

**100%** Money Back  
**Guarantee**

**Vendor:**Cisco

**Exam Code:**300-208

**Exam Name:**Implementing Cisco Secure Access  
Solutions

**Version:**Demo

### QUESTION 1

Which command enables static PAT for TCP port 25?

- A. nat (outside,inside) static 209.165.201.3 209.165.201.226 eq smtp
- B. nat static 209.165.201.3 eq smtp
- C. nat (inside,outside) static 209.165.201.3 service tcp smtp smtp
- D. static (inside,outside) 209.165.201.3 209.165.201.226 netmask 255.255.255.255

Correct Answer: C

---

### QUESTION 2

Which interface-level command is needed to turn on dot1x authentication?

- A. authentication pae authenticator
- B. aaa server radius dynamic-author
- C. authentication host-mode single-host
- D. dot1x system-auth-control

Correct Answer: D

In order to enable 802.1x functionality, enter this command: Switch(config)# dot1x system-auth-control

---

### QUESTION 3

Which OS has Anyconnect posture support?

- A. Windows
- B. Mac OS
- C. Linux

Correct Answer: AB

[http://www.cisco.com/c/en/us/td/docs/security/vpn\\_client/anyconnect/anyconnect40/release/notes/b\\_Release\\_Notes\\_AnyConnect\\_4\\_0.html](http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/release/notes/b_Release_Notes_AnyConnect_4_0.html)

---

### QUESTION 4

After you connected unmanaged switch to the port dot1x failed,what is the problem?

- A. missing command "mab"
- B. there is no Bpdu in the port
- C. eapol packet not received in the port
- D. missing command "authentication host-mode multi-host"
- E. missing command "authentication host-mode multi-auth"

Correct Answer: E

---

#### QUESTION 5

Which two options are valid for configuring IEEE 802.1AE MACSec between switches in a TrustSec network? (Choose two.)

- A. manually on links between supported switches
- B. in the Cisco Identity Services Engine
- C. in the global configuration of a TrustSec non-seed switch
- D. dynamically on links between supported switches
- E. in the Cisco Secure Access Control System
- F. in the global configuration of a TrustSec seed switch

Correct Answer: AD

---

#### QUESTION 6

A network security engineer is considering configuring 802.1x port authentication such that a single host is allowed to be authenticated for data and another single host for voice. Which port authentication host mode can be used to achieve this configuration?

- A. single-host
- B. multihost
- C. multauth
- D. multidomain

Correct Answer: D

---

#### QUESTION 7

Which three statements about the Cisco ISE profiler are true? (Choose three.)

- A. It sends endpoint data to AAA servers.
- B. It collects endpoint attributes.
- C. It stores MAC addresses for endpoint systems.
- D. It monitors and polices router and firewall traffic.
- E. It matches endpoints to their profiles.
- F. It stores endpoints in the Cisco ISE database with their profiles.

Correct Answer: BEF

---

### QUESTION 8

An engineer has discovered that a NAD is already configured to send packets to the cisco ISE node running session services, which probe profile requires the simplest configuration?

