



# FortiSandbox - Administration Guide

Version 3.0.7

**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](mailto:techdoc@fortinet.com)



July 27, 2021

FortiSandbox 3.0.7 Administration Guide

34-306-731217-20210727

# TABLE OF CONTENTS

<b>Introduction</b>	<b>7</b>
About this document	9
Connecting to the Command Line Interface	10
<b>Using the GUI</b>	<b>11</b>
GUI overview	11
Connecting to the GUI	11
Default Port Information	12
<b>Dashboard</b>	<b>15</b>
Customizing the dashboard	16
System Information	18
System Resources	20
System Resources Usage Timeline	21
Scanning Statistics	21
File Scanning Activity	22
Top Devices	22
Top Critical Logs	23
Pending Job Statistics	23
Disk Monitor	23
Sniffer Traffic Throughput	23
Threats Distribution	24
Customized Threats Distribution	24
Quick Download	24
Basic System Settings	24
Change the system host name	25
Change the administrator password	25
Change the GUI idle timeout	25
Configure the system time	26
Microsoft Windows VM license activation	27
Microsoft Office license upload and activation	27
Log out of the unit	27
Visit online help	27
Refresh current web page	27
Toggle left-side menu style	28
Update the FortiSandbox firmware	28
Reboot and shut down the unit	28
Backup or restore the system configuration	29
<b>FortiView</b>	<b>31</b>
Operation Center	32
Threats by Topology	34
Threats by Hosts	35
Threats by Hosts - level 1	35
Threats by Hosts - level 2	36
Threats by Hosts - level 3	37
Threats by Hosts - level 4	38

Threats by Files .....	38
Threats by Files - level 1 .....	38
Threats by Files - level 2 .....	39
Threats by Files - level 3 .....	40
Threats by Files - level 4 .....	41
Threats by Devices .....	41
Threats by Devices - level 1 .....	41
Threats by Devices - level 2 .....	42
Threats by Devices - level 3 .....	42
Threats by Devices - level 4 .....	43
Event Calendar .....	44
File Scan Search .....	45
URL Scan Search .....	46
<b>Network .....</b>	<b>49</b>
Interfaces .....	49
Edit an interface .....	51
Edit administrative access .....	51
Failover IP .....	51
DNS Configuration .....	52
System Routing .....	52
<b>System .....</b>	<b>54</b>
Administrators .....	55
Admin Profiles .....	58
Wildcard Admin Authentication .....	61
Device Groups .....	63
Certificates .....	63
LDAP Servers .....	65
RADIUS Servers .....	67
Mail Server .....	69
SNMP .....	70
Configuring the SNMP agent .....	71
MIB files .....	73
FortiGuard .....	74
Login Disclaimer .....	75
Settings .....	75
Job View Settings .....	76
Event Calendar Settings .....	78
<b>Virtual Machine .....</b>	<b>79</b>
Model, License and VM Information .....	79
VM Host Support .....	79
VM Status .....	80
VM Images .....	80
Clone Number for VM Image .....	84
VM Screenshot .....	84

<b>Scan Policy</b>	<b>85</b>
Scan Profile	85
File types	85
Scan Profile Job Queue Tab	86
Scan Profile VM Association Tab	87
File Scan Priority	89
File Scan Flow	90
URL Scan Flow	90
Job Queue Priority	90
General	91
Allowlist and blocklist (white/black lists)	94
Overridden Verdicts	96
YARA Rules	96
URL Category	98
Working Together With URL Pre-Filtering	100
Customized Rating	100
Job Archive	101
Global Network	102
Local Packages	104
Malware and URL Package Options	104
IOC Package	106
<b>Scan Input</b>	<b>108</b>
File Input	108
File On Demand	109
URL On Demand	113
Job Queue	117
Sniffer	119
Device	121
Supported Devices	123
Adapter	133
Configure Carbon Black/Bit9 Server	137
Configure ICAP Client	139
Configure FortiMail to integrate with FortiSandbox BCC Adapter	139
Network Share	143
Scan Details	147
Quarantine	147
Malware Package	149
URL Package	150
<b>HA-Cluster</b>	<b>151</b>
Centrally manage worker (slave) nodes on the primary (master) node	152
Requirements before Configuring a HA Cluster	153
Role of the primary (master) and worker (slave) node	153
Configure a cluster level failover IP set for primary (master) unit	154
Main HA-Cluster CLI Commands	154
What happens during a failover	158

Upgrading or rebooting a Cluster .....	159
Health Check .....	159
Job Summary .....	161
Status .....	161
<b>File Detection .....</b>	<b>163</b>
Summary Report .....	163
Customizing the summary report page .....	164
File Scan .....	165
<b>Network Alerts .....</b>	<b>168</b>
Summary Report .....	168
Customizing the summary report page .....	169
Network Alerts .....	170
<b>URL Detection .....</b>	<b>173</b>
Summary Report .....	173
Customizing the summary report page .....	174
URL Scan .....	174
<b>Log &amp; Report .....</b>	<b>176</b>
About Logs .....	176
Log Details .....	176
Logging Levels .....	176
Raw logs .....	177
Log Categories .....	178
Log Servers .....	179
Local Log .....	180
Diagnostic Logs .....	181
Viewing logs in FortiAnalyzer .....	181
Customizing the log view .....	182
Columns .....	183
Summary Reports .....	184
Generate reports .....	184
Report Center .....	185
<b>Appendix A - View Details Page Reference .....</b>	<b>186</b>
<b>Appendix B - FortiCloud Sandbox .....</b>	<b>190</b>
Deployment .....	190
Detection .....	190
File type and protocol support .....	191
Alerting, reporting and monitoring .....	192
Forensic, auditing, and third-party tools .....	192
<b>Change Log .....</b>	<b>194</b>

# Introduction

Fighting today's Advanced Persistent Threats (APTs) requires a multi-layer approach. FortiSandbox offers the ultimate combination of proactive mitigation, advanced threat visibility, and comprehensive reporting. More than just a sandbox, FortiSandbox deploys Fortinet's award-winning, dynamic antivirus and threat scanning technology, dual level sandboxing, and optional integrated FortiGuard cloud queries to beat Advanced Evasion Techniques (AETs) and deliver state-of-the-art threat protection.

FortiSandbox utilizes advanced detection, dynamic antivirus scanning, and threat scanning technology to detect viruses and APTs. It leverages the FortiGuard web filtering database to inspect and flag malicious URL requests, and is able to identify threats that standalone antivirus solutions may not detect.

FortiSandbox works with your existing devices, like FortiGate, FortiWeb, FortiClient and FortiMail, to identify malicious and suspicious files and network traffic. It has a complete extreme antivirus database that will catch viruses that may have been missed.

FortiSandbox can be configured to sniff traffic from the network, scan files on a network share with a predefined schedule, quarantine malicious files, and receive files from FortiGate, FortiWeb, FortiMail, and FortiClient. For example, FortiMail 5.2.0 and later allows you to forward email attachments to FortiSandbox for advanced inspection and analysis. Files can also be uploaded directly to it for sandboxing through the web GUI or JSON API. You can also submit a website URL to scan to help you identify web pages hosting malicious content before users attempt to open the pages on their host machines.

FortiSandbox executes suspicious files in the VM host module to determine if the file is High, Medium, or Low Risk based on the behavior observed in the VM sandbox module. The rating engine scores each file from its behavior log (tracer log) that is gathered in the VM module and, if the score falls within a certain range, a risk level is determined.

The following table lists infection types and attacks that are identified by FortiSandbox.

Infection Type	Description
<b>Infector</b>	Infector malware is used to steal system and user information. The stolen information is then uploaded to command and control servers. Once the infector installs on a computer, it attempts to infect other executable files with malicious code.
<b>Worm</b>	Worm malware replicates itself in order to spread to other computers. This type of malware does not need to attach itself to an existing program. Worms, like viruses, can damage data or software.
<b>Botnet</b>	Botnet malware is used to distribute malicious software. A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform a task. Computers that are infected by botnet malware can be controlled remotely. This type of malware is designed for financial gain or to launch attacks on websites or networks.
<b>Hijack</b>	Hijack malware attempts to hijack the system by modifying important registry keys or system files.
<b>Stealer</b>	Stealer malware is used to harvest login credentials of standalone systems, networks, FTP, email, game servers and other websites. Once the system is infected, the malware can be customized by the attacker.

Infection Type	Description
<b>Backdoor</b>	Backdoor malware installs a network service for remote access to your network. This type of malware can be used to access your network and install additional malware, including stealer and downloader malware.
<b>Injector</b>	Injector malware injects malicious code into system processes to perform tasks on its behalf.
<b>Rootkit</b>	Rootkit malware attempts to hide its components by replacing vital system executables. Rootkits allow malware to bypass antivirus detection as they appear to be necessary system files.
<b>Adware</b>	Adware malware is a software package which attempts to access advertising websites. Adware displays these unwanted advertisements to the user.
<b>Dropper</b>	Dropper malware is designed to install malicious software to the target system. The malware code may be contained within the dropper or downloaded to the target system once activated.
<b>Downloader</b>	Downloader malware attempts to download other malicious programs.
<b>Trojan</b>	Trojan malware is a hacking program which gains privileged access to the operating system to drop a malicious payload, including backdoor malware. Trojans can be used to cause data damage, system damage, data theft or other malicious acts.
<b>Riskware</b>	Riskware malware has security-critical functions which pose a threat to the computer.
<b>Grayware</b>	Grayware malware is a classification for applications that behave in a manner that is annoying or undesirable. Grayware includes spyware, adware, dialers, and remote access tools that are designed to harm the performance of computers on your network.
<b>Unknown</b>	No definitions currently exist for this type of attack.

FortiSandbox scans executable (Windows `.exe` and `.dll` script files), JavaScript, Microsoft Office, Adobe Flash, PDF, archives, and other file types the user defines. JavaScript and PDF are the two common software types that malware uses to execute malicious code. For example, JavaScript is often used to create heap sprays and inject malicious code to execute in other software products such as Adobe Reader (PDF).

When a malware is scanned inside a FortiSandbox VM environment, FortiSandbox scans its outgoing traffic for connections to botnet servers and determines the nature of the traffic and connection hosts.

Key features of FortiSandbox include:

- **Dynamic Antimalware updates/Cloud query:** Receives updates from FortiGuard Labs and send queries to the FortiSandbox Community Cloud in real time, helping to intelligently and immediately detect existing and emerging threats.
- **Code emulation:** Performs lightweight sandbox inspection in real time for best performance, including certain malware that uses sandbox evasion techniques and/or only executes with specific software versions.
- **Full virtual environment:** Provides a contained runtime environment to analyze high risk or suspicious code and explore the full threat life cycle.
- **Advanced visibility:** Delivers comprehensive views into a wide range of network, system and file activity, categorized by risk, to help speed up incident response.
- **Network Alert:** Inspects network traffic for requests to visit malicious sites, establish communications with C&C servers, and other activity indicative of a compromise. It provides a complete picture of the victim host's infection cycle.
- **Manual analysis:** Allows security administrators to manually upload malware samples via the FortiSandbox web GUI or JSON API to perform virtual sandboxing without the need for a separate appliance.



- Optional submission to FortiSandbox Community Cloud: Tracer reports, malicious files and other information may be submitted to FortiSandbox Community Cloud in order to receive remediation recommendations and updated in line protections.
- Schedule scan of network shares: Perform a schedule scan of network shares in Network File System (NFS) v2 to v4 and Common Internet File System (CIFS) formats to quarantine suspicious files.
- Scan job archive: You can archive scan jobs to a network share for backup and further analysis.
- Website URL scan: Scan websites to a certain depth for a predefined time period.
- Cluster supporting High Availability: Provide a non-interruption, high performance system for malware detection.

This section includes the following topics:

- [About this document](#)
- [Connecting to the Command Line Interface](#)

## About this document

This document describes how to configure and manage your FortiSandbox system and the connected FortiGate/FortiMail devices.

FortiSandbox system documentation assumes that you have one or more Fortinet products such as FortiGate/FortiMail units, the Fortinet system documentation, and you are familiar with configuring your Fortinet devices units before using the FortiSandbox system.



To configure your FortiGate device to submit files to FortiSandbox, your FortiGate must be running FortiOS or FortiOS Carrier version 5.0.4 and later or 5.2.0 and later.



To configure your FortiMail email gateway to identify suspicious or high risk files in email and submit them to FortiSandbox, your FortiMail must be running FortiMail version 5.2.0 and later. For more information, see the *FortiMail Administration Guide* in the [Fortinet Document Library](#).



To configure your FortiClient to send files to the FortiSandbox and receive results, your FortiClient must be running FortiClient 5.4.0 and later. For more information, see the *FortiClient Administration Guide* in the [Fortinet Document Library](#).



To configure your FortiWeb to submit files for FortiSandbox to evaluate, your FortiWeb must be running 5.4.0 and later. For more information, see the *FortiWeb Administration Guide* in the [Fortinet Document Library](#).

---

## Connecting to the Command Line Interface

The FortiSandbox CLI commands are intended to be used for initial device configuration and troubleshooting. The FortiSandbox device is primarily configured using the GUI. You can enable SSH and Telnet access on the port1 (administration) interface or any other administrative port set through the CLI command `set admin-port` and access the CLI through SSH or Telnet to troubleshoot the device including RAID related hard disk issues. You can also connect to the CLI through the console port.

### To connect to the CLI through the console port:

1. Connect the FortiSandbox unit console port to the management computer using the provided console cable.
2. Start a terminal emulation program on the management computer.
3. Use the following settings:

<b>Serial line to connect to</b>	COM1
<b>Speed (baud)</b>	9600
<b>Data bits</b>	8
<b>Stop bits</b>	1
<b>Parity</b>	None
<b>Flow Control</b>	None

4. Press *Open* to connect to the FortiSandbox CLI. The *login as* page is displayed.
5. Type a valid administrator name and press *Enter*.
6. Type the password for this administrator and press *Enter*.

For example, to configure the IP address and gateway of the FortiSandbox device, use the following commands:

```
set port1-ip 192.168.0.10/24
set default-gw 192.168.0.1
```

For more information on FortiSandbox CLI commands, see the *FortiSandbox CLI Reference Guide* available in the [Fortinet Document Library](#).

# Using the GUI

This section describes general information about using the GUI to access the FortiSandbox system from within a web browser. This section also explains common GUI tasks that an administrator does on a regular basis.

This section includes the following topics:

- [GUI overview](#)
- [Default Port Information](#)

## GUI overview

The GUI is a user-friendly interface for configuring settings and managing the FortiSandbox unit. The GUI can be accessed from a web browser on any management computer.

## Connecting to the GUI

The FortiSandbox unit is configured and managed using the GUI. This section will step you through connecting to the unit via the GUI.



To quickly locate a menu item, you can enter the term in the *Search* bar located at the top of the left side panel.

---



Information messages for certain pages will be displayed in the *Message Bar* located at the top of the right side panel. Messages will disappear after a few seconds.

---

### To connect to the FortiSandbox GUI:

1. Connect the port1 (administration) interface or any other administrative port set through the CLI command `set admin-port` to a management computer using the provided Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiSandbox unit:
  - a. Browse to *Network and Sharing Center > Change adapter settings > Local Area Connection Properties > Internet Protocol Version 4 (TCP/IPv4) Properties*. These directions may vary based on the version of your operating system.
  - b. Change the IP address of the management computer to `192.168.0.2` and the network mask to `255.255.255.0`.
3. Start a supported web browser and browse to `https://192.168.0.99`.
4. Type `admin` in the *Name* field, leave the *Password* field blank, and click *Login*.  
You can now proceed with configuring your FortiSandbox unit.



If the network interfaces have been configured differently during installation, the URL and/or permitted administrative access protocols may no longer be in their default state.

## Default Port Information

FortiSandbox treats Port1 or any other administrative port set through the CLI command `set admin-port` as reserved for device management, and Port3 be reserved for the Windows VM to communicate with the outside network. The other ports are used for file input and communication among cluster nodes. In Cluster mode, FortiSandbox uses TCP ports 2015 and 2018 for cluster internal communication. If the unit works as a *Collector* to receive threat information from other units, it uses TCP port 2443

The following tables list the default open ports for each FortiSandbox interface.

### FortiSandbox 3500D, 2000E, and 3000E default ports:

Port (Interface)	Type	Default Open Ports
Port1	RJ-45	<p>TCP ports, 22 (SSH), 23 (Telnet), 80 and 443 (GUI), 514 (OFTP communication with FortiGate, FortiWeb, FortiClient &amp; FortiMail), SNMP local query port.</p> <p>FortiGuard Distribution Servers (FDS) use TCP port 8890 for download. The FortiSandbox will use a random port picked by the kernel.</p> <p>FortiGuard Web Filtering servers use UDP port 53 or 8888. The FortiSandbox will use a random port picked up by the kernel.</p> <p>Fortinet FortiSandbox VM download uses TCP port 443 for download. The FortiSandbox will use a random port picked by the kernel.</p> <p>FortiSandbox uses UDP port 53 or 8888 and TCP port 443 of the Community Cloud server to query existing results. Before release 3.0.0, if enabled, FortiSandbox uploads detected malware information to TCP port 443 of the Community Cloud server. Since 3.0.0, the TCP ports to use on server-side are 25, 465 or 587. The FortiSandbox will use a random port picked up by the kernel.</p> <p>If you configure an internal mail server, internal DNS server, remote syslog server, LDAP server, SNMP managers, NTP server, or override the web filtering server IP address, communication is recommended to be through this interface. Ensure that the applicable routing is configured.</p>
Port2, Port4	RJ-45	No service listens except OFTP. If user specifies it as an administration port through CLI command <code>set admin-port</code> , TCP ports 80 and 443 will be opened for web UI.
Port3	RJ-45	No service listens. Reserved for guest VM to communicate with the outside network.
Port5, Port6	SFP+	No service listens except OFTP. If user specifies it as an administration port through CLI command <code>set admin-port</code> , TCP ports 80 and 443 will be opened for web UI.

**FortiSandbox 3000D default ports:**

Port (Interface)	Type	Default Open Ports
Port1	RJ-45	<p>TCP ports, 22 (SSH), 23 (Telnet), 80 and 443 (GUI), 514 (OFTP communication with FortiGate, FortiWeb, FortiClient &amp; FortiMail). SNMP local query port.</p> <p>FortiGuard Distribution Servers (FDS) use TCP port 8890 for download. The FortiSandbox will use a random port picked by the kernel.</p> <p>FortiGuard Web Filtering servers use UDP port 53 or 8888. The FortiSandbox will use a random port picked up by the kernel.</p> <p>FortiSandbox uses UDP port 53 or 8888 and TCP port 443 of the Community Cloud server to query existing results. Before release 3.0.0, if enabled, FortiSandbox uploads detected malware information to TCP port 443 of the Community Cloud server. Since 3.0.0, the TCP ports to use on server-side are 25, 465 or 587. The FortiSandbox will use a random port picked up by the kernel.</p> <p>If you configure an internal mail server, internal DNS server, remote syslog server, LDAP server, SNMP managers, NTP server, or override the web filtering server IP address, communication is recommended to be through this interface. Ensure that the applicable routing is configured.</p>
Port2, Port4	RJ-45	No service listens except OFTP (TCP port 514). If user specifies it as an administration port through CLI command <code>set admin-port</code> , TCP ports 80 and 443 will be opened for web UI.
Port3	RJ-45	All ports are open. Reserved for guest VM to communicate with the outside network.
Port5, Port6	SFP	No service listens except OFTP (TCP port 514). If user specifies it as an administration port through CLI command <code>set admin-port</code> , TCP ports 80 and 443 will be opened for web UI.
Port7, Port8	SFP+	No service listens except OFTP (TCP port 514). If user specifies it as an administration port through CLI command <code>set admin-port</code> , TCP ports 80 and 443 will be opened for web UI.

**FortiSandbox 1000D default ports:**

Port (Interface)	Type	Default Open Ports
Port1	RJ-45	<p>TCP ports 22 (SSH), 23 (Telnet), 80 and 443 (GUI), 514 (OFTP communication with FortiGate, FortiWeb, FortiClient &amp; FortiMail).</p> <p>FortiGuard Distribution Servers (FDS) use TCP port 8890 for download. The FortiSandbox will use a random port picked by the kernel.</p> <p>FortiGuard Web Filtering servers use UDP port 53 or 8888. The FortiSandbox will use a random port picked up by the kernel.</p> <p>FortiSandbox uses UDP port 53 or 8888 and TCP port 443 of the Community Cloud server to query existing results. Before release 3.0.0, if enabled, FortiSandbox uploads detected malware information to TCP port 443 of the Community Cloud server. Since 3.0.0, the TCP ports to use on server-side are 25, 465 or 587. The FortiSandbox will use a random port picked up by the kernel.</p>

Port (Interface)	Type	Default Open Ports
		If you configure an internal mail server, internal DNS server, remote syslog server, LDAP server, SNMP managers, NTP server, or override the web filtering server IP address, communication is recommended to be through this interface. Ensure that the applicable routing is configured.
Port2, Port4, Port5, Port6	RJ-45	No service listens except OFTP (TCP port 514). If user specifies it as an administration port through CLI command <code>set admin-port</code> , TCP ports 80 and 443 will be opened for web UI.
Port3	RJ-45	All ports are open. Reserved for guest VM to communicate with the outside network.
Port7, Port 8	SFP	No service listens except OFTP (TCP port 514). If user specifies it as an administration port through CLI command <code>set admin-port</code> , TCP ports 80 and 443 will be opened for web UI.



All ports mentioned above are the same for both IPv4 and IPv6 protocols.



You can dynamically change system firewall rules using the `iptables` CLI command. New rules will be lost after a system reboot.



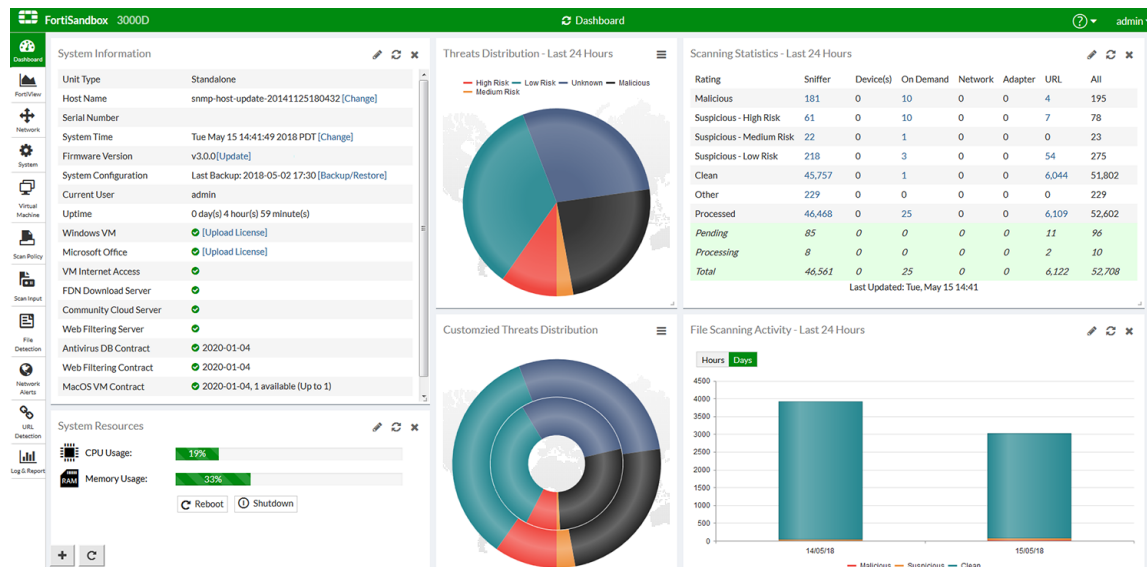
If port3 of the FortiSandbox is connected to an interface behind the FortiGate device, make sure that the egress WAN interface does not have the *Scan Outgoing Connections to Botnet Sites* feature enabled, nor any active security profiles as this might impact the detection rate. If this is not possible, we recommend connecting the FortiSandbox port3 to a different egress WAN port or directly to the Internet in front of the perimeter firewall.

For more information on FortiSandbox 1000D, FortiSandbox 3000D, FortiSandbox 3500D, FortiSandbox 2000E, and FortiSandbox 3000E interfaces, see [Interfaces on page 49](#).

# Dashboard

The System Status dashboard displays widgets that provide information and enable you to configure basic system settings. All of the widgets appear on a single dashboard, which can be customized as desired.

The menu is in *Compact* mode by default. You can toggle between *Compact* mode and *Full* mode in *System > Settings > Menu Mode*.



If the unit is the primary (master) node in a cluster, the displayed data will be a summary of all nodes in the cluster, otherwise only the individual unit's data is displayed.

The following widgets are available:

<b>System Information</b>	Displays basic information about the FortiSandbox system, such as the serial number, system up time, and license status information.
<b>System Resources</b>	Displays the real-time usage status of the CPU and memory.
<b>Scanning Statistics</b>	Displays a table providing information about the files scanned over a selected time span. This includes Sniffer, Device(s), On Demand, Network, Adapter, and URL.
<b>Scanning Activity</b>	Displays the number of clean, suspicious, and malicious events that have occurred at specific times over a selected time period. Hover the cursor over a colored portion of a bar in the graph to view the exact number of events of the selected type that occurred at that time.
<b>Threats Distribution</b>	Displays threat level distribution over a selected period.

<b>Customized Threats Distribution</b>	Displays threat level distribution over two customized time intervals.
<b>Quick Download</b>	To quickly search a file according to its checksum. If found, the user can download the file, download the PDF report, and view job detail.
<b>Sniffer Traffic Throughput</b>	Displays sniffed traffic throughput across time.
<b>Top Devices</b>	Displays the total scanning jobs for the top five devices over a selected time interval. Hover the cursor over a bar in the graph to view the exact number of scanning jobs for that device.
<b>Top Critical Logs</b>	Displays recent critical logs, including the time they occurred and a brief description.
<b>Pending Job Statistics</b>	Displays pending scan job numbers for a period of time. This widget allows you to monitor the workload trend on your FortiSandbox.
<b>Disk Monitor</b>	Displays the RAID level and status, disk usage, and disk management information. This widget is only available in hardware based models.

The following option is available:

<b>Refresh</b>	At the top of the website, there is a <i>Refresh</i> button and label to show the current user. Clicking the <i>Refresh</i> button will refresh the dashboard. <b>Note:</b> For certain pages, such as <i>FortiView &gt; File Scan Search</i> , if you click the <i>Refresh</i> button you will lose your current search criteria. Use the <i>Refresh</i> button inside the content pane to continue searching without losing your criteria.
<b>Online Help</b>	At the upper-right corner of the website, there is a dropdown list. Users can go to online help to quickly find reference information about FortiSandbox.
<b>Video Tutorials</b>	The Fortinet FortiSandbox Video Library contains video tutorials showing how to integrate various Fortinet products, including FortiGates to FortiSandbox. The Video Library can be found at <a href="https://video.fortinet.com/products">https://video.fortinet.com/products</a> .

This section includes the following topics:

- [Customizing the dashboard](#)
- [Basic System Settings](#)

## Customizing the dashboard

The FortiSandbox system dashboard can be customized. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized.

### To move a widget:

Position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.



**To refresh a widget:**

Select the refresh icon in the widget's title bar to refresh the data presented in the widget.

**To reset a widget back to default settings:**

Click the *Reset* button on the floating widget tool bar.

**To add a widget:**

In the floating dashboard toolbar, select *Add Widget*, then select the names of widgets that you want to add. To hide a widget, in its title bar, select the close icon.

The following is a list of widgets you can add to your dashboard:

- [System Information](#)
- [System Resources](#)
- [System Resources Usage Timeline](#)
- [Scanning Statistics](#)
- [File Scanning Activity](#)
- [Top Devices](#)
- [Top Critical Logs](#)
- [Pending Job Statistics](#)
- [Disk Monitor](#)
- [Sniffer Traffic Throughput](#)
- [Threats Distribution](#)
- [Customized Threats Distribution](#)
- [Quick Download](#)



Multiple widgets of the same type can be added to the dashboard. This can be useful for viewing information over different time intervals.

---

**To go to the top of the dashboard:**

After scrolling down the dashboard page, a *Back to top* button will appear in the floating widget tool bar. Click this button to go to the top of the dashboard.

**To edit a widget:**

1. Select the edit icon in the widget's title bar to open the edit widget window.
2. Configure the following information, and then select *OK* to apply your changes:

<b>Custom widget title</b>	Optionally, type a custom title for the widget. Leave this field blank to use the default widget title.
<b>Refresh interval</b>	Enter a refresh interval for the widget, in seconds. Some widget have default refresh values: <ul style="list-style-type: none"><li>• Scanning Statistics: 600</li></ul>

	<ul style="list-style-type: none"> <li>• Top Devices: 300</li> <li>• Scanning Activity: 300</li> <li>• System Resources: 60</li> <li>• Top Critical Logs: 3600</li> <li>• Disk Monitor: 300</li> </ul>
<b>Top Count</b>	<p>Select the number of entries to display in the widget. The top count can be between 5 to 20 entries.</p> <p>This option is only available in the following widgets: <i>Top Devices</i>, <i>Top Critical Logs</i>.</p>
<b>Time Period</b>	<p>Select a time period to be displayed from the dropdown list: <i>Last 24 hours</i>, <i>Last 7 days</i>, <i>Last 4 weeks</i>.</p> <p>This option is only available on the following widgets: <i>Scanning Statistics</i>, <i>Top Devices</i>, <i>Threats Distribution</i>, and <i>Scanning Activity</i>.</p>

## System Information

The *System Information* widget displays various information about the FortiSandbox unit and enables you to configure basic system settings.

This widget displays the following information and options:

<b>Unit Type</b>	<p>The HA cluster status of the device: <i>Standalone</i>, <i>Master</i> (primary), <i>Primary Slave</i> (secondary), or <i>Regular Slave</i> (worker).</p> <p>In an HA-Cluster, click <i>Change</i> to change the cluster status of the device.</p>
<b>Host Name</b>	<p>The name assigned to this FortiSandbox unit. Select <i>[Change]</i> to edit the FortiSandbox host name.</p>
<b>Serial Number</b>	<p>The serial number of this FortiSandbox unit. The serial number is unique to the FortiSandbox unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.</p>
<b>System Time</b>	<p>The current time on the FortiSandbox internal clock or NTP server. Select <i>[Change]</i> to configure the system time.</p>
<b>Firmware Version</b>	<p>The version and build number of the firmware installed on the FortiSandbox unit. When new firmware is available, a blinking <i>New firmware available</i> link appears. Clicking the link redirects you to a page where you can download and install available firmware, or manually upload firmware. You can also choose to create backup configurations.</p>
<b>System Configuration</b>	<p>The date and time of the last system configuration backup. Select <i>Backup/Restore</i> to browse to the <i>System Recovery</i> page.</p>
<b>Current User</b>	<p>The administrator that is currently logged on to the system.</p>
<b>Uptime</b>	<p>The duration of time that the FortiSandbox unit has been running since boot up.</p>
<b>Windows VM</b>	<p>Microsoft Windows VM license activation and initialization status.</p>

	<p>Displays an up icon if the Microsoft Windows VM is activated and initialized. Displays a <i>Caution</i> icon if the Microsoft Windows VM is initializing or having issues. Hover the mouse pointer on the status icon to view detailed information. More information can be found in the <i>Log &amp; Report &gt; VM Events</i> page.</p> <p>In addition to the pre-installed default set of Windows VM images, users can also download, install, and use optional images from the Optional VMs section in the <i>VM Image</i> page. Extra Windows OS licenses might be needed if the unit has none available. For example, when user tries to use Windows 10 image on a FSA-1000D unit, the user might need to purchase Windows 10 license keys from Fortinet. After purchase, the user should download their license file from the <a href="#">Fortinet Customer Service &amp; Support</a> portal. Then, click the <i>[Upload License]</i> link next to the Windows VM field. Browse to the license file on the management computer and click the Submit button. The system will reboot and activate the newly installed Windows guest VMs.</p>
<b>Microsoft Office</b>	<p>Microsoft Office product activation status. Select to upload a Microsoft Office license file.</p> <p>Displays an <i>Up</i> icon if the Microsoft Office is activated and initialized. Displays a <i>Caution</i> icon if the Microsoft Office is initializing or having issues. The <i>Up</i> icon and <i>Caution</i> icon can both show up when Microsoft Office software is activated on certain enabled VMs, but not activated on other enabled VMs. Hover the mouse pointer on the status icon to view detailed information. More information can be found in <i>Log &amp; Report &gt; VM Events</i> page.</p>
<b>VM Internet Access</b>	<p>Displays the status of the FortiSandbox guest VM accessing the outside network. Displays an <i>Up</i> icon if the VM can access the outside network. Displays a <i>Caution</i> icon if the VM cannot access the outside network. Hover the mouse pointer on the status icon to view detailed information. If the VM cannot access the outside network, a simulated network (SIMNET) will start by default. SIMNET provides responses of popular network services, like <code>http</code> where certain malware is expected. If the VM internet access is down, beside the <i>Down</i> icon, SIMNET status is displayed. Clicking it will enter the VM network configuration page.</p> <p>FortiSandbox guest VM accesses external network through port3. The next-hop gateway and DNS settings can be configured in <i>Scan Policy &gt; General &gt; Allow Virtual Machines to access external network through outgoing port3</i>.</p> <p>If port3 of FortiSandbox is behind a firewall with antivirus inspection enabled, an icon will be displayed.</p>
<b>FDN Download Server</b>	<p>Displays the status of the FDN download server. When the FDN download server is inaccessible, no update packages will be downloaded.</p> <p>Displays an up icon if the system can access the FDN download server. Displays a caution icon if the system cannot access the FDN download server. Hover the mouse pointer on the status icon to view detailed information.</p>
<b>Community Cloud Server</b>	<p>Displays the status of the Sandbox Community Cloud server.</p> <p>Displays an up icon if the system can access the cloud server. Displays a caution icon if the system cannot access the cloud server. Hover the mouse pointer on the status icon to view detailed information.</p>

<b>Web Filtering Server</b>	Displays the status of the Web Filtering query server. Displays an up icon if the system can access the Web Filtering query server. Displays a caution icon if the system cannot access the Web Filtering query server. Hover the mouse pointer on the status icon to view detailed information.
<b>Antivirus DB Contract</b>	The date that the antivirus database contract expires. If the contract expires within 15 days, a caution icon will appear.
<b>Web Filtering Contract</b>	The date that the web filtering contract expires. If the contract expires within 15 days, a caution icon will appear.
<b>MacOS VM Contract</b>	The date that the MacOS contract expires, and number of remote clones reserved in Fortinet MacOS cloud. In Cluster mode, the total reserved clone numbers will be displayed on the primary (master) node. All cluster units share collected pool of reserved clones from each unit. This means even a node that has no MacOS VM contract purchased, it can still upload MacOSX files to cloud to scan.
<b>Windows Cloud VM Contract</b>	This is only available on the VM00 model. Windows Cloud VMs are an extension of units' scan power by sending files to Fortinet Sandboxing cloud to scan. This line shows the date that Windows Cloud VM contract expires, and number of remote clones reserved in cloud.  In a cluster environment, each VM00 unit in the cluster can purchase Windows cloud VM seat counts to expand the cluster's scan power. These cloud VM clones are local to that VM00 unit and are not shared.



Select the edit icon to type a custom widget title and enter the refresh interval. The default refresh interval is 300 seconds.

## System Resources

This widget displays the following information and options:

<b>CPU Usage</b>	Gauges the CPU percentage usage.
<b>Memory Usage</b>	Gauges the Memory percentage usage.
<b>RAM Disk Usage</b>	Gauges the RAM Disk percentage usage. RAM Disk is used by the VM clone system.
<b>Reboot/Shutdown</b>	Options to shut down or reboot the FortiSandbox device.



Select the *Edit* icon to type a custom widget title and enter the refresh interval. The default refresh interval is 30 seconds.

## System Resources Usage Timeline

This widget displays a timeline chart of CPU, Memory, and Ram disk usage. The data shows a period of 24 hours or three days.

Use shift-select on a chart area to zoom in or out. Use the cursor to move the chart forward or backward. Hover the cursor over a colored portion of a bar in the graph to show the number of events for the selected type during that time period.



Select the *Edit* icon to type a custom widget title, enter the refresh interval, and select the time period. The default refresh interval is 300 seconds. The default time period is the last three days.

## Scanning Statistics

The *Scanning Statistics* widget displays information about the files that have been scanned over a specific time period.

This widget displays the following information:

<b>Rating</b>	The file rating refers to the rating categories.
<b>Sniffer, Device(s), On Demand, Network, Adapter, URL, All</b>	The input type from which the files were received. The URL type is for scanned URLs received from FortiMail devices, URLs extracted from forwarded email body of BCC adapter, URLs from ICAP adapter, and sniffed URLs in email traffic.
<b>Malicious</b>	The number of files scanned for each input type that were found to be malicious in the selected time period. Click the link to view the associated jobs.
<b>Suspicious - High Risk</b>	The number of files scanned for each input type that were found to be suspicious and posed a high risk in the selected time period. Click the link to view the associated jobs.
<b>Suspicious - Medium Risk</b>	The number of files scanned for each input type that were found to be suspicious and posed a medium risk in the selected time period. Click the link to view the associated jobs.
<b>Suspicious - Low Risk</b>	The number of files scanned for each input type that were found to be suspicious and posed a low risk in the selected time period. Click the link to view the associated jobs.
<b>Clean</b>	The number of files scanned for each input type that were found to be clean in the selected time period. Click the link to view the associated jobs.
<b>Other</b>	The number of files for each input type which have an unknown status. Unknown status files include jobs which have timed out, crashed, been canceled by the user through a JSON API call, or been terminated by the system. Click the link to view the associated jobs.

<b>Processed</b>	The total number of files processed for each input type in the selected time period.
<b>Pending</b>	The number of files pending. Pending files are files that have just been received and have not been put into the job queue, and files that have been put into the job queue but have not yet been processed.
<b>Processing</b>	The number of files that are being processed.
<b>Total</b>	The total number of files for each input type in the selected time period.



Select the *Edit* icon to type a custom widget title, enter the refresh interval, and select the time period. The default refresh interval is 600 seconds. The default time period is the last 24 hours.



If the device is the primary (master) node of a cluster, the numbers in this widget are the total job numbers of all cluster nodes.

## File Scanning Activity

The *File Scanning Activity* widget shows the number of clean, suspicious, and malicious events that have occurred at specific times over a selected time period.

The data can be displayed hourly or in daily. If it is set to *Hourly*, a bar will be displayed for each hour over selected time period. Hourly data is only available when selected time period is set to the *Last 24 hours*. If it is set to *Daily*, a bar will be shown for each day over selected time period.

When holding the shift key on keyboard, you can select an area in the chart to zoom it out. You can then use mouse pointer to move the chart forward and backward.

Hovering the cursor over a colored portion of a bar in the graph for a brief time will show the exact number of events of the selected type that occurred at that time.



Select the *Edit* icon to type a custom widget title, enter the refresh interval, and select the time period. The default refresh interval is 300 seconds. The default time period is the last seven days.

## Top Devices

The *Top Devices* widget displays the total number of scanning jobs for the top five devices over a selected time interval.

Hovering the cursor over a bar in the graph for a brief time will show the exact number of scanning jobs for that particular device.



Select the *Edit* icon to type a custom widget title, enter the refresh interval, top count, and select the time period. The default refresh interval is 300 seconds. The default time period is the last 24 hours.

## Top Critical Logs

The *Top Critical Logs* widget displays recent critical logs, including the time they occurred and a brief description of the event.



Select the *Edit* icon to type a custom widget title, enter the refresh interval, and top count. The default refresh interval is 3600 seconds.

## Pending Job Statistics

The *Pending Job Statistics* widget displays the pending job numbers of each input source.

Hovering the cursor over the graph displays the number of pending jobs for the on-demand, sniffer, and Fortinet devices over a selected time interval. The data can be displayed hourly or daily. When holding the shift key on keyboard, you can select an area in the chart to zoom it out. You can then use the mouse pointer to move the chart forward and backward.



Select the *Edit* icon to type a custom widget title and enter the refresh interval. The default refresh interval is 900 seconds (15 minutes).

## Disk Monitor

Displays the RAID level and status, disk usage, and disk management information. This widget is only available in hardware-based models.

This widget displays the following information:

<b>Summary</b>	Disk summary information including RAID level and status.
<b>RAID Level</b>	Displays the RAID level.
<b>Disk Status</b>	Displays the disk status.
<b>Disk Usage</b>	Displays the current disk usage.
<b>Disk Number</b>	Displays the disk number.
<b>Disk Size</b>	Displays the disk size.

## Sniffer Traffic Throughput

Displays the Sniffer Traffic Throughput in Mb/s across time.

By holding the keyboard's shift key, you can select an area in the chart to zoom out. You can then use the mouse pointer to move the chart forward and backward.

## Threats Distribution

Displays a pie chart of the detected malware rating distribution within a specified time period. Hovering the cursor over individual slice displays the total number, percentage, and time period of malware with that rating.



