FortiManager and FortiAnalyzer - Ports and Protocols

Version 6.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

June 8, 2021
FortiManager and FortiAnalyzer 6.4 Ports and Protocols
02-640-550874-20210608

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-04-11	Initial release.
2019-07-26	Changed UDP port to 8888.
2019-12-19	Added TCP 8880 to Outgoing ports on page 5.
2020-03-27	Updated Outgoing ports on page 5.
2021-02-26	Added TCP 4443 to Outgoing ports on page 5.
2021-06-08	Updated Incoming ports on page 6.

Open Ports

The following tables list the ports used by FortiManager and FortiAnalyzer:

- Ports for traffic originating from FortiManager and FortiAnalyzer units (Outgoing ports on page 5)
- Ports for traffic that can be received by FortiManager and FortiAnalyzer units (Incoming ports on page 6)

Traffic varies depending on the enabled options and configured ports for the FortiManager and FortiAnalyzer units. Only default ports are listed.

For FortiAnalyzer units with FortiManager Features enabled, the FortiGuard module is not supported. As a result, FortiAnalyzer units with FortiManager Features enabled do no use ports to communicate with FortiGuard.

However, FortiAnalyzer does use protocols to communicate with FortiGuard to retrieve information used by the FortiView and Reports modules. See FortiAnalyzer and FortiGuard on page 9.

This section contains the following topics:

- Outgoing ports on page 5
- Incoming ports on page 6

Outgoing ports

The following table identifies the ports for traffic originating from FortiManager and FortiAnalyzer units.

Outgoing Port Purpose	Port(s)
SMTP alert email	TCP/25
TACACS+ authentication	TCP/49
User name LDAP queries for reports	TCP/389 or TCP/636
Register FortiGate devices to FortiManager or FortiAnalyzer for configuration management	TCP/541 (IPv4) TCP/542 (IPv6)
RADIUS authentication	TCP/1812
Log aggregation client	TCP/3000
Fortinet registry for management extension applications, such as FortiWLM MEA	TCP/4443
FortiManager high-availability (HA) and configuration synchronization	TCP/5199
Turn *closed network mode* logic on/off	TCP/8880

Outgoing Port Purpose	Port(s)
	When applied, FortiManager cannot fetch FortiGuard content from the public FortiGuard cloud. If your are using FortiManager as a FortiGuard server for your managed devices, you will need to manually upload FortiGuard content in FortiManager.
DNS lookup	UDP/53
NTP synchronization	UDP/123
SNMP traps	UDP/162
Syslog, log forwarding	UDP/514 If reliable logging is enabled, syslog traffic can use TCP 514.

Incoming ports

The following table identifies ports for traffic that can be received by FortiManager and FortiAnalyzer units. The table excludes the incoming ports used between FortiManager and FortiGuard. For information about incoming ports used between FortiManager and FortiGuard, see FortiManager and FortiGuard on page 8.

Incoming Port Purpose	Port(s)
Ping	ICMP protocol
SSH administrative access to the CLI	TCP/22
Telnet administrative access to the CLI	TCP/23
HTTP administrative access to the GUI	TCP/80
HTTPS administrative access to the GUI	TCP/443
Receive logs from FortiGate and FortiClient Synchronize log database between FortiAnalyzer HA units	TCP/514
FortiManager listens for requests from FortiGate to set up central management (FGFM tunnel requests for IPv4)	TCP/541 (IPv4) TCP/542 (IPv6)
Log aggregation server (requires FortiManager 800 series or higher models).	TCP/3000
FortiManager high-availability (HA) and configuration synchronization	TCP/5199
Web Service	TCP/8080
SNMP query	UDP/161

Incoming Port Purpose	Port(s)
Syslog, log forwarding Log forwarding uses the OFTPD protocol.	UDP/514 If reliable logging is enabled, TCP 514 is used.
EMS for Chromebooks logging	TCP/8443
WebFilter queries, AV & IPS updates, when FortiManager is operating as a FortiGuard override server for FortiGate	UDP/53, UDP/8888 TCP/80, TCP/8888
Antispam, when FortiManager is operating as a FortiGuard override server for FortiGate	TCP/8889 UDP/8889
Registration for license validation and UTM updates (AV, IPS), when FortiManager is operating as a FortiGuard override server for FortiGate	TCP/443, TCP/8890

FortiGuard

This section describes how FortiManager and FortiAnalyzer communicate with FortiGuard. It contains the following topics:

- FortiManager and FortiGuard on page 8
- FortiAnalyzer and FortiGuard on page 9

FortiManager and FortiGuard

The FortiGuard Distribution Network (FDN) provides FortiGuard services for FortiManager systems and their managed devices as well as FortiClient agents. The FDN is a world-wide network of FortiGuard Distribution Servers (FDS), which update the FortiGuard services on your FortiManager system on a regular basis so that your FortiManager system is protected against the latest threats.

The FortiGuard services available on the FortiManager system include:

- Antivirus and IPS engines and signatures
- Web filtering and email filtering rating databases and lookups (select systems)
- Vulnerability scan and management support for FortiAnalyzer

In FortiGuard Management, you can configure the FortiManager system to act as a local FDS, or use a web proxy server to connect to the FDN. FortiManager systems acting as a local FDS synchronize their FortiGuard service update packages with the FDN, then provide FortiGuard these updates and look up replies to your private network's FortiGate devices. The local FDS provides a faster connection, reducing Internet connection load and the time required to apply frequent updates, such as antivirus signatures, to many devices.