- A. RADIUS
- B. DHCP
- C. SPAN
- D. NMAP
- E. HTTP

Correct Answer: A

---

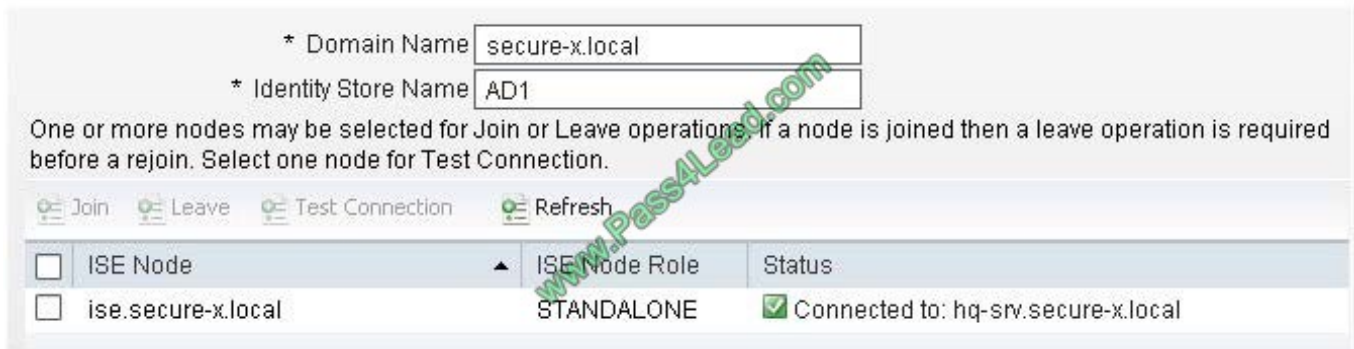
### QUESTION 9

#### CORRECT TEXT

The Secure-X company has started to test the 802.1X authentication deployment using the Cisco Catalyst 3560-X layer 3 switch and the Cisco ISEv12 appliance. Each employee desktop will be connected to the 802.1X enabled switch port and will use the Cisco AnyConnect NAM 802.1X supplicant to log in and connect to the network. Your particular tasks in this simulation are to create a new identity source sequence named AD\_internal which will first use the Microsoft Active Directory (AD1) then use the ISE Internal User database. Once the new identity source sequence

has been configured, edit the existing Dot1X authentication policy to use the new AD\_internal identity source sequence.

The Microsoft Active Directory (AD1) identity store has already been successfully configured, you just need to reference it in your configuration.



In addition to the above, you are also tasked to edit the IT users authorization policy so IT users who successfully authenticated will get the permission of the existing IT\_Corp authorization profile.

Perform this simulation by accessing the ISE GUI to perform the following tasks:

Create a new identity source sequence named AD\_internal to first use the Microsoft Active Directory (AD1) then use the ISE Internal User database

Edit the existing Dot1X authentication policy to use the new AD\_internal identity source sequence:

If authentication failed-reject the access request

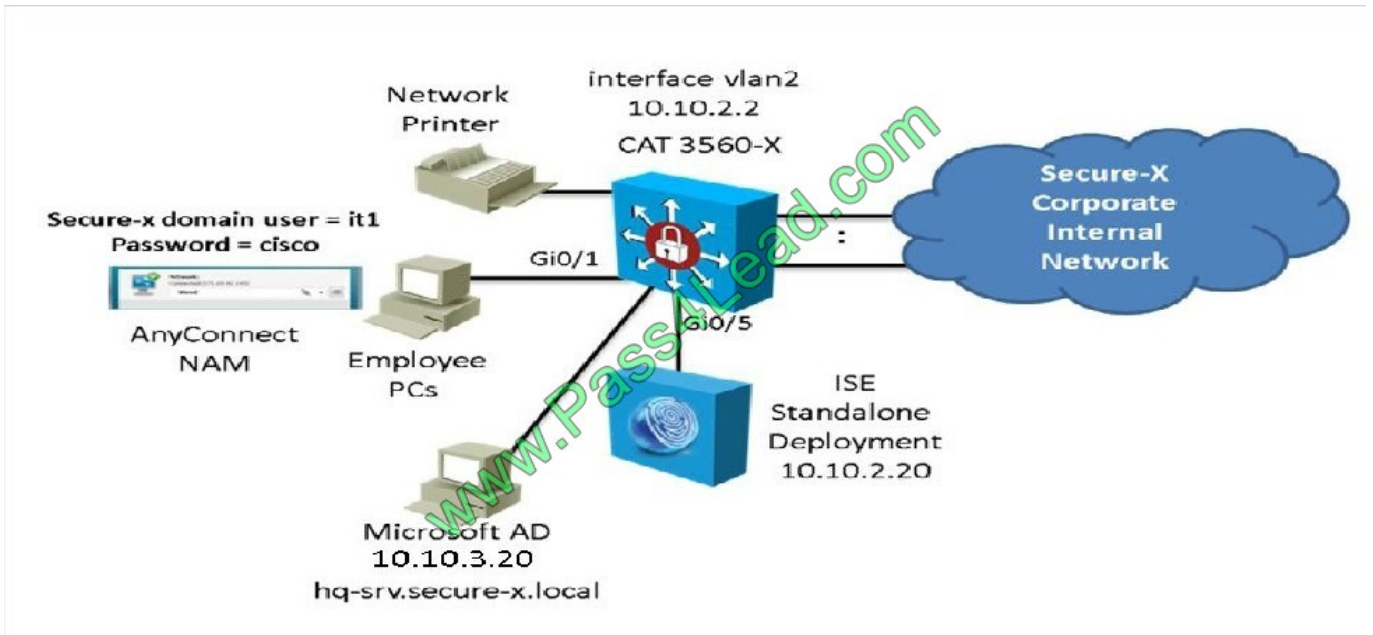
If user is not found in AD-Drop the request without sending a response

If process failed-Drop the request without sending a response

Edit the IT users authorization policy so IT users who successfully authenticated will get the permission of the existing IT\_Corp authorization profile.

