



300-715^{Q&As}

Implementing and Configuring Cisco Identity Services Engine (SISE)

Pass Cisco 300-715 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/300-715.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Which command displays all 802 1X/MAB sessions that are active on the switch ports of a Cisco Catalyst switch?

- A. show authentication sessions output
- B. Show authentication sessions
- C. show authentication sessions interface Gi 1/0/x
- D. show authentication sessions interface Gi1/0/x output

Correct Answer: B

QUESTION 2

Which protocol must be allowed for a BYOD device to access the BYOD portal?

- A. HTTP
- B. SMTP
- C. HTTPS
- D. SSH

Correct Answer: C

QUESTION 3

A security engineer must create an Antivirus remediation policy within Cisco ISE. Which two options can the engineer select in the new Antivirus remediation policy? (Choose two.)

- A. program installation path
- B. Antivirus vendor name
- C. uniform resource locator
- D. file to upload
- E. operating system

Correct Answer: BE

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_pos_pol.html#wp1655749

**QUESTION 4**

A network engineer has been tasked with enabling a switch to support standard web authentication for Cisco ISE. This must include the ability to provision for URL redirection on authentication Which two commands must be entered to meet this requirement? (Choose two)

- A. Ip http secure-authentication
- B. Ip http server
- C. Ip http redirection
- D. Ip http secure-server
- E. Ip http authentication

Correct Answer: BD

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0111001.html

QUESTION 5

Which CLI command must be configured on the switchport to immediately run the MAB process if a non-802.1X capable endpoint connects to the port?

- A. authentication order mab dot1x
- B. dot1x pae authenticator
- C. authentication fallback
- D. access-session port-control auto

Correct Answer: D

QUESTION 6

Which configuration is required in the Cisco ISE authentication policy to allow Central Web Authentication?

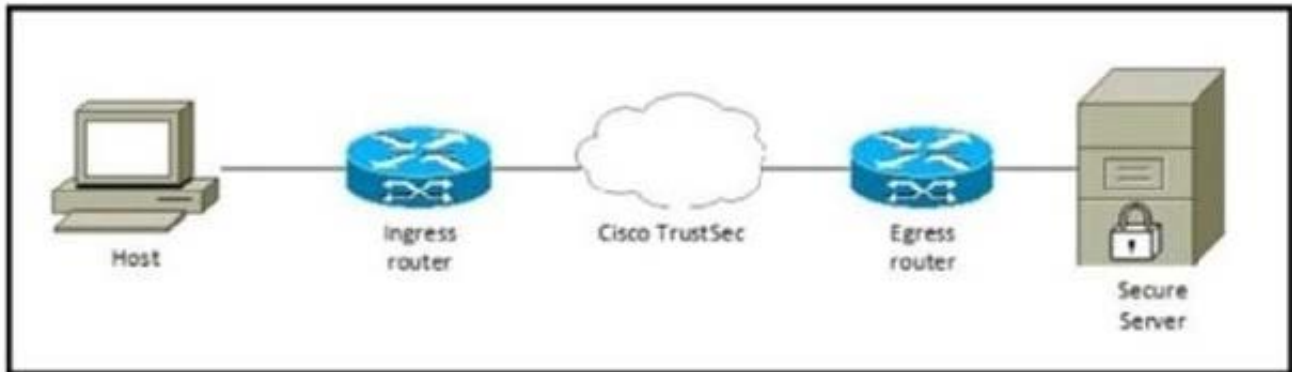
- A. MAB and if user not found, continue
- B. MAB and if authentication failed, continue
- C. Dot1x and if user not found, continue
- D. Dot1x and if authentication failed, continue

Correct Answer: A



QUESTION 7

Refer to the exhibit.



Which component must be configured to apply the SGACL?

- A. egress router
- B. host
- C. secure server
- D. ingress router

Correct Answer: A

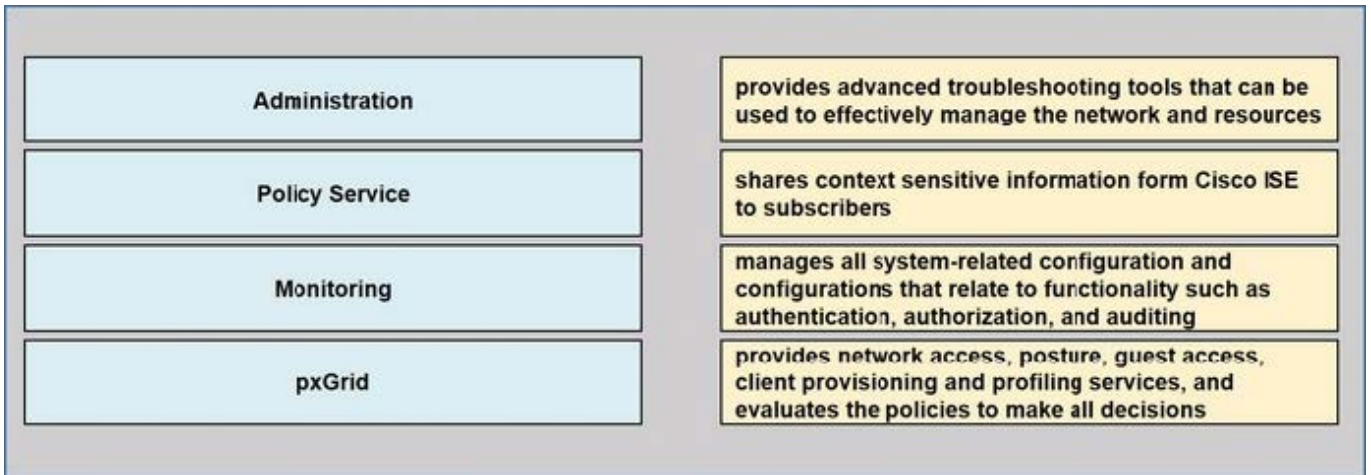
https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html#52796

