

Extra help: FortiGuard

This section contains tips to help you with some common challenges of using FortiGuard.

FortiGuard services appear as expired/unreachable.

Verify that you have registered your FortiGate unit, purchased FortiGuard services and that the services have not expired at support.fortinet.com.

Services are active but still appear as expired/unreachable.

Verify that the FortiGate unit can communicate with the Internet.

The FortiGate is connected to the Internet but can't communicate with FortiGuard.

Go to **System > Network > DNS** and ensure that the primary and secondary DNS servers are correct. If the FortiGate interface connected to the Internet gets its IP address using DHCP, make sure **Override internal DNS** is selected.

Also, determine if the default port used for FortiGuard traffic, port 53, is being blocked, either by a device on your network or by your ISP. If you cannot unblock the port, change it by going to **System > Config > FortiGuard** and selecting the service(s) where communication errors are occurring. Under **Port Selection**, select **Use Alternate Port**.

Communication errors remain.

FortiGate units contact the FortiGuard Network by sending UDP packets with typical source ports of 1027 or 1031, and destination ports of 53 or 8888. The FDN reply packets would then have a destination port of 1027 or 1031. If your ISP blocks UDP packets in this port range, the FortiGate unit cannot receive the FDN reply packets.

In effort to avoid port blocking, You can configure your FortiGate unit to use higher-numbered ports, such as 2048-20000, using the following CLI command:

```
config system global
    set ip-src-port-range 2048-20000
end
```

Trial and error may be required to select the best source port range. You can also contact your ISP to determine the best range to use.