

FortiManager as Local FortiGuard Server:

In **FortiManager** under **System Settings -> Network**, verify that service access for FortiGate Updates (FDS) or Web Filtering (FGD) is enabled on the FortiManager management interface.





Edit Network Interface

Name	port1
Alias	
IP Address/Netmask	192.168.100.210/255.255.255.0
IPv6 Address	::/0
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input checked="" type="checkbox"/> Web Service
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service
<u>Service Access</u>	
Bind to IP Address ⓘ	<input checked="" type="checkbox"/> FortiGate Updates 0.0.0.0/0.0.0.0
Bind to IP Address ⓘ	<input checked="" type="checkbox"/> Web Filtering 0.0.0.0/0.0.0.0
Status	<input type="button" value="Enable"/> <input type="button" value="Disable"/>

Edit Network Interface

Name	port2
Alias	
IP Address/Netmask	10.0.1.253/255.255.255.0
IPv6 Address	::/0
Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input checked="" type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input checked="" type="checkbox"/> Web Service
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service
<u>Service Access</u>	
Bind to IP Address ⓘ	<input checked="" type="checkbox"/> FortiGate Updates 0.0.0.0/0.0.0.0
Bind to IP Address ⓘ	<input checked="" type="checkbox"/> Web Filtering 0.0.0.0/0.0.0.0
Status	<input type="button" value="Enable"/> <input type="button" value="Disable"/>

In **FortiGate** make sure the interface connected to FortiManager **FMG-Access** is enabled.

Physical Interface 6				
 LAN (port3)	 Physical Interface		10.0.1.254/255.255.255.0	<div><div>PING</div><div>HTTPS</div><div>HTTP</div><div>FMG-Access</div></div>
 MGMT (port5)	 Physical Interface		192.168.100.200/255.255.255.0	<div><div>PING</div><div>HTTPS</div><div>SSH</div><div>HTTP</div><div>FMG-Access</div></div>

Go to **System > FortiGuard**. In the Override FortiGuard Servers table, click **Create New**.

The screenshot shows the FortiGuard configuration interface. On the left, the 'System' menu is expanded, and 'FortiGuard' is selected. The main content area displays the 'Override FortiGuard Servers' section. At the top, there are options for 'Email Filter cache' and 'FortiGuard filtering services'. Below this, a table lists the override servers. The first row shows the address '192.168.100.210', the type 'Both', and the availability status 'Unknown'. A red box highlights the '+ Create New' button in the table's header.

Server Address	Server Type	Availability
192.168.100.210	Both	Unknown

The **Create New Override FortiGuard Server** pane opens. Select the server **address type**: IPv4, IPv6, or FQDN. Enter the FortiManager address in the **Address** field. Select the type of server: AntiVirus & IPS Updates, Filtering, or Both. Click **OK**.

The screenshot shows the 'Create New Override FortiGuard Server' dialog box. It has three tabs: 'IPv4', 'IPv6', and 'FQDN'. The 'Address' field contains '192.168.100.210' and the 'Type' dropdown is set to 'Both'. There is an 'OK' button at the bottom right.

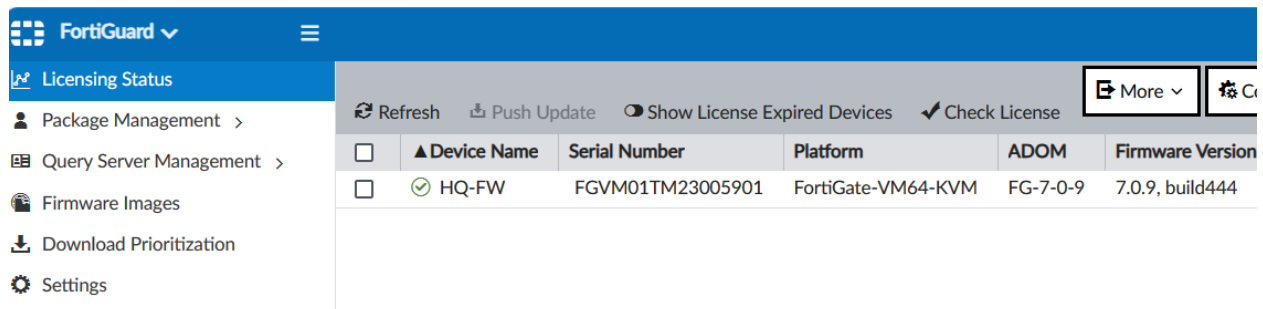
Click OK, then click **Apply**.