Select the *Edit* icon to type a customized widget title, change the refresh interval and time period.

---

## Customized Threats Distribution

Displays a donut chart of the detected malware rating distribution within two specified time periods. Hovering the cursor over individual slice displays the total number, percentage, and time period of malware with that rating.



Select the *Edit* icon to type a customized widget title, change the refresh interval and time range of inner and outer circle.

---

## Quick Download

Works with the CDR feature in FortiGate or FortiMail devices. You can quickly find a file according to its checksum (SHA1/MD5/SHA256). If found, you can download the original file, download the jobs PDF report, and view job details. The original file is in zip format and protected with the password *fortisandbox*.



Select the *Edit* icon to type a customized widget title.

---

## Basic System Settings

This section includes the following topics:

- [Change the system host name](#)
- [Change the administrator password](#)
- [Change the GUI idle timeout](#)
- [Configure the system time](#)
- [Microsoft Windows VM license activation](#)
- [Microsoft Office license upload and activation](#)
- [Log out of the unit](#)



- [Visit online help](#)
- [Refresh current web page](#)
- [Toggle left-side menu style](#)
- [Update the FortiSandbox firmware](#)
- [Reboot and shut down the unit](#)
- [Backup or restore the system configuration](#)

## Change the system host name

The *System Information* widget will display the full host name. You can change the FortiSandbox host name as required.

### To change the host name:

1. Go to *Dashboard > System Information widget > Host Name*.
2. Click *[Change]*.
3. In the *New Name* field, type a new host name.  
The host name may be up to 50 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.
4. Select *Apply*.

## Change the administrator password

By default, you can log into the GUI using the *admin* administrator account and no password. It is highly recommended that you add a password to the *admin* administrator account. For improved security, you should regularly change the *admin* administrator account password and the passwords for any other administrator accounts that you add.

### To change an administrator's password:

The user can click the current login username from the top right corner and select *Change Password* or:

1. Go to *System > Administrators*.
2. Select the administrator's account that you want to edit .
3. Click the *Edit* button in the toolbar.
4. Change the password.

## Change the GUI idle timeout

By default, the GUI disconnects administrative sessions if no activity takes place for five minutes. This idle timeout is recommended to prevent someone from using the GUI on a PC that has been logged into the GUI and left unattended.

### To change the idle timeout length:

1. Go to *System > Settings*.
2. Change the idle timeout minutes (1 to 480 minutes) as required.
3. Select *OK* to save the setting.



In this page you can also reset all widgets to their default settings.

## Configure the system time

The FortiSandbox unit's system time can be changed from the *Dashboard*. You can configure the FortiSandbox system time locally or select to synchronize with an NTP server.

### To configure the system time:

1. Go to *System Information widget > System Time*.
2. Click *[Update]*.

**Time Settings**

**System Time**  
 2019-04-03 10:18:31 UTC Refresh

**Time Zone**  
 (UTC)Coordinated Universal Time ▼

☒ **Set Time**  
 Hour  Minute  Second   
 Month  Day  Year

☐ **Synchronize with NTP Server**  
 Server

Apply
Back

3. Configure the following settings:

<b>System Time</b>	The date and time according to the FortiSandbox unit's clock at the time that this tab was loaded.
<b>Time Zone</b>	Select the time zone in which the FortiSandbox unit is located.
<b>Set Time</b>	Select this option to manually set the date and time of the FortiSandbox unit's clock, then select the <i>Hour</i> , <i>Minute</i> , <i>Second</i> , <i>Month</i> , <i>Day</i> , and <i>Year</i> fields before you select <i>Apply</i> .
<b>Synchronize with NTP Server</b>	Select this option to automatically synchronize the date and time of the FortiSandbox unit's clock with an NTP server. The synchronization interval is hard-coded to be 5 minutes. You can configure only one NTP server.
<b>Server</b>	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, go to <a href="http://www.ntp.org">http://www.ntp.org</a> . Ensure that the applicable routing is configured when an NTP server is used.

4. Click *Apply* to apply the changes, then select *OK* in the confirmation dialog box. You may need to log in again after changing the time.

## Microsoft Windows VM license activation

When Fortinet ships FortiSandbox, the default Windows guest VM image is activated. After a RMA or new Windows VM installation, the Windows VM license will be in an unactivated state and need re-activation.



If the user purchases a Windows VM upgrade package, or use an optional guest VM image, the downloaded license file should be uploaded here by clicking the *[Upload License]* link.

---

## Microsoft Office license upload and activation

User can purchase add-on Office licenses from Fortinet and upload it in the *System Information* widget.



By default, physical FortiSandbox models are shipped with a certain number of Microsoft Office license keys. Users can purchase more licenses from Fortinet to improve the scan capacity of Microsoft Office files, or to activate Microsoft Office software inside a newly installed optional Windows guest image. Users can upload the license file in the *System Information* widget.

---

### To upload a Microsoft Office license:

1. Go to *Dashboard > System Information widget > Microsoft Office*.
2. Click *[Upload License]*.
3. Click *Choose File* to browse for the license file on your management computer.
4. Click *Submit*.

The FortiSandbox will reboot after the license file is installed. After the license file is installed, you can scan Microsoft Office files including .docx and .pptx file.

## Log out of the unit

1. Select your user name from the top right corner of the banner.
2. Select *Logout* from the dropdown to log out of your administrative session.

If you only close the browser or leave the GUI to browse another website, you will remain logged in until the idle timeout period elapses.

## Visit online help

Click the *Help* icon to visit Online Help.

## Refresh current web page

Click the *Refresh* button on top of the website; the current web page will be refreshed.

## Toggle left-side menu style

By default, the left-side menu is in compact mode. If you want to revert back to the full style:

1. Go to *System > Settings*.
2. Select *Expanded in Menu Type* dropdown.
3. Click *OK* to save the setting.

## Update the FortiSandbox firmware

Before any firmware update, complete the following:

- Download the FortiSandbox firmware image and Release Notes document from the [Fortinet Customer Service & Support](#) portal. Review the Release Notes, including the special notices, upgrade information, product integration and support, and resolved and known issues.
- Backup your configuration file. It is highly recommended that you create a system backup file and save it to your management computer. You can also schedule to back up system configurations to a remote server.
- Plan a maintenance window to complete the firmware update. If possible, you may want to setup a test environment to ensure that the update does not negatively impact your network.
- Once the update is complete, test your FortiSandbox device to ensure that the update was successful.



Firmware best practice: Stay current on patch releases for your current major release. Only update to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiSandbox Release Notes* or contact Technical Support.

---

### To update the FortiSandbox firmware:

1. Go to *Dashboard > System Information widget > Firmware Version*.
2. Click *[Update]*.
3. Select *Choose File*, locate the firmware image on your management computer.
4. Click *Submit* to start the upgrade.

## Reboot and shut down the unit

Always reboot and shut down the FortiSandbox system using the options in the GUI or CLI to avoid potential configuration or hardware problems.

### To reboot the FortiSandbox unit:

1. Go to *Dashboard > System Resources widget*.
2. Select *Reboot*.
3. Enter a reason for the reboot in the *Reason* field, and then select *OK* to reboot the unit.
4. After reboot, the FortiSandbox VM system will initialize again. This initialization can take up to 30 minutes. The Windows VM icon in the *System Information* widget will show a warning sign before the process completes.



It is normal to see the following critical event log in *Log Access* after FortiSandbox boots up:  
*The VM system is not running and might need more time to startup. Please check system logs for more details. If needed, please reboot system.*

---



After FortiSandbox is upgraded to a new firmware version, the system might clean up data and a *Database is not ready message* will be displayed. The clean up time depends on the size of historical data.

---

#### To shut down the FortiSandbox unit:

1. Go to *Dashboard > System Resources widget*.
2. Select *Shutdown*.
3. Enter a reason for the shutdown in the *Reason* field.
4. Select *OK* to shutdown the unit.

## Backup or restore the system configuration

It is recommended that you create a system backup file as part of your maintenance plan. Always perform a backup before upgrading firmware or making major system configuration changes. Save these configuration backups to your management computer in the event that you need to restore the system after a network event.

---



The FortiSandbox configuration file is in binary format and manual editing is not supported.

---

#### To backup the FortiSandbox configuration to your local management computer:

1. Go to *Dashboard > System Information widget > System Configuration*.
2. Select *Backup/Restore*.
3. Click *Click here* to save your backup file to your management computer.

#### To backup the FortiSandbox configuration to a remote server:

1. Go to *Dashboard > System Information widget > System Configuration*.
2. Select *Backup/Restore*.

- Under Remote Backup, configure the following settings:

<b>Server Type</b>	SCP server type is selected by default.
<b>Server Address</b>	Enter the server IP address.
<b>File Path</b>	Enter the file path.
<b>Username</b>	Enter the username to log in to the remote server.
<b>Password</b>	Enter the password to log in to the remote server.
<b>Backup Schedule</b>	Set the back up frequency.

- Click *Set Remote Backup* to save your settings.

#### To restore the FortiSandbox configuration:

- Go to *Dashboard > System Information widget > System Configuration*.
- Select *Backup/Restore*.
- Click *Browse...*, locate the backup file on your management computer, then select *Restore* to load the backup file.
- Select *OK* in the confirmation dialog box. Once the configuration restore process is completed, you will be redirected to the log in page.



By performing a system restore, all of your current configurations will be replaced with the backup data. When users select *Restore Administrators, Admin Profiles, Certificates, LDAP Servers and Radius Servers*, all of this information will be overridden; otherwise, current settings are kept. The system will reboot automatically to complete the restore operation. Only backup configurations from the previous or same release are supported.



When you restore a backup configuration from to a unit in Cluster mode, the network configuration and HA cluster related configuration are not restored. The unit will be in Standalone mode. You will need to configure the network settings and add the unit back to Cluster.

# FortiView

The FortiView menu provides access to the following menus:

The FortiView pages allow you to view and search threats detected by FortiSandbox.	
<b>Operation Center</b>	On this page you can view malware which has been detected, as well as its status from a security update perspective. This page displays severity levels, victim IP addresses, incident time, threat, and current action status.
<b>Threats by Hosts</b>	On this page you can view and drill down all threats grouped by individuals or victim hosts in your organization. This page displays threats by user name or host IP address, the number of threats, the number of suspicious files (if available), and a button to show the victim's threat timeline chart. Select an entry in the table to view detailed information including attacker events, Botnet events, and URL events.
<b>Threats by Files</b>	On this page you can view and drill down all threats grouped by files. This page displays threats by file name, risk, and number of users. Select a file name in the table to view detailed information including user IP, destination, and number of detection times.
<b>Threats by Devices</b>	On this page you can view and drill down all threats grouped by devices. This page displays threats by device, number of malicious files, and number of suspicious files. Select a device in the table to view detailed information including malware name, destination, domain, and number of detection times.
<b>Event Calendar</b>	A calendar view of major events, including user login/logout, scan condition changes, and threat detection.
<b>File/URL Scan Search</b>	Search file or URL scan jobs by detection time, file MD5, file name, file SHA1 or SHA256, job ID, malware name, rating, service, source IP, user, submit device, detection OS, etc. You can add multiple search criteria by clicking the search field. If the search criteria is the file name you can also do a pattern search.

This section includes the following topics:

- [Operation Center](#)
- [Threats by Topology](#)
- [Threats by Hosts](#)
- [Threats by Files](#)
- [Threats by Devices](#)
- [Event Calendar](#)
- [File Scan Search](#)
- [URL Scan Search](#)

## Operation Center

On this page you can view malware which has been detected, as well as its status from a security update perspective.

When a dynamic signature is sent back to FortiGate, FortiMail, or FortiClient, the status information will be displayed so you can see that it has been done.

When a new antivirus update is received, FortiSandbox will recheck all samples not covered by the standard antivirus package and update its status. Malware detected by FortiSandbox before an antivirus signature is available will be marked as Zero-day.

<div> <input type="text" value="Detection"/> <span>2017-08-13 17:2... to 2017-08-14 17:2...</span> </div>					
	Severity	Victim IP	Incident Time	Threat Name	Action
	High Risk	208.91.113.110	Aug 14 2017 15:16:22	Suspicious - High	Action Required
	High Risk	208.91.113.110	Aug 14 2017 15:16:22	Suspicious - High	Action Required
	High Risk	208.91.113.110	Aug 14 2017 15:16:22	Suspicious - High	Action Required
	High Risk	208.91.113.110	Aug 14 2017 15:15:51	Suspicious - High	Action Required
	High Risk	208.91.113.110	Aug 14 2017 15:15:51	Suspicious - High	Action Required
	High Risk	208.91.113.110	Aug 14 2017 15:15:41	Suspicious - High	Action Required

The following options are available:

<b>Refresh</b>	Click the refresh icon to refresh the entries displayed after applying search filters.
<b>Search</b>	Show or hide the search filter field.
<b>Time Period</b>	Select the time period from the dropdown list. Select one of the following: 24 Hours, 7 Days, or 4 Weeks.
<b>Clear all removable filters</b>	Click the <i>trash can</i> icon to clear all removable filters.
<b>Export Data</b>	Click the <i>Export Data</i> button to create a PDF or CSV snapshot report. The time to generate the report is dependent on the number of events selected. You can wait till the report is ready to view, or navigate away and find the report later in <i>Log &amp; Report &gt; Report Center</i> page.
<b>Add Search Filter</b>	<p>Click the search filter field to add search filters. Click the cancel icon to the left of the search filter to remove the specific filter. Click the clear all filters icon in the search filter field to clear all filters.</p> <p>In this page, several fields, like victim host IP can be the search criteria. Search filters can be used to filter the information displayed in the GUI.</p>
<b>View Job</b>	Click the <i>View Jobs</i> icon show the job detail page.
<b>Number of Blocks</b>	After a malware's signature is added to a Malware package and downloaded by FortiGate, FortiGate can block subsequent occurrence of it. Hover your cursor on top of the icon, the number of blocks of this Malware is displayed.
<b>In Cloud</b>	An icon will appear if the malware is available in the FortiSandbox Community Cloud.



<b>In Signature</b>	An icon will appear if the malware is included in the current FortiSandbox generated Malware Package.
<b>Perform Rescan</b>	Click the icon to rescan the suspicious or malicious entry. In the Rescan Configuration dialog box you can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click <i>OK</i> to continue. Click the <i>Close</i> icon or the <i>Close</i> button to close the dialog box. The rescan job can be found in <i>File Input &gt; File On-Demand</i> page.
<b>Archived File</b>	An icon will appear if the file is an Archived File.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

This page displays the following information:

<b>Severity</b>	The severity rating of the malware. Severity levels include: <ul style="list-style-type: none"> <li>• Low Risk</li> <li>• Medium Risk</li> <li>• High Risk</li> <li>• Malicious</li> </ul> If a file is detected by FortiSandbox first before an antivirus signature is available, the Severity level will be Zero-day.
<b>Victim IP</b>	The IP address of the client that downloaded the malware. Use the column filter to sort the entries in ascending or descending order.
<b>Incident Time</b>	The date and time that the file was received by FortiSandbox. Use the column filter to sort the entries in ascending or descending order.
<b>Threat Name</b>	The name of the virus. Use the column filter to sort the entries in ascending or descending order. If the virus name is not available, the malware's Severity will be used as its Threat Name.
<b>Action</b>	Current action applied to the malware. Users use this field to track responses taken towards the incident. Three values are available: <ul style="list-style-type: none"> <li>• Action Taken</li> <li>• Ignore</li> <li>• Action Required. The user can mark an action against a single job, or to all jobs of the same file.</li> </ul>

#### To view file details:

1. Select a file.
2. Click the *View Details* icon. A new tab will open.
3. See [Appendix A - View Details Page Reference on page 186](#) for descriptions of the *View Details* page.
4. Close the tab to exit the *View Details* page.

## Threats by Topology

Go to *FortiView > Threats by Topology*. It combines both device and threat information together.

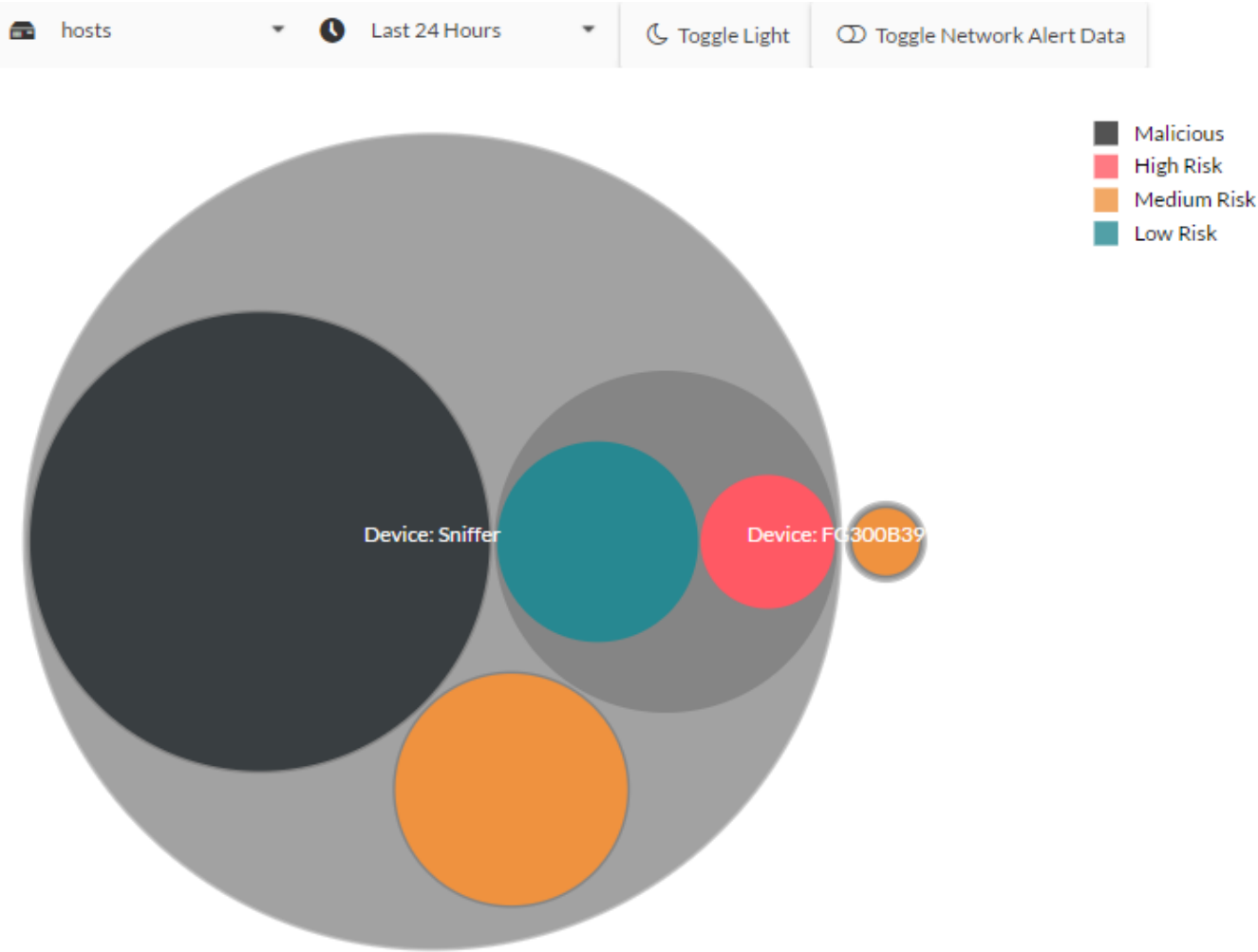
Devices (or input sources) are displayed in separated top level circles and the threats that occur on them are displayed inside them as second level circles. The radius of threat circle is proportional to threat event counts. Threat circles can be multiple levels and each level represents a subnet level.

Clicking on the circles will drill down to the host level. At the host level, clicking on a circle will display a new page to show threat details.

There are host and time range filters in the toolbar on top.

The following options are available:

<b>Hosts</b>	Select the host.
<b>Time Period</b>	Select the time period from the dropdown list. Select one of the following: <i>24 Hours</i> , <i>7 Days</i> , or <i>4 Weeks</i> .
<b>Toggle Light</b>	Select <i>Toggle Light</i> to change the topology background color.
<b>Toggle Network Alert Data</b>	Select to toggle and include Network Alert data from sniffed traffic.



Threats by Hosts

In this page you can view and drill down all threats grouped by hosts. The Host can be a user name or email address (if it is available) or a device that is the target of a threat. This page displays all threats that have occurred to the user or victim host during a time period. Click the *View Jobs* icon or double-click an entry in the table to view the second level.

Threats by Hosts - level 1

The following options are available:

Time Period	Select the time period from the dropdown list. Select one of the following: 24 Hours, 7 Days, or 4 Weeks.
-------------	---

<b>Export Data</b>	Click the <i>Export Data</i> button to create a PDF or CSV snapshot report. You can wait till the report is ready to view, or navigate away and find the report later in <i>Log &amp; Report &gt; Report Center</i> page.
<b>Search</b>	Show or hide the search filter field.
<b>Refresh</b>	Click the refresh icon to refresh the entries displayed after applying search filters.
<b>Add Search Filter</b>	Click the <i>Search Filter</i> field to add search filters. Click the <i>Cancel</i> icon to the left of the search filter to remove the specific filter. Click the <i>Clear All Filters</i> icon in the search filter field to clear all filters.  In this page, the threat target host or user name can be the search criteria. You can input a partial value to search all records that contain it.  Search filters can be used to filter the information displayed in the GUI.
<b>View Job</b>	Click the <i>View Jobs</i> icon to drill down the entry.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

This page displays the following information:

<b>Host/Username</b>	The device and username that is the target of threats. Click the column header to sort the table by this column.  <b>Note:</b> A duplicate user name or host from a different VDOM is considered a different user.
<b>Device Name</b>	The device name. Click the column header to sort the table by this column.
<b># of Malicious Files</b>	The number of unique malicious files associated with the user for the time period selected. Click the column header to sort the table by this column.
<b># of Suspicious Files</b>	The number of unique suspicious files associated with the user for the time period selected. Click the column header to sort the table by this column.
<b># of Network Threats</b>	The number of unique network threats (attacker, botnet, and suspicious URL events) associated with the user for the time period selected. Click the column header to sort the table by this column.
<b>Timeline</b>	View the Threat Timeline Chart. When you click on any dot in the chart, all events associated will be displayed. When you click on an event, the <i>View Details</i> page will open.
<b>Total Host</b>	The number of hosts displayed and total number of hosts.

## Threats by Hosts - level 2

Double-click an entry in the table or click the *View Jobs* icon to view the second level.

The following information is displayed:

<b>Back</b>	Click <i>Back</i> button to return to the main landing page.
-------------	--

<b>Threat Timeline Chart</b>	This chart displays the number of threats and types of threats which occurred to the threat target during the period of time. Hover the mouse pointer over the dots in the chart and more detailed threat information will be displayed.
<b>Summary</b>	The following fields are displayed: Device, Threat Target, Time Period, Total Files, number of: Malicious Files, Suspicious Files, and Network Events.
<b>Details</b>	
<b>Malicious Files</b>	Malicious file information including malware name, Threat Source, and number of detection times. The options are: <ul style="list-style-type: none"> <li>Click the <i>View Jobs</i> icon to drill down the entry.</li> <li>Click the malware name to view the related FortiGuard Encyclopedia page.</li> </ul>
<b>Suspicious Files</b>	Suspicious file information including file name, file type, rating, the malware hosting address and number of detection times. Click the <i>View Jobs</i> icon to drill down the entry.
<b>Attacker Events</b>	Attacker event information including backdoor name, attack origin address and port, attack destination address and port, and number of detection times.
<b>Botnet Events</b>	Botnet event information including botnet name, user IP address, user port, destination IP address, destination IP port and number of detection times.
<b>URL Events</b>	Suspicious URL event information including site category, host or IP address, URL, type, user IP address, user port and number of detection times.

## Threats by Hosts - level 3

The following options are available:

<b>Back</b>	Click the <i>Back</i> button to return to the main landing page.
<b>View Details</b>	Click the <i>View Details</i> icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
<b>Perform Rescan</b>	Click the icon to rescan the entry. In the <i>Rescan Configuration</i> dialog box you can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click <i>OK</i> to continue. Click the close icon or select the <i>Close</i> button to close the dialog box. The rescan job can be found in <i>File Input &gt; File On-Demand</i> page.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

The following information is displayed:

<b>Malicious Files</b>	Displays the date and time that the file was detected, malware name, source IP address, and destination IP address. Click the malware name to view the related FortiGuard Encyclopedia page.
<b>Suspicious Files</b>	Displays the date and time that the file was detected, file type, rating, source IP address, destination IP address and number of detection times, if available.

## Threats by Hosts - level 4

For more about the information available in the *View Details* pages for malicious and suspicious files, see [Appendix A - View Details Page Reference on page 186](#).



When a file has been rescanned, the results of the rescan are displayed on this page. Select the job ID to view the job details.

### To create a snapshot report for all threats by users:

1. Select a time period from the *Time Period* dropdown list.
2. Click the *Filter* field to apply filters to further drill down the information in the report.
3. Click the *Export Data* button in the toolbar.
4. In the *Report Generator*, select either PDF or CSV for the report type.
5. Click the *Generate Report* button to create the report.
6. When the report generation is completed, select the *Download* button to save the file to your management computer. You can navigate away and find the report later in *Log & Report > Report Center* page.
7. Click the *Cancel* button to exit the report generator.



In this release, the maximum number of events you can export to a PDF report is 1,000; the maximum number of events you can export to a CSV report is 15,000. Jobs over that limit will not be included in the report.

## Threats by Files

In this page you can view and drill down all threats group by malware file. This page displays threats by filename, rating, and number of targeted users and hosts. Click the *View Jobs* icon or double-click an entry in the table to view the second level.

### Threats by Files - level 1

The following options are available:

<b>Time Period</b>	Select the time period from the dropdown list. Select one of the following: <i>24 Hours</i> , <i>7 Days</i> , or <i>4 Weeks</i> .
<b>Export Data</b>	Click the <i>Export Data</i> button to create a PDF or CSV snapshot report. The time period of jobs included in the report depends on the selection made in the <i>Time Period</i> dropdown. The time to generate the report is dependent on the number of events selected. You can wait until the report is ready to view, or navigate away and find the report later in the <i>Log &amp; Report &gt; Report Center</i> page.

<b>Search</b>	Show or hide the search filter field.
<b>Refresh</b>	Click the <i>Refresh</i> icon to refresh the entries displayed after applying search filters.
<b>Add Search Filter</b>	Click the <i>Search Filter</i> field to add search filters. Click the <i>Cancel</i> icon to the left of the search filter to remove the specific filter. Click the <i>Clear All Filters</i> icon in the search filter field to clear all filters. When the filter <i>Filename</i> is used, click the = sign to toggle between the exact and pattern search. Search filters can be used to filter the information displayed in the GUI.
<b>View Jobs</b>	Click the <i>View Jobs</i> icon to drill down the entry.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

This page displays the following information:

<b>Filename</b>	The threat file name. Click the column header to sort the table by this column.
<b>Rating</b>	The file rating. Click the column header to sort the table by this column.
<b># of Users</b>	The number of users affected. Click the column header to sort the table by this column.
<b>Timeline</b>	View the Threat Timeline Chart. When you hover over any dot, all victim hosts infected by that malware will appear in five minutes. When you click on any dot in the chart, all events associated will be displayed. When you click on an event, the <i>View Details</i> page will open.
<b>Total Files</b>	The number of files displayed and the total number of files.

## Threats by Files - level 2

<b>Back</b>	Click the <i>Back</i> icon to return to the main landing page.
<b>Time Period</b>	Select the time period from the dropdown list. Select one of the following: <i>24 Hours</i> , <i>7 Days</i> , or <i>4 Weeks</i> .
<b>Search</b>	Show or hide the search filter field.
<b>Refresh</b>	Click the refresh icon to refresh the entries displayed after applying search filters.
<b>Add Search Filter</b>	Click the search filter field to add search filters. Click the cancel icon to the left of the search filter to remove the specific filter. Search filters can be used to filter the information displayed in the GUI.
<b>View Jobs</b>	Click the <i>View Jobs</i> icon to drill down the entry.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

The following information is displayed:

<b>Back</b>	Click the <i>Back</i> button to return to the main landing page.
-------------	--

<b>Summary of</b>	Summary information including the file name, source IP address, destination IP address, time period, download location, file type, threat type, submission information, and device information (if available). If the malware appears more than once, the information is from its most recent detection.
<b>Details</b>	Detail information including user IP address, destination IP address, and number of detection times. Select the <i>View Jobs</i> icon, or double-click on the row, to drill down the entry.

## Threats by Files - level 3

The following options are available:

<b>Back</b>	Click the <i>Back</i> icon to return to the main landing page.
<b>View Details</b>	Select the <i>View Details</i> icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
<b>Perform Rescan</b>	Click the icon to rescan the entry. In the <i>Rescan Configuration</i> dialog box you can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click <i>OK</i> to continue. Click the close icon or select the <i>Close</i> button to close the dialog box. The rescan job can be found in <i>File Input &gt; File On-Demand</i> page.
<b>Pagination</b>	Use the pagination options to browse entries displayed.



When a file has been rescanned, the results of the rescan are displayed in this page. Select the job ID to view the job details.

The following information is displayed:

<b>Detected</b>	The date and time that the file was detected by FortiSandbox. Click the column header to sort the table by this column.
<b>Filename</b>	Displays the filename. Clicking on the file name can link to a FortiGuard Encyclopedia to provide more information if the rating is Malicious.
<b>Source</b>	Displays the source IP address. Click the column header to sort the table by this column.
<b>Destination</b>	Displays the destination IP address. Click the column header to sort the table by this column.
<b>Rating</b>	Displays the file rating. Click the column header to sort the table by this column.
<b>Total Jobs</b>	The number of jobs displayed and the total number of jobs.



## Threats by Files - level 4

For more about the information available in the *View Details* pages for malicious and suspicious files, see [Summary Report on page 163](#)

**To create a snapshot report for all threats by files:**

1. Select a time period from the first dropdown list.
2. Select to apply search filters to further drill down the information in the report.
3. Click the *Export Data* button in the toolbar.
4. In the *Report Generator*, select either PDF or CSV for the report type.
5. Click the *Generate Report* button to create the report. You can wait until the report is ready to view, or navigate away and find the report later in *Log & Report > Report Center* page.
6. When the report generation is completed, select the *Download* button to save the file to your management computer.
7. Click the *Cancel* button to exit the report generator.



In this release, the maximum number of events you can export to a PDF report is 5,000; the maximum number of events you can export to a CSV report is 150,000.

## Threats by Devices

In this page you can view and drill down all threats grouped by devices. This page displays device name, number of malicious files, and number of suspicious files. Double-click an entry in the table to view the second level, *View Jobs*.

### Threats by Devices - level 1

The following options are available:

<b>Time Period</b>	Select the time period from the dropdown list. Select one of the following: <i>24 Hours</i> , <i>7 Days</i> , or <i>4 Weeks</i> .
<b>Export Data</b>	Click the <i>Export Data</i> button to create a PDF or CSV snapshot report. The time period of included jobs in the report depends on the selection made in the Time Period dropdown. The time to generate the report is dependent on the number of events selected. You can wait until the report is ready to view, or navigate away and find the report later in <i>Log &amp; Report &gt; Report Center</i> page.
<b>Search</b>	Show or hide the search filter field.
<b>Refresh</b>	Click the <i>Refresh</i> icon to refresh the entries displayed after applying search filters.
<b>Add Search Filter</b>	Click the <i>Search Filter</i> field to add search filters. Click the <i>Cancel</i> icon to the left of the search filter to remove the specific filter. Click the <i>S</i> icon in the search filter field to clear all filters.

	Search filters can be used to filter the information displayed in the GUI. You can input a partial value to search all records that contain it.
<b>View Jobs</b>	Click the <i>View Jobs</i> icon to drill down the entry.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

This page displays the following information:

<b>Device</b>	Displays the device name. Click the column header to sort the table by this column.  Note: A different VDOM or protected email domain on the same device is considered a different device.
<b># of Malicious Files</b>	The number of malicious files submitted by the device. Click the column header to sort the table by this column.
<b># of Suspicious Files</b>	The number of suspicious files submitted by the device. Click the column header to sort the table by this column.
<b>Timeline</b>	View the Threat Timeline Chart of the device. When you hover on any dot, all victim hosts managed by the device will appear in five minutes. When you click on any dot in the chart, all events associated will be displayed. When you click on an event, the View Details page will open.
<b>Total Devices</b>	The number of devices displayed and the total number of devices.

## Threats by Devices - level 2

The following information is displayed:

<b>Back</b>	Click the <i>Back</i> button to return to the main landing page.
<b>Summary of</b>	Displays a summary of the device type selected.
<b>Details</b>	Detailed information includes device name, selected time period, and total number of malicious and suspicious files.
<b>Malicious Files</b>	Malicious file information including malware name, destination IP address, and number of detection times. Click the <i>View Details</i> icon or double-click the row to drill down the entry.  Click the malware name to view the related FortiGuard Encyclopedia page.
<b>Suspicious Files</b>	Suspicious file information including file name, file type, risk level, destination IP address, and number of detection times.  Click the <i>View Details</i> icon or double-click the row to drill down the entry.

## Threats by Devices - level 3

The following options are available:

<b>Back</b>	Click the <i>Back</i> icon to return to the main landing page.
<b>View Details</b>	Select the <i>View Details</i> icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
<b>Perform Rescan</b>	Click the icon to rescan the entry. In the <i>Rescan Configuration</i> dialog box you can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click <i>OK</i> to continue. Click the <i>Close</i> icon or select the <i>Close</i> button to close the dialog box. The rescan job can be found in <i>File Input &gt; File On-Demand</i> page.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

The following information is displayed:

<b>Malicious Files</b>	Displays the date and time that the file was detected, malware name, source IP address, and destination IP address. Click the malware name to view the related FortiGuard Encyclopedia page.
<b>Suspicious Files</b>	Displays the date and time that the file was detected, file type, rating, source IP address, destination IP address, and number of detection times, if available.

## Threats by Devices - level 4

For more about the information available in the *View Details* pages for malicious and suspicious files, see [Appendix A - View Details Page Reference on page 186](#).



When a file has been rescanned, the results of the rescan are displayed in this page. Select the job ID to view the job details.

### To create a snapshot report for all threats by devices:

1. Select a time period from the first dropdown list.
2. Select to apply search filters to further drill down the information in the report.
3. Click the *Export Data* button in the toolbar. The *Report Generator* window opens.
4. Select either PDF or CSV for the report type. Optionally you can further define the report start/end date and time.
5. Click the *Generate Report* button to create the report. You can wait until the report is ready to view, or navigate away and find the report later in *Log & Report > Report Center* page.
6. When the report generation is completed, select the *Download* button to save the file to your management computer.
7. Click the *Close* icon or the *Cancel* button to quit the report generator.



In this release, the maximum number of events you can export to a PDF report is 1,000; the maximum number of events you can export to a CSV report is 15,000. Jobs over that limit will not be included in the report.

## Event Calendar

This page displays major events. You can show your events in a day, week, month, or timeline format. You can drill down to day level and click each event for its details.

TODAY   September, 2017							DAY	WEEK	MONTH	AGENDA	TIMELINE
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday					
27	28	29	30	31	01	02					
(14) Job Event (28) Notification Event (14) SNMP Event	(52) Job Event (11) System Event (58) SNMP Event (24) Notification Event	(23) Notification Event (422) SNMP Event (12) System Event (419) Job Event	(123) System Event (2) Input Event (623) Job Event (23) Notification Event (625) SNMP Event	(24) Notification Event (118) System Event (143) SNMP Event (139) Job Event	(95) System Event (24) Notification Event (90) Job Event (90) SNMP Event	(3) SNMP Event (25) Notification Event (87) System Event (3) Job Event					
03	04	05	06	07	08	09					
(28) Notification Event (92) System Event	(7) Job Event (24) Notification Event (7) SNMP Event (132) System Event	(804) Job Event (209) System Event (822) SNMP Event (4) Input Event (23) Notification Event	(122) System Event (284) SNMP Event (24) Notification Event (274) Job Event	(73) Job Event (24) Notification Event (75) SNMP Event (110) System Event	(24) Notification Event (94) System Event (87) Job Event (90) SNMP Event	(70) System Event (25) Notification Event					
10	11	12	13	14	15	16					
(28) Notification Event (132) System Event	(218) Job Event (2) Input Event (233) SNMP Event (2) VM Event (23) Notification Event ...	(10) Notification Event (18) SNMP Event (18) Job Event (46) System Event									
17	18	19	20	21	22	23					
24	25	26	27	28	29	30					

Job (19) System (53) Notification (28)

TODAY   Tuesday, September 12, 2017							DAY	WEEK	MONTH	AGENDA	TIMELINE
Tue 9/12											
12:00 AM	Package Options			Package Options			Device or FortiClient				
1:00 AM	Package Options			Package Options			Device or FortiClient				
2:00 AM	Malicious	SNMP	Device or	Package Options	Package Options	Package Options	Device or	Device or	Device or	Device or	Device or
3:00 AM	Device or FortiClient			Package Options			Package Options				
4:00 AM	Package Options			Package Options			Device or FortiClient				
5:00 AM	Device or FortiClient			Package Options			Package Options				
6:00 AM	Device or	Package Options	Package Options	Package Options	Package Options	Package Options	Device or	Device or	Device or	Device or	Device or
7:00 AM	Low	Medium	SNMP	Device or	Package Options	Package Options	Device or	Medium	Device or	Device or	SNMP
8:00 AM	Low	Medium	SNMP	Device or	Package Options	Package Options	Device or	Medium	Device or	Device or	SNMP
9:00 AM	Malicious	SNMP	Device or	Package Options	Package Options	Package Options	Device or	Medium	SNMP	Device or	Login
10:00 AM	Package Options	Package Options	Package Options	Reboot	SNMP	Adapter	Login				

The following options are available:

<b>Filter</b>	You can filter for the events you would like to see by turning on/off the event.
<b>Day</b>	Click to display the event calendar by day.
<b>Week</b>	Click to display the event calendar by week.
<b>Month</b>	Click to display the event calendar by month.
<b>Agenda</b>	Click the Agenda tab to schedule jobs.
<b>Timeline</b>	Click to display the event calendar by timeline.

The following events are displayed:

<b>System Events</b>	<ul style="list-style-type: none"> <li>• System login/logout</li> <li>• Reboot/shutdown</li> <li>• Firmware upgrade</li> <li>• System critical errors</li> <li>• System configuration changes (includes user creation, scan profile change etc.)</li> </ul>
<b>Notification Events</b>	<ul style="list-style-type: none"> <li>• PDF report generation</li> <li>• Network share scan</li> </ul>
<b>Threat Events</b>	<ul style="list-style-type: none"> <li>• Malware/URL detection. Double-clicking on the event will show its detailed information in a new browser tab.</li> </ul>

You can configure what types of events to show in the *System > Event Calendar Settings* page.

## File Scan Search

To view all files and search files, go to *FortiView > File Scan Search*. You can apply search filters to drill down the information displayed. Filenames can also be searched based on name patterns, and a snapshot report can be created for all search results.

If the device is the primary (master) node of a cluster, all jobs processed by the cluster are available to be searched. If the device is a worker (slave) node of a cluster, only jobs processed by this device are available to be searched.

The following options are available:

<b>Refresh</b>	Click the <i>Refresh</i> icon to refresh the entries displayed after applying search filters.
<b>Search Field</b>	Enter the detection time frame and click to add additional search filters for Device, File MD5, Filename, File SHA1, File SHA256, Job ID, Malware, Rating, Service, Source, User, Device, Infected OS, Rated by, Submit User, Submit Filename, Suspicious Type, or Scan Unit. When the search criteria is a <i>Filename</i> , click the = sign to toggle between the exact and pattern search.
<b>Time Period</b>	Select a time period to apply to the search.

<b>Export to Report</b>	Select to open the Report Generator dialog box. Select to generate a PDF or CSV report. You can wait until the report is ready to view, or navigate away and find the report later in <i>Log &amp; Report &gt; Report Center</i> page.
<b>Customize</b>	Click the <i>Customize</i> icon to customize the Job View settings page. Go to <a href="#">Job View Settings on page 76</a> for more information.
<b>Action</b>	
<b>View Details</b>	Click the <i>View Details</i> icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
<b>Archived File</b>	The icon displays that the file as an archived file.
<b>FortiGuard Advanced Static Scan</b>	The icon displays that the file is rated by user's overridden verdict or FortiGuard advanced static scan.
<b>File Inside Archive</b>	The icon displays that the file is a file extracted from an archive file.
<b>Rescan Job</b>	The icon displays that the job is Malicious from an AV Rescan or a customized rescan job of the Malicious file.
<b>Video</b>	Click on the <i>Video</i> button to play the video of the scan job. Scan videos are available in On Demand scans if user has the privilege.
<b>Perform Rescan</b>	Click the icon to rescan the entry. In the <i>Rescan Configuration</i> dialog box you can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click <i>OK</i> to continue. Click the close icon or select the <i>Close</i> button to close the dialog box. The rescan job can be found in <i>File Input &gt; File On-Demand</i> page.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

The following information is displayed:

<b>Total Jobs</b>	The number of jobs displayed and the total number of jobs.
-------------------	--

The displayed columns are determined by settings defined in *System > Job View Settings > File Detection Columns* page. Go to [Job View Settings on page 76](#) for more information.

