SY0-601$^{Q\&As}$

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.geekcert.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

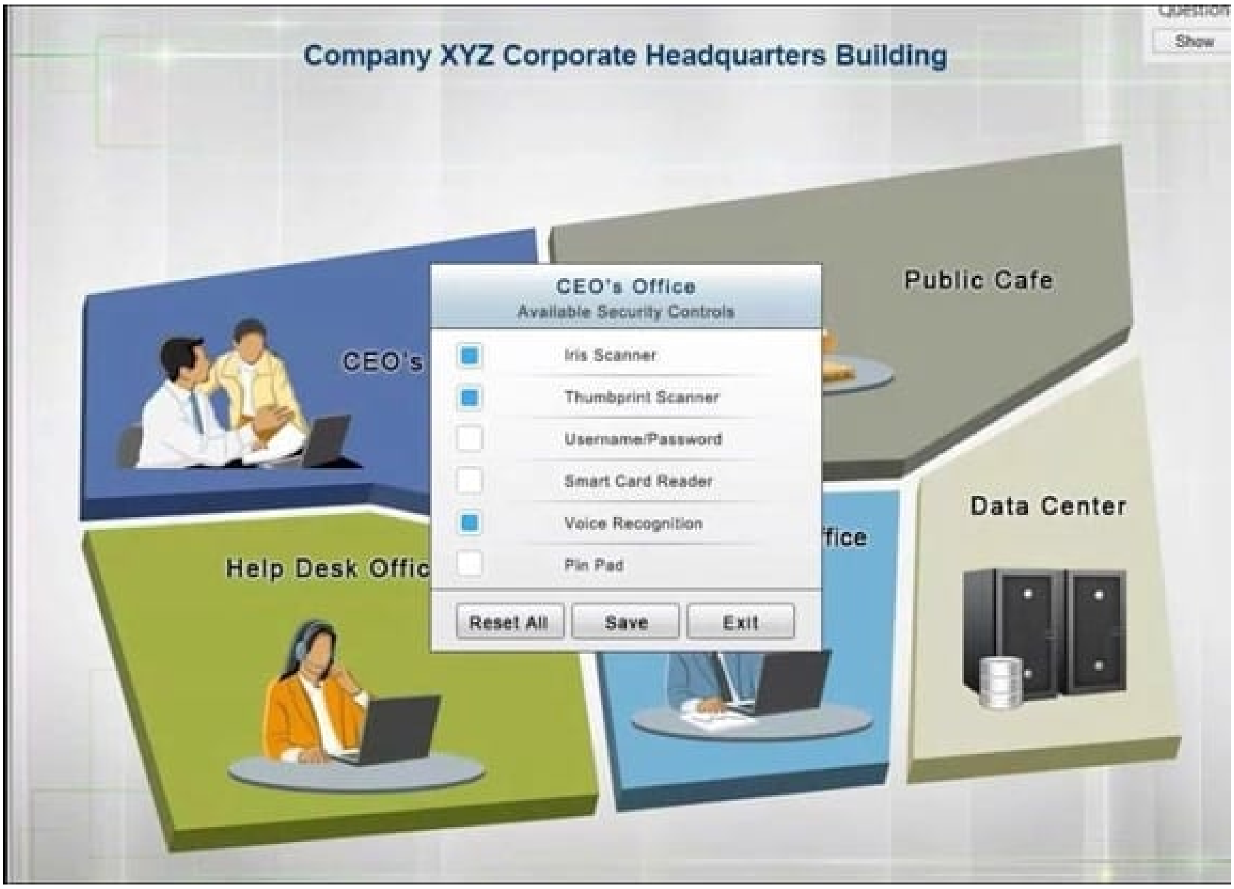
The Chief Executive Officer\\'s (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.

The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.

In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.

In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.

