

# ITCertMagic

ITCertMagic

HOME

ALL VENDORS

★ GUARANTEE

? FAQ

TESTIMONIALS

CART (0)



Try **PDF Demo** before you buy

### 28 Top Certifications

Apr

- ▶ HP CSE ▶ Avaya Specialist
- ▶ ACE InDesign ▶ LPIC Level1
- ▶ Apple Certified Pro ▶ VCP6-CMA
- ▶ JNCDA ▶ Aruba Certification ▶ CCA XP
- ▶ ICND1 ▶ RCSP ▶ GAQM LCP
- ▶ JNCDS-SEC ▶ Fireware Essentials
- ▶ Oracle Spatial 11g

### 28 Top Vendors

Apr

- ▶ ISM ▶ HRCI
- ▶ Palo Alto Networks ▶ NSCA
- ▶ SUN ▶ ISQI ▶ Huawei
- ▶ American College ▶ IIA ▶ ARM
- ▶ Pegasystems ▶ OMG ▶ Simens ▶ GRE
- ▶ HAAD ▶ PCI ▶ BBPSD ▶ SCO
- ▶ SugarCRM ▶ Logical Operations ▶ IIBA
- ▶ Altiris ▶ Alfresco ▶ AMA ▶ Informatca

### What Client's Say

“ There are some less than 8 new questions, so this 70-695 dump is still mostly valid. Wrote the exams today and passed. ”

 **Timothy**  
★★★★★

<http://www.itcertmagic.com/>

Pass-Guaranteed Certification Exam Questions | Exam Dumps - ITCertMagic

**Exam** : **FCP\_FAC\_AD-6.5**

**Title** : FCP—FortiAuthenticator 6.5  
Administrator

**Vendor** : Fortinet

**Version** : DEMO

**NO.1** Which two behaviors do certificate revocation lists (CRLs) on FortiAuthenticator exhibit? (Choose two.)

- A. CRLs can be distributed only through the SCEP server
- B. Revoked certificates are automatically placed on the CRL
- C. All local CAs share the same CRLs
- D. CRLs contain the serial number of the certificate that has been revoked

**Answer:** B D

Explanation:

Revoked certificates are automatically added to the CRL by FortiAuthenticator.

CRLs list the serial numbers of certificates that have been revoked, allowing clients to identify and reject them.

**NO.2** Refer to the exhibit.

The screenshot shows the 'Edit SSO Configuration' page for a FortiGate device. The configuration includes:

- Listening port: 8000
- Enable encryption:
- Enable authentication:
- Secret key: [masked]
- Login expiry: 480 minutes
- Extend user session beyond logoff by: 0 seconds (0-3600)
- Enable NTLM authentication:**  (highlighted with a red box)
- User domain: training.bb

Which functionality does the Enable NTLM option provide?

- A. It allows FortiAuthenticator to message end users using the FortiClient for SSO.
- B. It forces FortiClient users to use two-factor authentication when using FortiClient for SSO.
- C. It prevents users from authenticating to an unauthorized AD server.
- D. It enables tracking and recording all authentications performed through FortiClient.

**Answer:** C

Explanation:

Enabling NTLM authentication in this FortiAuthenticator SSO configuration ensures that user authentication requests are validated against the specified domain, preventing users from authenticating to an unauthorized Active Directory server.

**NO.3** Why would you configure an OCSP responder URL in an end-entity certificate?

- A. To identify the end point that a certificate has been assigned to
- B. To designate a server for certificate status checking
- C. To provide the CRL location for the certificate

**D.** To designate the SCEP server to use for CRL updates for that certificate

**Answer:** B

Explanation:

Configuring an OCSP responder URL in an end-entity certificate designates the server that will be queried to check the real-time revocation status of the certificate.

**NO.4** Refer to the exhibit.

Portal policy

Policy type Portal selection criteria Authorized clients Authentication type

Specify a condition on the parameters of the HTTP request that must be met to access this portal.  
For example, a condition to restrict the portal to users from subnet 192.168.1.0/24 would be:  
HTTP parameter = userid  
Operator = [ip]in\_range  
Value = 192.168.1.0/24

Portal Rule Conditions

Portal Rule Condition:

Not

HTTP parameter:  +

Operator:  ▾

Value:

Portal Rule Condition:

Not

HTTP parameter:  +

Operator:  ▾

Value:

+ Add Portal Rule Condition

Previous Discard and exit Next

An administrator has a captive portal configuration on their FortiGate that directs users to a portal page on FortiAuthenticator. A user whose laptop has an IP address of 10.0.1.85 and is connected through the Guest SSID, is failing to load the portal page.

What is the most likely cause of the problem?

- A.** The host IP address is not in the required range.
- B.** The host is connected to a prohibited SSID.
- C.** The portal page will only be presented to wired hosts.
- D.** The IP address is incorrect for the SSID.

**Answer:** B

Explanation:

The second portal rule condition explicitly uses Not with the SSID value "Guest", which means that users connected through the Guest SSID are excluded from accessing the portal, causing the failure

for this user.

**NO.5** Which FSSO discovery method transparently detects logged off users without having to rely on external features such as WMI polling?

- A. RADIUS accounting
- B. FortiClient SSO mobility agent
- C. DC polling
- D. Windows AD polling

**Answer:** B

Explanation:

The FortiClient SSO Mobility Agent runs on the endpoint and communicates login and logoff events directly to FortiAuthenticator, allowing transparent detection of logged-off users without relying on external mechanisms like WMI polling.

**NO.6** When configuring an active-passive HA deployment, what is the recommended data synchronization path?

- A. Dedicated fiber channel
- B. Same VLAN
- C. Dedicated point-to-point VPN connection
- D. Direct cable connection

**Answer:** D

Explanation:

A direct cable connection is the recommended data synchronization path in an active-passive HA deployment because it provides the fastest, most reliable, and secure method for synchronizing data between FortiAuthenticator units without depending on external network infrastructure.

**NO.7** An administrator has just learned that an intermediate CA certificate signed by a FortiAuthenticator device acting as the Root CA has been compromised. Which two steps should the administrator take to resolve the security issue? (Choose two.)

- A. Revoke the Intermediate certificate so it is added to the CRL of the Root CA.
- B. Revoke all end-system and end-user certificates that this compromised intermediate CA has signed.
- C. Create a new intermediate certificate with the same private key.
- D. Update the OCSP responder URLs for the certificate.

**Answer:** A B

Explanation:

Revoking the compromised intermediate CA certificate adds it to the Root CA's CRL, preventing its further use.

All end-entity certificates issued by the compromised intermediate must be revoked, as their trust is no longer valid.

**NO.8** Which two capabilities does FortiAuthenticator offer when acting as a self-signed or local CA? (Choose two.)

- A. Validating other CA CRLs using OCSP

- B. Merging local and remote CRLs using SCEP
- C. Importing other CA certificates and CRLs
- D. Creating, signing, and revoking of X.509 certificates

**Answer:** C D

Explanation:

FortiAuthenticator can import other CA certificates and CRLs for trust and validation purposes. It can create, sign, and revoke X.509 certificates when acting as a self-signed or local CA.

**NO.9** What are three key features of FortiAuthenticator? (Choose three.)

- A. Identity management device
- B. Portal services
- C. Certificate authority
- D. Log server
- E. RSO server

**Answer:** A B C

Explanation:

FortiAuthenticator functions as an identity management device, handling user authentication and authorization.

It provides portal services for user self-registration, guest management, and authentication portals. It acts as a certificate authority, issuing and managing digital certificates for secure authentication.

**NO.10** A network administrator is using FortiAuthenticator as their RADIUS server for wired and wireless network access. The administrator wants to pass the users' group information back to the RADIUS clients when the users authenticate.

How does FortiAuthenticator accomplish this?

- A. RADIUS attributes
- B. RADIUS accounting
- C. Syslog messages
- D. REST API

**Answer:** A

Explanation:

FortiAuthenticator uses RADIUS attributes to pass additional information, such as user group membership, back to RADIUS clients during the authentication process.