The screenshot shows the 'Override FortiGuard Servers' table after clicking 'Apply'. The table now contains the new server entry. A red box highlights the 'Apply' button at the bottom right of the page.

Server Address	Server Type	Availability
192.168.100.210	Both	Unknown

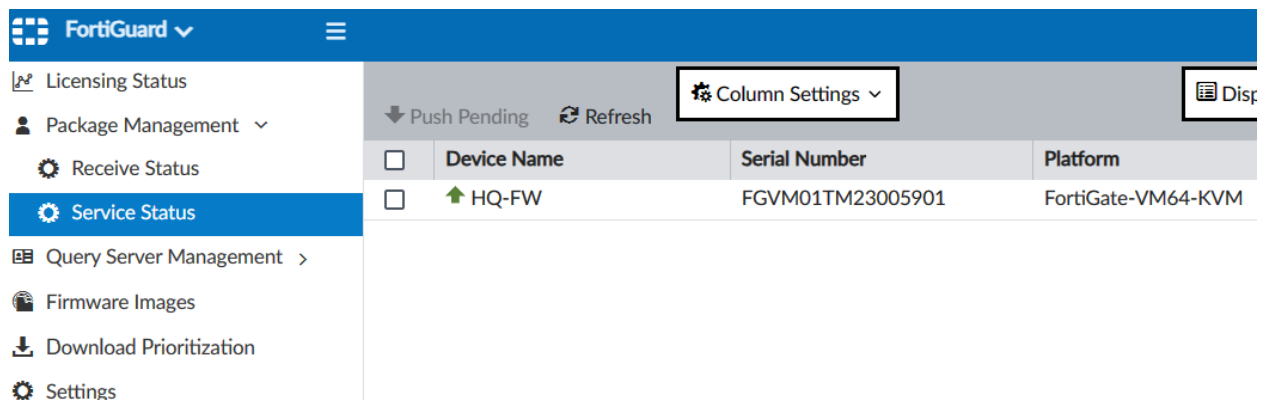
FortiManager as Local FortiGuard Server CLI

```
HQ-FW # config system central-management
HQ-FW (central-management) # set type fortimanager
HQ-FW (central-management) # set fmg 192.168.100.210
HQ-FW (central-management) # config server-list
HQ-FW (server-list) # edit 1
HQ-FW (1) # set server-type update rating
HQ-FW (1) # set server-address 192.168.100.210
HQ-FW (1) # next
HQ-FW (server-list) # edit 2
HQ-FW (2) # set server-type update
HQ-FW (2) # set server-address 192.168.100.210
HQ-FW (2) # next
HQ-FW (server-list) # end
HQ-FW (central-management) # set fmg-update-port 443
HQ-FW (central-management) # set include-default-servers enable
HQ-FW (central-management) # end
```



The screenshot shows the FortiGuard Licensing Status page. The left sidebar contains a menu with options: Licensing Status, Package Management, Query Server Management, Firmware Images, Download Prioritization, and Settings. The main content area has a header with 'Refresh', 'Push Update', 'Show License Expired Devices', and 'Check License' buttons. Below this is a table with columns: Device Name, Serial Number, Platform, ADOM, and Firmware Version. A single device is listed: HQ-FW with serial number FGVM01TM23005901 and platform FortiGate-VM64-KVM. A 'More' button is visible in the top right corner.

Device Name	Serial Number	Platform	ADOM	Firmware Version
HQ-FW	FGVM01TM23005901	FortiGate-VM64-KVM	FG-7-0-9	7.0.9, build444



The screenshot shows the FortiGuard Service Status page. The left sidebar contains a menu with options: Licensing Status, Package Management, Receive Status, Service Status, Query Server Management, Firmware Images, Download Prioritization, and Settings. The main content area has a header with 'Push Pending' and 'Refresh' buttons. Below this is a table with columns: Device Name, Serial Number, and Platform. A single device is listed: HQ-FW with serial number FGVM01TM23005901 and platform FortiGate-VM64-KVM. A 'Column Settings' button is visible in the top right corner.

Device Name	Serial Number	Platform
HQ-FW	FGVM01TM23005901	FortiGate-VM64-KVM