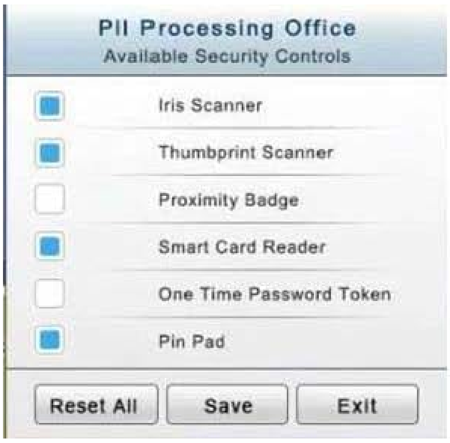
The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.



CEO's Office
Available Security Controls

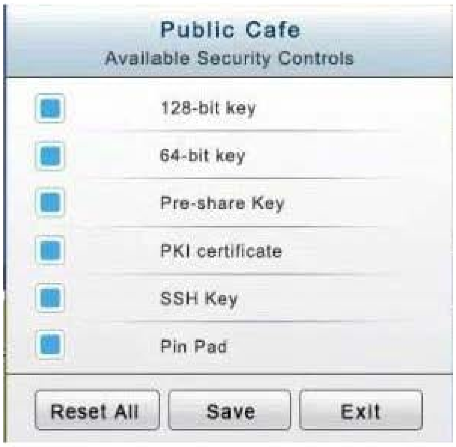
☑ Iris Scanner
☑ Thumbprint Scanner
☐ Username/Password
☐ Smart Card Reader
☑ Voice Recognition
☐ Pin Pad

Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



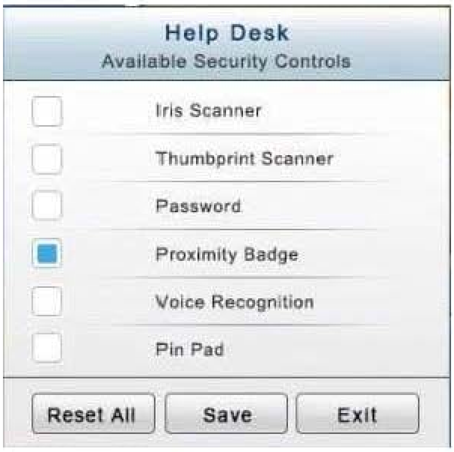
PII Processing Office
Available Security Controls

- ☑ Iris Scanner
- ☑ Thumbprint Scanner
- □ Proximity Badge
- ☑ Smart Card Reader
- □ One Time Password Token
- ☑ Pin Pad



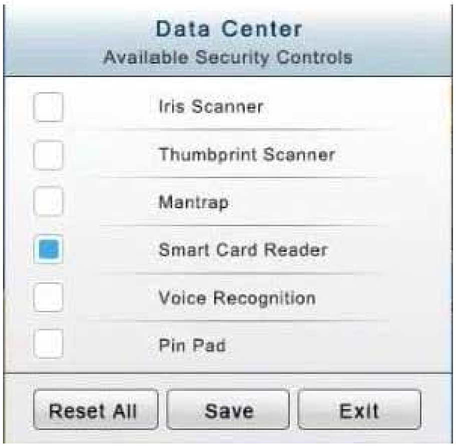
Public Cafe
Available Security Controls

- ☑ 128-bit key
- ☑ 64-bit key
- ☑ Pre-share Key
- ☑ PKI certificate
- ☑ SSH Key
- ☑ Pin Pad



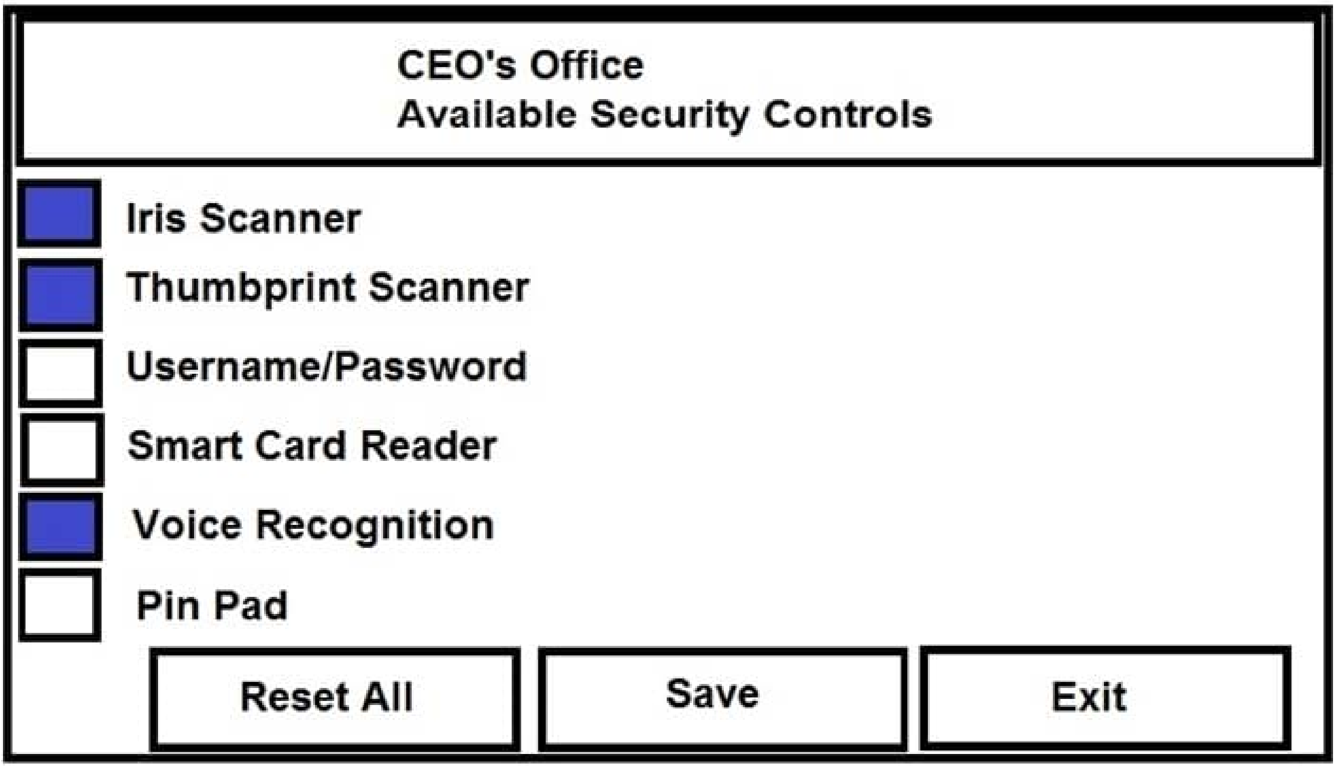
Help Desk
Available Security Controls

- □ Iris Scanner
- □ Thumbprint Scanner
- □ Password
- ☑ Proximity Badge
- □ Voice Recognition
- □ Pin Pad



Data Center
Available Security Controls

- □ Iris Scanner
- □ Thumbprint Scanner
- □ Mantrap
- ☑ Smart Card Reader
- □ Voice Recognition
- □ Pin Pad

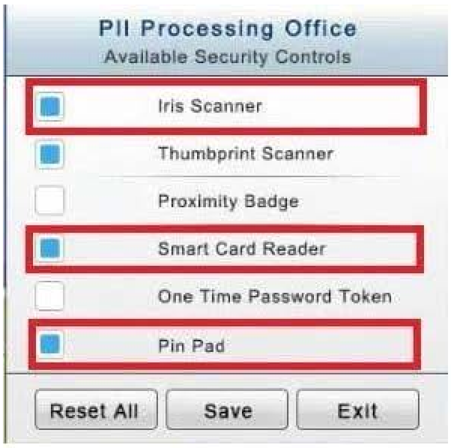


CEO's Office
Available Security Controls

☑ Iris Scanner
☑ Thumbprint Scanner
□ Username/Password
□ Smart Card Reader
☑ Voice Recognition
□ Pin Pad

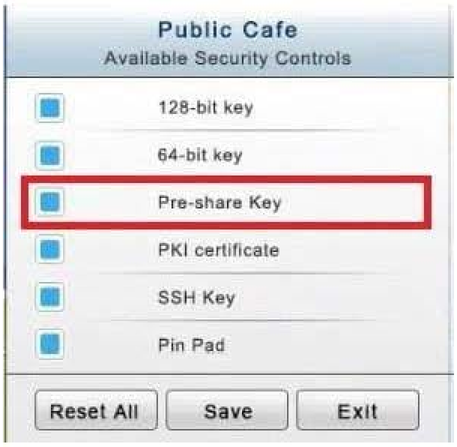
Correct Answer:

See the solution below.



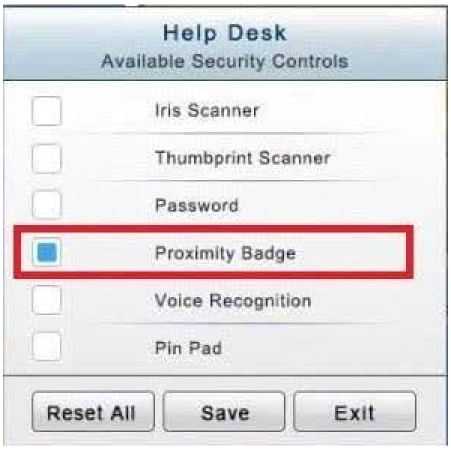
PII Processing Office
Available Security Controls

- ☑ Iris Scanner
- ☑ Thumbprint Scanner
- □ Proximity Badge
- ☑ Smart Card Reader
- □ One Time Password Token
- ☑ Pin Pad



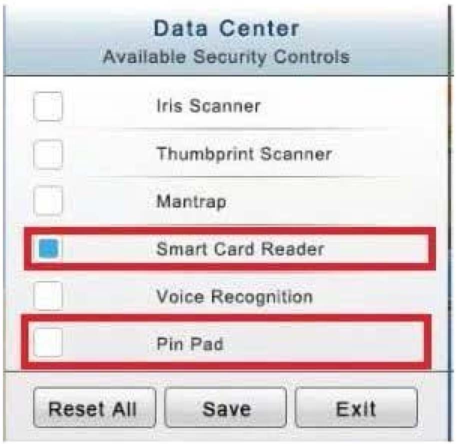
Public Cafe
Available Security Controls

- ☑ 128-bit key
- ☑ 64-bit key
- ☑ Pre-share Key
- ☑ PKI certificate
- ☑ SSH Key
- ☑ Pin Pad



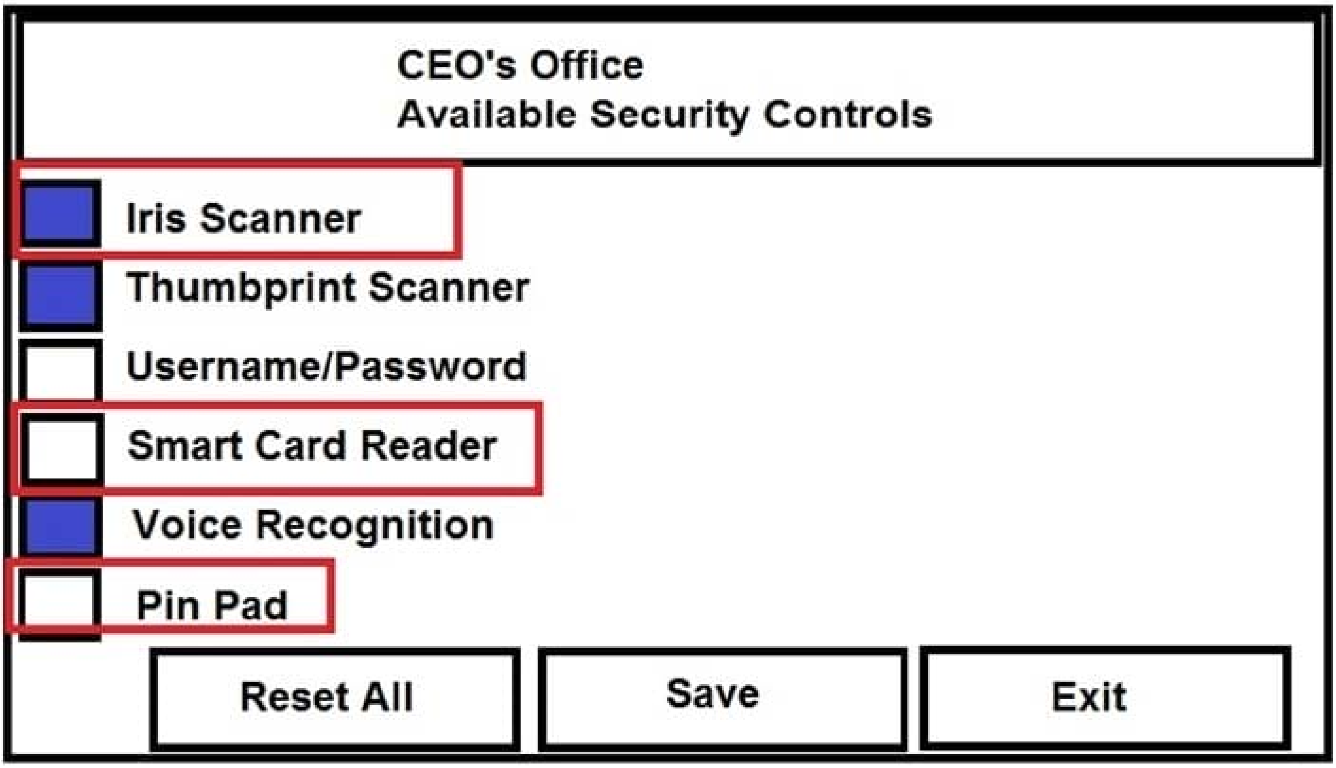
Help Desk
Available Security Controls

- □ Iris Scanner
- □ Thumbprint Scanner
- □ Password
- ☑ Proximity Badge
- □ Voice Recognition
- □ Pin Pad



Data Center
Available Security Controls

- □ Iris Scanner
- □ Thumbprint Scanner
- □ Mantrap
- ☑ Smart Card Reader
- □ Voice Recognition
- □ Pin Pad



CEO's Office
Available Security Controls

■ Iris Scanner

■ Thumbprint Scanner

□ Username/Password

□ Smart Card Reader

■ Voice Recognition

□ Pin Pad

QUESTION 2

A systems administrator is auditing all company servers to ensure they meet the minimum security baseline. While auditing a Linux server, the systems administrator observes the /etc/shadow file has permissions beyond the baseline recommendation.

Which of the following commands should the systems administrator use to resolve this issue?

A. chmod

B. grep

C. dd

D. passwd

Correct Answer: A

QUESTION 3

Field workers in an organization are issued mobile phones on a daily basis All the work is performed within one city and the mobile phones are not used for any purpose other than work The organization does not want these pnones used for personal purposes. The organization would like to issue the phones to workers as permanent devices so the pnones do not need to be reissued every day Qven the conditions described, which of the following technologies would BEST meet these requirements\\'

A. Geofencing

B. Mobile device management

C. Containenzation

D. Remote wiping

Correct Answer: B

MDM is the best solution here, Company wants to issue a COBO device therefore no containerization

Geofencing and remote wiping are capabilites that are provided by an MDM solution

QUESTION 4

An employee used a corporate mobile device during a vacation Multiple contacts were modified in the device vacation.

Which of the following method did attacker to insert the contacts without having \\'Physical access to device?

A. Jamming

B. BluJacking

C. Disassoaatm

D. Evil twin

Correct Answer: B

bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers. Bluejacking does not involve device hijacking, despite what the name implies. In this context, a human might say that the best answer to the question is B. BluJacking, because it is a method that can insert contacts without having physical access to the device.

QUESTION 5

A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan types would produce the BEST vulnerability scan report?

A. Port

B. Intrusive

C. Host discovery

D. Credentialed

Correct Answer: A

Credentialed scan will include versions of software applications that might be vulnerable