## URL Scan Search

To view all URL scan jobs and search URLs, go to *FortiView > URL Scan Search*. You can apply search filters to drill down the information displayed. URLs can be searched based on different criteria, and a snapshot report can be created for all search results.

If the device is the primary (master) node of a cluster, all jobs processed by the cluster are available to be searched. If the device is a worker (slave) node of a cluster, only jobs processed by this device are available to be searched.

Detection 2016-02-29 12... to 2016-03-01 12...						
	Submitted Time	URL	Rating	Submitted Filename	Submitted By	Infected OS
	Feb 29 2016 17:19:58	http://schneeeifelmusikanten.de/	N/A	bad_url.txt	admin	N/A
	Feb 29 2016 17:19:58	http://www.world-plants.co.uk/	N/A	bad_url.txt	admin	N/A
	Feb 29 2016 17:19:57	http://trevalon.co.uk/	N/A	bad_url.txt	admin	N/A
	Feb 29 2016 17:19:57	http://munkavedelminagyker.com/	N/A	bad_url.txt	admin	N/A
	Feb 29 2016 17:19:57	http://drpinna.com/	N/A	bad_url.txt	admin	N/A
	Feb 29 2016 17:19:57	http://www.bairescat.com/	N/A	bad_url.txt	admin	N/A
	Feb 29 2016 17:19:57	http://www.mynewscomer.com/?p=186	N/A	bad_url.txt	admin	N/A

The following options are available:

<b>Refresh</b>	Click the refresh icon to refresh the entries displayed after applying search filters.
<b>Search Field</b>	Enter the detection time frame and click to add additional search filters for Destination, Device, Infected OS Job ID, Job Status, Rated By, Rating, Scan Unit, Submit User, Submitted Filename and URL. When the search criteria is <i>Submitted Filename</i> , click the = sign to toggle between the exact and pattern search.
<b>Time Period</b>	Select a time period to apply to the search.
<b>Export to Report</b>	Select to open the Report Generator dialog box. Select to generate a PDF or CSV report. During generation, do not close the dialog box or navigate away from the page. You can wait till the report is ready to view, or navigate away and find the report later in <i>Log &amp; Report &gt; Report Center</i> page.
<b>Customize</b>	Click the <i>Customize</i> icon to customize the Job View settings page. Go to <a href="#">Job View Settings on page 76</a> for more information.
<b>Action</b>	
<b>View Details</b>	Click the <i>View Details</i> icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
<b>FortiGuard Advanced Static Scan</b>	The icon displays that the URL is rated by user's overridden verdict, or FortiGuard advanced static scan
<b>Rescan Job</b>	The icon displays that the job is a customized rescan job of a Malicious URL.
<b>Video</b>	Click on the <i>Video</i> button to play the video of the scan job. Scan videos are available in On Demand scans if user has the privilege.
<b>Archive File</b>	The icon displays that the URL is from a file from an On Demand scan
<b>File Downloading URL</b>	The icon displays that the URL is from a downloading URL, and its payload is also scanned as a file scan job.
<b>Perform Rescan</b>	Click the icon to rescan the suspicious or malicious entry. In the Rescan Configuration dialog box you can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing.

Click *OK* to continue. Click the *Close* icon or the *Close* button to close the dialog box. The rescan job can be found in *File Input > File On-Demand* page.

**Pagination** Use the pagination options to browse entries displayed.

The following information is displayed by default:

<b>Detection</b>	The date and time that the file was detected by FortiSandbox.
<b>URL</b>	Displays the URL.
<b>Rating</b>	The URL rating. The rating can be one or more of the following: Clean, Low Risk, Medium Risk, High Risk, Malicious, or Unknown. Click the column header to sort the table by this column.
<b>Submitted Filename</b>	The submitted filename associated with the URL. Click the column header to sort the table by this column.  If the URL is from the body of an Email, and submitted by FortiMail, the Email's session ID is used as the Submitted Filename.
<b>Submit User</b>	The user that submitted the URL to be scanned. Click the column header to sort the table by this column.
<b>Infected OS</b>	The OS version of the FortiSandbox VM that was used to make the Suspicious verdict
<b>Total Jobs</b>	The number of jobs displayed and the total number of jobs.

The displayed columns are determined by settings defined in *System > Job View Settings > URL Detection Columns* page. Go to [Job View Settings on page 76](#) for more information.



# Network

The Network page provides interface, DNS, and routing management options.

This section includes the following topics:

- [Interfaces](#)
- [DNS Configuration](#)
- [System Routing](#)

## Interfaces

To view and manage interfaces, go to *Network > Interfaces*.

This page displays the following information and options:

Interface	The interface name and description, where applicable. Failover IP will be listed under this field with the following descriptor: (cluster external port).
<b>port1 (administration port)</b>	port1 is hard-coded as the administration interface. You can select to enable or disable HTTP, SSH, Telnet access rights on port1. HTTPS is enabled by default. port1 can be used for Device mode, although a different, dedicated port is recommended.
<b>port2</b>	port2 can be used for Sniffer mode, Device mode, and inter-node communication within a cluster.
<b>port3 (VM outgoing interface)</b>	port3 is reserved for outgoing communication triggered by the execution of the files under analysis. It is recommended to put this interface on an isolated network behind a firewall.  One special type of outgoing communication from a guest VM is used to connect to the Microsoft Windows activation server to activate the Windows Sandbox VM product keys. You must enable <i>Allow Virtual Machines to access external network through outgoing port</i> and setup the next hop gateway and DNS server to allow files running inside VMs to access the external network. Office licenses are verified through the VM machines, so internet access via port3 is required to contact Microsoft for the license activation.
<b>port4</b>	port4 can be used for Sniffer mode, Device mode, and inter-node communication within a cluster.

<b>port5/port6</b>	port5 and port 6 can be used for Sniffer mode, Device mode, and inter-node communication within a cluster. On FortiSandbox 2000E, 3000E and 3500D devices, port5 and port6 are 10G fiber ports. We recommend using these ports on a primary (master) node or secondary (primary slave) as communications ports with cluster workers (slaves).
<b>port7/port8</b>	port7 and port8 can be used for Sniffer mode, Device mode, and inter-node communication within a cluster. On FortiSandbox 3000D devices, port7 and port8 are 10G fiber ports. We recommend using these ports on a primary (master) node or secondary (primary slave) as communications ports with cluster workers (slaves).
<b>IPv4</b>	The IPv4 IP address and subnet mask of the interface.
<b>IPv6</b>	The IPv6 IP address and subnet mask of the interface.
<b>Interface Status</b>	The state of the interface; one of the following states: <ul style="list-style-type: none"> <li>• Interface is up</li> <li>• Interface is down</li> <li>• Interface is being used by sniffer</li> </ul>
<b>Link Status</b>	The link status. <ul style="list-style-type: none"> <li>• Link up</li> <li>• Link down</li> </ul>
<b>Access Rights</b>	The access rights associated with the interface. HTTPS is enabled by default on port1 or any other administrative port set through the CLI command <code>set admin-port</code> . You can select to enable HTTP, SSH, and Telnet access on the administrative port.
<b>PCAP</b>	Click the PCAP icon to sniff the traffic of an interface for up to 60 seconds then download the PCAP file in a ZIP format (maximum 100MB file size). Users can define the tcpdump filter to use, such as host 172.10.1.1 and TCP port 443. Only one capture is allowed to run at a time for each port. Sniffing ports are combined and treated as a single port.
<b>Edit</b>	Select the interface and click <i>Edit</i> from the toolbar to edit the interface.



The FortiSandbox uses port 3 to allow scanned files to access the Internet. The Internet visiting behavior is an important factor to determine if a file is malicious.

As malicious files are infectious, you should ensure that the connection for port 3 is able to both access the Internet and be isolated. The connection should not belong to or be able to access any internal subnet that needs to be protected. Fortinet recommends placing this interface on an isolated network behind a firewall.



For more information on FSA-1000D, FSA-3000D, FSA-2000E, FSA-3500D, FSA-3000E ports, see [Default Port Information on page 12](#).



You can setup more administration ports with CLI command `set admin-port`.

---



The following subnets are reserved for use by FortiSandbox. Do not configure interface IP addresses as one falling into this range.

- 192.168.56.0/24
  - 192.168.57.0/24
  - 192.168.250.0/24
- 

## Edit an interface

1. The IPv4/IPv6 address of an interface can be edited by selecting the interface name and clicking the *Edit* button from the toolbar.
  2. Edit the IP address as required, then click *OK* to apply the changes. You can also change the interface status from *Up* to *Down* by clicking the status icon.
- 



Do not change settings on an interface used for sniffing traffic.

---

## Edit administrative access

1. The port1 interface or any other administrative port set through the CLI command `set admin-port` are used for administrative access to the FortiSandbox device. HTTPS is enabled by default, but you can edit this interface to enable HTTP, SSH, and Telnet support.
  2. Edit the IP address and the access rights as required, then click *OK* to apply the changes.
- 



Administrative access rights can only be set on *port1*; all other administrative ports follow *port1* settings.

---

## Failover IP

Users are able to configure a cluster level failover IP, which will be set only on primary (master) node. This failover IP can only be set on current primary (master) node through the CLI. It should be in the same subnet of the port's local IP. Clients, such as FortiGates, should point to the failover IP in order to use the HA functionality. When a failover occurs, failover IP will be applied on new primary (master) node.

The primary (master) node and secondary (primary slave) node local IP will be kept locally during failover.

### Example:

Here is an example to set a failover IP for port1.

```

> show
Configured parameters:
Port 1 IPv4 IP: 172.16.69.145/24 MAC: 14:18:77:52:37:72
Port 1 IPv6 IP: 2620:101:9005:69::145/64 MAC: 14:18:77:52:37:72
Port 2 IPv4 IP: 1.1.7.5/24 MAC: 14:18:77:52:37:73
Port 3 IPv4 IP: 192.168.199.145/24 MAC: 14:18:77:52:37:74
IPv4 Default Gateway: 172.16.69.1
> hc-settings -sc -tM -n145 -c3000d-cluster -p1234 -iport2
The unit was successfully configured.
> hc-settings -si -iport1 -a172.16.69.160/24
The external IP address 172.16.69.160 for cluster port1 was set successfully
> hc-settings -l
SN: FSA3KD3R16000xxx
Type: Master
Name: 145
HC-Name: 3000d-cluster
Authentication Code: 1234
Interface: port2
Cluster Interfaces:
port1: 172.16.69.160/255.255.255.0

```

## DNS Configuration

The primary and secondary DNS server addresses can be configured from *Network > System DNS*. FortiSandbox is configured to use the FortiGuard DNS servers by default.

## System Routing

The System Routing page allows you to manage static routes on your FortiSandbox device. Go to *Network > System Routing* to view the routing list.

The following options are available:

<b>Create New</b>	Select to create a new static route.
<b>Edit</b>	Select a static route in the list and click <i>Edit</i> in the toolbar to edit the entry.
<b>Delete</b>	Select a static route in the list and click <i>Delete</i> in the toolbar to delete the entry.

The following information is displayed:

<b>IP/Mask</b>	Displays the IP address and subnet mask.
<b>Gateway</b>	Displays the gateway IP address.
<b>Device</b>	Displays the interface associated with the static route.
<b>Number of Routes</b>	Displays the number of static routes configured.

**To create a new static route:**

1. Click *Create New* from the toolbar.
2. Enter a destination IP address and mask, and a gateway, in their requisite fields.



The destination IP/Mask can be entered in the format 192.168.1.2/255.255.255.0, 192.168.1.2/24, or fe80:0:0:0:0:c0a8:1fe.

The following subnets are reserved for use by FortiSandbox. Do not configure static routes for IP address ranges falling into it.

- 192.168.56.0/24
  - 192.168.57.0/24
  - 192.168.250.0/24
- 

3. Select a device (or interface) from the dropdown list.
4. Click *OK* to create the new static route.

**To edit a static route:**

1. Select a Static Route.
2. Click the *Edit* button.
3. Edit the destination IP address and mask, gateway, and device (or interface) as required.
4. Click *OK* to apply the edits to the static route.

**To delete a static route or routes:**

1. Select one or more Static Routes.
2. Click the *Delete* button from the toolbar.
3. Select *Yes, I'm sure* on the confirmation page to delete the selected route or routes.



Static route entries defined in this page is for the system to use and will not be applied to traffic originating from the guest VM during a file's execution.

---

# System

The System tree menu enables you to manage and configure the basic system options for the FortiSandbox unit. This includes administrator configuration, mail server settings, and maintenance information.

The System menu provides access to the following menus:

<b>Administrators</b>	Configure administrator user accounts.
<b>Admin Profile</b>	Configure user profiles to define user privileges.
<b>Device Groups</b>	Add devices to a device group and assign it to multiple device users.
<b>Certificates</b>	Configure CA certificates.
<b>LDAP Servers</b>	Configure LDAP Servers.
<b>RADIUS Servers</b>	Configure RADIUS Servers.
<b>Mail Server</b>	Configure the Mail Server.
<b>SNMP</b>	Configure SNMP.
<b>FortiGuard</b>	Configure FortiGuard.
<b>Login Disclaimer</b>	Configure the Login Disclaimer.
<b>Settings</b>	Configure the idle timeout value for the GUI and CLI interface and GUI language. You can also toggle left-side menu mode and reset all widgets to their default state.
<b>Job View Settings</b>	Define columns and orders of job result tables.
<b>Event Calendar Settings</b>	Define what kind of events to display in <i>Event Calendar</i> page.



Some menus are not displayed on the worker nodes in a cluster.

This section includes the following topics:

- [Administrators](#)
- [Admin Profiles](#)
- [Wildcard Admin Authentication](#)
- [Device Groups](#)
- [Certificates](#)
- [LDAP Servers](#)
- [RADIUS Servers](#)
- [Mail Server](#)
- [SNMP](#)
- [FortiGuard](#)

- [Login Disclaimer](#)
- [Settings](#)
- [Job View Settings](#)
- [Event Calendar Settings](#)

## Administrators

The *Administrators* menu allows you to configure administrator user accounts.

Users whose Admin Profile does not have *Read Write* privilege under *System > Admin access* will only be able to view and edit their own information.

The following options are available:

<b>Create New</b>	Select to create a new administrator account.
<b>Edit</b>	Select an administrator account from the list and click <i>Edit</i> in the toolbar to edit the entry.
<b>Delete</b>	Select an administrator account from the list and click <i>Delete</i> in the toolbar to delete the entry.
<b>Test Login</b>	Select an LDAP/RADIUS administrator account from the list and click <i>Test Login</i> to test the user's login settings. If an error occurs, a detailed debug message will display.

The following information is displayed:

<b>Name</b>	Displays the administrator account name.
<b>Type</b>	The administrator type: <ul style="list-style-type: none"><li>• Local</li><li>• LDAP</li><li>• RADIUS</li><li>• LDAP WILDCARD</li><li>• RADIUS WILDCARD</li></ul>
<b>Profile</b>	The Admin Profile the user belongs to.

### To create a new user:

1. Login as a user whose Admin Profile has *Read/Write* privileges under *System > Admin access*, and go to *System > Administrators*.

2. Select **+ Create New** from the toolbar.

New Administrator

Administrator:

admin

Type:

☒ Local
 ☐ LDAP
 ☐ RADIUS
 ☐ LDAP WILDCARD
 ☐ RADIUS WILDCARD

☐ Device User

Admin Profile:

Super Admin

Trusted Host #1:

0.0.0.0/0.0.0.0

Trusted Host #2:

255.255.255.255/255.255.255.255

Trusted Host #3:

255.255.255.255/255.255.255.255

IPv6 Trusted Host #1:

::/0

IPv6 Trusted Host #2:

::/0

IPv6 Trusted Host #3:

::/0

Comments:

Language:

English

OK

Cancel

3. Configure the following:

<b>Administrator</b>	Enter a name for the new administrator account. The administrator name must be 1 to 30 characters long and may only contain upper-case letters, lower-case letters, numbers, and the underscore character (_).
<b>Password</b>	Enter a password for the account. The password must be 6 to 64 characters long and may contain upper-case letters, lower-case letters, numbers, and special characters. This field is available when <i>Type</i> is set to <i>Local</i> .
<b>Confirm Password</b>	Confirm the password for the account. This field is available when <i>Type</i> is set to <i>Local</i> .
<b>Type</b>	Select either Local, LDAP, or RADIUS.
<b>LDAP</b>	When <i>Type</i> is <i>LDAP</i> , select the LDAP server from the dropdown list. For information on creating an LDAP server, see <a href="#">LDAP Servers on page 65</a> .
<b>RADIUS</b>	When <i>Type</i> is <i>RADIUS</i> , select the RADIUS server from the dropdown list. For information on creating a RADIUS server, see <a href="#">RADIUS Servers</a> .
<b>LDAP WILDCARD</b>	When <i>Type</i> is <i>LDAP WILDCARD</i> , select the LDAP server from the dropdown list. The Administrator is LDAP_WILDCARD and can not be edited. For more information, see <a href="#">Wildcard Admin Authentication on page 61</a> .



<b>RADIUS WILDCARD</b>	When <i>Type</i> is <i>RADIUS WILDCARD</i> , select the Radius server from the dropdown list. The Administrator is <i>RADIUS_WILDCARD</i> and can not be edited. For more information, see <a href="#">Wildcard Admin Authentication on page 61</a> .
<b>Device User</b>	<p>Tick the checkbox when user will be assigned devices. When the user logs in, only jobs belonging to the assigned devices or VDOMs/Protected Domains will be visible.</p> <p>Device group can be created in <i>System &gt; Device Groups</i> and then assigned to a device user.</p> <p>You can also assign devices on the fly by selecting <i>Self Assigned</i> in the Device Group dropdown list.</p>
<b>Admin Profile</b>	Select the Admin Profile the user belongs to.
<b>Assigned Devices</b>	<p>Assigned devices and/or VDOMs/Protected Domains to the user when the user is set to <i>Device User</i>.</p> <p>When the user clicks the panel, an Available Devices panel will slide out from the right side. This panel lists all available devices and VDOMs/Protected Domains. Users can assign devices and VDOMs/Protected Domains to the user by clicking the device serial number or VDOM/Protected Domains name. Users can also add or delete user defined devices which have not been seen by the FortiSandbox unit. After editing, click outside the device panel to accept the changes.</p>
<b>Trusted Host 1, Trusted Host 2, Trusted Host 3</b>	Enter up to three IPv4 trusted hosts. Only users from trusted hosts can access FortiSandbox.
<b>Trusted IPv6 Host 1, Trusted IPv6 Host 2, Trusted IPv6 Host 3</b>	Enter up to three IPv6 trusted hosts. Only users from trusted hosts can access FortiSandbox.
<b>Comments</b>	Enter an optional description comment for the administrator account.
<b>Language</b>	Set the GUI language for the user, either <i>English</i> , <i>Japanese</i> , or <i>French</i> .



Setting trusted hosts for administrators limits what computers an administrator can log in the FortiSandbox unit from. When you identify a trusted host, the FortiSandbox unit will only accept the administrator's login from the configured IP address or subnet. Any attempt to log in with the same credentials from any other IP address or any other subnet will be dropped.

4. Select *OK* to create the new user.

#### To edit a user account:

1. Login as a user whose Admin Profile has *Read/Write* privileges under *System > Admin access*, and go to *System > Administrators*.
2. Select the name of the user you would like to edit and click *Edit* from the toolbar.

3. Edit the account as required and then re-type the new password in the confirmation field.
4. Click *OK* to apply the changes.



When editing an *admin*, you will be required to type the old password before you can set a new password.



Only the *admin* user can edit its own settings.

---

#### To delete one or more user accounts:

1. Login as a user whose Admin Profile has *Read/Write* privileges under *System > Admin access*, and go to *System > Administrators*.
2. Select the user account you want to delete.
3. Click *Delete* from the toolbar.
4. Click *Yes, I'm sure* in the confirmation page to delete the selected user(s).

#### To test LDAP/RADIUS user login:

1. Login as an user whose Admin Profile has *Read/Write* privileges under *System > Admin access*, and go to *System > Administrators*.
2. Select a LDAP/RADIUS user to test.
3. Select *Test Login* from the toolbar.
4. In the dialog box, enter the user's password.
5. Click *OK*.

If an error occurs, a detailed debug message will appear.



When a remote RADIUS server is configured for two-factor authentication, RADIUS users must enter a FortiToken pin code or the code from email/SMS to complete login. For example, after the user clicks *Login*, the user must enter the code, and click *Submit* to complete the login.

A pin code is also needed for the test login page.

---

## Admin Profiles

Administrator profiles are used to control administrator access privileges to system features. Profiles are assigned to administrator accounts when an administrator is created.

There are three predefined administrator profiles, which cannot be modified or deleted:

- Super Admin: All functionalities are accessible.
- Read Only: Can view certain pages but cannot change any system setting.
- Device: Can view certain pages about assigned devices, but cannot change any system setting.

All previous created users in earlier builds are mapped to these three default profiles.

Only the Super Admin user can create, edit, and delete administrator profiles and new users if the user is assigned the *Read Write Privilege* in *System > Admin* setting page.

Read Write Privilege	User can view and make changes to the system.
Read Only Privilege	User can only view information.
None	User cannot view or make changes to the system.

Administrator Profile

Profile Name:
⚠

Comment:
0/255

Menu Access
None
Read Only
Read Write

Dashboard	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
FortiView	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Network	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Virtual Machine	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Scan Policy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Scan Input	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
HA Cluster	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
File Detection	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Network Alerts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
URL Detections	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Logs & Reports	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Control Access
Disable
Enable

Mark FPN	<input type="radio"/>	<input type="radio"/>
Download Original File	<input type="radio"/>	<input type="radio"/>
JSON API / CLI	<input type="radio"/>	<input type="radio"/>
Allow On-Demand Scan Interaction	<input type="radio"/>	<input type="radio"/>
Allow On-Demand Scan Video Recording	<input type="radio"/>	<input type="radio"/>

Save

Back



In the *Control Access* section, if *Download Original File* is enabled, the user can download the original file from *Job Detail* page. If *Allow On-Demand Scan Interaction* is enabled, the user can use *VM interaction* during the On-Demand scan or take scan snapshots in the *VM Status* page.

If *Allow On-Demand Scan Video Recording* is enabled, the user can take a video during the On-Demand scan and watch it later in the On-Demand page.

## Wildcard Admin Authentication

You can use wildcard admin authentication to add the RADIUS and LDAP accounts of a group to FortiSandbox all at once instead of adding each account individually.

### To add accounts on a RADIUS server:

This example uses FortiAuthenticator as the RADIUS server.

1. On FortiAuthenticator, create the users.
2. If required, create user groups and assign users to the groups.
  - To specify which devices the users have access to, you can define the group's *Attribute ID* as *Fortinet-Group-Name*, and enter a device group name as listed in FortiSandbox as the *Value*. This allows users in this group to view jobs only from the devices inside of that device group.
  - If the *Attribute ID* is not defined, when users log into FortiSandbox, device visibility will follow the device group assigned to the RADIUS\_WILDCARD administrator, if any exists.

Create New User Group RADIUS Attribute

Vendor:	Fortinet
Attribute ID:	Fortinet-Group-Name
Type:	String
Value:	fsa_device_grp

OK Cancel

3. Create a new RADIUS service client.
  - a. Set the client address as the FortiSandbox IP address.
  - b. Enter the secret key in the *Secret* field.

- c. Configure profiles and add the user groups whose users will log into the FortiSandbox.

4. On FortiSandbox, set up the RADIUS server in *System > RADIUS Servers*. See [RADIUS Servers on page 67](#).
5. Create a new administrator in *System > Administrators*.
  - a. Select *RADIUS WILDCARD* as the type.
  - b. Select the *RADIUS Server* created in the previous step.
  - c. The administrator name is *RADIUS\_WILDCARD* and it cannot be changed. The administrator can be a device user, however, the assigned device group will be overridden if the RADIUS user group has defined the *Attribute ID* as *Fortinet-Group-Name*.

### To add accounts on an LDAP server:

1. On the FortiSandbox, set up the LDAP server in *System > LDAP Server*. See [LDAP Servers on page 65](#).  
In this example, all users from OU=HQ under the LDAP tree dc=example, dc=org will be able to login to FortiSandbox.

2. Create a new administrator in the *System > Administrators* page.
  - a. Select *LDAP WILDCARD* as the *Type*.
  - b. Select the LDAP server from the previous step.  
The administrator name is *LDAP\_WILDCARD* and it cannot be changed.
  - c. Click *OK*.

## Device Groups

To simplify the process of assigning devices to users, administrators can add devices to a device group and assign the group to multiple users. Once created, the device group is selectable when modifying an existing user or creating a new device user. When the user logs in, they can only view jobs from the devices included in that device group.



Device groups cannot be deleted while in use by any device user.

### To create a device group:

1. Go to *System > Device Groups* and click *Create New*.
2. Enter a group name.
3. Enter a comment to identify this device group if required.
4. Select the devices to be included in the device group.
5. Click *Save*.

The device group is now available to select when modifying or creating a new administrator with device user privileges enabled.



Device groups are also used in LDAP/RADIUS wildcard authentication.  
See [Wildcard Admin Authentication on page 61](#).

## Certificates

In this page you can import, view, and delete certificates. Certificates are used for secure connection to an LDAP server, system HTTPS and SSH services. The FortiSandbox has one default certificate *firmware* which means the certificate is installed on the unit by Fortinet.



FSA does not support generating certificates, but importing certificates for SSH and HTTPS access to FSA. `.crt`, `PKCS12`, and `.pem` formats are supported.

The following options are available:

<b>Import</b>	Import a certificate.
<b>Service</b>	Select to configure specific certificates for the HTTP and SSH servers.
<b>View</b>	Select a certificate in the list and select <i>View</i> in the toolbar to view the CA certificate details.
<b>Delete</b>	Select a certificate in the list and select <i>Delete</i> in the toolbar to delete the certificate.

The following information is displayed:

<b>Name</b>	The name of the certificate.
<b>Subject</b>	The subject of the certificate.
<b>Status</b>	The certificate status, active or expired.
<b>Service</b>	HTTPS or SSH service that is using this certificate.

#### To import a certificate:

1. Go to *System > Certificates*.
2. Click *Import* from the toolbar.
3. Enter the certificate name in the text field.
4. Click *Choose File* and locate the certificate and key files on your management computer.
5. Click *OK* to import the certificate.



Users have the option to import a Password Protected PKCS12 Certificate. To import a PKCS12 Certificate, check the *PKCS12 Format* box upon importing a new certificate and writing down possible password.

#### To view a certificate:

1. Go to *System > Certificates*.
2. Select the certificate from the list and click *View* from the toolbar.
3. The following information is available:

<b>Certificate Name</b>	The name of the certificate.
<b>Status</b>	The certificate status.
<b>Serial number</b>	The certificate serial number.
<b>Issuer</b>	The issuer of the certificate.
<b>Subject</b>	The subject of the certificate.
<b>Effective date</b>	The date and time that the certificate became effective.
<b>Expiration date</b>	The date and time that the certificate expires.

4. Click *OK* to return to the Certificates page.

#### To delete a CA certificate:

1. Go to *System > Certificates*.
2. Select the certificate from the list and click *Delete* from the toolbar.
3. Click *Yes, I'm sure* in the *Are You Sure* confirmation page.



*Firmware* certificate(s) cannot be deleted.



## LDAP Servers

The FortiSandbox system supports remote authentication of administrators using LDAP servers. To use this feature, you must configure the appropriate server entries in the FortiSandbox unit for each authentication server in your network.

If you have configured LDAP support and require a user to authenticate using an LDAP server, the FortiSandbox unit contacts the LDAP server for authentication. To authenticate with the FortiSandbox unit, the user enters a user name and password. The FortiSandbox unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the FortiSandbox unit successfully authenticates the user. If the LDAP server cannot authenticate the user, the FortiSandbox unit refuses the connection.

The following options are available:

<b>Create New</b>	Select to add an LDAP server.
<b>Edit</b>	Select an LDAP server in the list and click <i>Edit</i> in the toolbar to edit the entry.
<b>Delete</b>	Select an LDAP server in the list and click <i>Delete</i> in the toolbar to delete the entry.

The following information is displayed:

<b>Name</b>	The LDAP server name.
<b>Address</b>	The LDAP server address.
<b>Common Name</b>	The LDAP common name.
<b>Distinguished Name</b>	The LDAP distinguished name.
<b>Bind Type</b>	The LDAP bind type.
<b>Connection Type</b>	The LDAP connection type.
<b>Number of LDAP servers</b>	The number of LDAP server configured on the device.

**To create a new LDAP server:**

1. Go to *System > LDAP Servers*.
2. Select *+ Create New* from the toolbar.

**New LDAP Server**

Name:	<input type="text"/>
Server Name/IP:	<input type="text"/>
Port:	<input type="text" value="389"/>
Common Name:	<input type="text"/>
Distinguished Name:	<input type="text"/>
Bind Type:	<input checked="" type="radio"/> Simple <input type="radio"/> Anonymous <input type="radio"/> Regular
<input type="checkbox"/> Enable Secure Connection	
<div> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </div>	

3. Configure the following settings:

<b>Name</b>	Enter a name to identify the LDAP server. The name should be unique to FortiSandbox.
<b>Server Name/IP</b>	Enter the IP address or fully qualified domain name of the LDAP server.
<b>Port</b>	Enter the port for LDAP traffic. The default port is 389.
<b>Common Name</b>	The common name identifier for the LDAP server. Most LDAP servers use <code>cn</code> . However, some servers use other common name identifiers such as <code>uid</code> .
<b>Distinguished Name</b>	The distinguished name used to look up entries on the LDAP servers use. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier.
<b>Bind Type</b>	Select the type of binding for LDAP authentication. The following options are available: <ul style="list-style-type: none"> <li>• Simple</li> <li>• Anonymous</li> <li>• Regular</li> </ul>
<b>Username</b>	When the <i>Bind Type</i> is set to <i>Regular</i> , type the user name.
<b>Password</b>	When the <i>Bind Type</i> is set to <i>Regular</i> , type the password.
<b>Enable Secure Connection</b>	Select to use a secure LDAP server connection for authentication.
<b>Protocol</b>	When <i>Enable Secure Connection</i> is selected, select either LDAPS or STARTTLS.
<b>CA Certificate</b>	When <i>Enable Secure Connection</i> is selected, select the CA certificate from the dropdown list.

4. Select *OK* to add the LDAP server.

## RADIUS Servers

The FortiSandbox system supports remote authentication of administrators using RADIUS servers. To use this feature, you must configure the appropriate server entries in the FortiSandbox unit for each authentication server in your network.

If you have configured RADIUS support and require a user to authenticate using a RADIUS server, the FortiSandbox unit contacts the RADIUS server for authentication. To authenticate with the FortiSandbox unit, the user enters a user name and password. The FortiSandbox unit sends this user name and password to the RADIUS server. If the RADIUS server can authenticate the user, the FortiSandbox unit successfully authenticates the user. If the RADIUS server cannot authenticate the user, the FortiSandbox unit refuses the connection.

The following options are available:

<b>Create New</b>	Select to add a RADIUS server.
<b>Edit</b>	Select a RADIUS server in the list and click <i>Edit</i> in the toolbar to edit the entry.
<b>Delete</b>	Select a RADIUS server in the list and click <i>Delete</i> in the toolbar to delete the entry.

The following information is displayed:

<b>Name</b>	The RADIUS server name.
<b>Primary Address</b>	The primary server IP address.
<b>Secondary Address</b>	The secondary server IP address.
<b>Port</b>	The port used for RADIUS traffic. The default port is 1812.
<b>Auth Type</b>	The authentication type the RADIUS server requires. The default setting of ANY has the FortiSandbox try all the authentication types. Select one of: <i>ANY</i> , <i>PAP</i> , <i>CHAP</i> , or <i>MSv2</i> .

**To add a RADIUS server:**

1. Go to *System > RADIUS Servers*.
2. Select **+ Create New** from the toolbar.

New RADIUS Server	
Name:	<input type="text"/>
Primary Server Name/IP:	<input type="text"/>
Secondary Server Name/IP:	<input type="text"/>
Port:	<input type="text" value="1812"/>
Auth Type:	<input checked="" type="radio"/> Any <input type="radio"/> PAP <input type="radio"/> CHAP <input type="radio"/> MSv2
Primary Secret:	<input type="text"/>
Secondary Secret:	<input type="text"/>
NAS IP:	<input type="text"/>
<div> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </div>	

3. Configure the following settings:

<b>Name</b>	Enter a name to identify the RADIUS server. The name should be unique to FortiSandbox.
<b>Primary Server Name/IP</b>	Enter the IP address or fully qualified domain name of the primary RADIUS server.
<b>Secondary Server Name/IP</b>	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
<b>Port</b>	Enter the port for RADIUS traffic. The default port is 1812.
<b>Auth Type</b>	Enter the authentication type the RADIUS server requires. The default setting of ANY has the FortiSandbox try all the authentication types. Select one of: <i>ANY, PAP, CHAP, or MSv2</i> .
<b>Primary Secret</b>	Enter the primary RADIUS server secret.
<b>Secondary Secret</b>	Enter the secondary RADIUS server secret.
<b>NAS IP</b>	Enter the NAS IP address.

4. Select **OK** to add the RADIUS server.



FortiSandbox supports the shared RADIUS secret key up to a maximum of 16 characters in length, the same as FortiOS.

## Mail Server

The Mail Server page allows you to adjust the mail server settings. Go to *System > Mail Server* to view the *Mail Server Settings* page. In this page you can configure notifications for malware detected, as well as the weekly report global email list.

The following options can be configured:

<b>SMTP Server Address</b>	Enter the SMTP server address.
<b>Port</b>	Enter the SMTP server port number. If port 587 is used, the SMTP process will use STARTTLS to encrypt the credentials and the email.
<b>E-Mail Account</b>	Enter the mail server email account. This will be used as the <i>from</i> address.
<b>Login Account</b>	Enter the mail server login account.
<b>Password</b>	Enter the password.
<b>Confirm Password</b>	Confirm the password.
<b>Send a notification email to the global email list when Files/URLs with selected rating are detected</b>	Select to enable this feature. When enabled, a notification email is sent to the global email list, individual device, and VDOM/Domain email address when malware is detected.
<b>What rating of job to send alert email</b>	Select the rating of jobs that are included in the email alerts. Options include: <i>Malicious</i> , <i>High Risk</i> , <i>Medium Risk</i> , and <i>Low Risk</i> .
<b>Global notification mail receivers list (separated by comma)</b>	Enter the email addresses that comprise the global email list.
<b>Notification mail subject template</b>	Enter the subject line for the notification emails.
<b>Send a notification email to the Device/Domain/VDOM email list when Files/URLs with selected ratings are detected</b>	When a malware from an input device is detected, send a notification email to its admin email address.
<b>What rating of job to send alert email</b>	Select the rating of jobs that will trigger email notification. Options include: <i>Malicious</i> , <i>High Risk</i> , <i>Medium Risk</i> , and <i>Low Risk</i> .
<b>Notification mail subject template</b>	Enter the subject line for the notification emails.
<b>Send a notification email to the below email list when malicious/suspicious verdict is returned to client device.</b>	When enabled, a notification email is sent to an email list when a malicious/suspicious rating is retrieved by a client device.
<b>Use FQDN as unit address for job detail link (default is IP address of Port1)</b>	Use FQDN instead of port1 IP for a job detail link inside alert emails and reports.

<b>FQDN Name</b>	Enter FQDN name.
<b>Send scheduled PDF report to global email receiver</b>	Select to send a report email to the global email list.
<b>Global email list to receive summary/detail report (separated by comma)</b>	Enter the email addresses that comprise the global email list.
<b>Send scheduled PDF report to Device/Domain/VDOM email address</b>	Select to send PDF report to device/Protected Domain/VDOM email address also. The report will only contain jobs sent from the device/FortiMail Protected Domain/VDOM.
<b>Report Schedule Type:</b>	Select the report schedule type: <i>Hourly</i> , <i>Daily</i> , or <i>Weekly</i> . For different schedule types, different frequency options are displayed. If the schedule type is <i>Daily</i> , the user can set the hour for which the report is generated.
<b>Week Day:</b>	Select the day the report is to be sent.
<b>At hour:</b>	Select the hour interval the report is to be sent.
<b>Include job data before Days (0-28) days:</b>	Select the job data before 0-28 days.
<b>Hours (0-23):</b>	Select the job data before 0-23 hours. For example, if the user wants to include job data from the last two days and three hours before report generation, the user should select two in the Day Field and three in the Hour field.
<b>What rating of job to be included in the detail report</b>	Select the rating of jobs that are included in the reports. Options include: <i>Malicious</i> , <i>High Risk</i> , <i>Medium Risk</i> , <i>Low Risk</i> , and <i>Clean</i> . Because there is a large amount of jobs with a Clean rating, it is recommended to exclude the Clean rating from the detail report.
<b>OK</b>	Select <i>OK</i> to apply any changes made to the mail server configuration.
<b>Send Test Email</b>	Select <i>Send Test</i> to send a test email to the global email list. If an error occurs, the error message will appear at the top of the page and recorded in the System Logs.
<b>Restore Default</b>	Select <i>Restore Default</i> to restore the default mail server settings.

## SNMP

In version 3.0.6 and later, all admin ports that are specified support SNMP.

SNMP is a method for a FortiSandbox system to monitor FortiSandbox on your local computer. You need an SNMP agent on your computer to read SNMP information.

Using SNMP, your FortiSandbox system monitors for system events including CPU usage, memory usage, log disk space, malware detection, HA topology changes, and health check status changes. Go to *System > SNMP* to configure the FortiSandbox SNMP settings.

SNMP has two parts - the SNMP agent or the device that is sending traps, and the SNMP manager that monitors those traps. The SNMP communities on the monitored FortiSandbox are hard coded and configured in the SNMP menu.

The FortiSandbox SNMP implementation is read-only — SNMP v1, v2c, v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiSandbox system information and can receive FortiSandbox system traps.

From here you can download FortiSandbox and Fortinet core MIB files.



When one plug is cut off, the unit will send out SNMP trap and generate a log. Only 3000D, 3500D, 2000E, and 3000E models are supported.

## Configuring the SNMP agent

The SNMP agent sends SNMP traps that originate on the FortiSandbox system to an external monitoring SNMP manager defined in one of the FortiSandbox SNMP communities. Typically an SNMP manager is an application on a local computer that can read the SNMP traps and generate reports or graphs from them.

The SNMP manager can monitor the FortiSandbox system to determine if it is operating properly, or if any critical events are occurring. The description, location, and contact information for this FortiSandbox system is part of the information for the SNMP manager. This information is useful if the SNMP manager is monitoring many devices, and it will enable faster responses when the FortiSandbox system requires attention.

### To configure the SNMP agent:

1. Go to *System > SNMP*.
2. Configure the following settings:

<b>SNMP Agent</b>	Enable the FortiSandbox SNMP agent to send FortiSandbox SNMP traps. Disable to stop sending SNMP traps.
<b>Description</b>	Description of this FortiSandbox system to help uniquely identify this unit.
<b>Location</b>	Location of this FortiSandbox system to help find it if it requires attention.
<b>Contact</b>	Contact information for the person in charge of this FortiSandbox system.
<b>SNMP v1/v2c</b>	Create, edit, or delete SNMP v1 and v2c communities. You can enable or disable communities in the edit page. Columns include <i>Community Name</i> , <i>Queries</i> , <i>Traps</i> , and <i>Enable</i> .
<b>SNMP v3</b>	Create, edit, or delete SNMP v3 entries. You can enable or disable queries in the edit page. Columns include <i>User Name</i> , <i>Security Level</i> , <i>Notification Host</i> , and <i>Queries</i> .

**To create a new SNMP v1/v2c community:**

1. Go to *System > SNMP*.
2. In the *SNMP v1/v2c* section, click *Create New*.
3. Configure the following settings:

<b>Enable</b>	Select to enable the SNMP community.
<b>Community Name</b>	Enter a name to identify the SNMP community.
<b>Hosts</b>	The list of hosts that can use the settings in this SNMP community to monitor the FortiSandbox system.
<b>IP/Netmask</b>	Enter the IP address and netmask of the SNMP hosts. Click <i>Add</i> to add additional hosts.
<b>Queries v1</b>	Enter the port number and select to enable. Enable queries for each SNMP version that the FortiSandbox system uses.
<b>Queries v2c</b>	Enter the port number and select to enable. Enable queries for each SNMP version that the FortiSandbox system uses.
<b>Traps v1</b>	Enter the local port number, remote port number, and select to enable. Enable traps for each SNMP version that the FortiSandbox system uses.
<b>Traps v2c</b>	Enter the local port number, remote port number, and select to enable. Enable traps for each SNMP version that the FortiSandbox system uses.
<b>SNMP Events</b>	Enable the events that will cause the FortiSandbox unit to send SNMP traps to the community. <ul style="list-style-type: none"><li>• CPU usage is high</li><li>• Memory usage is high</li><li>• Log disk usage is high</li><li>• Malware is detected</li><li>• Topology map for cluster has changed</li><li>• Health check status for cluster has changed</li></ul>

4. Click *OK*.

**To create a new SNMP v3 user:**

1. Go to *System > SNMP*.
2. In the *SNMP v3* section, click *Create New*.



## 3. Configure the following settings:

<b>Username</b>	Enter the name of the SNMPv3 user.
<b>Security Level</b>	Select the security level of the user. Select one of the following: <ul style="list-style-type: none"> <li>• None</li> <li>• Authentication only</li> <li>• Encryption and authentication</li> </ul>
<b>Authentication</b>	Authentication is required when <i>Security Level</i> is either <i>Authentication only</i> or <i>Encryption and authentication</i> .
<b>Method</b>	Select the authentication method: <ul style="list-style-type: none"> <li>• MD5 (Message Digest 5 algorithm)</li> <li>• SHA1 (Secure Hash algorithm)</li> </ul>
<b>Password</b>	Enter the authentication password of at least eight characters.
<b>Encryption</b>	Encryption is required when <i>Security Level</i> is <i>Encryption and authentication</i> .
<b>Method</b>	Select the encryption method: DES or AES.
<b>Key</b>	Enter the encryption key of at least eight characters.
<b>Notification Hosts (Traps)</b>	
<b>IP/Netmask</b>	Enter the IP address and netmask. Click <i>Add</i> to add additional hosts.
<b>Query</b>	
<b>Port</b>	Enter the port number. Select to <i>Enable</i> the query port.
<b>SNMP V3 Events</b>	Select the SNMP events to be associated with that user. <ul style="list-style-type: none"> <li>• CPU usage is high</li> <li>• Memory usage is high</li> <li>• Log disk usage is high</li> <li>• Malware is detected</li> <li>• Topology map for cluster has changed</li> <li>• Health check status for cluster has changed</li> </ul>

## 4. Click OK.

## MIB files

To download MIB files, scroll to the bottom of the SNMP page, and select the MIB file that you would like to download to your management computer.

### FortiSandbox SNMP MIB

- [Download FortiSandbox MIB File](#)
- [Download Fortinet Core MIB File](#)

## FortiGuard

Go to *System > FortiGuard* to view the FortiGuard page.

The following options and information are available:

<b>Module Name</b>	The FortiGuard module name, including: <i>AntiVirus Scanner, AntiVirus Extreme Signature, AntiVirus Active Signature, AntiVirus Extended Signature, Network Alerts Signature, Sandbox System Tools, Sandbox Rating Engine, Sandbox Tracer Engine, Android Analytic Engine, Android Analytic Rating Engine</i> and <i>Traffic Sniffer</i> .  All modules automatically install update packages when they are available on the FDN.
<b>Current Version</b>	The current version of the module.
<b>Last Check Time</b>	The time that module last checked for an update.
<b>Last Update Time</b>	The time that module was last updated.
<b>Last Check Status</b>	The status of the last update attempt.
<b>Upload Package File</b>	Select <i>Browse</i> to locate a package file on the management computer, then select <i>Submit</i> to upload the package file to the FortiSandbox.  When the unit has no access to the Fortinet FDN servers, the user can go to the <a href="#">Customer Service and Support</a> site to download package files manually.
<b>FortiGuard Server Location</b>	Select FDN servers for package update and Web Filtering query. By default, the selection is <i>Nearest</i> , which means the closest FDN server according to the unit's time zone is used. When US Region is selected, only servers inside United States are used.
<b>FortiGuard Server Settings</b>	
<b>Use override FDN server to download module updates</b>	Select to enable an override FDN server, or FortiManager, to download module update, then enter the server IP address or FQDN in the text box. When an overridden FDN server is used, FortiGuard Server Location will be disabled. Click <i>Connect FDN Now</i> button to schedule an immediate update check.
<b>Use Proxy</b>	Select to enable a Proxy. Configure the Proxy Type (HTTP Connect, SOCKS v4, or SOCKS v5), Server Name, Port, Proxy Username, and Password.
<b>Connect FDN Now</b>	Click the <i>Connect FDN Now</i> button to connect the override FDN server/Proxy.
<b>FortiGuard Web Filter Settings</b>	
<b>Use override server address for web filtering query</b>	Select to enable an override server address for web filtering query, then enter the server IP address (IP address or IP address:port) or FQDN in the text box.  By default, the closest web filtering server according to the unit's time zone is used.  If port is not provided, target UDP port 53 will be used.

<b>Use Proxy</b>	Select to enable a Proxy. Configure the SOCKS v5 server name or IP, Port, Proxy Username, and Password.
<b>VM Image Download Proxy Setting</b>	
<b>Use Proxy</b>	Select to enable a Proxy. Configure the Proxy Type (HTTP Connect, SOCKS v4, or SOCKS v5), Server Name/IP, Port, Proxy Username, and Password.
<b>FortiSandbox Community Cloud and Threat Intelligence Settings</b>	
<b>Use override server for community cloud server query</b>	<p>Select this option when a FortiManager is used for FortiGuard upgrades in your environment.</p> <p>When using a FortiManager for FortiGuard upgrades, only verdict information is available for malware. Malware's behavior information is not available.</p>
<b>Use Proxy</b>	Select to enable a Proxy. Configure the SOCKS v5 server name or IP, Port, Proxy Username, and Password.

Click *Apply* to apply your changes.

## Login Disclaimer

Go to *System > Login Disclaimer* to customize the warning message, and to enable or disable the Login Disclaimer.

If enabled, the Login Disclaimer will appear when a user tries to log into the unit.

## Settings

Go to *System > Settings* to configure the administrator account idle timeout, which is the amount of time after which the user's login session will expire if there is no activity. You can also temporarily change the GUI language to Japanese or French. After logging out and then back in, the language will be reset to English.



In this page you can select to reset all widgets in *Dashboard*, *File Detection > Summary Report*, *Network Alerts > Summary Report*, *URL Detection > Summary Report*.

### To configure the idle timeout:

1. Go to *System > Settings*.
2. Enter a value between 1 and 480 minutes.
3. Click *OK* to save the setting.

**To reset all widgets:**

You can reset all the widgets in the Dashboard by clicking the *Reset* button.

**To change left-side menu mode:**

You can toggle left-side menu between compact and expanded mode. In compact mode, the menu shrinks to a compact menu bar. Click on an icon to expand all its sub menus. The top-level menu icon of the current page is highlighted.

**To configure report saving days:**

When you export data to a report, you can wait until the report is ready to view, or navigate away and find the report later in *Log & Report > Report Center* page. You can decide how many days reports will be kept by setting *Report Saving Days*.

## Job View Settings

Go to *System > Job View Settings* to define columns and their order, applied in every job result page. You can set the number of jobs shown in each page when the view type supports pagination.

You can also determine how to load the next set of jobs. It can be one of three options:

- Pagination
- Infinite Scroll
- Both (infinite scroll but also showing paging information)

Job Result pages show job data. They include but not limited to:

- *FortiView > File Scan Search page*
- *File Detection > URL Scan Search Files page*
- *File Detection > File Scan page*
- *File Detection > URL Scan page*
- Job links in *Dashboard > Scanning Statistics* widget

Selected columns, and their order, are displayed in the top row. Available columns are displayed in the bottom row. Drag and drop columns to adjust their order.

Job result pages also have the *Customize* icon. Clicking it will open the *Job View Setting* page, where the user can adjust the settings dynamically.

The *File Detection Columns* section defines the columns and the order to display file scan results. The *URL Detection Columns* section defines the columns and the order to display URL scan results.

You can adjust column width or drag column headers to adjust their order and the change will be saved for future visits. You can also use the *Column Setting* button in the job result page to change settings on the fly and go back to the original page.



Column settings are user based, which means different users have their own settings.

---

Job View Settings

File Detection Columns

Customized Column Headers and Orders

ActionDetectionFilenameRatingMalwareSourceDestination

Available Column Headers

Job IDSHA1ServiceSuspicious TypeSubmitted FilenameSubmit UserDeviceScan UnitInfected OSSHAT56Rated ByMD5

URL Detection Columns

Customized Column Headers and Orders

ActionDetectionURLRatingSubmitted FilenameSubmit UserInfected OS

Available Column Headers

Job IDSHA1SourceSuspicious TypeDestinationDeviceScan UnitSHAT56Rated ByMD5

Table Settings

Page Size

50

View Type

PaginationInfinite ScrollBoth

Save

Reset

The following columns are available to choose from for the View Job pages:

<b>Action</b>	Extra information, such as showing if a file is an archive file, or if the file is detected through AV Rescan. Users can also view job details or perform a rescan of a Suspicious or Malicious file.
<b>Destination</b>	The IP address of the client that downloaded the file.
<b>Detection</b>	The date and time that the file was detected by FortiSandbox.
<b>Device</b>	The job's input source.
<b>Filename</b>	The file's name.
<b>Infected OS</b>	The OS version of the FortiSandbox VM that was used to make the Suspicious verdict.
<b>Job ID</b>	The ID of the scan job.
<b>Malware</b>	The name of the virus of a Malicious file.
<b>MD5/SHA1/SHA256</b>	The checksum values of the scanned file or URL.
<b>Rated By</b>	The method by which the job is rated, such as the VM Engine.
<b>Rating</b>	The rating of the scan job. It can be one of Malicious, High Risk, Medium Risk, Low Risk, Clean and Unknown.
<b>Scan Unit</b>	The serial number of the FortiSandbox unit which the file is scanned on.

<b>Service</b>	The traffic protocol that file is transferred, such as FTP, HTTP, IMAP, POP3, SMB, OTHER and SMTP.
<b>Source</b>	The IP address of the host where the file was downloaded.
<b>Submitted Filename</b>	The scan job's filename, or a file's parent archive filename, or the submitted filename associated with an On-Demand scan.
<b>Submit User</b>	The user name or IP address who submits the scan file or URL.
<b>Suspicious Type</b>	The malware's type, such as Attacker, Riskware or Trojan.
<b>URL</b>	The scanned URL. Only available in URL scan job pages.

## Event Calendar Settings

These settings, found in *System > Event Calendar Settings*, allow you to specify which types of events are displayed on the *Event Calendar* in *FortiView*. By default, all available event types are displayed.

Event types include: *Send Mail, Backup, Restore, Network Share, Network, DNS, Routing, Admin, Mail Server, Time Change, Hostname Change, LDAP, Certificate, VM, RADIUS, Login, Logout, System, Reboot, Job Alert, Shutdown, Backup, Restore, Firmware Upgrade, Operation Center, Scan Profile, Scan Policy, White/Black List, and Job Details*.

Moving an event into the *Unapplied Event Types* category will hide all instances of those events within the *Event Calendar*. Moving an event into the *Applied Event Types* category will restore these events to the calendar, including past events.

Events can be moved between the two categories by dragging and dropping them.

# Virtual Machine

The FortiSandbox VM host is based on a modified hypervisor. The following table shows installed Windows OS license and installed Windows guest image OS types on each model.

## Model, License and VM Information

	FSA-1000D	FSA-3500D	FSA-2000E	FSA-3000E
<b>Windows License</b>	Windows 7 Microsoft Office	Window 7 Windows 8.1 Windows 10 Microsoft Office	Windows 7 Windows 8.1 Windows 10 Microsoft Office	Windows 7 Windows 8.1 Windows 10 Microsoft Office
<b>Default Windows VMs</b>	WIN7X86VM (with Office) WIN7X64VM	WIN7X86VM (with Office) WIN7X64VM	WIN7X86SP1O16 (with Office)	WIN7X86VM (with Office) WIN7X64VM



For FortiSandbox devices purchased after March 17, 2017, WINXP VM type and its licenses are no longer supported due to Microsoft EOL.

## VM Host Support

<b>FSA-1000D</b>	Supports 8 VM hosts.
<b>FSA-3000D</b>	Supports 28 VM hosts.
<b>FSA-3500D</b>	Supports 8 VM hosts on each blade.
<b>FSA-2000E</b>	Supports 4 VM hosts by default, maximum up to 24 VM hosts.
<b>FSA-3000E</b>	Supports 8 VM hosts by default, maximum up to 56 VM hosts.
<b>FSAVM00</b>	No VM host by default, maximum up to 8 VM hosts. To expand the unit's scan power, you can purchase cloud Windows VM subscription. Files can be sent to Fortinet Cloud Sandboxing to scan.



The number of supported VM hosts mentioned above of each model is for images published by Fortinet. When using customized images, the number may be less because of possible higher resource requirements of those images.

Users can also download, install and use optional images from the Optional VMs section in the *VM Image page*. Extra Windows OS licenses might be needed if the unit has none available. For example, when user tries to use Windows 10 image on a FSA-1000D unit, the user needs to purchase Windows 10 license keys from Fortinet.

Android VM is free to download, install and use. Users can also build and install their own customized images. For customized images, the user must apply their own software license. The following software is installed on each pre-installed Windows guest image:

- Adobe Flash Player
- Adobe Reader
- Java Run Time
- MSVC Run Time
- Microsoft .Net Framework
- Microsoft Office software (only on certain VM types)
- Web Browsers



For Optional VMs, the name shows the Windows OS type. If the name has *O16* in it, it means it has Microsoft Office 2016 installed.

For Android license, it's free

---

This section includes the following topics:

- [VM Status](#)
- [VM Images](#)

## VM Status

Go to *Virtual Machine > VM Status* to view files currently scanned inside the VM. The page displays the file name, and progress. Users can also click the VM Screenshot button, then the PNG Link button to view a screenshot of running scan. If the scan allows VM interaction, users can click the VM Interact icon to interact with the scan.



Making snapshots of scans or interaction with VM is only available when login user's admin profile defines *Read Write* privilege for All On-Demand Scan Interaction.

---

## VM Images

Go to *Virtual Machine > VM Images* to view all installed VM Images and configure the number of instances of each image.

VM Images are grouped to three categories:

Default VMs	
	Basic set of images installed on FortiSandbox by default. For FSA-AWS model, it's the installed Windows VMs on AWS.



<b>Optional VMs</b>	Fortinet published optional VM images.
<b>Customized VMs</b>	User created images and uploaded to FortiSandbox.
<b>Remote VMs</b>	<p>MACOSX and Windows Cloud VM are supported as remote VMs. You can purchase subscription services from Fortinet to reserve clone numbers in the Fortinet Sandboxing Cloud.</p> <p>From 3.0, no TRIAL license is provided for MACOSX VM.</p> <p>In Cluster mode for MACOSX remote VMs, all cluster node share collected pool of reserved clones from each unit. This means even a node that has no remote VM contract purchased, it can still upload files to the cloud for scanning. For the cluster as whole, at any moment, the number of files being scanned in Cloud will no exceed total reserved clone numbers.</p> <p>In Cluster mode for Windows Cloud VM, VM00 units in the cluster can purchase Windows cloud VM seat counts. These cloud VM clones are local to that VM00 unit and are not shared.</p>



A new Ubuntu18 optional VM has been introduced in FortiSandbox 3.1.0.

When Fortinet publishes a new version of VM image on its image server, the image will show up in the *Optional VMs* group. A download button will show up in *Status* column. Users can click the button to start downloading. After the image has downloaded, a *Ready to Install* button will be displayed. When the user clicks on it, all downloaded images will start installing. After installation, the system will reboot automatically. Users can also click the *Remove* button to delete a downloaded image.

After an image is installed, its license key will be checked. If no key is available, the image's status will be installed but disabled, until the key is installed and the image is activated. After the image is activated, users can start using it by setting its clone number to be greater than 0. Thereafter, the Image's status will become activated.

FortiSandbox 3000D

VM Images

admin

Dashboard

FortiView

Network

System

Virtual Machine

Scan Policy

Scan Input

File Detection

Network Alerts

URL Detection

Log & Report

VM Images

Edit Clone Number

Delete VM

Undelete VM

VM Screenshot

Enabled VM Types: 4 / 4

Keys: 25 / 25

Clone Number: 28 / 28

Name	Version	Status	Enabled	Clone #	Load #	Extensions
Default VMs (2/2)						
WIN7X64VM	7	activated		15	15	jse exe msi wsf upx vbs bat cmd dll ps1 jar pdf swf
WIN7X86VM	6	activated		10	10	pdf ppsx ppt pptx xls xlsx doc docx rtf dotx docm dotm xltb xlsx xltm xlsb xlam potx sltx pptm ppsm potm ppam slidm msg dot xlt pps pot pub
Optional VMs (9/9)						
AndroidVM	2	activated		2	2	apk
WIN10X64VM	2	installed		0	0	exe msi vbs bat cmd ps1 jar WEBLink
WIN10X64VMO16	2	installed		0	0	
WIN10X86VM	2	installed		0	0	exe msi bat cmd vbs ps1 jar
WIN7X64SP1	1	installed		0	0	
WIN7X86SP1O16	1	installed		0	0	
WIN81X64VMO16	1	installed		0	0	
WINXPVM	7	activated		0	0	ppsx ppt pptx xls xlsx doc docx rtf dotx docm dotm xltb xlsx xltm xlsb xlam potx sltx pptm ppsm potm ppam slidm msg dot xlt pps pot zip
WINXPVM1	6	activated		0	0	exe
Customized VMs (2)						
win7x64newtool	1	installed		0	0	pdf WEBLink
win7x64v5	1	activated		1	1	
Remote VMs (1)						
MACOSX	0	activated		0	0	mac dmg

Apply

The following options are available:

#### Edit Clone Number

Select a VM Image and select *Edit Clone Number* from the toolbar to edit the entry. Click the green checkmark to save the new number. Then, click the *Apply* button to apply the changes.

#### Delete VM

Select a VM Image and select *Delete VM* from the toolbar to delete the entry. The default set of four Windows VMs cannot be deleted. Deleted VMs will only be deleted after the system reboots.

#### Undelete VM

After deleting a VM you have the option to *Undelete the VM* to recover it. After the system reboots and the delete action has been completed, the user cannot undelete a VM.

#### VM Screenshot

Select to take a screenshot of a running VM, and the file name the VM is scanning. The button is only available for *admin* user.

The following information is displayed:

#### Enabled VM Types

Max number of VM types that can concurrently run. It cannot exceed four on models other than FSA-3000E. On FSA-3000E, the number is six.

#### Keys

Max number of keys. This includes used key numbers and installed key numbers.

#### Clone Number

Max Clone number. It is the number of the installed Windows license. For example:

- FSA-3000D, the maximum clone number is 28.
- FSA-1000D, the maximum clone number is 8.
- FSA-3500D, the maximum clone number is 8.
- FSA-3000E, the maximum clone number is 56.

	<ul style="list-style-type: none"> <li>• FSA-2000E, the maximum clone number is 24.</li> <li>• FSAVM00, the maximum clone number is 8. To expand the unit's scan power, you can purchase cloud Windows VM subscription. Files can be sent to Fortinet Cloud Sandboxing to scan.</li> </ul>
<b>Name</b>	<p>Name of the VM Image. The name is unique in the system. If the user uploads a new VM image of the same name, the current installation will be replaced.</p> <p>A <i>Chart</i> icon is located beside the <i>Name</i> column on the left side. When you click on the <i>Chart</i> icon, the VM's usage chart will appear.</p>
<b>Version</b>	<p>VM Image version. If a new version of an image is published on the Fortinet Image Server, a <i>New Version Available</i> icon will appear. Users can download, install and activate it.</p>
<b>Status</b>	<p>VM Image status. A VM image can be one of the following statuses:</p> <ul style="list-style-type: none"> <li>• Ready to Download</li> <li>• Ready to Upgrade</li> <li>• Downloading (shows a progress bar)</li> <li>• Ready to Install (Install or Remove downloaded image)</li> <li>• Installing</li> <li>• Installed (Disabled)</li> <li>• Installed (No Key Available)</li> <li>• Activated</li> </ul>
<b>Enabled</b>	<p>If an image's clone number is 0, it is disabled. Otherwise it is enabled.</p>
<b>Clone#</b>	<p>VM Clone number. The user can double click the number to edit it, then click the green check mark to save the new number. Click Apply to apply the change. The VM system will initialize again. The total clone number of all VM images cannot exceed the number of installed Windows license(s). For example, for FSA-3000D, the maximum clone number is 28.</p>
<b>Load#</b>	<p>The used VM clone number. For example, if a cluster primary (master) node is set to use 50% of sandboxing scan power, the load # is half of clone #.</p>
<b>Extensions</b>	<p>List of all the file types the VM image is associated with. It means files of these types will be scanned by this VM if these types are determined to enter the job queue. The system decides if they need to be sandboxed.</p> <p>If the sandbox prefiltering is turned off for a file type, it will be scanned inside each associated VM type.</p> <p>If sandbox prefiltering is turned on, files of this file type will be statically scanned first by an advanced analytic engine and only suspicious ones will be scanned inside associated VM type.</p> <p>File type and VM association can be defined in the <i>Scan Policy &gt; Scan Profile</i> page. Users can double click the value to access the <i>Scan Profile</i> page to edit the list.</p>



Enabled clone numbers will be checked against allocated CPU and memory resources. If they are not enough, a warning message will appear and the setting will be denied.

## Clone Number for VM Image

By default, the clone number for the VM image(s) is set to the following:

### FSA-2000E

VM Image	Number of Clones
WIN7X86SP1O16	4

### FSA-1000D, FSA-3500D and FSA-3000E

VM Image	Number of Clones
WIN7X64VM	4
WIN7X86VM	4

### FSA-3000D

VM Image	Number of Clones
WIN7X64VM	14
WIN7X86VM	14



For FortiSandbox devices purchased after March 17, 2017, WINXP VM types and its licenses are no longer supported due to Microsoft EOL.

The user can change the default settings according to the majority of file types in their environment. For example, if the majority file type is Office files and WIN7X86VM is associated with Office files, the user can decrease the clone number of other VM images and increase the clone number of the WIN7X86VM image.

In a cluster environment, clone numbers should be configured individually on each node as their models might be different.

## VM Screenshot

When the user *admin* clicks the *VM Screenshot* button, all currently running guest images along with the processed file name will be displayed. Click the *VM Screenshot* button, then the *PNG Link* button to view a screenshot of running clones. Clicking on the *Refresh* button in upper-left corner of the popup window will refresh the running image list.

This feature is useful to troubleshoot issues related to guest images.



This button is only available when login user is *admin*.

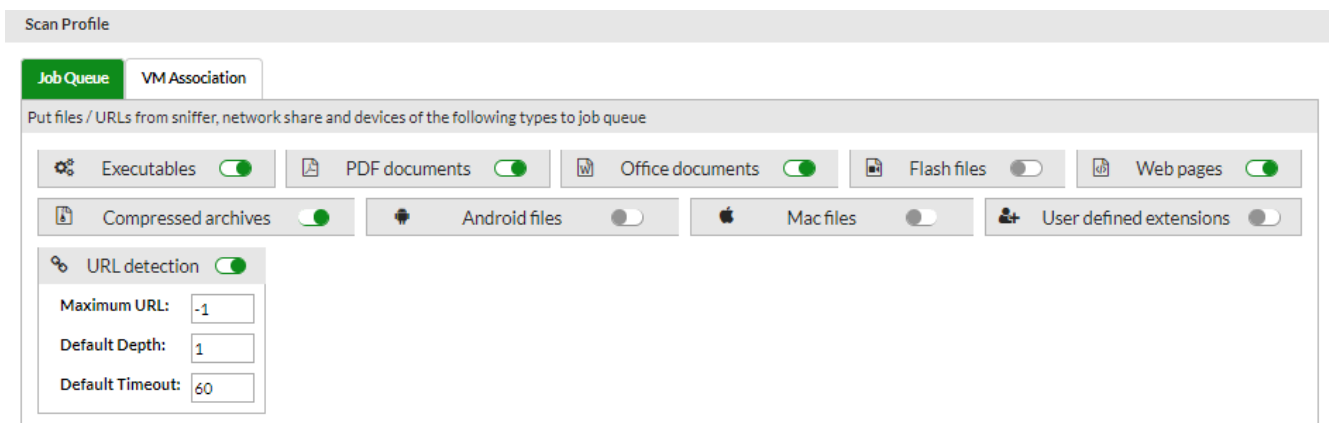
# Scan Policy

This section includes the following topics:

- [Scan Profile](#)
- [Job Queue Priority](#)
- [General](#)
- [Allowlist and blocklist \(white/black lists\)](#)
- [Overridden Verdicts](#)
- [YARA Rules](#)
- [URL Category](#)
- [Customized Rating](#)
- [Job Archive](#)
- [Local Packages](#)

## Scan Profile

The profile page allows you to configure the types of files that are put into the job queue. It also allows you to configure the VM image to scan pre-defined file types and user defined file types.



## File types

FortiSandbox, by default, supports the following file types:

### Executables

BAT, CMD, DLL, EML, EXE, JAR, JSE, MSI, PS1, UPX, WSF, and VBS.

Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command:

```
sandboxing-prefilter -e -tdll
```

	Only the DLL files which can be executed inside a VM will be put into the Job Queue.
<b>Archives</b>	7Z, ARB, BZIP, BZIP2, CAB, ISO, EML, GZIP, LZW, RAR, TAR, XZ and more. Archive files will be extracted up to six levels and each file inside will be scanned according to Scan Profile settings. The max file number extracted: <ul style="list-style-type: none"> <li>On-Demand input: 10,000</li> <li>JSON API: 1,000</li> <li>All other input sources: 100</li> </ul>
<b>Microsoft Office</b>	Word, Excel, PowerPoint, Outlook and more.
<b>Adobe</b>	PDF, SWF, and Flash.
<b>Static Web Files</b>	HTML, JS, URL, and LNK.
<b>Android File</b>	APK.
<b>MACOSX Files</b>	MACH_O, FATMACH, DMG, XAR, and APP.
<b>WEBLink</b>	URLs submitted by FortiMail devices or sniffed from email body by sniffer.



You can create a custom file type and associate it to an existing VM. Therefore, file type analysis is not limited to just the file types listed in the table above.

Sometimes input sources send `.eml` files to FortiSandbox. For example, FortiMail sends `.eml` files to FSA when the `.eml` file is attached inside an email. FSA will parse the `.eml` file to extract its attachments and perform file scans.

When `sandboxing-embeddedurl` is enabled, the top three URLs inside the email body will be extracted and scanned along with the `.eml` inside the same VM.

This feature is useful when user wants to scan older emails when they are loaded to FSA, such as through an On-Demand scan or Network Share scan.



By default, FortiMail will hold a mail for a set period to wait for the verdict from FortiSandbox. Before FortiSandbox scans a file or URL sent from FortiMail, it will check if the verdict is still needed by FortiMail, as FortiMail might already release the email after time out. If not, FortiSandbox will give the job an *Unknown* rating and skipped status.

Users can use CLI command `fortimail-expired` to enable or disable this expiration check.



To use remote VMs including MACOSX and Windows Cloud VM, you need to purchase subscription service from Fortinet. Files will be uploaded to Fortinet Sandboxing cloud to scan according to *Scan Profile* settings.

## Scan Profile Job Queue Tab

The *Job Queue* tab is to define file types and URLs that are allowed to enter the job queue if they are from a sniffer, device, adapter and/or network share.



If files or URLs are submitted through On-Demand or RPC JSON API, they will always be put into the job queue, even if their file types are not set to enter the job queue.

---

### To allow a file type to enter the job queue:

Click its toggle button on the right side to enable it. If the button is greyed out, files of that type will be dropped.

### URL Detection

When URL detection is enabled, it means FortiSandbox will scan URLs (WEBLinks). The user can also define Default Depth setting (from 0 to 5) FortiSandbox should visit the URL and the Default Timeout value that FortiSandbox should stop even when not all depths have been scanned.

---



If the FortiSandbox unit has a long queue of pending jobs, users should consider turning off certain file types to job queue. For example, in most network environments, static web files (JavaScript, html, aspx files, etc...) and Adobe Flash files comprise a large portion of all files. When performance issue are met, users can consider turning them off.

If a file type is turned off, files of this type already in the job queue will still be processed. Users can use the `pending-jobs` CLI command or *Scan Input > Job Queue* page to purge them if required.

---



To determine the number of each file type and its input source, users can use CLI command `pending-jobs` or *Scan Input > Job Queue* page.

---

## Scan Profile VM Association Tab

The *VM Association* tab defines file type and VM type association. Association means files of a certain file type will be sandboxed by the associated VM type. This page displays all installed VM image(s), their clone numbers, versions, and status.

---



If a VM type is disabled (clone # is 0), its Clone # field will be red.

---

### To configure association:

Click the VM image's name. The left side panel shows installed applications and right side panel shows current associated file types.



For an associated file to be sandboxed in the VM image:

- Its file type has to be configured to enter a job queue.
- The VM image has a non-zero clone number (i.e. it is enabled).
- The file is not filtered out from Sandboxing scan. For more information, see the `sandboxing-prefilter` command in the CLI Reference guide.

---

If sandboxing pre-filtering is *OFF* for a file type, it will be scanned by each associated VM type; if sandboxing pre-filtering is *ON*, files of this file type will be statically scanned first by an advanced analytic engine and only suspicious ones will be scanned by associated VM type. Other files go through all scan steps except the Sandboxing scan step.

To improve the system scan performance, you can turn on the sandbox pre-filtering of a file type through the `sandboxing-prefilter` CLI command. For example, you can associate web files to VM types. If the `sandboxing pre-filtering` is *OFF* for `js/html` files, all of them will be scanned inside associated VM types. This may use up system's sandboxing scan capacity because web files are usually large in amount. It is recommended to enable `sandboxing pre-filtering` for web files. For more details, refer to the *FortiSandbox 3.0.7 CLI Reference Guide*.

#### To edit associated file type:

1. Click *Scanned File Types* area and a file type list will be displayed.
2. File types are grouped in different categories. Clicking the category title will toggle associations of all grouped file types. Clicking on an individual file type will toggle its own association. When the file type is displayed in full length, it means the file type is associated.

#### Add a user defined extension:

Make sure the user defined extension is enabled.

1. Click the + sign and enter a non-existing extension.
2. Click the green check mark. The user can then click on the new extension to toggle its association.

#### Finalizing the list of Scanned File Types:

1. After the user has finished the association configuration, click the *Scanned File Types* to finalize the list.
2. Click the *Apply* button to apply the changes.  
Files will then be scanned by the associated VM images.



For files with a user defined extension, they will be scanned by a VM image no matter what file types they really are. Only a file's extension counts.

---

FortiSandbox provides default scan profile settings.





In a cluster environment, it is highly recommended that all cluster nodes have the same enabled VM, although it is not enforced.

If cluster nodes do not have the same list of enabled VM types, a warning message will show up on top of the Scan Profile page for five seconds.

The Scan Profile can only be configured on the primary (master) node and the configurations will be synced to worker (slave) nodes. The primary (master) node will collect all installed VM image information. If a unique VM image is only installed on a worker (slave) node, the user can still configure on the primary (master) node and the result will be synchronized to that worker (slave) node.



`lnk` file type in *Web pages* group is for shortcut of a web link. While *WEBLink* type in *URL detection* group is for URL scans, which follows depth and timeout settings in *Job Queue* tab.



There might be malicious URLs inside Office files and PDF files. Users can choose to scan randomly selected URLs along with the original file inside files' associated VM. To turn this feature *ON*, use the `sandboxing-embeddedurl` CLI command. For more details, refer to the *FortiSandbox 3.0.7 CLI Reference Guide*.

A unit can join global threat network as *Contributor* to allow the *Collector* to control its *Scan Profile*, or it can work as *Collector* to manage *Scan Profile* of all units in the network. Only Standalone unit or primary (master) node in a cluster can join the network.

After you configure the Scan Profile on the *Collector*, the settings will be downloaded by all *Contributors*. On Contributor units, the *Scan Profile* page becomes read-only.

## File Scan Priority

Files of different file types and input sources have different processing priority. Priority means, under the same situation, files in the high priority queue will have a higher chance of being processed first. This means if a VM image is configured to scan two different job queues, the job queue with high priority will be scanned first and only when this queue is empty will the low priority job queue be processed. Therefore, it is recommended that different job queues are associated with different VM image(s). In this release, job queue priority can be adjusted in the *Scan Policy > Job Queue Priority* page. By default, the job queue priority is:

```
Files from On-Demand/RPC
sniffer/device submitted executable files
user defined file types
sniffer/device submitted Office files
sniffer/device submitted PDF files
sniffer/device submitted Android files sniffer/device submitted MacOS files
URLs of all sources
device submitted Adobe flash/web files
sniffer submitted Adobe flash/web files
Adapter submitted files
Network share submitted files
```

## File Scan Flow

After a file is received from an input source, it goes through the following steps before a verdict is reached. If a verdict can be reached at any step, the scan will stop.

### 1. Filtering and Static Scan

In this step, the file is scanned by the antivirus engine and the YARA rules engine. Its file type is checked against the *Scan Profile page > Job Queue* tab settings to decide if it should be put in the job queue. If yes, it is checked against the blocklist/allowlist (black/white list) and overridden verdict list.

For some file types, such as Office and PDF files, they are scanned statistically in virtual engines to detect suspicious contents. If they contain embedded URLs, the URLs are checked to see if the website is malicious.

### 2. Community Cloud Query

The file will be queried against the Community Cloud Server to check if an existing verdict is available. If yes, the verdict and behavior information will be downloaded. This makes the malware information shareable amongst the FortiSandbox Community for fast detection.

### 3. Sandboxing Scan

If the file type is associated with a VM type, as defined in the *Scan Profile page > VM Association*, the file will be scanned inside a clone of that VM type. A file that is supposed to be scanned inside a VM might skip this step if it's filtered out by sandboxing prefiltering. For more information, see the *FortiSandbox CLI Guide* for the `sandboxing-prefiltering` command.

## URL Scan Flow

After a URL is received from an input source, it goes through the following steps before a verdict is reached. If a verdict can be reached at any step, the scan will stop.

### 1. Static Scan

In this step, the URL is checked against the user uploaded allowlist/blocklist *White/Black* list and the *Overridden Verdicts* list.

### 2. Sandboxing Scan

If WEBLink is associated with a VM type as defined in the *Scan Profile page > VM Association* tab, the URL will be scanned inside a clone of that VM type. If the *URL* type is enabled with the `sandboxing pre-filtering` command, only URLs whose webfiltering category is *UNRATED* will be scanned inside a VM. For more information, please refer to the *FortiSandbox CLI Guide*, for the `sandboxing-prefiltering` command.























During the Static Scan step, URLs will be checked against the user uploaded allow (white) list and block (black) list in this order, and rated as *Clean* or *Malicious* respectively: *URL REGEX black list > URL black list > Domain black list > URL REGEX white list > URL white List > Domain white list*. For example, if users enter `*.microsoft.com` in the domain allowlist and `http://www.microsoft.com/. *abc/bad.html` in the URL blocklist, URL `http://www.microsoft.com/labc/bad.html` will be rated as *Malicious*.

## Job Queue Priority

This page displays the job queue priority list. The priority list can be dynamically adjusted by dragging and dropping the file type entry in order of priority. The closer an entry is to the top, the higher the priority.

Once you have ordered your list, click *Apply* to save the change or *Reset* to go back to its default settings.

Job Queue Priority		
#	Input Source	File Type
1	 On-Demand	 Executables/DLL/VBS/BAT/PS1/JAR/MSI/WSF files
2	 On-Demand	 User defined extensions
3	 On-Demand	 PDF files
4	 On-Demand	 Microsoft Office files (Word, Excel, PowerPoint files etc)
5	 On-Demand	 Adobe Flash files
6	 On-Demand	 Static Web files
7	 On-Demand	 Android files
8	 On-Demand	 Mac files
9	 URL On-Demand	 URL detection
10	 File RPC	 Executables/DLL/VBS/BAT/PS1/JAR/MSI/WSF files


## General

Go to *Scan Policy > General* to view and configure the General Options.

General Options

Upload Settings

☒ Upload malicious and suspicious file information to Sandbox Community Cloud  
☐ Submit suspicious URL to Fortinet WebFilter Service  
☒ Upload statistics data to FortiGuard service  
☒ Allow Virtual Machines to access external network through outgoing port3

Status: 

Port3 IP:

Gateway:

☐ Disable SIMNET if Virtual Machines are not able to access external network through outgoing port3  
 DNS:

☐ Use Proxy

☒ Apply default passwords to extract archive files  
 Password list:

☐ Disable Community Cloud Query  
☐ Disable AV Rescan of finished jobs  
☒ Enable URL callback detection  
☒ Enable log event of file submission

☒ Devices  
☐ Adapter  
☐ Network Share  
☐ BCC Adapter  
☒ ICAP

☐ Reject duplicate file from device  
☐ Delete original files of Clean or Other rating after  
☐ Delete original files of Malicious or Suspicious rating after  
☒ Delete all traces of jobs of Clean or Other rating after

Day (0-27):   
 Hour:   
 Minute:

☒ Delete all traces of jobs of Malicious or Suspicious rating after  
 Day:   
 Hour:   
 Minute:

OK

Cancel

The following options are available:

<b>Upload malicious and suspicious file information to Sandbox community Cloud</b>	Enable to upload malicious and suspicious file information to the Sandbox community Cloud. If enabled, the file checksum, tracer log, verdict, submitting device serial number, downloading URL, and original files are uploaded.
<b>Submit suspicious URL to Fortinet WebFilter Service</b>	Enable to submit malware downloading URL to the FortiGuard Web Filter Service.
<b>Allow Virtual Machines to access external network through outgoing port3</b>	<p>Enable to allow Virtual Machines to access external network through the outgoing port3.</p> <p>If the VM cannot access the outside network, a simulated network (SIMNET) will start by default. SIMNET provides responses of popular network services, like <code>http</code> where certain malware is expected. If the VM internet access is down, beside the down icon, SIMNET status is displayed. Clicking it will enter the VM network configuration page. <b>Note:</b> SIMNET is not a real internet. This can affect catch rate. Do not to have an IP from the production IP pool for the IP assignment on port3 because there is a chance it will get added to the blocklist. FortiSandbox VM accesses external network through port3. The next-hop gateway and DNS settings can be configured in <i>Scan Policy &gt; General &gt; Allow Virtual Machines to access external network through outgoing port3</i>.</p>
<b>Status</b>	Port3 status to access the Internet.
<b>Gateway</b>	Enter the next hop gateway IP address.
<b>Disable SIMNET if Virtual Machines are not able to access external network through outgoing port3</b>	Enable to disable SIMNET when Virtual Machines are not able to access external network through the outgoing port3.
<b>DNS</b>	DNS server used by VM images when a file is scanned.
<b>Use Proxy</b>	<p>Enable to use the proxy. Configure the Proxy Type, Server Name/IP, Port, Proxy Username, and Proxy Password.</p> <p>When the proxy server is enabled, all the non UDP outgoing traffic started from Sandbox VM will be directed to the proxy server.</p> <p>When a proxy server is used, if the proxy server type is not SOCKS, the system level DNS server is used. If the type is SOCKS5, users need to configure an external DNS server that port3 can access.</p> <p>For other traffic started by FortiSandbox firmware, such as FortiGuard Distribution Network (FDN) upgrades, the configurations should be done under the <i>Network</i> menu.</p>
<b>Proxy Type</b>	<p>Select the proxy type from the dropdown list. The following options are available:</p> <ul style="list-style-type: none"> <li>• HTTP Connect</li> <li>• HTTP Relay</li> <li>• SOCKS v4</li> <li>• SOCKS v5; requires DNS</li> </ul>

	UDP protocol is not supported.
<b>Server Name/IP</b>	Enter the proxy server name or IP address.
<b>Port</b>	Enter the proxy server port number.
<b>Proxy Username</b>	Enter a proxy username.
<b>Proxy Password</b>	Enter the proxy password.
<b>Apply default passwords to extract archive files</b>	User can define a list of passwords that can be tried to extract archive files. Input passwords line by line.
<b>Disable Community Cloud Query</b>	By default the Cloud Query is enabled. Disable the Cloud Query in the following scenarios: <ul style="list-style-type: none"> <li>You have an enclosed environment. Disabling the Cloud Query will improve the scan speed.</li> <li>You receive an incorrect verdict from the Cloud Query and before Fortinet fixes it, you can turn it off temporarily.</li> </ul>
<b>Disable AV Rescan of finished Jobs</b>	AV signature updates are frequent (every hour). Running an AV rescan against finished jobs of the last 48 hours could hinder performance. You have the option to disable the AV Rescan to improve performance.
<b>Enable URL call back detection</b>	Enable URL call back detection. When enabled, previously detected clean URLs in sniffed traffic are frequently queried against Web Filtering service.
<b>Enable log event of file submission</b>	Enable to log the file submission events of an input source.
<b>Devices</b>	Select to log the file submission events of a device, like FortiGate, FortiMail or FortiClient.
<b>Adapter</b>	Select to log the file submission events from an adapter like a Carbon Black server.
<b>Network Share</b>	Select to log the file submission events when they are from a network share.
<b>BCC Adapter</b>	Select to log the file submission events from a BCC client.
<b>ICAP</b>	Select to log the file submission events from an ICAP client.
<b>Reject duplicate file from device</b>	Enable to reject duplicate files from devices.
<b>Delete original files of Clean or Other rating after</b>	Enable to delete original files of Clean or Other ratings after a specified time. If the time is 0, the original files with either Clean or Other ratings will not be kept on the system. Original files of Clean or Other rating can be kept in system for a maximum of 4 weeks.
<b>Day</b>	Enter the day.
<b>Hour</b>	Enter the hour.
<b>Minute</b>	Enter the minute.
<b>Delete original files of Malicious or Suspicious rating after</b>	Enable to delete original files of Malicious or Suspicious ratings after a specified time.

<b>Day</b>	Enter the day.
<b>Hour</b>	Enter the hour.
<b>Minute</b>	Enter the minute.
<b>Delete all traces of jobs of Clean or Other rating after</b>	Enable to delete all traces of jobs of Clean or Other ratings after a specified time. Traces of jobs with Clean or Other rating can be kept in system for a maximum of 4 weeks.
<b>Day</b>	Enter the day.
<b>Hour</b>	Enter the hour.
<b>Minute</b>	Enter the minute.
<b>Delete all traces of jobs of Malicious or Suspicious after</b>	Enable to delete all traces of jobs of Malicious or Suspicious ratings after a specified time.
<b>Day</b>	Enter the day.
<b>Hour</b>	Enter the hour.
<b>Minute</b>	Enter the minute.



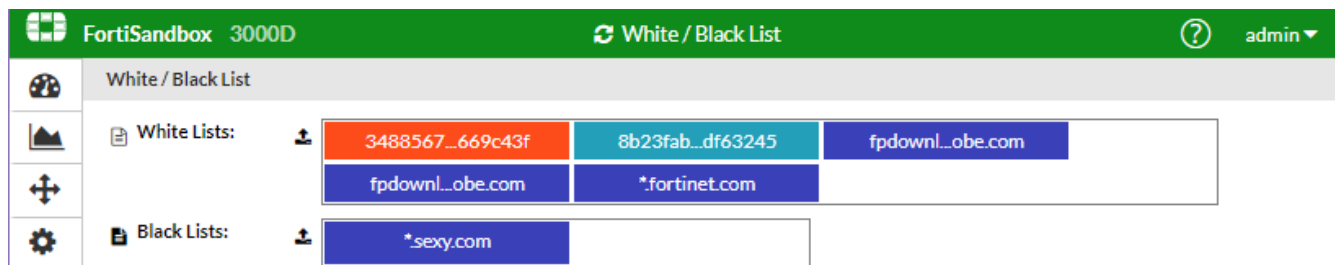
By default, job traces of files with a Clean or Other rating will be kept for three days.

## Allowlist and blocklist (white/black lists)

Allowlists and blocklists (white and black lists) help improve scan performance and malware catch rate as well as reduce false positives and can be appended to, replaced, cleared, deleted, and downloaded. These lists contain file checksum values (MD5, SHA1, or SHA256) and domain/URLs. Domain and URL lists are used in both file and URL scanning. For files, the file's downloading URL is checked against the list. *Wild Card* formats, like `*.domain`, are supported. For example, when the user adds `windowsupdate.microsoft.com` to the *White Domain List*, all files downloaded from this domain will be rated as *Clean* files immediately. If the user adds `*.microsoft.com` to the *White Domain List*, all files downloaded from sub-domains of `microsoft.com` will be rated as *Clean* immediately.

For URLs, you can add a raw URL or a regular expression pattern to the list. For example, if the user adds `.*amazon.com/. *subscribe` to the allowlist, all subscription URLs from `amazon.com` will be immediately rated as *Clean*. This way, subscription links will not be opened inside the VM and become invalid.

- If an allowlist entry is hit, the job rating will be *Clean* with a local overwrite flag.
- If a blocklist entry is hit, the job rating will be *Malicious* with a local overwrite flag. Malware names will be FSA/BL\_DOMAIN, FSA/BL\_MD5, FSA/BL\_SHA1, or FSA/BL\_SHA256.
- If the same entry exists on both lists and is hit, the blocklist will take priority and the file will be rated *Malicious*.



### To manage the allow/block list manually:

1. Go to *Scan Policy > White/Black List*.
2. Click the *White List* or *Black List* panel and the *Detail* panel will slide out from the right side.
3. Click the head of each type to expand or collapse the list.
4. Click the + button to add a new entry.



The URL pattern will have a higher rating priority than a domain pattern. For example, if you enter \*.microsoft.com in a domain allowlist and http://www.microsoft.com/\*abc/bad.html in a URL blocklist, a file from http://www.microsoft.com/labc/bad.html will be rated as Malicious.

Alternatively, click the *Trash* button to either remove the whole list or remove a single entry.

5. Click outside the *Detail* panel to accept the change.

### To manage the allow/block list through files:

1. Go to *Scan Policy > White/Black List*.
2. Click the *File Upload* icon for either the *White List* or *Black List*.
3. Select the list type from the dropdown menu:
  - Domain
  - MD5
  - SHA1
  - SHA256
  - URL
  - URL REGEX
4. Select the *Action* to take from the dropdown menu:
  - *Append*: Add checksums to the list.
  - *Replace*: Replace the list.
  - *Clear*: Remove the list.
  - *Download*: Download the list to the management computer.
  - *Delete*: Delete an entry from the list if the entry is in the uploaded file.
5. If the action is *Download*, click *OK* to download the list file to the management computer.
6. If the action is *Append* or *Replace*, click *Choose File*, locate the checksum file on the management computer, then click *OK*.
7. If the action is *Clear*, click *OK* to remove the list.



In a cluster setting, allowlists and blocklists should only be created on the primary (master) node. They will be synchronized with other nodes.



The total number of URL REGEXs in allowlists and blocklists should be less than 1000. The total number of domains plus URLs in allowlists and blocklists should be less than 50000.

## Overridden Verdicts

The *Overridden Verdicts* page displays jobs that users have manually marked as *False Positive* or *False Negative*. *Job IDs*, *Comment*, *Job Finish Time*, and the time that the user manually marked the verdict will be displayed. If the job's detailed information is still available, the user can click on *Job ID* to display them.

Users can easily delete a FP/FN verdict in this page by selecting an entry and clicking the *Delete* button.

Overridden Verdicts			
Delete			
FPN	Job	Detected Time	Override Time
	2092455118275295516	N/A	Jan 20 2015 15:56:01
	2217051432347746846	N/A	Apr 14 2015 15:18:14

## YARA Rules

YARA is a pattern matching engine for malware detection. The *YARA Rules* page allows you to upload your own YARA rules. The rules must be compatible with the 3.x schema and put inside ASCII text files.

The following options are available:

<b>Import</b>	Select to import a YARA rule file. You can apply one YARA rule to multiple file types.
<b>Edit</b>	Select to edit a YARA rule file. You can apply one YARA rule to multiple file types.
<b>Delete</b>	Select to delete a YARA rule file.
<b>Change Status</b>	Select to change the status (Active or Inactive) of a YARA rule.
<b>Export</b>	Select to export a YARA rule file.

The following information is displayed:

<b>Name</b>	The name of the YARA rule set.
-------------	--------------------------------



<b>File Type</b>	The file types the YARA rule is applied to.
<b>Modify Time</b>	The date and time the YARA rule set was last modified.
<b>Size</b>	The size of the YARA rule file.
<b>Sha256</b>	The Sha256 checksum of the YARA rule file.
<b>Status</b>	The current status (Active or Inactive) of the YARA rule set.

#### To upload YARA Rule File:

1. Go to *Scan Policy > YARA Rules*.
2. Select *Import*.
3. Configure the following settings:

<b>YARA Rule Name</b>	Enter a name for the YARA rule set.
<b>Default Description</b>	Enter a description of the YARA rule set.
<b>Rules Risk Level</b>	<p>Select a rule risk level between 1-10.</p> <ul style="list-style-type: none"> <li>• 0-1: Clean</li> <li>• 2-4: Low Risk</li> <li>• 5-7: Medium Risk</li> <li>• 8-10: High Risk</li> </ul> <p>All the YARA rules inside the YARA rule file will share the same risk level.</p>
<b>File Type</b>	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
<b>YARA Rule File</b>	Choose a text file containing YARA rules.

4. Select *OK* to import rules.
5. After a YARA Rule file is imported, you can select the *Activate/Deactivate* icon to enable/disable the YARA rule set.



If a file hits multiple rules, a complicated algorithm is used to calculate the final rating of the file. For example, if a file hits more than one Low Risk YARA rules, the file's verdict can be higher than the Low Risk rating.

#### To edit a YARA Rule set:

1. Go to *Scan Policy > YARA Rules*.
2. Select a YARA Rule.
3. Click the *Edit* button from the toolbar.

## 4. Configure the following options:

<b>ID</b>	YARA ID number. You cannot edit this field.
<b>Yara Rule Name</b>	Enter a name for the YARA rule set.
<b>Default Description</b>	Enter a description of the YARA rule set.
<b>Rules Risk Level</b>	Select a rule risk level between 1-10. <ul style="list-style-type: none"> <li>• 0-1: Clean</li> <li>• 2-4: Low Risk</li> <li>• 5-7: Medium Risk</li> <li>• 8-10: High Risk</li> </ul> All the YARA rules inside the YARA rule file will share the same risk level.
<b>File Type</b>	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
<b>YARA Rule File</b>	Choose a text file containing YARA rules.

## 5. Click OK to apply changes.

**To delete a YARA rule set:**

1. Go to *Scan Policy > YARA Rules*.
2. Select a YARA Rule set.
3. Click *Delete* from the toolbar.
4. Click *Yes I'm sure* button from the *Are you sure?* confirmation box.

**To change the status of a YARA rule set:**

1. Go to *Scan Policy > YARA Rules*.
2. Select a YARA Rule set.
3. Click *Change Status*.  
The status of the selected YARA rule will switch to *Active* or *Inactive* depending on its previous status.

## URL Category

Go to *Scan Policy > URL Category* to define specific URL categories as non-suspicious. URLs of these categories will be treated as *Clean*. By default, the following categories are in the list:

- Abortion
- Advocacy Organizations
- Alcohol
- Alcohol and Tobacco
- Child Abuse
- Dating
- Discrimination
- Drug Abuse
- Explicit Violence

- Extremist Groups
- Gambling
- Grayware
- Hacking
- Homosexuality
- Illegal or Unethical
- Marijuana
- Nudity and Risque
- Occult
- Other Adult Materials
- Plagiarism
- Pornography
- Tobacco
- Weapons (Sales)

### Benign URL Category

Treat the following URL categories as benign, excluding Malicious Websites, Phishing and Spam URLs:

- ☐ Abortion
- ☐ Advocacy Organizations
- ☐ Alcohol
- ☐ Alcohol and Tobacco
- ☐ Child Abuse
- ☒ Dating
- ☐ Discrimination
- ☐ Drug Abuse
- ☐ Explicit Violence
- ☐ Extremist Groups
- ☒ Gambling
- ☐ Grayware
- ☐ Hacking
- ☐ Homosexuality
- ☐ Illegal or Unethical
- ☐ Marijuana
- ☒ Nudity and Risque
- ☐ Occult
- ☒ Other Adult Materials
- ☐ Plagiarism
- ☐ Pornography
- ☐ Tobacco
- ☒ Weapons (Sales)

OK

## Working Together With URL Pre-Filtering

By default, URL scanning is done inside a VM. However, if performance is a concern, users can turn on URL Pre-Filtering.

When URL Pre-Filtering is enabled, it will work together with the Scan Profile settings and URL Category settings.

### Scenarios

#### URL Sandboxing Pre-Filtering is Enabled

1. If the category or URL is Unrated, the URL will be scanned inside the VM.
2. If the URLs category falls into one defined in the *Scan Policy > URL Category* page, but is not checked as *Benign*, a job will be created and the URL will be rated as *Suspicious* (Low Risk, Medium Risk or High Risk according to category).
3. If the URLs category falls into one defined in the *Scan Policy > URL Category* page, but is checked as *Benign*, a job will be created and the URL will be rated as *Clean* and will not be scanned inside the VM.

#### URL Sandboxing Pre-Filtering is Disabled

In this case, all URLs will be scanned inside the VM.

## Customized Rating

The Customized Rating page allows you to set verdicts for the following cases: VM Timeout, Tracer Engine Timeout, and Unextractable Encrypted Archive.

The following options can be configured:

<b>VM Timeout</b>	<p>Windows VM cannot be launched properly. This usually occurs on FSA-VM model running on hardware with limited resources.</p> <p>Select one of the following ratings:</p> <ul style="list-style-type: none"><li>• Unknown</li><li>• Clean</li><li>• Malicious</li><li>• Low Risk</li><li>• Medium Risk</li><li>• High Risk</li></ul>
<b>Tracer Engine Timeout</b>	<p>Tracer engine is not working properly. For example, the malware crashes the Windows VM or kills the tracer engine process. Thus, the tracer log is not available.</p> <p>Select one of the following ratings:</p> <ul style="list-style-type: none"><li>• Unknown</li><li>• Clean</li><li>• Malicious</li><li>• Low Risk</li></ul>

- Medium Risk
- High Risk

**Unextractable Encrypted Archive**

The archive file is password protected and cannot be extracted with a predefined password list set in the *Scan Policy > General* page.

Select one of the following ratings:

- Unknown
- Clean
- Malicious
- Low Risk
- Medium Risk
- High Risk

## Job Archive

The Job Archive page allows you to setup a network share folder to save a copy of scan job information. Archive location is a network share folder. Archiving job information is useful when processing job files and data with third party tools.

Go to *Scan Policy > Job Archive* to view the *Archive Location* page.

Archive Location	
<input type="checkbox"/> Enabled	
Mount Type:	CIFS ▼
Server Name/IP:	<input type="text"/>
Share Path:	<input type="text" value="\path1"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
File Name:	Scan Job ID as File Name ▼
Folder Structure:	Save all files in the same folder ▼
<input type="checkbox"/> Save meta data	
<input type="checkbox"/> Save tracer log	
<input type="checkbox"/> Save Malicious rating jobs	
<input type="checkbox"/> Save Suspicious rating jobs	
<input type="checkbox"/> Save Clean rating jobs	
<input type="checkbox"/> Save Unknown rating jobs	
<input type="button" value="OK"/> <input type="button" value="Test Connectivity"/> <input type="button" value="Restore Default"/>	

The following options can be configured:

**Enabled**

Select to enable the job archive feature.

<b>Mount Type</b>	Select the mount type of the network share folder. The following options are available: <ul style="list-style-type: none"> <li>• CIFS (SMB v1.0, v2.0, v2.1, v3.0)</li> <li>• NFSv2</li> <li>• NFSv3</li> <li>• NFSv4</li> </ul>
<b>Server Name/IP</b>	Enter the server fully qualified domain name (FQDN) or IP address.
<b>Share Path</b>	Enter the file share path in the format of /path1/path2.
<b>Username</b>	Enter a user name. The username should have the write privilege of the remote network share folder.
<b>Password</b>	Enter the password.
<b>Confirm Password</b>	Enter the password a second time for verification.
<b>File Name</b>	Select the file name from the dropdown list. The following options are available: <ul style="list-style-type: none"> <li>• Scan Job ID as File Name</li> <li>• Original File Name</li> </ul>
<b>Folder Structure</b>	Select the folder structure from the dropdown list. The following options are available: <ul style="list-style-type: none"> <li>• Save all files in the same folder</li> <li>• Save file in folders of the scan finish time</li> <li>• Save file in folders of ratings</li> </ul>
<b>Save meta data</b>	When selected, the job summary information will be saved.
<b>Save tracer log</b>	When selected, the job's tracer log will be saved.
<b>Save Malicious rating jobs</b>	When selected, files of Malicious rating will be saved.
<b>Save Suspicious rating jobs</b>	When selected, files of Suspicious rating will be saved.
<b>Save Clean rating jobs</b>	When selected, files of Clean rating will be saved.
<b>Save Other rating jobs</b>	When selected, files of Other rating will be saved.

## Global Network

The FortiSandbox can generate antivirus database packages (malware packages) and blocklist URL packages from scan results, and distribute them to FortiGate devices and FortiClient end points for antispayware/antivirus scan and web filtering extension to block and quarantine malware.

This feature requires that:

- The FortiGate device, running FortiOS 5.4 or later, is authorized on the FortiSandbox.
- The FortiClient endpoint is running version 5.4 or later and has successfully connected to the FortiSandbox, and
- FortiSandbox is running version 2.1 or later.

The FortiGate or FortiClient sends a malware package request to FortiSandbox every two minutes that includes its installed version (or 0.0, if none exists). The FortiSandbox receives the request then compares the version with the latest

local version number. If the received version is different, FortiSandbox sends the latest package to the FortiGate or FortiClient. If the versions are the same, then FortiSandbox will send an already-up-to-date message.

Multiple FortiSandbox units can work together to build up a Global Threat Network to share threat information. One unit works as a Collector to collect threat information from other units, while other units work as Contributors to upload locally detected threat information to the Collector, then download a full copy. A new package is generated on a unit when:

- The FortiSandbox has a new malware detection, either from local detection, or detected on another unit inside the Global Threat Network, whose rating falls into configured rating range.
- Malware in the current malware package is older than the time set in the malware package configuration.
- The malware package generation condition is changed in the configuration page.
- The malware's rating has been overwritten manually.

The Collector can also manage the Scan Profile of all units in the network. However, only a standalone unit or primary (master) node in a cluster can join the network.

### To join the global network to share threat information and scan profiles:

1. Go to *Scan Policy > Global Network*.
2. Enable *Join global network to share threat information and manage scan profiles*.
3. You have the following two options:
  - a. *Work as threat information collector and scan profile manager.*

If the unit works as a *Collector*, configure the following:

<b>Alias</b>	Enter the network Alias name.
<b>Authentication Code</b>	Enter the authentication code for Contributor to join the network.
<b>Contributors</b>	List the units who are in the network.
<b>Local Malware Package Options</b>	These options define how each unit generates local packages after it has threat information. Please refer to <a href="#">Local Packages on page 104</a> for more information.
<b>Local URL Package Options</b>	
<b>Enable Local STIX IOC Package</b>	

- b. *Work as threat information contributor. Scan profile is managed by manager.*

If the unit works as a *Contributor*, configure the following:

<b>Collector IP Address</b>	Enter the Collector's IP address.
<b>Alias</b>	Enter the global network Alias name.
<b>Authentication Code</b>	Enter the authentication code to join the network.
<b>Local Malware Package Options</b>	These options define how each unit generates local packages after it has threat information. Please refer to <a href="#">Local Packages on page 104</a> for more information.
<b>Local URL Package Options</b>	

### Enable Local STIX IOC Package

#### Scan Profile is Managed by Manager

By enabling this option, the unit can choose to allow its scan profile to be managed by the Collector. The Collector will combine all VM types from the Contributors. After the user configures a scan profile on the Collector, the configurations will be downloaded by each Contributor. On the Contributor unit, its *Scan Profile* page will become *Read-Only*.

- Click **OK** to save the settings.



When the Contributor's scan profile is managed by the Collector, the Collector must have network access to the Contributor's HTTPS port, which is port 443.

## Local Packages

The local package page defines conditions to generate threat packages. If the unit joins the Global Threat Network, the page will display: *The unit has joined the threat information global network and is working as a contributor/collector. To configure settings, please go to the Global Network page.* The user should configure package conditions there.

## Malware and URL Package Options

The malware package options allow you to configure how many days worth of data the malware packages save and the malware ratings that are included in the packages.



In a cluster environment, only the primary (master) node generates malware packages and URL packages.

The URL package contains downloaded URLs of detected malware.

### Local Malware Package Options

**Include past \_\_ day(s) of data. (1-365 days)** Enter the number of days. If the user changes the current days to a longer value, the unit will not go back to include historical data older than current days.

#### Include the job data of the following ratings

##### Malicious

Include malware with malicious ratings.  
By default, only data with Malicious or High Risk rating will be included in the Malware Package.

##### High Risk

Include malware with high risk ratings and URLs sent by FortiMail devices of high risk ratings and whose scan depth is 0.



<b>Medium Risk</b>	Include malware with medium risk ratings and URLs sent by FortiMail devices of medium risk ratings and whose scan depth is 0.
<b>Local URL Package Option</b>	
<b>Include past __ day(s) of data. (1-365 days)</b>	Enter the number of days. If the user changes current days to a longer value, the unit will not go back to include historical data older than current days.
<b>Include the job data of the following ratings</b>	
<b>Malicious</b>	Include downloaded URLs of malware with malicious ratings. By default, only downloaded URLs of malware with a Malicious or High Risk rating will be included in the URL Package.
<b>High Risk</b>	Include downloaded URLs of malware with high risk ratings.
<b>Medium Risk</b>	Include downloaded URLs of malware with medium risk ratings.
<b>Enable STIX IOC</b>	Enable to generate STIX IOC packages.
<b>STIX Malware Package Options</b>	
<b>Include past __ day(s) of data. (1-365 days)</b>	Enter the number of days.
<b>Include the job data of the following ratings</b>	
<b>Malicious</b>	Include malware with malicious ratings.
<b>High Risk</b>	Include malware with high risk ratings.
<b>Medium Risk</b>	Include malware with medium risk ratings.
<b>Download STIX</b>	Download most recently generated Malware STIX IOC package.
<b>STIX URL Package Options</b>	
<b>Include past __ day(s) of data. (1-365 days)</b>	Enter the number of days.
<b>Include the job data of the following ratings</b>	
<b>Malicious</b>	Include malware with malicious ratings.
<b>High Risk</b>	Include downloaded URLs of malware with high risk ratings and URLs sent by FortiMail devices of high risk ratings and whose scan depth is 0.
<b>Medium Risk</b>	Include downloaded URLs of malware with medium risk ratings and URLs sent by FortiMail devices of medium risk ratings and whose scan depth is 0.
<b>Download STIX</b>	Download most recently generated URL STIX IOC package.



Users can also select to include files or URLs to packages during an *On Demand* scan if their results meet package settings.



Because of size limitations, malware packages can only have a maximum of 100K entries.



Because of size limitations, URL package can only have a maximum of 1000 entries.

## IOC Package

Indicator of Compromise (IOC), in computer forensics, is an artifact observed on a network or in an operating system which indicates a computer intrusion. Typical IOCs are virus signatures and IP addresses, malware files or URLs MD5 hashes, or domain names of botnet command and control servers. In order to share, store and analyze in a consistent manner, Structured Threat Information Expression (STIX™) is commonly adopted by the industry.

FortiSandbox supports IOC in STIX v1.2 format. Two types of IOC packages are generated:

1. A File Hash Watchlist package contains the Malware's file hash and is generated along with each Malware package. If the malware is detected in local unit, behavioral information is also included. The most recent package can be downloaded from *Scan Input > Global Network* or *Scan Input > Local Packages*, depending on if the unit joins a Global Threat Network.
2. A URL Watchlist package contains the Malware's download URL and is generated along with each URL Package. It also contains URLs sent by FortiMail devices of suspicious ratings and whose scan depth is 0. The most recent package can be downloaded from *Scan Policy > Global Network* or *Scan Policy > Local Packages*, depending on if the unit joins a Global Threat Network. Behavioral information is not included in URL package.

The following is a example snippet of a File Hash Watchlist ICO package in STIX format:

```
<stix:STIX_Package
  xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
  xmlns:FortiSandbox="http://www.fortinet.com"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:ttp="http://stix.mitre.org/ttp-1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" id="FortiSandbox:Package-ba2ad205-
    b390-40fd-96e4-44c2efaacab1" version="1.2">
<stix:STIX_Header/>
<stix:Indicators>
  <stix:Indicator id="FortiSandbox:indicator-7d3e889e-957c-428c-9f68-8e48d3346316"
    timestamp="2016-08-12T18:25:52.674621+00:00" xsi:type='indicator:IndicatorType'>
    <indicator:Title>File hash for Suspected High Risk - Riskware</indicator:Title>
```

```
<indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">File Hash
  Watchlist</indicator:Type>
<indicator:Observable id="FortiSandbox:Observable-723483db-a3e0-4de0-93cd-
  5bd37b3c4611">
  <cybox:Object id="FortiSandbox:File-3d9e7590-b479-4352-9a11-8fa313cee9f0">
    <cybox:Properties xsi:type="FileObj:FileObjectType">
      <FileObj:Hashes>
        <cyboxCommon:Hash>
          <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-
            1.0">SHA256</cyboxCommon:Type>
          <cyboxCommon:Simple_Hash_Value
            condition="Equals">0696e7ec6646977967f2c6f4dcb641473e76b4d5c9beb6
            e433e0229c2acce5d</cyboxCommon:Simple_Hash_Value>
          </cyboxCommon:Hash>
        </FileObj:Hashes>
      </cybox:Properties>
    </cybox:Object>
  </indicator:Observable>
<indicator:Indicated_TTP>
  <stixCommon:TTP idref="FortiSandbox:ttp-afa9d28b-9602-4936-8b94-93e29cc8830c"
    xsi:type='ttp:TTPType' />
</indicator:Indicated_TTP>
</stix:Indicator>
</stix:Indicators>
<stix:TTPs>
  <stix:TTP id="FortiSandbox:ttp-afa9d28b-9602-4936-8b94-93e29cc8830c" timestamp="2016-08-
    12T18:25:52.674181+00:00" xsi:type='ttp:TTPType'>
    <ttp:Title>Suspected High Risk - Riskware</ttp:Title>
    <ttp:Behavior>
      <ttp:Malware>
        <ttp:Malware_Instance>
          <ttp:Type xsi:type="stixVocabs:MalwareTypeVocab-1.0">Exploit Kits</ttp:Type>
          <ttp:Name>Suspected High Risk - Riskware</ttp:Name>
        </ttp:Malware_Instance>
      </ttp:Malware>
    </ttp:Behavior>
  </stix:TTP>
</stix:TTPs>
</stix:STIX_Package>
```



If the IOC package includes behavior information, it can be very large.

---

# Scan Input

This section includes the following topics:

- [File Input](#)
- [File On Demand](#)
- [URL On Demand](#)
- [Job Queue](#)
- [File On Demand](#)
- [Sniffer](#)
- [Device](#)
- [Adapter](#)
- [Network Share](#)
- [Quarantine](#)
- [Malware Package](#)
- [URL Package](#)

## File Input

FortiSandbox utilizes Fortinet antivirus to scan files for known threats and then executes files in a VM host environment. Unlike traditional sandboxing solutions, FortiSandbox is able to perform advanced static scans, which can quickly and accurately filter files, and utilize up-to-the-minute threat intelligence of FortiGuard services.

There are five methods to import files to your FortiSandbox: sniffer mode, device mode (including FortiGate, FortiMail, FortiWeb, and FortiClient endpoints), adapter, network share, and on demand (including on demand through JSON API call and GUI submission). In sniffer mode, the FortiSandbox sniffs traffic on specified interfaces, reassembles files, and analyzes them. In device mode, your FortiGate, FortiWeb, FortiMail, or FortiClient end points are configured to send files to your FortiSandbox for analysis, and can receive malware packages from the FortiSandbox. Network share allows you to scan files located on a remote file share as scheduled, and quarantine bad files. On demand allows you to upload files, URLs inside a file, or archived files directly to your FortiSandbox for analysis. Different adapters allow FortiSandbox to work with third-party products smoothly.

FortiSandbox will execute code in a contained virtual environment by simulating human behavior and the output is analyzed to determine the characteristics of the file. Inspection is run post-execution and all aspects of the file are examined. FortiSandbox checks files for the dozens of suspicious characteristics, including but no limited to:

- Evasion techniques
- Known virus downloads
- Registry modifications
- Outbound connections to malicious IP addresses
- Infection of processes
- File system modifications
- Suspicious network traffic

FortiSandbox can process multiple files simultaneously since it has a VM pool to dispatch files to for sandboxing. The time to process a file depends on the hardware and the number of sandbox VMs used to scan the file. It can take from 60 seconds to five minutes to process a file.

## File On Demand

To view on-demand files and submit new files to be sandboxed, go to *Scan Input > File On-Demand*. You can drill down the information and apply search filters. You can select to create a PDF or CSV format snapshot report for all on-demand files. Search filters will be applied to the detailed report.

File On-Demand allows you to upload various file types directly to your FortiSandbox device. You can then view the results and decide whether or not to install the file on your network.

FortiSandbox has a rescan feature. When a Suspicious or Malicious file is detected, you can click the *ReScan* icon to rescan the file. This is useful when you want to understand the file's behavior being executed on the Microsoft Windows host. You can select to bypass Static Scan, AV Scan, Cloud Query, or Sandboxing in the *Rescan Configuration* dialog box. All rescanned jobs can be found in the On-Demand page.

You can select VM types to do the sandboxing by overwriting what is defined in the Scan Profile. When MacOSX or WindowsCloud VM is selected, the file will be uploaded to the cloud to be scanned. For password protected archive files or Microsoft Office files, write down all possible passwords. The default password list set in the *Scan Policy > General* page will also be used to extract the archive files.

All files submitted through the JSON API are treated as On-Demand files. Their results will also be shown on this page.

### File On-Demand page - level 1

The following options are available:

<b>Submit File</b>	Click the button to submit a new file. You can upload a regular or archived file. Six levels of file compression is supported. All files in the archive will be treated as a single file.
<b>Show Rescan Job</b>	Jobs either generated from AV Rescan or manually launched Rescan of files can be shown/hidden by this option.
<b>Search</b>	Show or hide the search filter field.
<b>Add Search Filter</b>	Click the search filter field to add search filters. Click the cancel icon to the left of the search filter to remove the specific filter. Click the clear all filters icon in the search filter field to clear all filters.  When the search filter is Filename, select the equal icon to toggle between exact search and pattern search.
<b>Refresh</b>	Click the refresh icon to refresh the entries displayed after applying search filters.
<b>Clear all removable filters</b>	Click the <i>trash can</i> icon to clear all removable filters.

<b>Export Data</b>	Click the <i>Export Data</i> button to create a PDF or CSV snapshot report. The time period of included jobs in the report depends on the selection of Time Period dropdown. You can wait until the report is ready to view, or navigate away and find the report later in <i>Log &amp; Report &gt; Report Center</i> .
<b>View Jobs</b>	Click the icon to view the scan job(s) associated with the entry. In this page you can view detailed information for files scanned. If the file is an archive file, all files in the archive are displayed in this page. Click the back button to return to the on-demand page.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

This page displays the following information:

<b>Submission Time</b>	The date and time that the file was submitted to FortiSandbox. Use the column filter to sort the entries in ascending or descending order.
<b>Submitted Filename</b>	The file name.
<b>Submitted By</b>	The name of the administrator that submitted the file. Use the column filter to sort the entries in ascending or descending order.
<b>Rating</b>	<p>Hover over the icon in this column to view the file rating. The rating can be one or more of the following: Clean, Low Risk, Medium Risk, High Risk, Malicious, or Other. For archive files, the possible ratings of all files in the archive will be displayed.</p> <p>During the file scan, the rating is displayed as N/A. If a scan times out or is terminated by the system, the file will have an Other rating.</p>
<b>Status</b>	The scan status can be <i>Queued</i> , <i>In-Process</i> , or <i>Done</i> .
<b>File Count</b>	The number of files associated with the entry. It is in the format of (finished file count)/(total files of this submission) when the scan is <i>In-Progress</i> . When the scan is done, it will display the total number of files in this submission.
<b>Comments</b>	The comments user enters when submitting the file.
<b>Rescan Job</b>	This icon indicates that this file is a rescanned version of another file.
<b>Archive Submission</b>	This icon indicates that an archived file has been submitted for scanning.
<b>Total Jobs</b>	The number of jobs displayed and the total number of jobs.



After a file is submitted, the file might not be visible immediately until the file, or any file, inside an archive file is put into a job queue. In a cluster setting, the file will not be visible until the file is put into a worker node's job queue.

### To view the scan job(s) associated with the entry:

1. Click the *View Jobs* icon or double click on the row. The view jobs page is displayed.



In this page you can view detailed information for files scanned. If the file is an archive file, all files in the archive are displayed in this page.

2. This page displays the following information and options:

<b>Back</b>	Click the <i>Back</i> button to return to the On Demand page.
<b>Search</b>	Show or hide the search filter field.
<b>Refresh</b>	Click the <i>Refresh</i> icon to refresh the entries displayed after applying search filters.
<b>Add Search Filter</b>	Click the search filter field to add search filters. Click the <i>Cancel</i> icon to the left of the search filter to remove the specific filter. When the search filter is Filename, select the <i>Equal</i> icon to toggle between exact search and pattern search.
<b>View Details</b>	Click the <i>View Details</i> icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
<b>Scan Video</b>	When the scan is submitted, if <i>Record scan process in video</i> is selected, a video icon is displayed. Clicking it will allow the user to select one VM type in which the scan is done and recorded. Select the VM type to play the video or save it to a local hard disk. The order of displayed columns is determined by the settings defined in the <i>System &gt; Job View Settings &gt; File Detection Columns</i> page. For more information, refer to <a href="#">Job View Settings on page 76</a> .
<b>Pagination</b>	Use the pagination options to browse entries displayed.

3. Click the *View Details* icon to view file details. The *View Details* page will open a new tab. See [Appendix A - View Details Page Reference on page 186](#) for descriptions of the *View Details* page.
4. Click the parent job ID icon to view rescan file details.  
If the parent job is an archive file, the childrens' file names are included in the Archive Files dropdown list. Select a child's file name to view its detail.
5. Close the tab to exit the *View Details* page.

### To create a snapshot report for all on-demand files:

1. Select a time period from the first dropdown list.
2. Select to apply search filters to further drill down the information in the report.
3. Click the *Export Data* button in the toolbar, opening the *Report Generator* window.
4. Select either PDF or CSV and define the report start and end date and time.
5. Click the *Generate Report* button to create the report.  
You can wait until the report is ready to view, or navigate away and find the report later in *Log & Report > Report Center*.
6. Click the *Close* icon or the *Cancel* button to quit the report generator.



In this release, the maximum number of events you can export to a PDF report is 1,000; the maximum number of events you can export to a CSV report is 15,000. Jobs over that limit will not be included in report.

### To submit a file to FortiSandbox:

1. Click the *Submit File* button from the toolbar.
2. You can configure the following:

<b>Select a File</b>	Click the <i>Browse</i> button and locate the sample file or archived sample file on your management computer.
<b>Possible password(s) for archive/office file</b>	List all possible passwords to extract password protected archive file, or open password protected Microsoft Office file. One password per line. Default password list set in the Scan Policy > General page will also be used to extract the archive files.
<b>Comments</b>	Optional comments for future reference.
<b>Debug Options</b>	Unchecked by default and enables viewing advanced options.
<b>Skip</b>	Select one or more of the following steps to skip. When a step is skipped, the verdict of that step won't be taken: <ul style="list-style-type: none"> <li>• Static Scan</li> <li>• AV Scan</li> <li>• Cloud Query</li> <li>• Sandboxing</li> </ul>
<b>Follow VM Association Settings in Scan Profile</b>	If the sandboxing step is not skipped, the file will be sent to its associated VMs defined in Scan Profile.
<b>Force to Scan Inside the Following VMs</b>	Overwrite VM association settings in Scan Profile by selecting one or more of the enabled VMs.
<b>Allow Interaction</b>	Select the <i>Allow Interaction</i> checkbox to interact with the Windows VM. See <a href="#">To use the Allow Interaction Feature: on page 112</a> for more information.
<b>Record scan process in video</b>	Select to enable video recording. After scan finishes, a video icon will show in the File On-Demand second level detail page. Clicking it will trigger a download or play the video.

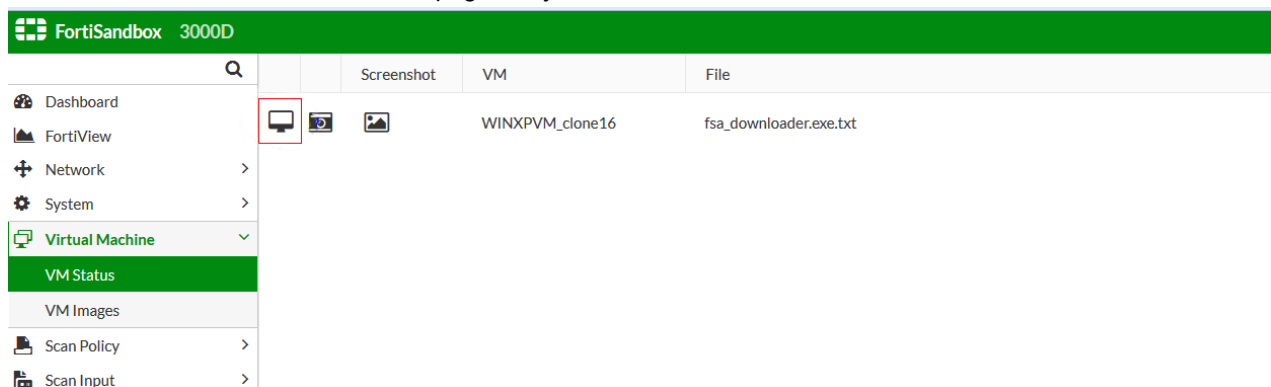
3. Click the *Submit* button. A confirmation dialog box will be displayed. Click *OK* to continue. The file will be uploaded to FortiSandbox for inspection.
4. Click the *Close* button to exit.  
The file will be listed in the *On-Demand* page. Once FortiSandbox has completed its analysis, you can select to view the file details.

### To use the Allow Interaction Feature:

1. Go to *Scan Input > File On-Demand* and click *Submit File* in the toolbar.
2. In the *Submit New File* window, check the *Allow Interaction* checkbox.  
When selected, only one VM can be specified.
3. Click *Submit*.



4. Go to the *Virtual Machine > VM Status* page, the job will be launched when a clone of a selected VM is available.



There are two ways to interact with the windows VM:

1. Use a VNC client and connect to `fsa_ip:port`. The port number can be found in the *Interaction* icon tooltip. Click the *Interaction* icon, the login password will appear in the address bar.
2. Click the *Interaction* icon to use web based VNC client. Click *Yes* in the *Do you want to start the scan?* popup, the scan will start and the question becomes *Do you want to stop the scan?* Click *Yes* to stop the scan and the VNC session will close after a few seconds. Go back to the *On-Demand* page to check the scan result.



The user has 30 minutes to finish the interaction. After that, the VNC session will be closed automatically.



VM Interaction and Scan video recording features are only available to users whose admin profile has *Allow On-Demand Scan Interaction* enabled.



The VM Interaction feature is only available in a standalone mode unit or a primary (master) unit in cluster mode. For a primary (master) unit, there should be an enabled VM which is associated with the scanned file's file type.

## URL On Demand

URL On Demand allows you to upload a plain-text file containing a list of URLs, or an individual URL directly to your FortiSandbox device. Upon upload, the URLs inside the file, or the individual URL, is inspected. The *Depth* to which the URL is examined as well as the length of time that the URL is scanned can be set. You can then view the results and decide whether or not to allow access to the URL.

To view On Demand URLs and submit URLs to scan, go to *Scan Input > URL On-Demand*. You can drill down the information displayed and apply search filters.

The following options are available:

<b>Submit File/URL</b>	Click the button to submit a file containing a list of scanned URLs, or submit an individual URL.
<b>Show Rescan Job</b>	Jobs generated from a customized rescan of a URL can be shown/hidden by this option.
<b>Refresh</b>	Click the <i>Refresh</i> icon to refresh the entries displayed after applying search filters.
<b>Search</b>	Show or hide the search filter field.
<b>Add Search Filter</b>	Click the search filter field to add search filters. Click the close icon in the search filter field to clear all search filters. The search filter will be displayed below the search filter field. Click the close icon beside the search filter to remove the filter. Search filters can be used to filter the information displayed in the GUI.
<b>Clear all removable filters</b>	Click the <i>Trash can</i> icon to clear all removable filters.
<b>Export Data</b>	Click the <i>Export Data</i> button to create a PDF or CSV snapshot report. The time period of included jobs in the report depends on the selection of Time Period filter. You can wait until the report is ready to view, or navigate away and find the report later in <i>Log &amp; Report &gt; Report Center</i> .
<b>View Jobs</b>	Click the icon to view the scan job(s) associated with the entry. Click the <i>Back</i> button to return to the on-demand page.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

This page displays the following information:

<b>Submission Time</b>	The date and time that the URL file or individual URL was submitted to FortiSandbox. Use the column filter to sort the entries in ascending or descending order.
<b>Submitted Filename</b>	The submitted URL file name. If the scan is about an individual URL, the name is <code>scan_of_URL</code> .
<b>Submitted By</b>	The name of the administrator that submitted the file scan.
<b>Rating</b>	Hover over the icon in this column to view the rating. The rating can be one or more of the following: Clean, Low Risk, Medium Risk, High Risk, Malicious, or Other.  During the URL scan, the rating is displayed as N/A. If a scan times out or is terminated by the system, the file will have an Other rating.
<b>Status</b>	The scan status can be <i>Queued</i> , <i>In-Process</i> , or <i>Done</i> .
<b>URL Count</b>	The number of URLs associated with the submission when the scan is done. When the scan is <i>In-Progress</i> , it shows (finished scan)/(total URLs of this submission).
<b>Comments</b>	The comments user enters when submitting the file scan.

**To view the scan job(s) associated with the entry:**

1. Double-click an entry in the table or select the *View Jobs* icon to view the specific URLs that were scanned.
2. This page displays the following information and options:

<b>Back</b>	Click the <i>Back</i> button to return to the on-demand page.
<b>Search</b>	Show or hide the search filter field.
<b>Refresh</b>	Click the <i>Refresh</i> icon to refresh the entries displayed after applying search filters.
<b>Add Search Filter</b>	Click the search filter field to add search filters. Click the <i>Close</i> icon in the search filter field to clear all search filters. Search filters can be used to filter the information displayed in the GUI.
<b>View Details</b>	Select the <i>View Details</i> icon to view file information.
<b>Scan Video</b>	When the scan is submitted, if <i>Record scan process in video</i> is selected, a video icon is displayed. Clicking it allows users to select the VM type in which the scan is performed and recorded. Select the VM type to play the video or save it to a local hard disk.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

The reset of displayed columns are determined by settings defined in *System > Job View Settings > URL Detection Columns*. For more information, refer to [Job View Settings on page 76](#).

3. Click the *View Details* icon to view file details. The *View Details* page will open a new tab. See [Appendix A - View Details Page Reference on page 186](#) for descriptions of the *View Details* page.
4. Close the tab to exit the *View Details* page.

**To submit a file containing a list of URLs or an individual URL to FortiSandbox:**

1. Click the *Submit File / URL* button from the toolbar. The *Submit New File* window opens.
2. Enter the following information:

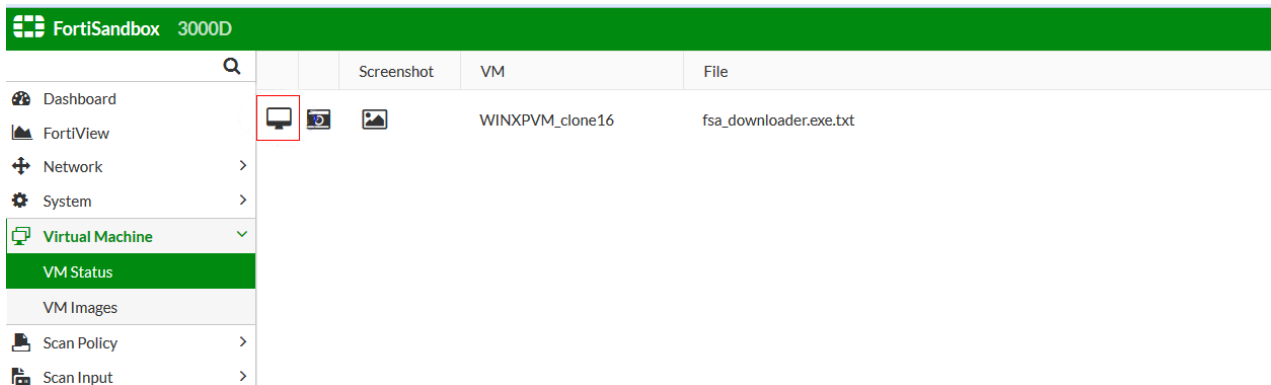
<b>Depth</b>	Enter the <i>Recursive Depth</i> in which URLs are examined. The original URL is considered level 0. A depth of 1 will open all links on the original URL page and crawl into them. The default value is define in the <i>Scan Policy &gt; Scan Profile</i> page.
<b>Timeout</b>	Enter the <i>Timeout Value</i> . The Timeout Value controls how long the device will scan the URL. If the network bandwidth is low, the timeout value should be larger to accommodate higher depth values. The default value is defined in the <i>Scan Policy &gt; Scan Profile</i> page.
<b>Direct URL</b>	To scan only a single URL, check the <i>Direct URL</i> checkbox. Enter the URL in the <i>Enter a URL</i> field.
<b>Select a File</b>	Click the <i>Browse</i> button and locate the plain-text file on your management computer. The maximum number of URLs in this file is determined by <i>Maximum URL Value</i> in <i>Scan Policy &gt; Scan Profile</i> page.
<b>Comments</b>	You can choose to enter optional comments for future reference.

<b>Debug Options</b>	To display the advanced options, check the <i>Debug Options</i> toggle. Users can choose to follow scan profile settings or specify the VMs.
<b>Follow VM Association settings in Scan Profile</b>	The URL will be sent to its associated VMs for the WEblink defined in the Scan Profile. Enabled VM means its clone number is larger than 0. <b>Note:</b> To use WindowsCloud VM, you need to purchase the subscription service. URL will be sent to Fortinet Sandboxing cloud to scan.
<b>Force to Scan the URL Inside VM</b>	A VM type must be selected. Settings from the Scan Profile will be overridden and the URL will only be scanned in selected VM types. If VM images are not ready, the VM list will not be displayed.
<b>Allow Interaction</b>	Select the <i>Allow Interaction</i> checkbox to interact with the Windows VM. See To use the <a href="#">To use the Allow Interaction Feature: on page 116</a> for more information.
<b>Record scan process in video</b>	Select to enable video recording. After scan finishes, a video icon will show in the second level detail page. Clicking it will trigger a download or play the video.
<b>Add URL sample to threat package</b>	Select to add the sample to malware package, if the result meets settings in Package Options

3. Click *Submit*.

#### To use the Allow Interaction Feature:

1. Go to *Scan Input > URL On-Demand* and click *Submit File/URL* from the toolbar.
2. In the *Submit New File* window, check the *Allow Interaction* checkbox.  
When selected, only one VM can be specified.
3. Click *Submit*.
4. Go to the *Virtual Machine > VM Status* page. The job will be launched when a clone of a selected VM is available.



There are two ways to interact with the Windows VM.

1. Use a VNC client and connect to `fsa_ip:port`. The port number can be found in the *Interaction* icon tooltip. Click the *Interaction* icon and the login password will appear in the address bar.
2. Click the *Interaction* icon to use web based VNC client.
3. Click *Yes* in the *Do you want to start the scan?* popup, the scan will start and the question becomes *Do you want to*

*stop the scan?*

Click **Yes** to stop the scan and VNC session will be closed. Go back to *On Demand* page to check the scan result.



The user has 30 minutes to finish the interaction. After that, the VNC session will be closed automatically.



VM Interaction and Scan video recording features are only available to users whose admin profile has *Allow On-Demand Scan Interaction* enabled.

## Job Queue

In this page, users can view the current pending job number, average scan time, and arrival rate of each job queue. The associated VM is also displayed for each queue. The user can click the VM name to go to the *Scan Profile* page and change its settings.

Users can use this page's information to ensure each Job Queue is not piling up with too many jobs. If there are a lot of jobs pending in the Job Queue, the user can try to associate it with less VM types and/or allocate more clone numbers to its associated VM types.

To refresh the data, click the *Job Queue* menu again or the *Refresh* button on the top of the web site.

FortiSandbox 3500D		Job Queue				
Input Source	File Type	Queued #	Ave Scan Time in Last 24 hrs (s)	Expected Finish Time	Arrival Rate (Last 1 hr)	VM Type (Clone #)
FortiMail URL	URL detection	29		00:58:00		
FortiMail	Executables/DLL/VBS/BAT/PS1/JAR/MSI/WSF/JS files	23		00:46:00		WIN7X86VM(4)
URL On-Demand	URL detection	11		00:22:00		
Device	Executables/DLL/VBS/BAT/PS1/JAR/MSI/WSF/JS files	0	3		22	WIN7X86VM(4)
Device	User defined extensions	0	388			WIN7X64VM(4) , WIN7X86VM(4)
Device	Microsoft Office files (Word, Excel, PowerPoint files etc)	0	90		5	WIN7X86VM(4)
Device	PDF files	0	5		25	WIN7X86VM(4)
URL Device	URL detection	0	1		64	
Non Sandboxing files	Non Sandboxing files	8				
FortiMail	Microsoft Office files (Word, Excel, PowerPoint files etc)	4		00:08:00		WIN7X86VM(4)
FortiMail	PDF files	4		00:08:00		WIN7X86VM(4)

The following options are available:

### Chart icon

Clicking the *Chart* icon beside the VM Type displays the VM's *Usage Chart*.

### Trash icon

Clicking the *Trash* icon beside the Pending Job Number purges the job queue.

### Prioritize

Clicking the *Prioritize* button takes you to the *Job Queue Priority List* page where you can adjust the list.

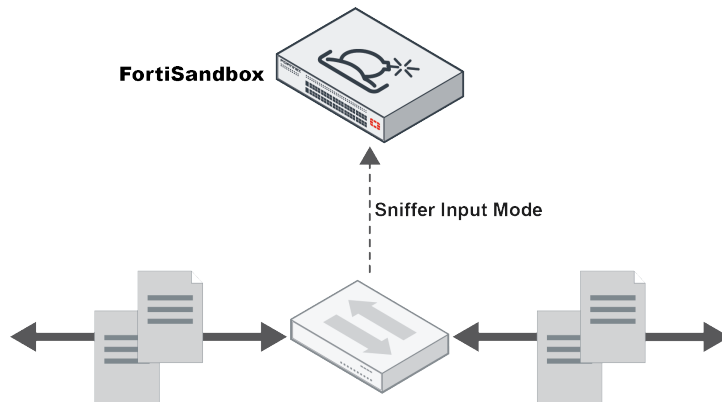
The following information is displayed:

### Input Source

The type of Input Source. Input source types can be the following values:

	<ul style="list-style-type: none"> <li>• On Demand</li> <li>• File RPC</li> <li>• Device</li> <li>• Sniffer</li> <li>• Adapter</li> <li>• Network Share</li> <li>• URL On Demand</li> <li>• URL RPC</li> <li>• URL Device</li> <li>• URL Adapter</li> </ul>
<b>File Type</b>	<p>File types can be one of the following values:</p> <ul style="list-style-type: none"> <li>• Executables /DLL/VBS/BAT/PS1/JAR/MSI/WSF files</li> <li>• Microsoft Office files (Word, Excel, Powerpoint etc)</li> <li>• Adobe Flash files</li> <li>• Archive files (extensions: .7z, .xz, .bz2, .gz, .tar, .zip, .Z, .kbg, .ace, etc.)</li> <li>• PDF files</li> <li>• Static Web files</li> <li>• Android files</li> <li>• MACOSX files</li> <li>• URL detection</li> <li>• User defined extensions</li> <li>• Job Queue Assignment Pending files (files received from input sources and not yet processed)</li> <li>• Non Sandboxed files (files that do not enter the Sandboxing scan step according to the current Scan Profile settings. If the Scan Profile settings are changed, they may enter the Sandboxing scan step eventually.)</li> </ul>
<b>Queued #</b>	<p>Current pending job number.</p> <p>A <i>Trash Can</i> appears beside the pending job number. Clicking on the <i>Trash Can</i> icon purges the job queue.</p> <p>Select the icon next to the <i>Non Sandboxing files</i> Input Source to expand the selection to view and purge non-sandboxing files separately.</p>
<b>Ave Scan Time in Last 24 hrs (s)</b>	Average scan time of one file in the last 24 hours, in seconds.
<b>Expected Finish Time</b>	The expected time when the pending jobs will finish.
<b>Arrival Rate (Last 1 hr)</b>	Files put in the Job Queue in the last hour.
<b>VM Type (Clone #)</b>	<p>The VM type with its clone number.</p> <p>A <i>Chart</i> icon appears beside the VM Type (Clone#). If you click on the <i>Chart</i> icon, the VM's usage chart appears. This chart shows a rough percentage of used clones of this VM type across time. If the usage percentage is consistently at a high level across time, the user should consider allocating more clone numbers to it.</p>

## Sniffer



Sniffer mode relies on inputs from spanned switch ports. It is the most suitable infrastructure for adding protection capabilities to existing threat protection systems from various vendors.

Sniffer mode enables you to configure your FortiSandbox to sniff all traffic on specified interfaces. When files are received by FortiSandbox, they are executed and scanned within the VM modules. Sniffer mode supports the following protocols: HTTP, FTP, POP3, IMAP, SMTP, SMB and raw TCP protocol. To enable and configure sniffer settings, go to *Scan Input > Sniffer*.



FortiSandbox reserves port1 for device management and port3 for scanned files to access the Internet. Port1, , admin port, and the port used for cluster internal communication can not be used as a sniffed interface.



In FortiSandbox you can select to sniff multiple interfaces. For example, when FortiSandbox is deployed with a network tap device you can sniff both the incoming and outgoing traffic on separate FortiSandbox interfaces.

Sniffer Settings	
<input checked="" type="checkbox"/>	Enable file based detection
<input checked="" type="checkbox"/>	Enable network alert detection
<input type="checkbox"/>	Keep incomplete files
<input checked="" type="checkbox"/>	Enable conserve mode
Max file size:	<input type="text" value="100"/> KB (The limit of max file size is 200,000 KB)
Sniffed Interfaces:	
<input checked="" type="checkbox"/>	port2
<input type="checkbox"/>	port4
<input type="checkbox"/>	port5
<input type="checkbox"/>	port6
Service Types:	
<input checked="" type="checkbox"/>	FTP
<input checked="" type="checkbox"/>	HTTP
<input checked="" type="checkbox"/>	IMAP
<input checked="" type="checkbox"/>	OTHER
<input checked="" type="checkbox"/>	POP3
<input checked="" type="checkbox"/>	SMB
<input checked="" type="checkbox"/>	SMTP
File Types:	<input type="text"/> <input type="button" value="Add"/>
<input type="checkbox"/>	All (the following file types and any other file type)
<input checked="" type="checkbox"/>	bzip
<input checked="" type="checkbox"/>	bzip2
<input checked="" type="checkbox"/>	cab
<input checked="" type="checkbox"/>	com
<input checked="" type="checkbox"/>	doc
<input checked="" type="checkbox"/>	exe
<input checked="" type="checkbox"/>	flash
<input checked="" type="checkbox"/>	gzip
<input type="checkbox"/>	html
<input checked="" type="checkbox"/>	jar
<input checked="" type="checkbox"/>	java
<input checked="" type="checkbox"/>	js
<input checked="" type="checkbox"/>	pdf
<input checked="" type="checkbox"/>	ppt
<input checked="" type="checkbox"/>	rar
<input checked="" type="checkbox"/>	tar
<input checked="" type="checkbox"/>	zip
<input checked="" type="checkbox"/>	URLs in Email
Extract and scan URLs in Email message body, up to	<input type="text" value="3"/> URLs (1 to 5)
<input type="button" value="OK"/>	

Configure the following settings:

<b>Enable file based detection</b>	Select the checkbox to enable file based detection.
<b>Enable network alert detection</b>	<p>Select the checkbox to enable network alerts detection. This feature detects sniffed live traffic for connections to botnet servers and intrusion attacks and visited suspicious web sites with Fortinet IPS and Web Filtering technologies. Alerts can be viewed in the <i>Network Alerts</i> page.</p> <p>For URL visits, certain categories can be treated as benign in <i>Scan Policy &gt; URL Category</i>.</p>
<b>Keep incomplete files</b>	Keep files without completed TCP sessions. Select the checkbox to keep incomplete files. Sometimes incomplete files can be useful to detect known viruses.
<b>Enable Conserve mode</b>	When conserve mode is enabled, if there are already too many jobs in the pending queue (250K, or sniffed traffic throughput exceeds optimal throughput), sniffer will enter conserve mode, during which time only executable (.exe) and MS Office files are extracted.



	<p>Optimal traffic throughput values for different models:</p> <ul style="list-style-type: none"> <li>• FSA-1000D: 1Gbps</li> <li>• FSA-2000E: 4 Gbps</li> <li>• FSA-3000D: 4.6 Gbps</li> <li>• FSA-3000E: 8 Gbps</li> <li>• FSA-3500D: 2 Gbps</li> <li>• FSA-VM00: 1Gbps</li> <li>• FSA-VM-BASE: 4.6Gbps</li> </ul>
<b>Maximum file size</b>	<p>The maximum size of files captured by sniffer. Enter a value in the text box. The default value is 2048kB and the maximum file size is 200,000kB.</p> <p><b>Note:</b> Files that exceed the maximum file size will not be sent to FortiSandbox.</p>
<b>Sniffed Interfaces</b>	Select the interface to monitor.
<b>Service Types</b>	<p>Select the traffic protocol that the sniffer will work on. Options include: <i>FTP</i>, <i>HTTP</i>, <i>IMAP</i>, <i>POP3</i>, <i>SMB</i>, <i>OTHER</i> and <i>SMTP</i>.</p> <p>The <i>OTHER</i> service type is for raw TCP protocol traffic.</p>
<b>File Types</b>	<p>Select the file types to extract from traffic. When <i>All</i> is checked, all files in the traffic will be extracted. Users can also add extra file extensions by putting it in <i>File Types</i> field and clicking <i>Add &gt; OK</i>. The user can delete it later by clicking the <i>Trash</i> can icon beside it and clicking <i>OK</i>.</p> <p>When <i>URLs in Email</i> type is selected, URLs embedded inside Email body will be extracted and scanned as <i>WEblink</i> type. User can define the number of URLs to extract for each Email, from 1 to 5.</p>



When an interface is used in sniffer mode, it will lose its IP address. The interface settings cannot be changed.

## Device

In Device mode, you can configure your FortiGate, FortiWeb, FortiClient EMS, FortiClient or FortiMail devices to send files to your FortiSandbox. For FortiGate, you can select to send all files for inspection. For FortiMail, you can select to send email attachments or URLs in the email body to FortiSandbox for inspections or just the Suspicious ones. When files or URLs are received by FortiSandbox, they are executed and scanned within the VM modules. FortiSandbox also sends statistics back to the FortiGate, FortiWeb and FortiMail. When integrated with FortiGate, the following protocols are supported: HTTP, FTP, POP3, IMAP, SMTP, MAPI, IM, and their equivalent SSL encrypted versions. To view, edit, and authorize devices, go to *Scan Input > Device*.

For FortiOS 5.2.3 and later, the FortiGate can query a file's verdict, and retrieve detailed information from FortiSandbox.

For FortiOS 5.4.0 and later, the FortiGate can download Malware packages and URL packages from FortiSandbox as complementary AV signatures and web filtering blocklists. These packages contain detected malware signatures and their downloading URLs.



The default file size scanned and forwarded by FortiGate is 10MB and the maximum depends on the memory size of the FortiGate. You can change the file size on the FortiGate side using the following CLI command:

```
config firewall profile-protocol-options
edit <name_str>
config http
set oversize-limit <size_int>
end
end
```

**Note:** The `profile-protocol-options` setting decides the maximum file size that will be AV scanned on the FortiGate. After a virus scan verdict has been made (Clean or Suspicious), if the file's size is less than `analytics-max-upload` size, it will be set over to FortiSandbox according to *Send All/Suspicious Only* settings on the FortiGate.

For more information on configure the oversize limit for `profile-protocol-options` and `analytics-max-upload`, see the *FortiOS CLI Reference* in the [Fortinet Document Library](#).

The following options are available:

<b>Refresh</b>	Click the <i>Refresh</i> icon to refresh the entries displayed after applying search filters.
<b>Device Filter</b>	Users can filter devices by entering part of device name or serial number.
<b>Clear all removable filters</b>	Click the <i>Trash can</i> icon to clear all removable filters.

This page displays the following:

<b>Device Name</b>	The name of the device and the VDOM or protected email domain that send files to FortiSandbox. For device, it has the format of: <i>Device Name</i> . For VDOM, it has the format of: <i>Device Name: VDOM Name</i> . For a FortiMail protected domain, it has the format: <i>Device Name : Domain Name</i> .
<b>Serial</b>	The FortiGate, FortiWeb, FortiClient, FortiClient EMS, or FortiMail serial number.
<b>Malicious</b>	The number of malicious files submitted by the device to FortiSandbox in the last seven days. FortiClient EMS displays the number of malicious files submitted to FortiSandbox by FortiClient endpoints that are managed by EMS.
<b>High</b>	The number of high risk files submitted by the device to FortiSandbox in the last seven days. FortiClient EMS displays the number of high risk files submitted to FortiSandbox by FortiClient endpoints that are managed by EMS.
<b>Medium</b>	The number of medium risk files submitted by the device to FortiSandbox in the last seven days. FortiClient EMS displays the number of medium risk files submitted to FortiSandbox by FortiClient endpoints that are managed by EMS.
<b>Low</b>	The number of low risk files submitted by the device to FortiSandbox in the last seven days. FortiClient EMS displays the number of low risk files submitted to FortiSandbox by FortiClient endpoints that are managed by EMS.
<b>Clean</b>	The number of clean files submitted by the device to FortiSandbox in the last seven days. FortiClient EMS displays the number of clean files submitted to FortiSandbox by FortiClient endpoints that are managed by EMS.

<b>Others</b>	The number of other files submitted by the device to FortiSandbox in the last seven days. FortiClient EMS displays the number of other rating files submitted to FortiSandbox by FortiClient endpoints that are managed by EMS.
<b>Malware Pkg</b>	The malware package version currently on the device.
<b>URL Pkg</b>	The URL package versions currently on the device.
<b>Authorized</b>	If the device or VDOM/Protected Domain is authorized to submit files. Only authorized device or VDOM/Protected Domain is allowed to submit files to FortiSandbox.
<b>Limit</b>	If a submission limit is set for this device.
<b>Status</b>	The status of the device. This field displays an <i>Up</i> icon when the device is connected and a <i>Down</i> icon for devices which are disconnected. If a device, its VDOM, or protected domain does not contact FortiSandbox for more than 15 minutes, the status will change to <i>Disconnected</i> .
<b>Delete</b>	Click to delete the device or VDOM/Protect Domain. If a device is deleted, all its VDOMs/Protected Domains will also be deleted. If the device is FortiClient EMS, its managed FortiClient endpoints are still kept. If the device connects to FortiSandbox later, it will show up again as a new device.



FortiSandbox uses a Fortinet proprietary traffic protocol (OFTP) to communicate with connected devices. This communication occurs on TCP port 514. The traffic is encrypted.

## Supported Devices

You can configure your Fortinet devices, such as FortiGate to send files to FortiSandbox for inspection and analysis. These devices query scan results and retrieves scan details. Device can also download Malware packages as a complimentary AV signature database to block future appearances of the same malware and download URL packages as complimentary web filtering blacklist.

FortiSandbox supports the following devices:

<b>FortiGate</b>	<p>FortiSandbox is able to perform additional analysis on files that have been AV scanned by your FortiGate. You can configure your FortiGate to send all files or only suspicious files passing through the AV scan.</p> <p>FortiGate can retrieve scan results and details from FortiSandbox, and also receive antivirus and web filtering signatures to supplement the current signature database.</p> <p>When FortiGate learns from FortiSandbox that a terminal is infected, the administrator can push instruction for self-quarantine on a registered FortiClient host.</p>
<b>FortiMail</b>	<p>You can configure your FortiMail to send suspicious, high risk files and suspicious attachments. FortiSandbox is able to perform additional analysis on files that have been scanned by your FortiMail email gateway.</p> <p>Suspicious email attachments include:</p> <ul style="list-style-type: none"> <li>Suspicious files detected by heuristic scan of the AV engine.</li> </ul>

- Executable files and executable files embedded in archive files.
  - Type 6 hashes (binary hashes) of spam email detected by FortiGuard AntiSpam service.
- Recent release of FortiMail build can send suspicious URLs in the email body to FortiSandbox to do URL scans and block suspicious emails based on the scan result.

**FortiWeb**

You can now use a file upload restriction policy to submit uploaded files to FortiSandbox for evaluation. FortiSandbox evaluates whether the file poses a threat and returns the result to FortiWeb. If FortiSandbox determines that the file is malicious, FortiWeb performs the following tasks:

- Generates an attack log message that contains the result (for example, messages with the Alert action in the illustration).
- For 10 minutes after it receives the FortiSandbox results, takes the action specified by the file upload restriction policy. During this time, it does not re-submit the file to FortiSandbox (for example, messages with the Alert\_Deny action in the illustration).

**FortiClient EMS**

FortiClient EMS administrators can configure a FortiSandbox IP address in an endpoint profile. After the configuration is saved, FortiClient EMS attempts to submit an authorization request to the configured FortiSandbox. FortiSandbox administrators can authorize it and set limitations about submission speed. Subsequently, all FortiClient endpoints managed by FortiClient EMS are considered authorized by the same FortiSandbox and follow the submission speed limit.

**FortiClient**

FortiSandbox can accept files from FortiClient to perform additional analysis, while FortiClient holds the files until the scan results are received. FortiClient will also receive additional antivirus signatures from FortiSandbox, generated from scan results, to supplement current signatures.

## FortiGate devices

### To verify the FortiGate is connected to FortiSandbox:

On your FortiSandbox device, go to *Scan Input > Devices*. Your FortiGate device and VDOMs will be listed on this page.

The communication protocol does not include a way for the FortiGate to notify FortiSandbox whether VDOMs are enabled. When VDOMs are disabled on the FortiGate, the files received from the FortiGate will be marked with *vdom=root*.



Since the FortiGate does not explicitly send a list of possible VDOMs to FortiSandbox, the FortiSandbox only learns about a VDOM once it receives a file associated with it. Each of the devices VDOMs listed on this page will only be displayed after the first file has been received from that specific VDOM.

If VDOMs are enabled on your FortiGate, you can select the checkbox to have new VDOMs inherit authorization based on the device level setting. If the FortiGate authorization is disabled, all VDOMs under it will not be authorized even if authorization is enabled for a VDOM.

### To edit FortiGate settings in FortiSandbox:

1. On your FortiSandbox device, go to *Scan Input > Device*. All FortiGate devices and VDOMs will be listed on this page.

2. Click the device name. The *Edit FortiGate Settings* page opens.
3. Edit the following settings:

Device Status	
<b>Serial Number</b>	The device serial number is displayed.
<b>Alias</b>	The host name of the FortiGate unit. This is a read-only value.
<b>IP</b>	The IP address of the FortiGate is displayed.
<b>Status</b>	The status of the device, either connected or not connected. This field cannot be edited.
<b>Last Modified</b>	The date and time that the FortiGate settings were last changed is displayed.
<b>Last Seen</b>	The date and time that the FortiGate last connected to the FortiSandbox is displayed.
Permissions	
<b>Authorized</b>	Select the checkbox to authorize the FortiGate device. If this field is not checked, files sent from the FortiGate will be dropped. The date and time that the authorization status was changed is displayed.
<b>New VDOMs/Domains inherit authorization</b>	Select the checkbox to have new VDOMs inherit the authorization setting configured at the device level.
Email Settings	
<b>Administrator Email</b>	The email address entered in the <i>Notifier Email</i> field configured on the FortiGate device at <i>System &gt; Config &gt; FortiSandbox</i> . You cannot edit this field on the FortiSandbox.
<b>Send Notifications</b>	Select the checkbox to send notifications. When notifications are enabled, you will receive email notifications when a file from your environment has been detected as potential malware. The email will contain a link to the scan job details page.  To receive notification emails, you must configure a mail server and enable <i>Send a notification email to the global email list when malicious files are detected</i> settings in <i>System &gt; Mail Server</i> . Otherwise, a warning icon is displayed.
<b>Send Reports</b>	Select the checkbox to send job detail PDF reports. To receive reports and define report generation frequency, you must configure mail server and enable <i>Send scheduled PDF report about an individual VDOM/Domain to its email address</i> in <i>System &gt; Mail Server</i> . Otherwise, a warning icon is displayed.

4. Click *OK* to save the settings.

#### To edit VDOM settings:

1. On your FortiSandbox device, go to *Scan Input > Device*. All FortiGate devices and VDOMs will be listed on this page.
2. Click the VDOM name.

## 3. Edit the following settings:

Device Status	
<b>Domain/VDOM</b>	The device VDOM name. This field cannot be edited.
<b>Alias</b>	VDOM name is in the <i>Device Name: VDOM name</i> format.
<b>IP</b>	The IP address of the FortiGate. This field cannot be edited.
<b>Status</b>	The status of the device, either connected or not connected. This field cannot be edited.
<b>Files Transmitted</b>	The total number of files transmitted to FortiSandbox in the last seven days.
<b>Last Modified</b>	The date and time that the authorization status was changed. This field cannot be edited.
<b>Last Seen</b>	The date and time that the FortiGate VDOM last connected to the FortiSandbox. This field cannot be edited.
Permissions & Policy	
<b>Authorized</b>	Select the checkbox to authorize the FortiGate VDOM.
<b>Submission Limitation</b>	Limit the VDOM submission speed. Specify the number of submissions per <i>Hour, Day, or Unlimited</i> . When limitation is reached, FSA will send a signal to FGT to stop file submission. This will save resources on both sides.
<b>Send Reach Limit Alert Email</b>	When checked, an alert email is sent to the VDOM email address when limitation is reached.
<b>Email Settings</b>	If this field is checked, when submission limitation is reached, an alert email will be sent to VDOM email address. A mail server should be configured.
<b>Email</b>	Enter the Administrator Email address for the VDOM, separated by a comma.
<b>Send Notifications</b>	Select checkbox to send notifications when viruses or malware from this VDOM is detected. To receive notification emails, you must configure a mail server and enable <i>Send a notification email to the global email list when malicious files are detected</i> settings in <i>System &gt; Mail Server</i> . Otherwise, a warning icon is displayed.
<b>Send PDF Reports</b>	Select checkbox to send PDF reports of jobs. To receive reports and define report generation frequency, you must configure <i>System &gt; Mail Server</i> page. Also the <i>Send scheduled PDF report about an individual VDOM/Domain to its email address</i> in that page should be checked. Otherwise, a warning icon is displayed.

## 4. Click OK to save the settings.

## FortiMail Devices

In FortiMail version 5.2.0 or later, you can configure your FortiMail device to send suspicious files, URLs, and suspicious attachments to FortiSandbox for inspection and analysis. FortiSandbox statistics for total detected and total clean are displayed on FortiMail.

If FortiMail sends over protected domain information, those domain names and jobs counts of them are listed. For each protected domain, the user can set a submission limitation.

If protected domain information is not available, such as files from older versions of FortiMail or outgoing emails, jobs from them will be grouped in Unprotected domain name.

For more information on how to configure FortiMail to send files to FortiSandbox, please refer to the *FortiMail Administration Guide* available in the [Fortinet Document Library](#).

### To edit FortiMail Settings in FortiSandbox:

1. On your FortiSandbox device, go to *Scan Input > Device*.  
All FortiMail devices and protected domains will be listed on this page. Since the FortiMail does not explicitly send a list of possible protected domains to FortiSandbox, the FortiSandbox only learns about a domain once it receives a file or URL sent to it. Each of the domains listed on this page will only be displayed after the first file or URL has been received to that specific domain.
2. Click the FortiMail device name. The *Edit Device Settings* page opens.

## 3. Edit the following settings:

Device Status	
<b>Serial Number</b>	The device serial number.
<b>Alias</b>	The host name of the FortiMail unit. This is a read-only value.
<b>IP</b>	The IP address of the FortiMail.
<b>Status</b>	The status of the device, either connected or disconnected. This field cannot be edited.
<b>Last Modified</b>	The date and time that the FortiMail settings were last changed.
<b>Last Seen</b>	The date and time that the FortiMail last connected to the FortiSandbox.
Permissions	
<b>Authorized</b>	Select the checkbox to authorize the FortiMail device. If this field is not checked, files sent from the FortiMail will be dropped. The date and time that the authorization status was changed.
<b>New VDOMs/Domains Inherit Authorization</b>	Select the checkbox to have protected domains inherit the authorization setting configured at the device level.
Email Settings	
<b>Administrator Email</b>	The email address entered in the <i>Notifier Email</i> field configured on the FortiMail device. You cannot edit this field on the FortiSandbox.
<b>Send Notifications</b>	Select the checkbox to send notifications. When notifications are enabled, you will receive email notifications when a file inside an email has been detected as potential malware. The email will contain a link to the scan job details page. To receive notification emails, you must configure a mail server and enable the <i>Send a notification email to the global email list when malicious files are detected</i> setting in System > Mail Server. Otherwise, a warning icon is displayed.
<b>Send Reports</b>	Select the checkbox to send job detail PDF reports. To receive reports and define report generation frequency, you must configure System > Mail Server page. Also, the <i>Send scheduled PDF report about an individual VDOM/Domain to its email address</i> in that page should be checked. Otherwise, a warning icon is displayed.

4. Click *OK* to save the settings.**To edit Domain settings:**

1. On your FortiSandbox device, go to *Scan Input > Device*. All FortiMail devices and protected Domains will be listed on this page.
2. Click the domain name.



## 3. Edit the following settings:

Device Status	
<b>Domain/VDOM FQDN</b>	The protected domain name. This field cannot be edited.
<b>Alias</b>	The value is <i>FortiMail Device Name: Domain name</i> .
<b>IP</b>	The IP address of the FortiMail . This field cannot be edited.
<b>Status</b>	The status of the device, either connected or disconnected. This field cannot be edited.
<b>Files/URLs Transmitted</b>	The total number of files and URLs sent to the domain in the last seven days.
<b>Last Modified</b>	The date and time that the authorization status was changed. This field cannot be edited.
<b>Last Seen</b>	The date and time that last file/URL sent to this domain
Permissions and Policy	
<b>Authorized</b>	Select the checkbox to authorize the FortiMail domain.
<b>Submission Limitation</b>	Limit the FortiMail submission speed regarding to a protected domain. Specify the number of submissions per <i>Hour, Day, or Unlimited</i> . When limitation is reached, FSA will reject files and URLs to this domain. <b>Note:</b> This feature is only working for new version FortiMail who can send over domain information.
<b>Send Reach Limit Alert Email</b>	When checked, an alert email is sent to the domain email address when limitation is reached.
<b>Email Settings</b>	If this field is checked, when submission limitation is reached, an alert email will be sent to domain email address.
<b>Email</b>	Enter the Administrator Email address for the domain, separated by a comma.
<b>Send Notifications</b>	Select checkbox to send notifications when viruses or malware to this domain is detected. To receive notification emails, you must configure a mail server and enable the <i>Send a notification email to the global email list when malicious files are detected</i> setting in <i>System &gt; Mail Server</i> . Otherwise, a warning icon is displayed.
<b>Send Reports</b>	Select checkbox to send PDF reports of jobs. To receive reports and define report generation frequency, you must configure the <i>System &gt; Mail Server</i> page. Also the <i>Send scheduled PDF report about an individual VDOM/Domain to its email address</i> in that page should be enabled. Otherwise, a warning icon is displayed.

4. Click *OK* to save the settings.

## Upload suspicious attachments to FortiSandbox

For more information on how to configure FortiMail e to send files to FortiSandbox, please refer to the *FortiMail Administration Guide* available on the [Fortinet Document Library](#).

## Device and VDOM/Domain level notifications

When enabling *Send notifications* in the *Edit Device Settings* or *Edit VDOM/Domain Settings* page, you will receive an email every time a file from your environment has been detected as potential malware.

## Device and VDOM/Domain level PDF reports

When enabling *Send PDF reports* in the *Edit Device Settings* or *Edit VDOM/Domain Settings* page, you will receive a PDF report by email at defined moment in *Config > Mail Server* page. This email will contain a FortiSandbox Summary Reports PDF. The report lists statistics of scan jobs from the defined previous time period configured from the *System > Mail Server* page. This report contains the following information:

- Scanning Statistics: A table listing the number of files processed by FortiSandbox and a breakdown of files by rating.
- Scanning Statistics by Type: A table listing the file type, rating and event count.
- Scanning Activity: A table and graph listing the number of clean, suspicious, and malicious files processed by FortiSandbox per day.
- Top Targeted Hosts: A list of the top targeted hosts.
- Top Malware Files: A list of the top malware programs detected by FortiSandbox.
- Top Infectious URLs: A list of the top infectious URLs detected by FortiSandbox.
- Top Callback Domains: A list of the top call back domains detected by FortiSandbox.

## FortiWeb Devices

For more information on how to configure FortiWeb to send files to FortiSandbox, please refer to the *FortiWeb Administration Guide* available in the [Fortinet Document Library](#).

## FortiClient EMS Devices

For more information on how to configure FortiClient EMS to send files to FortiSandbox, please refer to the *FortiClient EMS Administration Guide* available in the [Fortinet Document Library](#).

### To edit EMS settings in FortiSandbox:

1. On your FortiSandbox device, go to *Scan Input > Device*.
2. Click the device name. The *Edit Device Settings* page opens.

## 3. Edit the following settings:

Device Status	
<b>Serial Number</b>	The device serial number is displayed.
<b>Hostname</b>	The host name of the EMS unit. This is a read-only value.
<b>IP</b>	The IP address of the EMS is displayed.
<b>Status</b>	The status of the device, either connected or not connected. This field cannot be edited.
<b>Last Modified</b>	The date and time that the EMS settings were last changed is displayed.
<b>Last Seen</b>	The date and time that the EMS last connected to the FortiSandbox is displayed.
Permissions	
<b>Authorized</b>	Select the checkbox to authorize the EMS device. All FortiClient endpoints that are managed by EMS will inherit this authorization setting.
<b>Submission Limitation</b>	Limit submission speed of FortiClient endpoints that are managed by EMS. Specify the number of submissions per Hour, Day, or Unlimited. When limitation is reached, FortiSandbox will send a signal to FortiClient to stop file submission. This will save resources on both sides.

4. Click *OK* to save the settings.

## FortiClient

FortiClient 5.4 and previous versions can silently connect to FortiSandbox without needing to be authorized. Users can de-authorize a FortiClient host manually. If a FortiClient endpoint is managed by EMS, it will follow the authorization status and file submission speed setting of EMS. Users can change them manually.

For more information on how to configure FortiClient to send files to FortiSandbox, please refer to the *FortiClient Administration Guide* on the [Fortinet Document Library](#).

To view connected FortiClient endpoints in FortiSandbox, go to *Scan Input > FortiClient*.

The following options are available:

<b>Refresh</b>	Click the <i>Refresh</i> icon to refresh the entries displayed after applying search filters.
<b>Device Filter</b>	Users can filter FortiClient by entering part of host name, host IP or serial number.

This page displays the following information:

<b>FCT Serial</b>	The FortiClient serial number.
<b>Hostname</b>	Hostname.
<b>User</b>	Current login user on the FortiClient host, if the information is available.
<b>IP</b>	Host IP Address.

<b>Malicious</b>	The number of malicious files forwarded by the FortiClient to FortiSandbox in the last seven days. Malicious files are not executed in the FortiSandbox VM module as the antivirus scanner has already determined the file rating.
<b>High Risk</b>	The number of high risk rating files submitted to FortiSandbox in the last seven days.
<b>Medium Risk</b>	The number of medium rating risk files submitted to FortiSandbox in the last seven days.
<b>Low Risk</b>	The number of low risk rating files submitted to FortiSandbox in the last seven days.
<b>Clean</b>	The number of clean rating files submitted to FortiSandbox in the last seven days.
<b>Others</b>	The number of other rating files submitted by FortiGate or FortiMail to FortiSandbox in the last seven days.
<b>Malware Pkg</b>	The malware package currently on the device.
<b>URL Pkg</b>	The URL package versions currently on the device.
<b>Auth</b>	If the FortiClient is authorized. The user can click on the FortiClient serial number and modify its authorization status manually.
<b>Limit</b>	If a submission limit is set for this device.
<b>Status</b>	The status of the FortiClient host. This field displays an up icon when the device is connected and a down icon for devices which are disconnected.
<b>Delete</b>	Click to delete the FortiClient. If FortiClient connects to FortiSandbox later, it will show up again as a new one.

#### To edit FortiClient settings in FortiSandbox:

1. On your FortiSandbox device, go to *Scan Input > FortiClient*.
2. Click the device name. The *Edit FortiClient Settings* page opens.

## 3. Edit the following settings:

FortiClient Status	
<b>Serial Number</b>	The device serial number is displayed.
<b>Hostname</b>	The host name of the FortiClient unit. This is a read-only value.
<b>IP</b>	The IP address of the FortiClient is displayed.
<b>Status</b>	The status of the device, either connected or not connected. This field cannot be edited.
<b>Files Transmitted</b>	The total number of files transmitted to FortiSandbox in the last seven days.
<b>Last Seen</b>	The date and time that FortiClient last connected to FortiSandbox is displayed.
Permissions	
<b>Authorized</b>	Click the checkbox to toggle the authorization device.
<b>Submission Limitation</b>	Limit submission speed. Specify the number of submissions per Hour, Day, or Unlimited. When limitation is reached, FortiSandbox will send a signal to FortiClient to stop file submission. This will save resources on both sides.

4. Click *OK* to save the settings.

A FortiSandbox system, either a Standalone unit or a cluster system has no number limitation on authorized devices and FortiClients. However, the concurrent connections of all client devices is limited to 30,000.

## Adapter

FortiSandbox uses adapters to connect to third party products. Carbon Black/Bit9 server, ICAP and Mail gateway clients are supported.

With an Adapter, FortiSandbox can analyze files downloaded from the Carbon Black server to send notifications of file verdict back to the server, or receive HTTP message from an ICAP client and return a response to it.

FortiSandbox supports the BCC adapter to receive forwarded emails from an upstream email gateway and scan them. FortiSandbox will extract email attachments and URLs in an email body and send them to the Job Queue.



The BCC adapter feature is for information only, it will not block any email. FortiSandbox includes an MTA adapter, which can be used to inspect and quarantine suspicious emails. For detailed information, please refer to the FortiSandbox user guide in the AWS marketplace.

The following options are available:

<b>Create New</b>	Create a new adapter. ICAP and BCC adapters are automatically created by the system.
-------------------	---

<b>Edit</b>	Edit an adapter.
<b>Delete</b>	Delete an adapter. ICAP and BCC adapters cannot be deleted.

This page displays the following information:

<b>Adapter Name</b>	The Adapter's name. When the adapter type is ICAP, the value is ICAP. When the adapter type is BCC, the value is BCC.
<b>Vendor Name</b>	Vendor name. When the adapter type is ICAP, the value is ICAP. When the adapter type is BCC, the value is BCC.
<b>Serial</b>	Serial number. When the adapter type is ICAP, the value is ICAP. When the adapter type is BCC, the value is BCC.
<b>FQDN/IP</b>	FQDN/IP address. When the adapter type is ICAP, the value is empty. When the adapter type is BCC, the value is empty.
<b>Malicious</b>	File and URL count of Malicious rating from this Adapter in the last seven days. Separated by  .
<b>High</b>	File and URL count of Highly Suspicious rating from this Adapter in the last seven days. Separated by  .
<b>Medium</b>	File and URL count of Medium rating from this Adapter in the last seven days. Separated by  .
<b>Low</b>	File and URL count of Low rating from this Adapter in the last seven days. Separated by  .
<b>Clean</b>	File and URL count of Clean rating from this Adapter in the last seven days. Separated by  .
<b>Other</b>	File and URL count of Other rating from this Adapter in the last seven days. Separated by  .

#### To create a new adapter:

1. Go to *Scan Input > Adapter*.
2. Click the + *Create New* button from the toolbar.

**3. Configure the following:**

<b>Vendor Name</b>	Select <i>Carbon Black/Bit9</i> as the vendor name.
<b>Adapter Name</b>	Enter the adapter name.
<b>Server FQDN/IP</b>	Enter the FQDN/IP address of the Carbon Black server.
<b>Token</b>	Enter the token string. Authentication token is assigned by the Carbon Black or ICAP server.
<b>Timeout (seconds)</b>	Enter the timeout value.
<b>Serial</b>	Auto-generated serial number for this adapter. It works as a device serial number to denote file's input device.

**4. Click OK to save the entry.****To edit an adapter:**

1. Go to *Scan Input > Adapter*.
2. Select an adapter.
3. Click the *Edit* button from the toolbar.
4. Make edits as necessary.

When the adapter type is ICAP, the user can:

- Enable or disable FortiSandbox to work as an ICAP server.
- Define the port for encrypted and non-encrypted communication ports with the client.
- Extract URLs or files from HTTP messages from the client and put them into the Job Queue.
- Define which ratings are treated as bad to return a block code.
- Enable a *Real Time AV Scan* for a faster response of a known virus before a file is put into the job queue.

ICAP Settings

Status

Enable

☒

Connection

Port

1344

SSL Support

☐

Methods

Receive URL

☒

URLs with selected risk and above will be blocked:

Low Risk Medium Risk High Risk

Receive File

☒

Files with selected risk and above will be blocked:

Low Risk Medium Risk High Risk

Realtime AV Scan

☐

Apply

Back

When the adapter type is BCC, the user can:

- Enable or disable FortiSandbox to work as an email server.
- Enable Parse URL to allow FortiSandbox to extract the first three URLs in an email.
- Input the SMTP port number that FortiSandbox listens on to receive emails. The default port number is 25.
- Select the interface port that FortiSandbox listens to. The default is port1.

FortiSandbox 3500D Adapter

Dashboard

FortiView

Network

System

Virtual Machine

Scan Policy

Scan Input

BCC Settings

Status

Enable

☒

Options

Parse URL

☒

Connection

SMTP Port

25

Interface:

port1

Apply

Back

FortiSandbox 3.0.7 Administration Guide  
Fortinet Technologies Inc.

136



- Click *Apply* to save the entry.

### To delete an adapter

- Go to *Scan Input > Adapter*.
- Select an adapter.  
ICAP and BCC adapters cannot be selected.
- Click the *Delete* button from the toolbar.
- Click *Yes I'm sure* button from the *Are you sure* confirmation box.



After a Carbon Black adapter is created, FortiSandbox will try to communicate with Carbon Black server. If the connection and authentication is successful, the status column will show a green icon, otherwise a red icon is displayed.



CLI command: `diagnose-debug adapter` can be used to troubleshoot communications with the adapter clients.

## Configure Carbon Black/Bit9 Server

To be able to configure a Carbon Black (Bit9) server to work with FortiSandbox, you will need to login.

### Submitting selected files to FortiSandbox

Computers

Computers connected: 2    Total computers: 2    Current CL version: 862

Saved Views:

(none) ▾

Add

Group By:

(none) ▾

Ascending ▾

Days Disconnected:

(none) ▾



Show/Hide Filter ▾ | Show/Hide Columns ▾ | [Export to CSV](#) | [Refresh Page](#)

Action ▾

Search: 

Go

Clear

<input type="checkbox"/>	Computer Name ▲	Connected	Policy Status	Upgrade Status	Connected Enforcement	Disconnected Enforcement
<input type="checkbox"/>	 WORKGROUP\HENRYDU-PC	<div></div>	Up to date	Up to date	Low (Monitor Unapproved)	Low (Monitor Unapproved)
<input type="checkbox"/>	 WORKGROUP\WIN-KMIGPUGGB6H	<div></div>	Up to date	Up to date	High (Block Unapproved)	High (Block Unapproved)

2 items

Page 1/1

1. Go to **Assets > Computers**. All computers that are managed by the server will be listed.
2. In the left panel, select **Files on Computers**. All files will be listed on this computer.



3. Select one or more files.
4. Click the **Action button > Analyze with FortiSandbox**. The files will be submitted to FortiSandbox for analysis.

### Creating an event rule to automatically submit files to FortiSandbox

1. Go to **Rules > Event Rules**.
2. Click the **Create Rule** button.
3. Configure the settings.

## How to view analysis results

Go to *Reports > External Notifications*. All files analyzed by FortiSandbox will be listed.

## Configure ICAP Client

FortiSandbox can work as an ICAP server with any ProxySG that supports ICAP.

When ICAP client sends a HTTP request to FortiSandbox, FortiSandbox extracts the URL and checks if a verdict is available. If the verdict is not a *user selected blocking rating* or is not available, a 200 return code is sent back to client so the request can move on on the client side. If the verdict is *user selected blocking rating*, a 403 return code along with a block page is sent back to the client. If no verdict is available, the URL will be put into the Job Queue for a scan. URL scan flow will apply.

When the ICAP client sends a HTTP response to FortiSandbox, FortiSandbox extracts file from it and checks if verdicts are available. If verdicts are not a user selected blocking rating, a 200 return code is sent back to client so the response can be delivered to the endpoint host. If a verdict is *user selected blocking rating*, a 403 return code along with a block page is sent back to the client. If the user enables Realtime AV Scan, the file will be scanned by the AV Scanner. If the file is a known virus, a 403 return code along with a blocked page is sent back to the client. If no verdict is available, these files will be put into the Job Queue for a scan. File scan flow will apply.

When ICAP client sends a preview request, FortiSandbox returns a 204 return code, which means it is not supported.

The following is an example ICAP configurations for a SQUID 4.x proxy server, which should be added to the end of `squid.conf` file:

```
cache deny all
icap_enable on
icap_send_client_ip on
icap_send_client_username on
icap_client_username_header X-Authenticated-User
icap_preview_enable off
icap_persistent_connections off
icap_service svcBlocker1 reqmod_precache icap://fortisandbox_ip:port_number/reqmod bypass=0
    ipv6=off
adaptation_access svcBlocker1 allow all
icap_service svcLogger1 respmod_precache icap://fortisandbox_ip:port_number/respmod
    routing=on ipv6=off
adaptation_access svcLogger1 allow all
### add the following lines to support ssl ###
#icap_service svcBlocker2 reqmod_precache icaps://sandbox_ip:ssl_port_number/reqmod bypass=1
    tls-flags=DONT_VERIFY_PEER
#adaptation_access svcBlocker2 allow all
#icap_service svcLogger2 respmod_precache icaps://sandbox_ip:ssl_port_number/respmod
    bypass=1 tls-flags=DONT_VERIFY_PEER
#adaptation_access svcLogger2 allow all
```

## Configure FortiMail to integrate with FortiSandbox BCC Adapter

FortiSandbox has a BCC adapter to receive and scan forwarded emails from upstream MTA servers. FortiSandbox extracts attachment files and URLs from the email body and sends them to the job queue.



This feature is for information only, like sniffer mode. It will not block any email.

---

### To configure the FortiSandbox:

1. Enable the BCC adapter:
  - a. Go to *Scan Input > Adapter* in the navigation tree.
  - b. Select *BCC* and click *Edit* in the toolbar. The BCC adapter is disabled by default.
  - c. Enable the BCC adapter.
  - d. Enable *Parse URL* to allow the FortiSandbox to extract the first three URLs in an email.
  - e. Enter the SMTP port that the FortiSandbox listens on to receive emails. The default port is 25.
  - f. Select the interface that the FortiSandbox listens on. The default is port1.
  - g. Click *Apply*.
2. Enable file submission from the BCC adapter to create log events:
  - a. Go to *Scan Policy > General*.
  - b. Under *Enable log event of file submission*, select *BCC Adapter*.
  - c. Click *OK*.
3. View BCC adapter debug logs in run time, execute the following CLI command:  
`diagnose-debug adapter_bcc`  
For more information about the `diagnose-debug` command, see the *FortiSandbox CLI Reference*.

### To configure the upstream MTA (in this case a FortiMail device):

1. Go to *Profile > AntiSpam* and create a new AntiSpam profile:
  - a. Enable *Apply default action without scan upon policy match*.
  - b. Configure *BCC* as the default action.

- c. Edit the default action: enable BCC, and add a BCC address, such as *fortimail207@fsabcctest.com*.

The screenshot shows the FortiGate configuration interface. On the left, the 'AntiSpam Profile' section is expanded, showing 'Domain: --System--', 'Profile name: triggerall\_bcc', and 'Default action: bcc'. The 'Scan Configurations' section is also expanded, showing various scanning options like FortiGuard, Greylist, SPF check, DMARC check, Behavior analysis, Header analysis, Heuristic, SURBL, DNSBL, Banned word, Safelist word, Dictionary, Image spam, Bayesian, Suspicious newsletter, and Newsletter. The 'Scan Options' section is also expanded, showing options like Max message size to scan, Bypass scan on SMTP authentication, Scan PDF attachment, and Apply default action without scan upon policy match.

On the right, the 'Antispam Action Profile' dialog box is open. It shows 'Domain: system' and 'Profile name: bcc'. The 'BCC' option is checked. Below it, there is a list of BCC addresses, with 'fortimail207@fsabcctest.com' added. The 'Final action' is set to 'Discard'.

## 2. Go to *Policy > Recipient Policy*:

- Select the domain for forwarding emails to the FortiSandbox, and apply the new AntiSpam profile.
- Add a new inbound policy, select the domain for forwarding emails to the FortiSandbox, and apply the new AntiSpam profile.

The screenshot shows the 'Inbound Recipient Policy' configuration window. The 'Enable' checkbox is checked. The 'Domain' is set to 'ftntsandboxbcc.com'. The 'Sender Pattern' is set to 'User' with a pattern of '\* @ \*'. The 'Recipient Pattern' is set to 'User' with a pattern of '\* @ ftntsandboxbcc.com'. The 'Profiles' section shows 'AntiSpam: triggerall\_bcc', 'AntiVirus: --None--', 'Content: --None--', and 'Resource: Res\_Default'. The 'Advanced Settings' section is also visible.

- c. Add a new outbound policy, select the domain for forwarding emails to the FortiSandbox, and apply the new

## AntiSpam profile.

Outbound Recipient Policy

Enable: ☒

Domain:

Comments:

**Sender Pattern**

Type:   @

**Recipient Pattern**

Type:   @

**Profiles**

AntiSpam:

AntiVirus:

Content:

3. Go to *Policy > Access Control*:

- a. On the *Delivery* tab, add a TLS policy with a recipient pattern matching the previously added BCC address (in this example: *\*@fsabcctest.com*).
- b. Set *TLS Profile* as *none* or *Preferred*.

Message Delivery Rule

Enabled: ☒

Sender pattern:

Recipient pattern:

Destination IP/netmask:

TLS profile:

Encryption profile:

Comments:

**TLS Profile**

Profile name:

TLS level:

4. For the DNS server that your upstream mail server is accessing, add an MX record for the BCC email domain to resolve the FortiSandbox device's IP address. In the above example, the email domain is fsabcctest.com and the IP address is that of the port that is receiving the email.

## Network Share

FortiSandbox can scan files stored on a network share and optionally quarantine any malicious files. Go to *Scan Input > Network Share* to view and configure network share information.

Network share scans can be scheduled or run on-demand, and connectivity with the network share can be tested.

The following options are available:

<b>Create New</b>	Click to create a new network share.
<b>Edit</b>	Select an entry from the list and then click <i>Edit</i> in the toolbar to edit the entry selected.
<b>Delete</b>	Select an entry from the list and then click <i>Delete</i> in the toolbar to remove the entry selected.
<b>Scan Now</b>	Select an entry from the list and then click <i>Scan Now</i> in the toolbar to scan the entries.
<b>Scan Details</b>	Select an entry from the list and then click <i>Scan Details</i> in the toolbar to view the scheduled scan entries.
<b>Test Connection</b>	Select an entry from the list and then click <i>Test Connection</i> in the toolbar to test the connection. Result message will be displayed in the top message bar.

The following information is displayed:


<b>Name</b>	The name of the network share.
<b>Scan Scheduled</b>	The scan scheduled status. Scheduled network scans are done in parallel.
<b>Type</b>	The mount type.
<b>Share Path</b>	The file share path.
<b>Quarantine</b>	Displays if quarantine is enabled status.
<b>Enabled</b>	Displays if the network share is enabled. If a network share is disabled, its scheduled scan will not be executed.
<b>Status</b>	Displays the network share status. One of the following states: <ul style="list-style-type: none"> <li>• Network is Accessible</li> <li>• Network Down</li> </ul>

**To create a new network share:**

1. Go to *Scan Input > Network Share*.
2. Click the + *Create New* button from the toolbar.
3. Configure the following options:


**Enabled**

Select to enable network share configuration. If network share is not enabled, its scheduled scan will not run.

<b>Network Share Name</b>		Enter the network share name.
<b>Mount Type</b>	<p>Select the mount type from the dropdown list. The following options are available:</p> <ul style="list-style-type: none"> <li>• CIFS (SMB v1.0, v2.0, v2.1, v3.0) For Microsoft DFS, CIFS mount type should be used, and only SMB v1.0 is supported.</li> <li>• NFSv2</li> <li>• NFSv3</li> <li>• NFSv4</li> <li>• Azure File Share</li> <li>• AWS S3</li> </ul> <hr/> <div style="display: flex; align-items: center;">  <p>For domain-based DFS namespace, the domain name should be able to be resolved with the system Primary DNS server.</p> </div> <hr/>	
<b>SMB and NFS Settings</b>	<b>Server Name/IP</b>	Enter the server fully qualified domain name (FQDN) or IP address.
	<b>Share Path</b>	Enter the file share path. In the format <code>/path1/path2</code>
	<b>Username</b>	Enter a user name. For a domain users, use format <code>domain_name\user_name</code> .
	<b>Password</b>	Enter the password.
	<b>Confirm Password</b>	Enter the password a second time for verification.
<b>Azure File Share Settings</b>	<b>Domain of the Share URL</b>	Enter the Azure file share URL's domain name, found in the Azure server's menu at <i>Storage Accounts &gt; storage account name &gt; Settings &gt; Properties &gt; URL</i> .
	<b>Path of the Share URL</b>	Enter the path of the URL, found in the Azure server's menu at <i>Storage Accounts &gt; storage accounts name &gt; File Service &gt; Files &gt; Share path starting with /</i> .
	<b>Name of the Storage Account</b>	Enter the name of the storage account, found in the Azure server's menu at <i>Storage Account &gt; storage account name</i> .
	<b>Access Key of the Account</b>	Enter the access key of the account, found in the Azure server's menu at <i>Storage Account &gt; storage account name &gt; Settings &gt; Access Keys</i> .
	<b>Confirm Access Key</b>	Confirm the access key.
<b>AWS S3 Settings</b>	<b>AWS S3 Bucket Name</b>	Enter the bucket name, found in the AWS management console in the <i>S3 Service</i> page.
	<b>S3 Bucket Folder Path</b>	Enter the folder's path, starting with <code>/</code> .



<b>AWS IAM Access Key ID</b>	Enter the access key ID. To find the key ID, go to the AWS management console, click on the username in the top-right of the page, then click the <i>Security Credentials</i> link to generate the access key ID.
<b>Secret Access Key</b>	Enter the secret key matching the access key ID. The secret access key is displayed when you generate the access key ID.
<b>Confirm Secret Access Key</b>	Confirm the secret access key.
<b>Scan Files Of Specified Pattern</b>	Select to include or exclude files which match a file name pattern.
<b>File Name Pattern</b>	Enter the file name pattern.
<b>Scan Job Priority</b>	When multiple network share scans run at the same time, the higher priority scans will get more scan power compared to those having lower priority. The priority can be set to <i>High</i> , <i>Medium</i> (default), or <i>Low</i> .
<b>Keep A Copy Of Original File On FortiSandbox</b>	Select to keep a copy of the original file on FortiSandbox.
<b>Skip Sandboxing for the same unchanged files</b>	Select to skip Sandboxing scan on existing files (if applicable) and only Sandboxing scan new files. Existing files will only be scanned by AntiVirus engine and Community Cloud query. This is to improve scan speed.
<b>Enable Quarantine of Malicious Files</b>	<p>Select to enable quarantine then select the quarantine location from the dropdown list. Files with a Malicious rating will be quarantined in the quarantine location.</p> <p>Quarantined file is placed inside a folder with the name of the Job ID. Inside the folder each quarantined file is renamed with the corresponding Job ID for that particular file and a meta file with more information.</p>
<b>Enable Quarantine of Suspicious - High Risk Files</b>	<p>Select to enable quarantine of <i>Suspicious High Risk</i> files, then select the quarantine location from the dropdown list. Files with a High Risk rating will be quarantined in the quarantine location.</p> <p>Quarantined file is placed inside a folder with the name of the Job ID. Inside the folder each quarantined file is renamed with the corresponding Job ID for that particular file and a meta file with more information.</p>
<b>Enable Quarantine of Suspicious - Medium Risk Files</b>	<p>Select to enable quarantine of <i>Suspicious Medium Risk</i> files, then select the quarantine location from the dropdown list. Files with a Medium Risk rating will be quarantined in the quarantine location.</p> <p>Quarantined file is placed inside a folder with the name of the Job ID. Inside the folder each quarantined file is renamed with the corresponding Job ID for that particular file and a meta file with more information.</p>

<b>Enable Quarantine of Suspicious - Low Risk Files</b>	<p>Select to enable quarantine of <i>Suspicious Low Risk</i> files, then select the quarantine location from the dropdown list. Files with a Low Risk rating will be quarantined in the quarantine location.</p> <p>Quarantined file is placed inside a folder with the name of the Job ID. Inside the folder each quarantined file is renamed with the corresponding Job ID for that particular file and a meta file with more information.</p>
<b>Enable Quarantine of Other rating files</b>	<p>Select to enable quarantine of <i>Other Rating</i> files, then select the quarantine location from the dropdown list. Files with a Other rating , which means the scan was not completed for some reason, will be quarantined in the quarantine location.</p> <p>Quarantined file is placed inside a folder with the name of the Job ID. Inside the folder each quarantined file is renamed with the corresponding Job ID for that particular file and a meta file with more information.</p>
<b>Enable moving clean files to a sanitized location</b>	<p>Select to move Clean rating files to another location. By default, a new folder is created for each scheduled scan job in the sanitized location and all clean files are copied under it with the original folder structure. To save storage size, the user can un-check <i>Keep a complete copy of clean files for every scheduled scan</i>, then files of the same path will have only one copy saved in the sanitized location.</p>
<b>Enable Scheduled Scan</b>	<p>Select to enable scheduled scan. Select the schedule type from the dropdown list. Select the minute or hour from the second dropdown list.</p>
<b>Description</b>	<p>Enter an optional description for the network share entry.</p>
<div>  <p>When a file is moved, to leave a copy in its original location, the user can go to the Quarantine edit page or sanitized share and select the <i>Keep Original File At Current Location</i> checkbox.</p> </div>	

4. Select **OK** to save the entry.

#### To run a network share scan immediately:

1. Go to *Scan Input > Network Share*.
2. Select a share.
3. Click the *Scan Now* button to run the scan immediately.

#### To test network share connectivity:

1. Go to *Scan Input > Network Share*.
2. Select a share.
3. Click *Test Connection* to test connectivity with the network share.

## Scan Details

The *Scan Details* page shows scheduled scans for the selected network share. To open the page, select a network share, then select *Scan Details* from the toolbar.

The following information is shown:

<b>Back</b>	Go back to the network share page.
<b>Refresh</b>	Refresh the scans page.
<b>Delete</b>	Delete the selected scan.
<b>Total</b>	The total number of finished scanned jobs.
<b>Start</b>	The start time of the scan.
<b>End</b>	The end time of the scan.
<b>Finished</b>	Percentage of files that finished the scan. Click on the number to show details.
<b>Malicious</b>	The number of Malicious files discovered. Click on the number to show detected Malicious rating files. The number of quarantined files are also displayed.
<b>Suspicious</b>	The number of Suspicious files discovered, divided in High Risk, Medium Risk and Low Risk columns. Click on the number to show detected Suspicious rating files. The number of quarantined files are also displayed.
<b>Clean</b>	The number of Clean files detected. Click on the number to show detected Clean rating files.
<b>Others</b>	The number of files that do not finish scanning for various reasons. Click on the number to show them. The number of quarantined files are also displayed.

When jobs are displayed after clicking links on numbers, clicking the *Job Detail* button will display the details. If the detailed job information has been deleted according to the settings in the *Scan Profile > General* page, the job details will not be displayed.

## Quarantine

Go to *Scan Input > Quarantine* to view the quarantine information.

The following options are available:

<b>Create New</b>	Select to create a new quarantine location.
<b>Edit</b>	Select an entry from the list and then select <i>Edit</i> in the toolbar to edit the entry selected. When editing an entry you can select to test connectivity to ensure that the quarantine location is accessible.
<b>Delete</b>	Select an entry from the list and then select <i>Delete</i> in the toolbar to remove the entry selected.

**Test Connection**

Select an entry from the list and then select *Test Connection* in the toolbar to test the connection. The result will show in the top message panel and will disappear after a few seconds.

The following information is displayed:

<b>Name</b>	The name of the quarantine location.
<b>Type</b>	The mount type.
<b>Share Path</b>	The file share path.
<b>Enabled</b>	Displays if the quarantine location is enabled.
<b>Status</b>	Displays the quarantine access status. One of the following states: <ul style="list-style-type: none"> <li>Quarantine is Accessible</li> <li>Quarantine Down</li> </ul>

**To create a new quarantine entry:**

1. Go to *Scan Input > Quarantine*.
2. Click the + *Create New* button from the toolbar.
3. Configure the following options:

<b>Enabled</b>	Select to enable quarantine location.
<b>Quarantine Name</b>	Enter the quarantine name.
<b>Mount Type</b>	Select the mount type from the dropdown list. The following options are available: <ul style="list-style-type: none"> <li>CIFS (SMB v1.0, v2.0, v2.1 and v3.0)</li> <li>NFSv2</li> <li>NFSv3</li> <li>NFSv4</li> </ul>
<b>Server Name/IP</b>	Enter the server fully qualified domain name (FQDN) or IP address.
<b>Share Path</b>	Enter the file share path. In the format /path1/path2.
<b>Username</b>	Enter a user name. For a domain user, use the format domain_name\user_name.
<b>Password</b>	Enter the password.
<b>Confirm Password</b>	Enter the password a second time for verification.
<b>Keep Original File At Current Location</b>	Select to keep the original file at the current location when a file is quarantined from a network share. By default, the original file is kept at its current location when being moved.
<b>Description</b>	Enter an optional description for the quarantine location entry.

4. Select *OK* to save the entry.

**To edit a quarantine:**

1. Go to *Scan Input > Quarantine*.
2. Select a quarantine.
3. Click the *Edit* button from the toolbar.
4. Make the necessary changes.
5. Click *OK* to save the entry.

**To delete a quarantine:**

1. Go to *Scan Input > Quarantine*.
2. Select a quarantine.
3. Click the *Delete* button from the toolbar.
4. Click *Yes I'm sure* button from the *Are you sure* confirmation box.

## Malware Package

Go to *Scan Input > Malware Package*, to view the Malware Package list.

The following options are available:

<b>Refresh</b>	Refresh the Malware Package list.
<b>View</b>	<p>Select a package version number and click the <i>View</i> button from the toolbar. The following information is shown:</p> <ul style="list-style-type: none"> <li>• Job Detail: View the file's detailed information. If the unit is joining a global threat information sharing network, only local detection has the Job Detail button available.</li> <li>• Mark the detection as False Positive: If marked, the entry will be removed from future <i>Malware Packages</i>. If the unit is joining a global threat information sharing network, the change is also reported to the <i>Collector</i> and is shared by all units in the network.</li> <li>• Detected: The time and date that the item was detected.</li> <li>• Checksum: The file checksum (SHA256).</li> <li>• Rating: The risk rating.</li> <li>• Serial Number: From which unit the threat information is from.</li> <li>• Global/Local: If this threat information is from a local unit or from another unit.</li> </ul>
<b>Download SHA256</b> <b>Download SHA1</b> <b>Download MD5</b>	You have the option to download packages containing malware SHA256, SHA1, and MD5.

This page displays the following:

<b>Version</b>	The malware package release version.
<b>Release Time</b>	The malware package release time.

<b>Total</b>	The total number of malware antivirus signatures inside the package. The maximum number of signatures is 100K.
--------------	--



FortiSandbox only keeps malware packages generated in last 7 days.

## URL Package

Go to *Scan Input > URL Package* to view the URL Package list.

The following options are available:

<b>Refresh</b>	Refresh the URL Package list.
<b>View</b>	<p>Select a package version number and click the <i>View</i> button from the toolbar. The following information is shown:</p> <ul style="list-style-type: none"> <li>• <b>Job Detail:</b> View the downloaded file's detailed information. If the unit is joining a global threat information sharing network, only local detection has the Job Detail button available.</li> <li>• <b>Mark the URL as False Positive:</b> If marked, the URL will be removed from future URL packages. If the unit is joining a global threat information sharing network, the change is also reported to the <i>Collector</i> and is shared by all units in the network. A new package will generate after removing the entry.</li> <li>• <b>Detected:</b> The time and date that the item was detected.</li> <li>• <b>URL:</b> The URL in the package.</li> <li>• <b>Rating:</b> The risk rating of the downloaded file.</li> <li>• <b>Serial Number:</b> From which unit the threat information is from.</li> <li>• <b>Global/Local:</b> If this threat information is from a local unit, or from another unit.</li> </ul>
<b>Download URL</b>	Download a text file which contains URLs in the package.

This page displays the following:

<b>Version</b>	The URL package release version.
<b>Release Time</b>	The URL package release time.
<b>Total</b>	The total number of malware antivirus signatures inside the package. The maximum number of signatures is 1000.

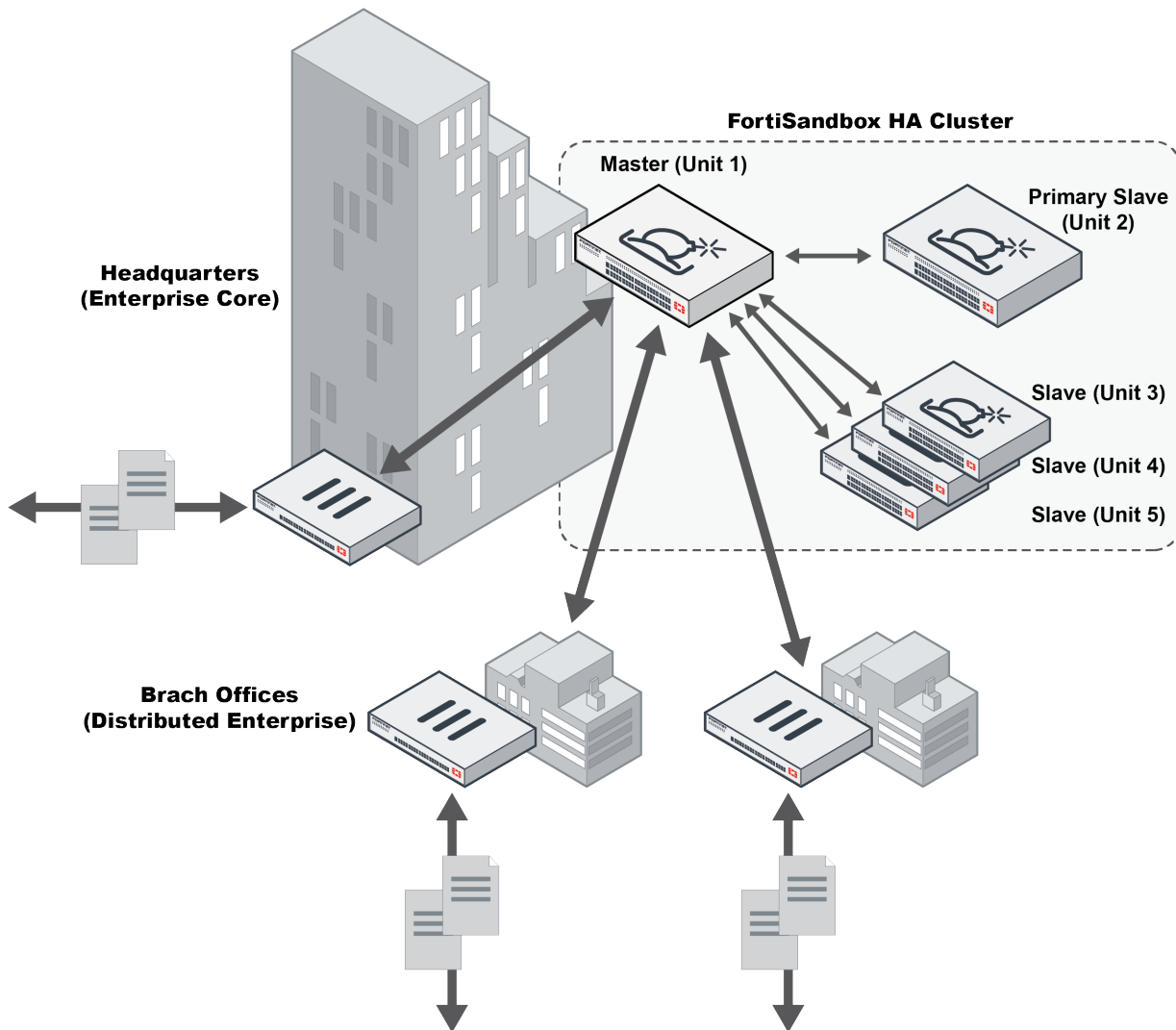


FortiSandbox only keeps URL packages generated in last 7 days.

# HA-Cluster

There are limits to the number of files that a single FortiSandbox can scan in a given time period. To handle heavier loads, multiple FortiSandbox devices can be used together in a load-balancing high availability (HA) cluster.

There are three types of nodes in a cluster: primary or master, secondary or primary slave, and worker or slave.



**Primary (or Master)** The primary node (Unit 1 in the diagram) manages the cluster, distributes jobs and gathers the results, and interacts with clients. It can also perform normal file scans. All of the scan related configuration should be done on the primary node and they will be broadcasted from the primary node to the other nodes. Any scan related configuration that has been set on a worker will be overwritten.

On the primary node, users can:

- Change a worker node's role (secondary and worker)

- Configure a worker node's network settings
- Upgrade worker nodes
- View VM status page of worker nodes
- Configure FortiGuard settings of worker nodes
- Configure VM images of worker nodes, such as setting clone numbers of each VM image
- Configure a Ping server to frequently check unit's network condition and downgrade itself as a secondary node when necessary to trigger a failover

Although all FortiSandbox models can work as a primary (master) node, we recommend using a FortiSandbox-3000D or higher.

**Secondary (or primary slave)**

The secondary node (Unit 2 in the diagram) is for HA support and normal file scans. It monitors the primary's condition and, if the primary node fails, the secondary will assume the role of primary. The former primary will then become a secondary when it is back up.

The secondary node must be the same model as the primary node.

**Worker (or slave)**

The worker nodes (Units 3 - 5 in the diagram) perform normal file scans and report results back to the primary and secondary nodes. They can also store detailed job information. Worker nodes should have its own network settings and VM image settings.

The worker nodes can be any FortiSandbox model, including FortiSandbox VM. Worker nodes in a cluster does not need to be the same model.

The total number of worker nodes, including the secondary node, cannot exceed 100.

FortiSandbox units in an HA cluster can be set up with different management ports such as port1 and port2.

For heavy job loads, use FortiSandbox-3000D or higher models.

## Centrally manage worker (slave) nodes on the primary (master) node

On a primary node, you can select a worker to view and manage information pertaining to that worker. In the Dashboard, the following widgets are displayed: *System Information*, *Scanning Statistics*, *System Resources*, and *Disk Monitor*.

### To manage worker nodes on the primary node:

1. Go to *HA Cluster*.
2. Select the worker node's serial number.
3. Users can perform any of the following tasks:
  - View the worker node's dashboard.
  - Switch the worker node's role using the *Dashboard > System Information* widget.
  - Configure the worker node's network settings (such as its IP address, routing table, DNS, and Proxy settings).
  - Configure the worker nodes' network settings for VM external traffic through port3.
  - Upgrade the worker node (including firmware, AV database etc.).
  - View the worker node's VM Status page.
  - View and configure the worker node's VM image settings.



## Requirements before Configuring a HA Cluster

1. The scan environment on all cluster nodes should be the same.  
For example, the same set of Windows VM should be installed on all nodes so the same scan profile can be used.
2. Port3 on all nodes should be connected to the Internet separately.
3. All nodes should be on the same firmware build.
4. Each node should have a dedicated network port for internal cluster communication.  
Internal cluster communication is encrypted and includes:
  - Job dispatch
  - Job result reply
  - Setting synchronization
  - Cluster topology broadcasting



It's recommended that these ports are connected to the same switch and have IP addresses in the same subnet. If the job load is heavy, the 10G fiber port is recommended to be used as the internal communication port.



Port1 and any other administrative port set through the CLI command `set admin-port` are not recommended to be used as the internal communication port.

---

## Role of the primary (master) and worker (slave) node

On the primary (master) node, all functionality can be turned on. This includes accepting files from different input sources, sending alert emails, and generating malware packages. Scan profiles should also be configured on the primary node and will be synchronized to other nodes.

The following information is synchronized from the primary node to all other nodes so they should not be configured on worker nodes:

- Job cleanup schedule
- FortiGuard page settings
- Malware package generation settings
- VM access to the Internet settings.

Only the *Allow Virtual Machines to access external network through outgoing Port3* status is synchronized. The network settings for Port3 (IP address) and next hop gateway, etc., are not synchronized. They have to be set on each unit separately.

- Blocklists and allowlists (black and white lists)
- YARA rules
- Scan profile settings



Although it is possible to assign different VM types to each node in a cluster, it is recommended that all nodes share the same VM types.

This is because VM types are collected from all nodes and are displayed in the primary node's *Scan Profile > VM Association* page, where VM associations can be configured and synchronized to the entire cluster. If an association is created for a VM type missing on the worker node, the sandbox scan will not be completed.

For example, if you associate WIN10X64VM to scan all executable files when configuring the *Scan Profile* on the primary node, but do not enable WIN10X64VM on a worker node, all executable files distributed to that worker will not be sandbox scanned.

The following information is synchronized from the primary (master) node to secondary (primary slave) nodes only, and is only applied when the secondary node becomes a primary (master) during a failover:

- Users
- Sniffer settings
- Mail server settings
- Network settings (including DNS, proxy, and routing tables)
- Scheduled task settings (network share scans, and scheduled report generation)
- Log server settings
- Uploaded certificates
- Devices
- SNMP settings
- Widget settings
- Adapter settings
- Global network settings
- Others (login disclaimers)

## Configure a cluster level failover IP set for primary (master) unit

The user can configure a cluster level failover IP for each port except port3 and ports the sniffer is sniffing. This IP set works as an alias IP of the primary (master) node network port. The primary (master) node Local IP set and secondary (primary slave) node Local IP set are kept locally during failover.

This failover IP set should be set on the current primary (master) node through the CLI command `hc-settings`. It should be in the same subnet of each port's local IP. Client devices such as FortiGate should point to this failover IP. When a failover occurs, this failover IP set will be applied on the new primary (master) node .

## Main HA-Cluster CLI Commands

In the primary (master) and secondary (primary slave) node, you must enable interface port1 so that they can communicate with each other.

`hc-settings`

Configure the unit as a HA-Cluster mode unit. Configure cluster failover IP set.

<code>hc-status -l</code>	List the status of HA-Cluster units.
<code>hc-slave</code>	<ul style="list-style-type: none"> <li><code>-a</code> to add that worker unit to the cluster.</li> <li><code>-r</code> to remove that worker unit from the cluster.</li> <li><code>-u</code> to update that worker unit information.</li> </ul>
<code>hc-master -s&lt;10-100&gt;</code>	Turn on file scan on the primary (master) node with 10% to 100% processing capacity.
<code>hc-master -r[slave serial number]</code>	Remove the worker unit with the specified serial number from the primary node.

After removing a worker node, use `hc-status -l` on the primary node to verify that the worker unit has been removed.

## Example configuration

This example shows the steps for setting up an HA cluster using three FortiSandbox 3000D units.

### Step 1 - Prepare the hardware:

The following hardware will be required:

- Nine cables for network connections.
- Three 1/10 Gbps switches.
- Three FortiSandbox 3000D units with proper power connections (units A, B, and C).



Put the primary (master) and secondary (primary slave) nodes on different power circuits.

### Step 2 - Prepare the subnets:

Prepare three subnets for your cluster (customize as needed):

- Switch A: 192.168.1.0/24: For system management.
  - Gateway address: 192.168.1.1
  - External management IP address: 192.168.1.99
- Switch B: 192.168.2.0/24: For internal cluster communications.
- Switch C: 192.168.3.0/24: For the outgoing port (port 3) on each unit.
  - Gateway address: 192.168.3.1

### Step 3 - Setup the physical connections:

1. Connect port 1 of each FortiSandbox device to Switch A.
2. Connect port 2 of each FortiSandbox device to Switch B.
3. Connect port 3 of each FortiSandbox device to Switch C.

### Step 4 - Configure the primary (master):

1. Power on the device (Unit A), and log into the CLI (See [Connecting to the Command Line Interface on page 10](#))
2. Configure the port IP addresses and gateway address with the following commands:

```
set port1-ip 192.168.1.99/24
set port2-ip 192.168.2.99/24
set port3-ip 192.168.3.99/24
```

3. Configure the device as the primary node and its cluster failover IP for Port1 with the following commands:

```
hc-settings -sc -tM -nMasterA -cTestHCsystem -ppassw0rd -iport2
hc-settings -si -iport1 -a192.168.1.98/24
```

See the FortiSandbox CLI Reference Guide available on the [Fortinet Document Library](#) for more information about the CLI commands.

4. Review the cluster status with the following command:

```
hc-status -l
```

Other ports on the device can be used for file inputs.

