

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.pass2lead.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

An administrator wants to configure network device administration and is trying to decide whether to use TACACS* or RADIUS. A reliable protocol must be used that can check command authorization

Which protocol meets these requirements and why?

- A. TACACS+ because it runs over TCP
- B. RADIUS because it runs over UDP
- C. RADIUS because it runs over TCP.
- D. TACACS+ because it runs over UDP

Correct Answer: A

QUESTION 2

What must be configured on the Cisco ISE authentication policy for unknown MAC addresses/identities for successful authentication?

- A. pass
- B. reject
- C. drop
- D. continue

Correct Answer: D

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_id_stores.html

QUESTION 3

Which two actions must be verified to confirm that the internet is accessible via guest access when configuring a guest portal? (Choose two.)

- A. The guest device successfully associates with the correct SSID.
- B. The guest user gets redirected to the authentication page when opening a browser.
- C. The guest device has internal network access on the WLAN.
- D. The guest device can connect to network file shares.
- E. Cisco ISE sends a CoA upon successful guest authentication.

Correct Answer: BE

QUESTION 4

A network engineer is configuring a portal on Cisco ISE for employees. Employees must use this portal when registering personal devices with native supplicants. For onboarding devices connected with Cisco switches and Cisco wireless LAN controllers, the internal CA must be used. Which portal type must the engineer configure?

- A. Personal Device portal
- B. Client Provisioning portal
- C. Bring Your Own Device portal
- D. My Devices portal

Correct Answer: B

QUESTION 5

An engineer is configuring a guest password policy and needs to ensure that the password complexity requirements are set to mitigate brute force attacks. Which two requirements complete this policy? (Choose two.)

- A. minimum password length
- B. active username limit
- C. access code control
- D. password expiration period
- E. username expiration date

Correct Answer: AD

QUESTION 6

Which two components are required for creating a Native Supplicant Profile within a BYOD flow? (Choose two)

- A. Windows Settings
- B. Connection Type
- C. iOS Settings

D. Redirect ACL

E. Operating System

Correct Answer: BE

https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010101.html#reference_21024A3B2B27427EAC78495E56962729

QUESTION 7

Which description of the use of low-impact mode in a Cisco ISE deployment is correct?

A. It continues to use the authentication open capabilities of the switch port, which allows traffic to enter the switch before an authorization result.

B. Low-impact mode must be the final phase in deploying Cisco ISE into a network environment using the phased approach.

C. It enables authentication (with authentication open), sees exactly which devices fail and which succeed, and corrects the failed authentications before they

D. The port does not allow any traffic before the authentication (except for EAP, Cisco Discovery Protocol, and LLDP), and then the port is assigned to specific authorization results after the authentication

Correct Answer: C

QUESTION 8

Which file setup method is supported by ZTP on physical appliances?

A. cfg

B. iso

C. img

D. ova

Correct Answer: C

QUESTION 9

An engineer needs to create a Self-Registered Guest Portal in Cisco ISE in which guest users receive their passwords via SMS. Which two settings must be configured to accomplish this task? (Choose two.)

A. Choose the SMS provider previously configured as a SMS gateway under the Registration Form Settings.

- B. Select SMS for the Send Credential upon notification setting under Registration Form Settings.
- C. Choose the SMS provider previously configured as a SMS gateway under Device Registration Settings.
- D. Select Allow employees to use personal devices and SMS for notifications under BYOD.
- E. Select SMS for the Send Credential upon notification setting under the Login Page Settings.

Correct Answer: AE

Explanation:

Option A because under the registration form settings, the engineer needs to choose the SMS provider that has been previously configured as an SMS gateway. This ensures that the guest user's password will be sent via SMS.

Option E because under the login page settings, the engineer needs to select SMS for the Send Credential upon notification setting. This setting ensures that the guest user's password is sent to them via SMS when they complete the

registration process.

QUESTION 10

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

Correct Answer: C

QUESTION 11

When configuring Active Directory groups, an administrator is attempting to retrieve a group that has a name that is ambiguous with another group. What must be done so that the correct group is returned?

- A. Use the SID as the identifier for the group.
- B. Configure MAB to utilize one group, and 802.1x to utilize the conflicting group.
- C. Select both groups, and use a TCT pointer to identify the appropriate one.
- D. Utilize MIB entries to identify the desired group.

Correct Answer: A

QUESTION 12

During BYOD flow, from where does a Microsoft Windows PC download the Network Setup Assistant?

- A. Cisco App Store
- B. Microsoft App Store
- C. Cisco ISE directly
- D. Native OTA functionality

Correct Answer: C

QUESTION 13

An engineer must configure guest access on Cisco ISE for company visitors. Which step must be taken on the Cisco ISE PSNs before a guest portal is configured?

- A. Install SSL certificates
- B. Create a node group
- C. Enable profiling services
- D. Enable session services

Correct Answer: A

QUESTION 14

Which two default endpoint identity groups does Cisco ISE create? (Choose two)

- A. Unknown
- B. whitelist
- C. end point
- D. profiled
- E. blacklist

Correct Answer: AD

Default Endpoint Identity Groups Created for Endpoints Cisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints, Profiled, RegisteredDevices, and Unknown. In addition, it creates two more identity groups, such as Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group. A parent group is the default identity group that exists in the system.

Cisco ISE creates the following endpoint identity groups:

1.

Blacklist--This endpoint identity group includes endpoints that are statically assigned to this group in Cisco ISE and endpoints that are block listed in the device registration portal. An authorization profile can be defined in Cisco ISE to permit, or deny network access to endpoints in this group.

2.

GuestEndpoints--This endpoint identity group includes endpoints that are used by guest users.

3.

Profiled--This endpoint identity group includes endpoints that match endpoint profiling policies except Cisco IP phones and workstations in Cisco ISE.

4.

RegisteredDevices--This endpoint identity group includes endpoints, which are registered devices that are added by an employee through the devices registration portal. The profiling service continues to profile these devices normally when they are assigned to this group. Endpoints are statically assigned to this group in Cisco ISE, and the profiling service cannot reassign them to any other identity group. These devices will appear like any other endpoint in the endpoints list. You can edit, delete, and block these devices that you added through the device registration portal from the endpoints list in the Endpoints page in Cisco ISE. Devices that you have blocked in the device registration portal are assigned to the Blacklist endpoint identity group, and an authorization profile that exists in Cisco ISE redirects blocked devices to a URL, which displays "Unauthorised Network Access", a default portal page to the blocked devices.

5.

Unknown--This endpoint identity group includes endpoints that do not match any profile in Cisco ISE.

In addition to the above system created endpoint identity groups, Cisco ISE creates the following endpoint identity groups, which are associated to the Profiled identity group:

1.

Cisco-IP-Phone--An identity group that contains all the profiled Cisco IP phones on your network.

2.

Workstation--An identity group that contains all the profiled workstations on your network.

https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html

QUESTION 15

A laptop was stolen and a network engineer added it to the block list endpoint identity group What must be done on a new Cisco ISE deployment to redirect the laptop and restrict access?

- A. Select DenyAccess within the authorization policy.
- B. Ensure that access to port 8443 is allowed within the ACL.
- C. Ensure that access to port 8444 is allowed within the ACL.

D. Select DROP under If Auth fail within the authentication policy.

Correct Answer: C

https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_010000.html

[300-715 PDF Dumps](#)

[300-715 VCE Dumps](#)

[300-715 Study Guide](#)