAN assignment
B. downloadable ACLs
C. security group access
D. dynamic ACLs

Answer: B
Explanation:

QUESTION NO: 6

What is the process for Cisco ISE to obtain a signed certificate from a CA?

A. Request a certificate from the CA, and import the CA-signed certificate into ISE.
B. Generate a CSR; download the certificate from the CA; bind the CA-signed certificate with its private key, and import the CA-signed certificate into ISE.
C. Generate a CSR; export the CSR to the local file system and send to the CA; download the certificate from the CA, and bind the CA-signed certificate with its private key.
D. Submit a CSR to the CA; download the certificate from the CA; bind the CA-signed certificate with its private key, and import the CA-signed certificate into ISE.

Answer: C
Explanation:

QUESTION NO: 7

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

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

Answer: D
Explanation:

QUESTION NO: 8

What are two methods to verify that Cisco ISE is properly connected to AD? (Choose two.)

A. Use the Test Connection feature in the Cisco ISE External Identity Sources Active Directory.
B. View the Active Directory Log /opt/CSCOcmp/logs/ad_agent.log.
C. Use the ISE Dashboard Summary alarms.
D. Use ktpass to determine if the Kerberos ticket is valid.

Answer: A,B
Explanation:

QUESTION NO: 9

Where is the license installed within Cisco ISE deployment?

A. A license is installed on the Policy Service node within ISE deployment.
B. A license is installed on the primary or secondary Administration node within ISE deployment.
C. A license is installed only on the primary Administration node within ISE deployment.
D. A license is preinstalled for ISE deployment.

Answer: C
Explanation: