

# NSE5\_FMG-6.0<sup>Q&As</sup>

Fortinet NSE 5 - FortiManager 6.0





## Pass Fortinet NSE5\_FMG-6.0 Exam with 100% Guarantee

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

[https://www.leads4pass.com/nse5\\_fmg-6-0.html](https://www.leads4pass.com/nse5_fmg-6-0.html)

100% Passing Guarantee  
100% Money Back Assurance

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

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



**QUESTION 1**

An administrator is unable to log in to FortiManager. Which one of the following troubleshooting step should you take to resolve the issue?

- A. Make sure FortiManager Access is enabled in the administrator profile
- B. Make sure Offline Mode is disabled
- C. Make sure the administrator IP address is part of the trusted hosts.
- D. Make sure ADOMs are enabled and the administrator has access to the Global ADOM

Correct Answer: C

---

**QUESTION 2**

View the following exhibit.

## Starting Log (Run the device)

### Start installing

```
Local-FortiGate $ config user device
```

```
Local-FortiGate (device) $ edit "mydevice"
```

```
new entry 'mydevice' added
```

```
Local-FortiGate (mydevice) $ next
```

```
MAC address can not be 0
```

```
Node_check_object fail!for mac 00:00:00:00:00:00
```

```
Attribute 'mac' value '00:00:00:00:00:00' checkingfail -33
```

```
Command fail. Return code 1
```

```
Local-FortiGate (device) $ end
```

```
...
```

```
Local-FortiGate $ config firewall policy
```

```
Local-FortiGate (policy) $ edit 2
```

```
New entry '2' added
```

```
Local-FortiGate (2) $ set name "Device_policy"
```

```
Local-FortiGate (2) $ set uuid 64...
```

```
Local-FortiGate (2) $ set srcintf "port3"
```

```
Local-FortiGate (2) $ set dstintf "port1"
```

```
Local-FortiGate (2) $ set srcaddr "all"
```

```
Local-FortiGate (2) $ set dstaddr "all"
```

```
Local-FortiGate (2) $ set action accept
```

```
Local-FortiGate (2) $ set schedule "always"
```

```
Local-FortiGate (2) $ set service "ALL"
```

```
Local-FortiGate (2) $ set devices "mydevice"
```

```
Entry not found in datasource
```

```
Value parse error before 'mydevice'
```

```
Command fail. Return code -3
```

```
Local-FortiGate (2) $ set nat enable
```

```
Local-FortiGate (2) $ next
```

```
Local-FortiGate (policy) $ end
```

```
...
```

Which statement is true regarding this failed installation log?

- A. Policy ID 2 is installed without a source address
- B. Policy ID 2 will not be installed
- C. Policy ID 2 is installed in disabled state
- D. Policy ID 2 is installed without a source device

Correct Answer: D

---

### QUESTION 3

View the following exhibit, which shows the Download Import Report:

```
Start to import config from devices(Remote-FortiGate) vdom (root)to adom (MyADOM),
Package(Remote-FortiGate)
"firewall address", SUCCESS,"(name=REMOTE_SUBNET,oid=580, new object)"
"firewall policy",SUCCESS,"(name=1, oid=990,new object)"
"firewall policy",FAIL,"(name=ID:2(#2), oid=991, reason=interface(interface binding
Contradiction.detail:any<-port6)binding fail)"
```

Why it is failing to import firewall policy ID 2?

- A. The address object used in policy ID 2 already exist in ADON database with any as interface association and conflicts with address object interface association locally on the FortiGate
- B. Policy ID 2 is configured from interface any to port6 FortiManager rejects to import this policy because any interface does not exist on FortiManager
- C. Policy ID 2 does not have ADOM Interface mapping configured on FortiManager
- D. Policy ID 2 for this managed FortiGate already exists on FortiManager in policy package named Remote-FortiGate.

Correct Answer: A

---

### QUESTION 4

- A. port2
- B. virtual-wan-link
- C. port1
- D. auto-discovery

Correct Answer: B

## QUESTION 5

View the following exhibit:

```
#diagnose fmupdate view-serverlist fds
Fortiguard Server Comm: Enabled
Server Override Mode: Loose
FDS server list :
Index Address          Port    TimeZone  Distance  Source
-----
*0    10.0.1.50             8890    -5         0         CLI
1     96.45.33.89           443     -5         0         FDNI
2     96.45.32.81           443     -5         0         FDNI
....
38  fds1.fortinet.com     443     -5         0         DEFAULT
```

How will FortiManager try to get updates for antivirus and IPS?

- A. From the list of configured override servers with ability to fall back to public FDN servers
- B. From the configured override server list only
- C. From the default server fds1.fortinet.com
- D. From public FDNI server with highest index number only

Correct Answer: A

[Latest NSE5\\_FMG-6.0 Dumps](#)

[NSE5\\_FMG-6.0 Exam Questions](#)

[NSE5\\_FMG-6.0 Braindumps](#)