The following table identifies what ports FortiManager uses with FortiGuard:

Functionality	Port(s)
FortiManager Antispam or Web Filtering rating lookup from a FortiClient endpoint or FortiGate unit	UDP/53 and 8888, TCP/80
FortiManager Antivirus or IPS (Intrusion Prevention System) update request from a FortiGate unit	TCP/8890
FortiManager listens to FortiGuard for FortiClient AV/IPS database and WebFilter database updates	TCP/80/8891
FortiManager Antivirus or IPS update FDN connection FortiManager WF/AS update FortiManager firmware images update	TCP/443
FortiGuard Antivirus or IPS Push update to FortiManager	UDP/9443

Enabling FDN updates and FortiGuard services

In the FortiManager GUI, the *FortiGuard* > *Settings* pane provides a central location for configuring and enabling your FortiManager system’s built-in FDS as an FDN override server.

By default, this option is enabled. After configuring FortiGuard and configuring your devices to use the FortiManager system as their FortiGuard server, you can view overall and per device statistics on FortiGuard service benefits.

In order to receive FortiGuard subscription updates, the FortiManager unit must have access to the Internet and be able to connect to a DNS server in order to resolve the following URLs:

- *fds1.fortinet.com*: For AV and IPS updates
- *guard.fortinet.net*: For web filtering and anti-spam updates
- *fqsvr.fortinet.net*: For file query and GEIP DB updates
- *forticlient.fortinet.net*: For FortiClient signature updates

FortiAnalyzer and FortiGuard

FortiAnalyzer uses proprietary Fortinet protocols to communicate with FortiGuard to retrieve information for use by the FortiView and Reports modules. This section describes what FortiAnalyzer retrieves by using the different protocols and where the information is stored in FortiAnalyzer systems.

Metadata

FortiAnalyzer uses the fmupdate protocol to communicate with FortiGuard to get metadata updates for use by the FortiView and Reports modules. The following FortiAnalyzer metadata is updated:

FortiAnalyzer Version	What is Retrieved from FortiGuard	FortiAnalyzer Storage Location
	TIDB (for indicators of compromise)	/var/fds/vsig/0001000
5.0.0, 5.2.0 and later	app-ctrl	/var/fds/vsig/05000000
	GeoIP	/var/fds/vsig/05000000/IPGE00000
	IPS	/var/fds/vsig/05000000/NIDS0220
	app-ctrl	/var/fds/vsig/05000000/NIDS02300
5.4.0 and later	IPS	/var/fds/vsig/05004000/NIDS02200
	app-ctrl	/var/fds/vsig/05004000/NIDS02300
6.0.0 and later	FGT FortiFlowDB (for ISDB owner lookup)	/var/fds/vsig/06000000/FFDB00305 /var/fds/vsig/06000000/FFDB00405

FortiClient

FortiAnalyzer also uses the fmupdate protocol to communicate with FortiGuard to retrieve and store the following metadata for FortiClient in the Reports module:

FortiAnalyzer Version	What is Retrieved from FortiGuard	FortiAnalyzer Storage Location
5.6.0 and earlier	FVDB	/var/fct/vsig/05004000/FVDB01800/
5.6.1 and later	FVDB	/var/fct/vsig/05004000/FVDB01800/

Application icons and FortiGuard encryclopedia link prefixes

FortiAnalyzer uses the fazcfgd protocol to communicate with FortiGuard to retrieve application icons and encryclopedia link prefixes for use by the FortiView and Reports modules. FortiAnalyzer retrieves the following information:

What is Retrieved	URL	FortiAnalyzer Storage Location
Encyclopedia link prefix	https://productapi.fortinet.com/v1/fgd/prefixlinks	/var/fgd_cache/encyclopedia_link_prefixes.json
Application icons, sprite map files (small_sprite.png, sprite_map.css, webfilter_categories.json)	Based on link prefix, for example, https://filestore.fortinet.com/fortiguard/app_logos96/small_sprite.png	/var/fgd_cache/

FortiAnalyzer communicates with productapi.fortinet.com for the sprite map. The productapi.fortinet.com site resolves to an IP address of 96.45.36.123 or 208.91.114.142.

Disabling FortiAnalyzer communication with FortiGuard

With FortiAnalyzer 5.6.1 and 6.0.0 and later, you can disable communication between FortiAnalyzer and FortiGuard by using the `config fmupdate publicnetwork` command:

```
config fmupdate publicnetwork
(publicnetwork)# set status disable
(publicnetwork)# end
```

You can use the same command to disable communication between FortiManager and FortiGuard.

Protocols

This section describes the proprietary Fortinet protocols used by FortiManager and FortiAnalyzer:

- FortiGate-FortiManager protocol on page 11
- FortiGuard protocol on page 11
- Logging protocol on page 11

FortiGate-FortiManager protocol

The FortiGate-FortiManager (FGFM) communication protocol is used by the Device Manager module in FortiManager. Device Manager contains all devices that are managed by the FortiManager unit. You can create new device groups, provision and add devices, and install policy packages and device settings. Device Manager communicates with devices by using the FGFM protocol.

FortiGuard protocol

The FortiGuard communication protocol is used by the FortiGuard module in FortiManager. FortiGuard communicates with devices using the FortiGuard protocol.

Logging protocol

The logging protocol is used by FortiAnalyzer or by FortiManager when FortiAnalyzer features are enabled. When FortiAnalyzer features are enabled for FortiManager, the FortiView, NOC, Log View, Event Management, and Reports modules are available in FortiManager and FortiAnalyzer. FortiAnalyzer features include tools for viewing and analyzing log messages, and the feature communicates with devices using the logging protocol.