To access the ISE GUI, click the ISE icon in the topology diagram. To verify your configurations, from the ISE GUI, you should also see the Authentication Succeeded event for the it1 user after you have successfully defined the Dot1X authentication policy to use the Microsoft Active Directory first then use the ISE Internal User Database to authenticate the user. And in the Authentication Succeeded event, you should see the IT\_Corp authorization profile being applied to the it1 user. If your configuration is not correct and ISE can't authenticate the user against the Microsoft Active Directory, you should see the Authentication Failed event instead for the it1 user.

Note: If you make a mistake in the Identity Source Sequence configuration, please delete the Identity Source Sequence then re-add a new one. The edit Identity Source Sequence function is not implemented in this simulation.



Virtual Terminal

CISCO Identity Services Engine

ise | admin | Logout | Feedback

Home Operations Policy Administration Setup As

Metrics

Total Endpoints: 2

Active Endpoints: 0

Active Guests: 0

Prohibited Endpoints: 2

Posture Compliance: 0%

System Summary

Name	Utilization and Latency 24h		
	CPU	Memory	Authentic...
ise			

Alarms

Name	Occurrences	Last Occu
Insufficient Virtual Mac...	39 times	1 Hr 7 ...
Authentication Inactivity	629 times	1 Hr 49 ...
No Configuration Back...	133 times	1 Hr 57 ...
Configuration Changed	432 times	4 mont...
RTP Sync Failure	545 times	6 mont...
DNS Resolution Failure	551 times	6 mont...
Unknown NAD	23 times	6 mont...

Authentications

Passed: 0

Failed: 0

Distribution By:

- Identity Store: No Data Available
- Identity Group: No Data Available
- Network Devi...: No Data Available
- Location: No Data Available
- Failure Reason: No Data Available

Profiler Activity

Total: 0

Distribution By:

- Endpoint Pro...: No Data Available

Posture Compliance

Total: 0

Distribution By:

- Posture Status: No Data Available

Correct Answer: Review the for full configuration and solution.

Step 1: create a new identity source sequence named AD\_internal which will first use the Microsoft Active Directory (AD1) then use the ISE Internal User database as shown below:

Terminal

Cisco Identity Services Engine

Home Operations Policy Administration

System Identity Management Network Resources Web Portal Management Feed Service

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequences List > New Identity Source Sequence

### Identity Source Sequence

Identity Source Sequence

\* Name: AD\_Internal

Description:

Certificate Based Authentication

Select Certificate Authentication Profile: CommonName

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Internal Endpoints Guest Users	>	AD1 Internal Users	⌵
-----------------------------------	---	-----------------------	---

Scenario | **TOPOLOGY**

Step 2: Edit the existing Dot1x policy to use the newly created Identity Source:

Terminal

ise | admin | Logout

**Identity Services Engine**

Home Operations Policy Administration

Authentication Authorization Profiling Posture Client Provisioning Security Group Access

### Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity policy Type

Simple  Rule-Based

MAB : If Wired\_802.1X OR Wireless\_802.1X Allow Protocols : Default Network

and  Default : use Default

Dot1X : If Wired\_802.1X OR Wireless\_802.1X Allow Protocols : Default Network

Default Use Internal Endpoints

Identity Source AD\_Internal

**Options**

If authentication failed Reject

If user not found Reject

Scenario **TOPOLOGY**

Then hit Done and save.

#### QUESTION 10

Which protocol is EAP encapsulated in for communications between the authenticator and the authentication server?

- A. EAP-MD5
- B. IPsec
- C. EAPOL
- D. RADIUS

Correct Answer: D

#### QUESTION 11



A user reports that a switch's RADIUS accounting packets are not being seen on the Cisco ISE server Which command is the user missing in the switch's configuration?

- A. radius-server vsa send accounting
- B. aaa accounting network default start-stop group radius
- C. aaa accounting resource default start-stop group radius
- D. aaa accounting exec default start-stop group radius

Correct Answer: A

---

#### **QUESTION 12**

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

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

Correct Answer: B

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

## Try our product !

**100%** Guaranteed Success

**100%** Money Back Guarantee

**365** Days Free Update

**Instant Download** After Purchase

**24x7** Customer Support

Average **99.9%** Success Rate

More than **800,000** Satisfied Customers Worldwide

Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

## Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p><b>One Year Free Update</b> Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p><b>Money Back Guarantee</b> To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p><b>Security &amp; Privacy</b> We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.