QUESTION 8

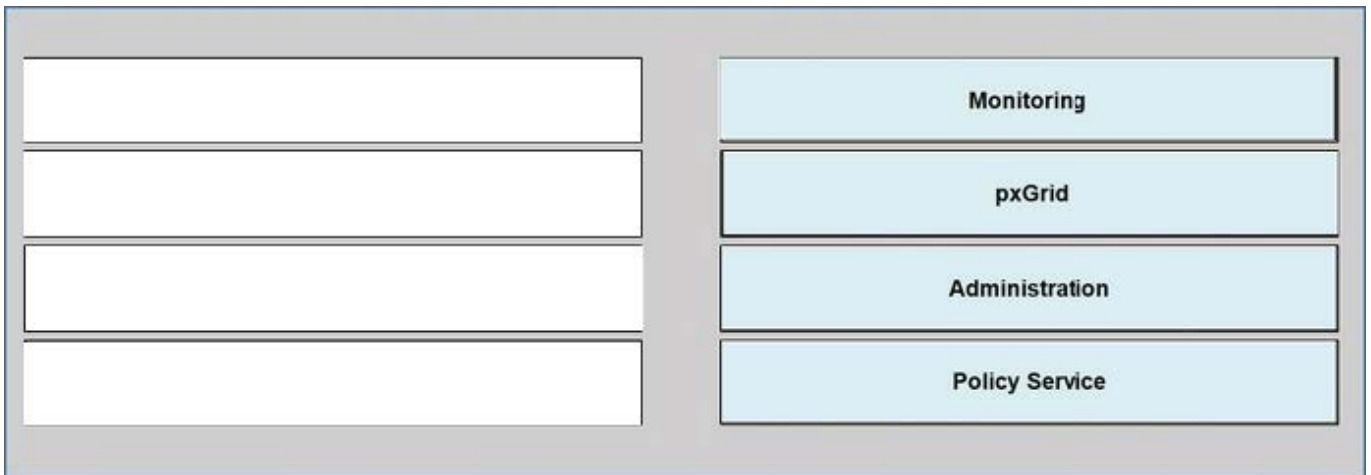
DRAG DROP

Drag the Cisco ISE node types from the left onto the appropriate purposes on the right.

Select and Place:



Correct Answer:



Monitoring = provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources

Policy Service = provides network access, posture, guest access, client provisioning, and profiling services.

This persona evaluates the policies and makes all the decisions.

Administration = manages all system-related configuration and configurations that relate to functionality such as authentication, authorization, auditing, and so on pxGrid = shares context-sensitive information from Cisco ISE to subscribers

https://www.cisco.com/c/en/us/td/docs/security/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_011.html#ID57

QUESTION 9

An administrator is manually adding a device to a Cisco ISE identity group to ensure that it is able to access the network when needed without authentication Upon testing, the administrator notices that the device never hits the correct authorization policy line using the condition EndPoints LogicalProfile EQUALS static_list Why is this occurring?

A. The dynamic logical profile is overriding the statically assigned profile



- B. The device is changing identity groups after profiling instead of remaining static
- C. The logical profile is being statically assigned instead of the identity group
- D. The identity group is being assigned instead of the logical profile

Correct Answer: C

QUESTION 10

Refer to the exhibit.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# aaa authorization network default group radius
```

A network engineer is configuring the switch to accept downloadable ACLs from a Cisco IAS server. Which two commands should be run to complete the configuration? (Choose two)

- A. AAA authorization auth-proxy default group radius
- B. radius server vsa send authentication
- C. radius-server attribute 8 include-in-access-req
- D. IP device tracking
- E. dot1x system-auth-control

Correct Answer: BC

QUESTION 11

An engineer is configuring 802.1X and is testing out their policy sets. After authentication, some endpoints are given an access-reject message but are still allowed onto the network. What is causing this issue to occur?

- A. The switch port is configured with authentication event server dead action authorize vlan.
- B. The authorization results for the endpoints include a dACL allowing access.
- C. The authorization results for the endpoints include the Trusted security group tag.
- D. The switch port is configured with authentication open.

Correct Answer: D

**QUESTION 12**

An administrator has manually added the MAC address of a wireless device to the Blocklist Identity Group for testing. When the device connects to the wireless network it triggers the Wireless Block List Default rule, but the device is still allowed to access the wireless network. What additional step must be taken to resolve this issue?

- A. Disable URL redirection on the Authorization Profile.
- B. Enable SNMP with read and write access on the Cisco WLC.
- C. Create an ACL named BLOCKHOLE on the Cisco WLC.
- D. Change the Access Type under the Authorization Profile to ACCESS_REJECT.

Correct Answer: D

QUESTION 13

Which deployment mode allows for one or more policy service nodes to be used for session failover?

- A. centralized
- B. secondary
- C. standalone
- D. distributed

Correct Answer: D

[Latest 300-715 Dumps](#)

[300-715 Practice Test](#)

[300-715 Exam Questions](#)