### Step 5 - Configure the secondary (primary slave):

1. Power on the device (Unit B), and log into the CLI.

2. Configure the port IP addresses and gateway address with the following commands:

```
set port1-ip 192.168.1.100/24
set port2-ip 192.168.2.100/24
set port3-ip 192.168.3.100/24
```

3. Configure the device as the secondary node with the following commands:

```
hc-settings -sc -tP -nPslaveB -cTestHCsystem -ppassw0rd -iport2
hc-settings -l
hc-slave -a -s192.168.2.99 -ppassw0rd
```

4. Review the cluster status with the following command:

```
hc-status -l
```

### Step 6 - Configure the worker (slave):

1. Power on the device (Unit C), and log into the CLI.

2. Configure the port IP addresses and gateway address with the following commands:

```
set port1-ip 192.168.1.101/24
set port2-ip 192.168.2.101/24
set port3-ip 192.168.3.101/24
```

3. Configure the device as a worker node with the following commands:

```
hc-settings -sc -tR -cTestHCsystem -ppassw0rd -nSlaveC -iport2
hc-settings -l
hc-slave -a -s192.168.2.99 -ppassw0rd
```

4. Review the cluster status with the following command:

```
hc-status -l
```

### Step 7 - Configure other settings:

VM Image settings and network settings, such as default gateway, static route, and DNS servers etc., should be configured on each unit individually. Scan related settings, such as the scan profile, should be set on primary unit only; they will be synchronized to the worker node. For more details, refer to [Role of the primary \(master\) and worker \(slave\) node on page 153](#).

### Step 8 - Finish:

The HA-Cluster can now be treated like a single, extremely powerful standalone FortiSandbox unit.

In this example, files are submitted to, and reports and logs are available over IP address 192.168.1.99.



FortiSandbox 3500D is configured as a cluster system, with blade 1 configured as the primary node, blade 2 as the secondary node, and the other blades as worker nodes.

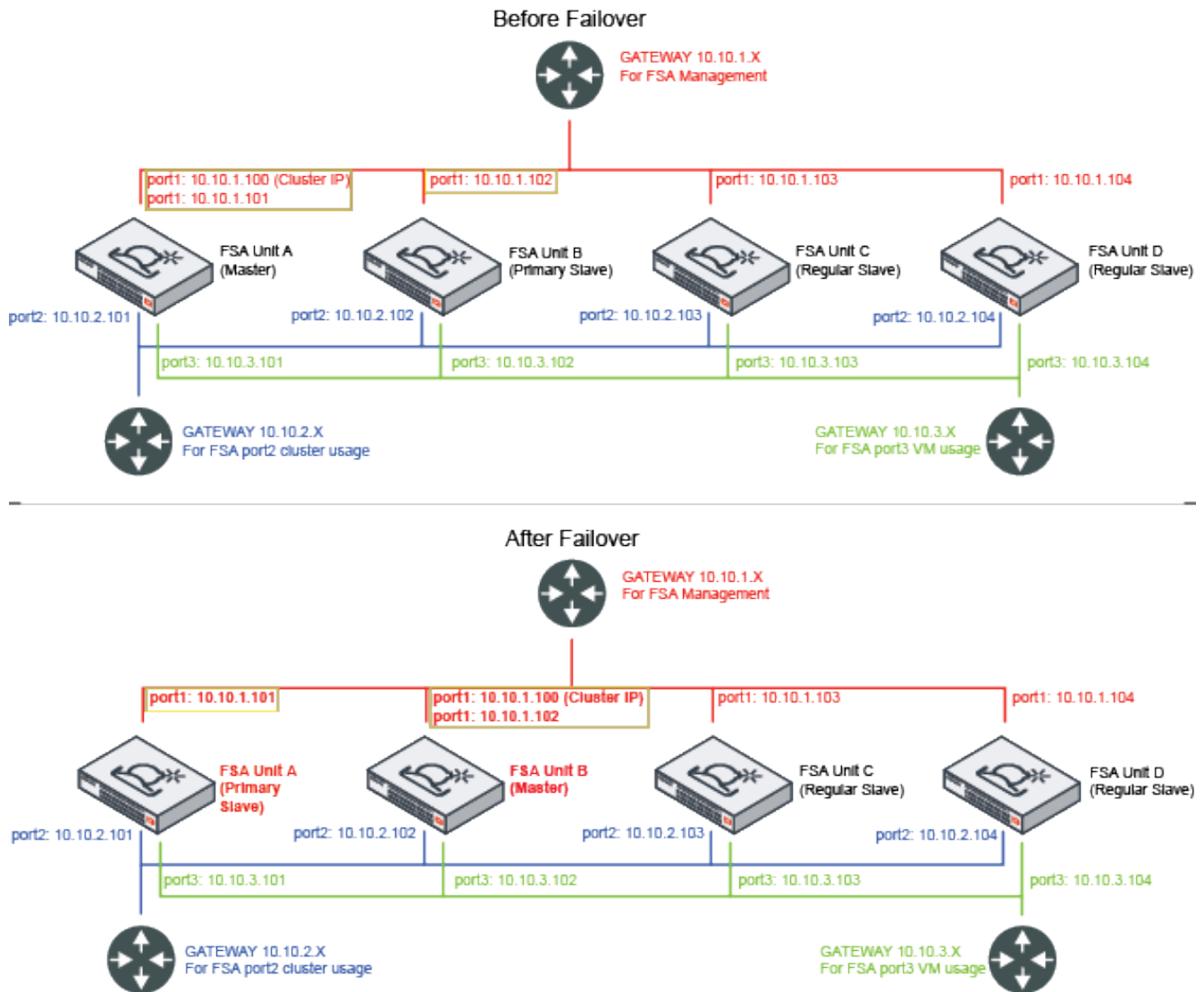


If you use the GUI to change a role from worker to standalone, you must remove the worker from the primary using the CLI command `hc-master -r` or `hc-master -r<slave serial number>`; then use `hc-status -l` to verify that the worker unit has been removed.

---

## What happens during a failover

The primary (master) node and secondary (primary slave) node sends heartbeats to each other to detect if its peers are alive. If the primary node is not accessible, such as during a reboot, a failover will occur. Users can also configure a Ping server to frequently check the unit's network condition and downgrade itself to secondary (primary slave) type when the condition is appropriate to trigger a failover. The failover logic handles two different scenarios:



### Objective node available

The Objective node is a worker (slave) (either secondary or worker) that can justify the new primary. For example, if a cluster is consisted of one primary node, one secondary node, and one worker node, the worker node is the objective node. After a secondary node takes over the primary role, and the new role is accepted by the objective node, the original primary node will accept the decision when it is back online. After the original primary is back online, it will become a secondary node.

### No Objective node available

This occurs when the cluster's internal communication is down.

For example, the cluster contains one primary node and one secondary node and the primary node reboots; or the internal cluster communication is down due to a failed switch, all secondary nodes become the primary (more than one primary unit).

When the system is back online, the unit with the largest Serial Number will keep the primary role and the other will return back to a secondary.

When the new primary is decided, it will:

1. Build up the scan environment.
2. Apply all the setting synchronized from the original primary except port3 IP and the internal communication port IP of the original primary.

After a failover occurs, the original primary might become a secondary node.

It keeps its original Port3 IP and internal cluster communication IP. All other interface ports will be shutdown as it becomes a worker node. Some functionality will be turned off such as Email Alerts. If the user wants to re-configure its settings, such as the interface IP, the user must do that through the CLI command or the primary's Central Management page.



As the new primary takes over the port that client devices communicate with will switch to it. As the new primary needs time to start up all the services, clients may experience a temporary service interruption.

---

## Upgrading or rebooting a Cluster

Upgrading or rebooting a Cluster has to be done by logging into each device or through the primary unit's central management interface by going into each device's dashboard page. You must upgrade the cluster in the following order:

1. Worker (slave) devices
2. Secondary (primary slave)
3. Primary (master)



It is highly recommended to setup cluster level failover IP set so the failover between primary and secondary can occur smoothly. If the user does not want the failover to happen, the user can change the secondary unit role to worker. You can either do this through the UI dashboard or the CLI prior to the failover, then change the role back after the unit boots up.

---

## Health Check

The Health Check page is only available on the primary (master) node. Users can use the HA Health Check to set up a Ping server to ensure the network condition between client devices and FortiSandbox is always up. If not, the primary node will downgrade itself to a secondary (primary slave) node if there is at least one secondary (primary slave) node existing, a failover will occur after the configured period elapses. If no secondary (primary slave) node exists, the primary node will keep its primary role.

The following options are available:

<b>Create New</b>	Create a new health check Ping server.
<b>Edit</b>	Edit a health check Ping server.
<b>Delete</b>	Delete a health check Ping server.

This page displays the following information:

<b>Interface</b>	The interface port to connect to the Ping server. Port3 cannot be used.
<b>Remote Server</b>	IP address or fully-qualified domain name of the remote Ping server.
<b>Ping</b>	Enable or disable sending the Ping packet to the remote server to ensure the network connection is up.
<b>TCP Echo</b>	Enable or disable sending TCP Echo packet to ensure the network connection to the remote sever is up.
<b>Interval</b>	Time interval in seconds (30-180 seconds) to send a Ping or TCP Echo packets.
<b>Failover Threshold</b>	Failover threshold (3-120 times). After a certain number of consecutive missing responses of Ping or TCP Echo packets, the primary node will downgrade itself as a secondary (primary slave) if there is an existing secondary (primary slave) node.

#### To create a new HA Health Check:

1. Go to *HA-Cluster > Health Check*.
2. Click + *Create New* from the tool bar.
3. Configure the settings.
4. Click *Ok*.

#### To edit a HA Health Check:

1. Go to *HA-Cluster > Health Check*.
2. Select the Health Check you want to edit.
3. Click the *Edit* button from the toolbar.
4. Edit the settings.
5. Click *Ok*.

#### To delete a HA Health Check:

1. Go to *HA-Cluster > Health Check*.
2. Select the Health Check you want to delete.
3. Click the *Delete* button from the toolbar.
4. Click the *Yes, I'm sure* button to delete the Health Check.



## Job Summary

The Job Summary page shows job statistics data of each node in a cluster. It is only available on the primary (master) node.

### To view a HA Job Summary:

1. Go to *HA-Cluster > Job Summary*.
2. Select either *File* or *URL* button to view file-based scan results and URL scan results.

The following information is shown:

<b>Time Period Drop down</b>	Select the period of time over which the data was collected from the drop down. You have the following options: <i>Last 24 Hours</i> , <i>Last 7 Days</i> , and <i>Last 4 Weeks</i> .
<b>Serial Number</b>	The serial number of the device in the cluster.
<b>Pending</b>	The number of files in the job queue waiting to be scanned.
<b>Malicious</b>	The number of malicious files detected.
<b>Suspicious</b>	The number of suspicious files detected.
<b>Clean</b>	The number of clean files detected.
<b>Other</b>	Other files that have been scanned and have an Unknown rating.

Select a number from the Malicious, Suspicious, Clean, or Other columns to view details about those specific files.

## Status

The Status page shows the basic information of cluster nodes.

### To view a HA Status:

1. Go to *HA-Cluster > Status*.

The following information is shown:

<b>Serial Number</b>	The serial number of the device in the cluster.
<b>Type</b>	The type of the device: <i>Master</i> (primary), <i>Primary Slave</i> (secondary), or <i>Regular Slave</i> (worker).
<b>Alias</b>	The device's alias.
<b>IP Address</b>	The device's internal communication IP address.
<b>Status</b>	The status of the device: <i>Active</i> or <i>Inactive</i> .



The total number of cluster members are shown at the bottom of the list. This number cannot exceed 101, including the primary (master).

---

# File Detection

This section includes the following topics:

- [Summary Report](#)
- [File Scan](#)

## Summary Report

The *Summary Reports* page provides a page similar to the *System* dashboard. You can add and customize widgets in this page. By selecting a device and time period, you can customize what data is displayed.

If the unit is the primary (master) node in a cluster, the data displayed is a summary from all cluster nodes. Otherwise, only the individual unit's data is displayed.



On-Demand job data is not included.

Scanning Statistics			
Rating	Count	WIN7X64VM	WIN7X86VM
Malicious	2,781	0	0
Suspicious - High Risk	838	7	1
Suspicious - Medium Risk	156	0	0
Suspicious - Low Risk	14	13	2
Clean	28,669	0	0
Total	32,458	20	3

Last Updated: Sat, Jul 6, 2019 12:47

The following options are available:

<b>Add Widget</b>	Click the + button to add widgets to the summary report page.
<b>Reset View</b>	Click the <i>Reset</i> button to restore widgets to the default setting. A confirmation dialog box will be displayed, select <i>OK</i> to continue.
<b>Time Period</b>	Select a time period to be displayed from the dropdown list on the top. The options are: <i>Last 24 hours</i> , <i>Last 7 days</i> , <i>Last 4 weeks</i> .
<b>Device</b>	Select the device from the dropdown list.

The following widgets are available:

<b>Scanning Statistics</b>	Displays a table providing information about the files scanned for a selected device for a selected time period.
----------------------------	--

<b>Scanning Statistics by Type</b>	Displays a table providing information about file types, rating, and event count for a selected device over a selected time period.
<b>Top Targeted Hosts</b>	<p>Displays a chart providing the number of infection events for specific hosts that have occurred for a selected device over a selected time period.</p> <p>Hover the cursor over a colored portion of a bar in the chart to view the exact number of infection events that have occurred for the host selected.</p> <p>Selecting the infected host allows you to drill down to the job details.</p>
<b>File Scanning Activity</b>	<p>Displays the number of clean, suspicious, and malicious events that have occurred at specific times over a selected time period for the selected device.</p> <p>Hover the cursor over a colored portion of a bar in the graph to view the exact number of events of the selected type that occurred at that time.</p>
<b>Top Malware</b>	<p>Displays a chart providing the number of infection events for specific malware that have occurred for a selected device over a selected time period.</p> <p>Hover the cursor over a colored portion of a bar in the chart to view the exact number of infection events that have occurred for the malware selected.</p> <p>Selecting the malware name allows you to drill down to the job details related to them.</p>
<b>Top Callback Domains</b>	<p>Displays a chart providing the top callback domains that have been detected over a selected time period. Callback domains are hosts that files visit when executing in VM.</p> <p>Hover the cursor over a colored portion of a bar in the chart to view the exact number of infection events that have occurred for the malware selected.</p>
<b>Top File Types</b>	Displays a chart providing the top file types that have been detected over a selected time period. When <i>Scanned by Sandboxing</i> is selected, only files that have finished sandboxing will be counted.

## Customizing the summary report page

The FortiSandbox summary reports page can be customized. You can select the device and time period in the toolbar to display specific information. You can also select which widgets to display, where they are located in the page, and whether they are minimized or maximized.

### To move a widget:

Position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

### To refresh a widget:

Click the refresh icon in the widget's title bar to refresh the data presented in the widget.



Multiple widgets of the same type can be added to the dashboard. This can be useful for viewing information over different refresh time intervals.

**To edit a widget:**

Click the edit icon in the widget's title bar to open the edit widget settings window.

Configure the following information, and then select *OK* to apply your changes:

<b>Custom widget title</b>	Optionally, enter a custom title for the widget. Leave this field blank to use the default widget title.
<b>Refresh interval</b>	Enter a refresh interval for the widget, in seconds. The widgets have default refresh values: <ul style="list-style-type: none"> <li>• <i>Scanning Statistics</i>: 3600 seconds</li> <li>• <i>Scanning Statistics by Type</i>: 3600 seconds</li> <li>• <i>Top Malware</i>: 3600 seconds</li> <li>• <i>Scanning Activity</i>: 300 seconds</li> <li>• <i>Top Targeted Hosts</i>: 10 seconds</li> <li>• <i>Top Callback Domains</i>: 3600 seconds</li> </ul>
<b>Top Count</b>	Select the number of entries to display in the widget. The top count can be between 5 to 20 entries. This setting is available in all widgets except <i>Scanning Statistics</i> , <i>Scanning Statistics by Type</i> , and <i>Scanning Activity</i> .

## File Scan

File Scan page shows file based job scans grouped by their ratings. Files submitted through On-Demand are not included. Users can toggle to view Malicious, Suspicious and Clean job ratings. By default, Suspicious jobs are displayed.

In this page, you can view job details and apply search filters. You can select to create a PDF or CSV format snapshot report for files based on search filters.

The following options are available:

File Scan Options	
<b>Suspicious</b>	Click the <i>Suspicious</i> icon to view the suspicious jobs.
<b>Clean</b>	Click the <i>Clean</i> icon to view the clean or unknown jobs.
<b>Malicious</b>	Click the <i>Malicious</i> icon to view the malicious jobs.
<b>Show Rescan Job Only</b>	Whenever a new AV signature is downloaded, all jobs from last 48 hours will be done in one AV Scan. Detected viruses will receive a Malicious rating. Users can display them in <i>File Detection &gt; File Scan &gt; Malicious</i> and enable <i>Show Rescan Job Only</i> .
<b>Refresh</b>	Click the button to refresh the entries displayed.
<b>Search</b>	Show or hide the search filter field.
<b>Add Search Filter</b>	Click the search filter field to add search filters. Click the close icon in the search filter field to clear all search filters.

	<p>The search filter will be displayed below the search filter field. Click the close icon beside the search filter to remove the filter.</p> <p>Search filters can be used to filter the information displayed in the GUI.</p>
<b>Export Data</b>	Click the <i>Export Data</i> button to create a PDF or CSV snapshot report. The time to generate the report is dependent on the number of events selected. You can wait till the report is ready to view, or navigate away and find the report later on the <i>Log &amp; Report &gt; Report Center</i> page.
<b>Customize</b>	Click the <i>Customize</i> button to customize the Job View Settings. The change will be applied to all file based scan result pages.
<b>Action</b>	
<b>View Details</b>	Click the <i>View Details</i> icon to view the file description and analysis details. The information displayed is dependent on the file selected.
<b>Perform Rescan</b>	For Malicious jobs, users can also select the <i>Rescan</i> icon to perform a manual rescan of the file. By this way, you can find out the behavior of a known virus. You can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing in the rescan settings. You can find the job on the <i>Scan Input &gt; File On-Demand</i> page.
<b>Archived File</b>	An icon will appear if the file is an Archived File.
<b>FortiGuard Static Scan</b>	The icon displays that the file is rated by the user's overridden verdict or FortiGuard advanced static scan.
<b>File Inside Archive</b>	The icon displays that the file is a file extracted from an archive file.
<b>Rescan Job</b>	The icon displays that the job is Malicious from an AV Rescan or a customized rescan job of a Malicious file.
<b>AV Scan</b>	An icon will appear if this job is from an AV Rescan.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

FortiSandbox has an Anti Virus rescan feature. When a new antivirus signature is available, FortiSandbox will perform a second antivirus scan of all the jobs from the last 48 hours whose ratings are *Clean* or *Suspicious* using the new signatures. Detected viruses will be displayed as *Malicious* jobs with the *Rescan* icon beside the *View Details* icon. The original job can still be viewed in the job detail page of the rescanned file by clicking the original job ID.



Virus behavior information is not collected as viruses are detected by the AV scanner. The rescan feature allows you to see how a virus behaves while it is being executed inside a VM.

The displayed columns are determined by settings defined in *System > Job View Settings > File Detection Columns* page. For more information, see [Job View Settings on page 76](#).

#### To view file details:

1. Select a file.
2. Click the *View Details* icon. A new tab will open. See [Appendix A - View Details Page Reference on page 186](#) for

descriptions of the *View Details* page.

3. Close the tab to exit the *View Details* page.

**To rescan a file:**

1. Select a file with Suspicious or Malicious Rating.
2. Click the *Perform Rescan* icon.
3. You can select to skip *Static Scan*, *AV Scan*, *Cloud Query*, and *Sandboxing*.
4. Click *OK* to start the rescan.
5. Click the close icon or select the *Close* button to close the dialog box.



Rescan results are found in the *Scan Input > File On-Demand*.



In this release, the maximum number of events you can export to a PDF report is 1,000; the maximum number of events you can export to a CSV report is 15,000. Jobs over that limit will not be included in the report.

---

# Network Alerts

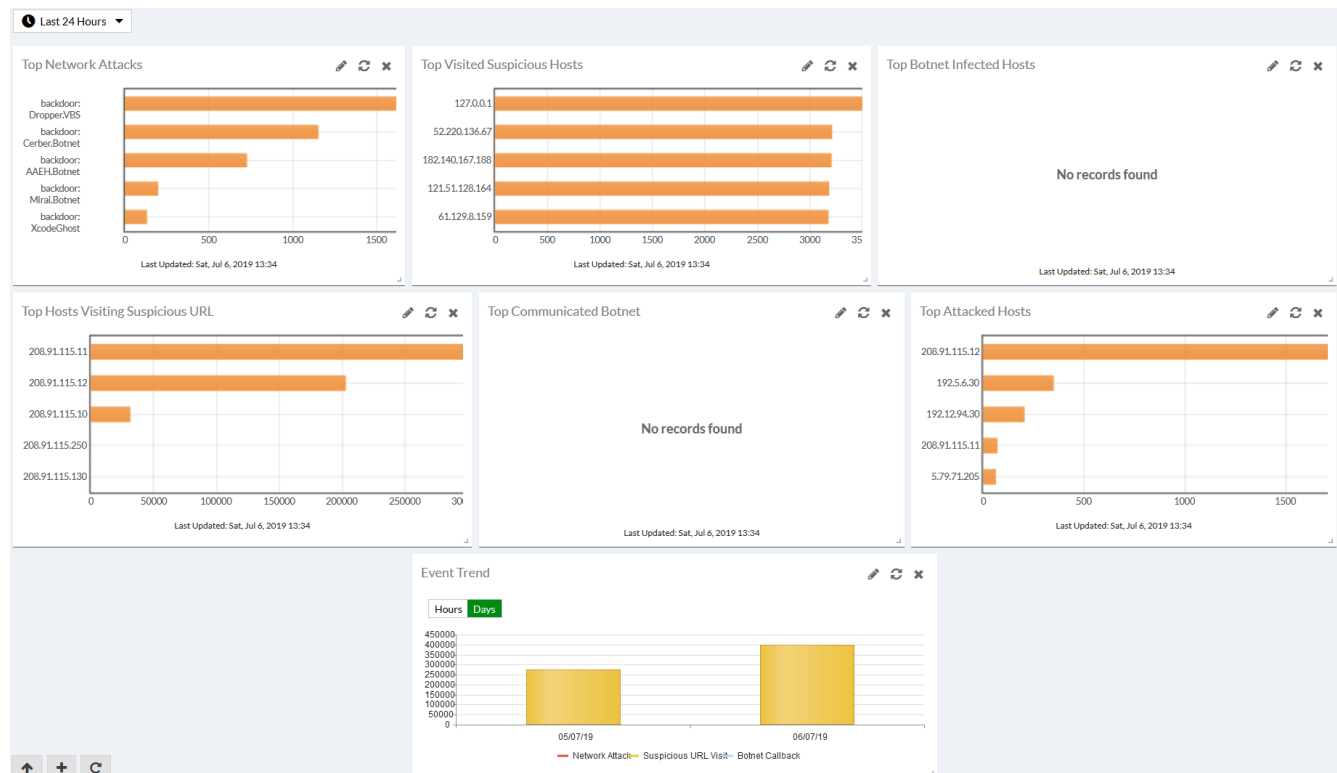
Network alerts show detected connection attempts to known botnets, attacks on hosts on your network, and harmful websites visited from your network. You must enable network alerts detection in *Scan Input > Sniffer*. Sniffed data is scanned by the IPS engine to populate data on this page. You can select to view data for a specific time period. In the Networks Alerts page, you can view alerts (Attacker, Botnet, and URL), and drill down the information displayed and apply search filters.

This section includes the following topics:

- [Summary Report](#)
- [Network Alerts](#)

## Summary Report

The *Summary Reports* page provides a page similar to the *System* dashboard. You can add and customize widgets in this page. By selecting the time period, you can customize what data is displayed.



The following options are available:

### Add Widget

Click the + button to add widgets to the summary report page.



<b>Reset View</b>	Click the <i>Reset</i> button to restore widgets to the default setting. A confirmation dialog box will be displayed, select <i>OK</i> to continue.
<b>Time period</b>	Select a time period to be displayed from the dropdown list. The options are: <i>Last 24 hours</i> , <i>Last 7 days</i> , <i>Last 4 weeks</i> .

The following widgets are available:

<b>Event Trend</b>	Displays a chart providing information about the number of network attacks, suspicious URL visits, and Botnet callbacks over a period of time.  Hover the cursor over a colored portion of a bar in the graph to view the exact number of events that occurred at that time. You can toggle between hourly data view and daily data view.
<b>Top Network Attacks</b>	Displays a table providing information about the number and type of network attacks.  Hover the cursor over a colored portion of a bar in the graph to view the exact number of events that occurred at that time.
<b>Top Attacked Hosts</b>	Displays a table providing information about the top attacked hosts on your network.  Hover the cursor over a colored portion of a bar in the graph to view the exact number of events that occurred at that time.
<b>Top Communicated Botnet</b>	Displays a table providing information about the top communicated botnets on your network.  Hover the cursor over a colored portion of a bar in the graph to view the exact number of events that occurred at that time.
<b>Top Botnet Infected Hosts</b>	Displays a table providing information about the top botnet infected hosts on your network.  Hover the cursor over a colored portion of a bar in the graph to view the exact number of events that occurred at that time.
<b>Top Visited Suspicious Hosts</b>	Displays a table providing information about the top visited suspicious hosts.  Hover the cursor over a colored portion of a bar in the graph to view the exact number of events that occurred at that time.
<b>Top Hosts Visiting Suspicious URL</b>	Displays a table providing information about the top hosts on your network that visit suspicious URLs.  Hover the cursor over a colored portion of a bar in the graph to view the exact number of events that occurred at that time.

## Customizing the summary report page

The FortiSandbox summary reports page can be customized. You can select the time period in the toolbar to display specific information. You can also select which widgets to display, where they are located on the page, and whether they are minimized or maximized.

**To move a widget:**

Position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

**To refresh a widget:**

Click the refresh icon in the widget's title bar to refresh the data presented in the widget.

**To edit a widget:**

Click the edit icon in the widget's title bar to open the edit widget settings window.

Configure the following information, and then select *OK* to apply your changes:

<b>Custom widget title</b>	Optionally, enter a custom title for the widget. Leave this field blank to use the default widget title.
<b>Refresh interval</b>	Enter a refresh interval for the widget, in seconds. Set the field to 0 to disable. The widgets have default refresh values: <ul style="list-style-type: none"> <li>• <i>Event Trend</i>: 3600 seconds</li> <li>• <i>Top Network Attacks</i>: 3600 seconds</li> <li>• <i>Top Attacked Hosts</i>: 3600 seconds</li> <li>• <i>Top Communicated Botnet</i>: 3600 seconds</li> <li>• <i>Top Botnet Infected Hosts</i>: 3600 seconds</li> <li>• <i>Top Visited Suspicious URL Hosts</i>: 3600 seconds</li> <li>• <i>Top Hosts Visiting Suspicious URLs</i>: 3600 seconds</li> </ul>
<b>Top Count</b>	Select the number of entries to display in the widget. The top count can be between 5 to 20 entries. This setting is available in all widgets except <i>Event Trend</i> .

## Network Alerts

Network alerts show detected connection attempts to known botnets, attacks to hosts on your network, and harmful websites visited from your network.

To view network alerts (Attacker, Botnet, and URL), go to *Network Alerts*. You can drill down the information displayed and apply search filters. You can select to create a PDF or CSV format snapshot report for specific types of network alert files. Search filters will be applied to the detailed report and will be displayed in the Report Profile section.

<div> <span>🕒 Last 24 Hours</span> <span>👤 Attacker</span> <span>📄 Export Data</span> <span>🔍 Search</span> </div>				
<div> <span>🔄</span> <input type="text" value="Filter ..."/> </div>				
Detected	Backdoor	Source	Destination	
Mar 01 2016 12:02:21	backdoor: Nitol.Botnet	208.91.115.11	50.63.202.40	
Mar 01 2016 12:02:11	backdoor: Nitol.Botnet	208.91.115.11	50.63.202.40	
Mar 01 2016 12:01:38	backdoor: Nitol.Botnet	208.91.115.11	50.63.202.40	
Mar 01 2016 12:01:07	backdoor: Nitol.Botnet	208.91.115.11	50.63.202.40	
Mar 01 2016 11:58:42	applications3: Malicious.JavaScript.Obfuscation.Code.Packer.Detection	190.36.171.72	208.91.115.10	
Mar 01 2016 11:58:04	backdoor: Nitol.Botnet	208.91.115.11	50.63.202.40	

This page has the following options:

<b>Time Period</b>	<p>Select the time period from the dropdown list. Select one of the following: <i>24 Hours</i>, <i>7 Days</i>, or <i>4 Weeks</i>.</p> <p>You can select the time period to filter the information displayed in the GUI. This selection is also applied to exported data for the snapshot report.</p>
<b>Alert Type</b>	<p>Select Attacker, Botnet, or URL from the dropdown list. You can select the alert type to filter the information displayed in the GUI. This selection is also applied to exported data for the snapshot report.</p>
<b>Attacker</b>	<p>Shows attacks against hosts on your network. When selecting <i>Attacker</i> from the dropdown list, the following information is displayed:</p> <ul style="list-style-type: none"> <li>• Detected: The date and time that the attack was detected by FortiSandbox.</li> <li>• Backdoor: The name of the attack.</li> <li>• Source: The attacker's IP address.</li> <li>• Destination: The attacked host IP address.</li> </ul> <p>All columns include a filter to allow you to sort the entries in ascending or descending order.</p>
<b>Botnet</b>	<p>Shows detected connections to known botnets. When selecting <i>Botnet</i> from the dropdown list, the following information is displayed:</p> <ul style="list-style-type: none"> <li>• Detected: The date and time that the botnet contact was detected by FortiSandbox.</li> <li>• Name: The botnet name.</li> <li>• Source: The IP address of the infected host.</li> <li>• Destination: The botnet command and control IP address.</li> </ul> <p>The <i>Detected</i>, <i>Name</i>, and <i>Source</i> columns include a filter to allow you to sort the entries in ascending or descending order.</p>
<b>URL</b>	<p>Shows visited suspicious websites from your network. When selecting <i>URL</i> from the dropdown list, the following information is displayed:</p> <ul style="list-style-type: none"> <li>• Detected: The date and time that the malicious URL was visited.</li> <li>• Rating: The severity of the visiting activity.</li> <li>• Category: The URL's web filtering category.</li> <li>• Host: The host IP address. The first level domain name of the URL.</li> <li>• URL: The visited URL address.</li> <li>• Type: The URL type, http or https</li> <li>• Source: The IP address of the host who visited the malicious URL.</li> </ul> <p>The <i>Detected</i>, <i>Category</i>, <i>Hostname</i>, <i>URL</i>, <i>Type</i>, and <i>Source</i> columns include a filter to allow you to sort the entries in ascending or descending order.</p> <p><b>Tooltip:</b> Certain URL categories are set as <i>Benign</i> by default. To view and change, go to <i>Scan Policy &gt; URL Category</i>.</p>
<b>Export Data</b>	<p>Select to create a PDF or CSV snapshot report. The time to generate the report is dependent on the number of events selected. You can wait till the report is ready to view, or navigate away and find the report later on the <i>Log &amp; Report &gt; Report Center</i> page.</p>
<b>Refresh</b>	<p>Click the icon to refresh the log message list.</p>
<b>Search</b>	<p>Show or hide the search filter field.</p>

**Add Search Filter**

Click the search filter field to add search filters. Click the close icon in the search filter field to remove the search filter.

Search filters can be used to filter the information displayed in the GUI.

**To create a snapshot report for all network alert files:**

1. Select a time period from the first dropdown list.
2. Select Attacker, Botnet, or URL from the second dropdown list.
3. Select to apply search filters to further drill down the information in the report.
4. Click the *Export Data* button in the toolbar. The *Report Generator* window opens.
5. Select either PDF or CSV for the report type.
6. Click the *Generate Report* button to create the report.  
When the report generation is completed, select the *Download* button to save the file to your management computer.
7. You can wait till the report is ready to view, or navigate away and find the report later on the *Log & Report > Report Center* page.

# URL Detection

This section includes the following topics:

- [Summary Report](#)
- [URL Scan](#)

## Summary Report

The *Summary Report* page provides a page similar to the *System* dashboard. You can add and customize widgets in this page. By selecting a time period, you can customize what data is displayed.



Job data of URLs submitted through On-Demand or JSON API are also included in the *Summary Report*.

The following options are available:

<b>Add Widget</b>	Click the + button to add widgets to the <i>Summary Report</i> page.
<b>Reset View</b>	Click the <i>Reset</i> button to restore widgets to the default setting. A confirmation dialog box will be displayed, select <i>OK</i> to continue.
<b>Time Period</b>	Select a time period to be displayed from the dropdown list. The options are: <i>Last 24 hours</i> , <i>Last 7 days</i> , <i>Last 4 weeks</i> .
<b>Device</b>	Click the button to filter for a specific device.

The following widgets are available:

<b>Scanning Statistics</b>	Displays a table providing information about the URLs scanned per OS for a selected time period. Clicking on the number in the widget will drill down to the associated job list.
<b>Scanning Statistics by Type</b>	Displays a table proving information about URL types, rating, and event count for a selected time period.
<b>Scanning Activity</b>	Displays the number of clean, suspicious, and malicious jobs that have occurred at specific times over a selected time period.  Hover the cursor over a colored portion of a bar in the graph to view the exact number of events of the selected type that occurred at that time. You can toggle between hourly data view and daily data view.

## Customizing the summary report page

The FortiSandbox summary reports page can be customized. You can select the time period in the toolbar to display specific information. You can also select which widgets to display, where they are located in the page, and whether they are minimized or maximized.

### To move a widget:

Position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

### To refresh a widget:

Click the refresh icon in the widget's title bar to refresh the data presented in the widget.



Multiple widgets of the same type can be added to the dashboard. This can be useful for viewing information over different refresh time intervals.

---

### To edit a widget:

Click the edit icon in the widget's title bar to open the edit widget settings window.

Configure the following information, and then select *OK* to apply your changes:

<b>Custom widget title</b>	Optionally, enter a custom title for the widget. Leave this field blank to use the default widget title.
<b>Refresh interval</b>	Enter a refresh interval for the widget, in seconds. The widgets have default refresh values: <ul style="list-style-type: none"><li>• <i>Scanning Statistics</i>: 3600 seconds</li><li>• <i>Scanning Statistics by Type</i>: 3600 seconds</li><li>• <i>Scanning Activity</i>: 300 seconds</li></ul>
<b>Top Count</b>	Select the number of entries to display in the widget. The top count can be between 5 to 20 entries. This setting is available in the <i>Top Infectious URLs</i> widget.

## URL Scan

The *URL Scan* page shows jobs of URL based scans grouped by their ratings. URLs submitted through On-Demand are not included. Users can toggle to view jobs of different ratings. By default, Suspicious jobs are displayed.

In this page, you can view job details and apply search filters. You can select to create a PDF or CSV format snapshot report for files based on search filters.

The following options are available:

URL Scan Options	
<b>Suspicious</b>	Click the <i>Suspicious</i> icon to view the suspicious jobs.
<b>Clean</b>	Click the <i>Clean</i> icon to view the clean jobs.
<b>Malicious</b>	Click the <i>Malicious</i> icon to view the malicious jobs.
<b>Refresh</b>	Click the button to refresh the entries displayed.
<b>Search</b>	Show or hide the search filter field.
<b>Add Search Filter</b>	Click the search filter field to add search filters. When the search criteria is the <i>Submitted Filename</i> , click the equals sign to toggle between exact and pattern search. Click the close icon in the search filter field to clear all search filters. Search filters can be used to filter the information displayed in the GUI.
<b>Export Data</b>	Select to create a PDF or CSV snapshot report. The time to generate the report is dependent on the number of events selected. You can wait till the report is ready to view, or navigate away and find the report later on the <i>Log &amp; Report &gt; Report Center</i> page.
<b>Customize</b>	Click the <i>Customize</i> button to customize the Job View Settings.
<b>Action</b>	
<b>View Details</b>	Click the <i>View Details</i> icon to view the file description and analysis details. The information displayed is dependent on the file selected.
<b>FortiGuard Static Scan</b>	The icon displays that the URL is rated by the user's overridden verdict or FortiGuard advanced static scan.
<b>Archive File</b>	The icon displays that the URL is from a file through On Demand scan.
<b>File Downloading URL</b>	The icon displays that the URL is from FortiMail and its payload is also scanned as a file scan job.
<b>Pagination</b>	Use the pagination options to browse entries displayed.

The displayed columns are determined by settings defined in *System > Job View Settings > URL Detection Columns* page. For more information, go to [Job View Settings on page 76](#).

#### To create a snapshot report for all search results:

1. Select to apply search filters.
2. Select the generate to report button. The *Report Generator* window opens.
3. Select either PDF or CSV and click the *Generate Report* button to create the report.
4. When report generation is completed, select the *Download* button to save the file to your management computer.
5. You can wait until the report is ready to view, or navigate away and find the report later on the *Log & Report > Report Center* page.



In this release, the maximum number of events you can export to a PDF report is 1,000; the maximum number of events you can export to a CSV report is 15,000. Jobs over that limit will not be included in report.

# Log & Report

The Log & Reports menu allows you to view and download all logs collected by the device, access scheduled reports, and generate reports. You can log locally to FortiSandbox, or a remote log server like FortiAnalyzer.

This section includes the following topics:

- [About Logs](#)
- [Log Categories](#)
- [Log Servers](#)
- [Local Log](#)
- [Viewing logs in FortiAnalyzer](#)
- [Summary Reports](#)
- [Report Center](#)

## About Logs

This section includes the following topics:

- [Log Details](#)
- [Logging Levels](#)
- [Raw logs](#)

## Log Details

To view more details about a specific log in the log list, simply select that log. A log details pane is available at the bottom of the window.

The log details pane contains the same information as the log message list, except with a full message in lieu of a shortened one.

## Logging Levels

FortiSandbox logs can be Emergency (reserved), Alert, Critical, Error, Warning, Information, or Debug. The following table provides example logs for each log level.

Log Level	Description	Example Log Entry
<b>Alert</b>	Immediate action is required.	Suspicious URL visit domain.com from 192.12.1.12 to 42.156.162.21:80.



Log Level	Description	Example Log Entry
<b>Critical</b>	Functionality is affected.	System database is not ready. A program should have started to rebuild it and it shall be ready after a while.
<b>Error</b>	An erroneous condition exists and functionality is probably effected.	Errors that occur when deleting certificates.
<b>Warning</b>	Functionality might be affected.	Submitted file AVSInstallPack.exe is too large: 292046088.
<b>Information</b>	General information about system operations.	LDAP server information that was successfully updated.
<b>Debug</b>	Detailed information useful for debugging purposes.	Launching job for file. jobid=2726271637747836543 filename=log md5=ebe5ae2bec3b653c2970e8cec9f5f1d9 sha1=06ea6108d02513f0d278ecc8d443df86dac2885b sha256=d678da5fb9ea3ee20af779a4ae13c402585ebb070edcf20091cb20509000f74b

## Raw logs

Raw logs can be downloaded and saved to the management computer using the *Download Log* button. The raw logs will be saved as a text file with the extension *.log.gz*. The user can search the system log for more information.

### Sample raw logs file content

```
itime=1458669062 date=2016-03-22 time=17:51:02 logid=1220000020 type=event subtype=unknown
pri=alert user=system ui=system action=rating status=success reason=none letype=6
msg=fname=v32.cab jobid=2725911139058114340
sha1=f61045626e5f4f74108fb6b15dde284fe0249370
sha256=f75fca6300e48ec4876661314475cdd7f38d4c73e87dfb5a423ef34a7ce0154f rating=Clean
scantime=11 malwarename=N/A srcip=204.79.197.200 dstip=208.91.115.250 protocol=HTTP
device=() url=http://officecdn.microsoft.com/pr/492350f6-3a01-4f97-b9c0-
c7c6ddf67d60/Office/Data/v32.cab
itime=1458669062 date=2016-03-22 time=17:51:02 logid=0106000001 type=event subtype=system
pri=debug user=system ui=system action=controller status=success reason=none letype=6
pid=8605 msg="Sandboxing environment is not available for job 2725913445926977878,
file type: htm, file extension: htm"
itime=1458669062 date=2016-03-22 time=17:51:02 logid=1220000020 type=event subtype=unknown
pri=alert user=system ui=system action=rating status=success reason=none letype=6
msg=fname=0_22_93_0_0_2_0_0_1.html jobid=2725913445926977878
sha1=098a2ca8d81979f2bb281af236f9baa651d557d5
sha256=424c62eaaa4736740e43f5c7376ec6f209b0d3df0e0cadcc94324280eafal01f rating=Clean
scantime=12 malwarename=N/A srcip=125.39.193.250 dstip=208.91.115.12 protocol=HTTP
device=() url=http://all.17k.com/lib/book/0_22_93_0_0_2_0_0_1.html
```



Fort detailed log format information, please refer to the *FortiSandbox 3.0.7 Log Reference* available on the [Fortinet Document Library](#).

## Log Categories

In FortiSandbox, logs are group into different categories:

<b>All Events</b>	Shows all logs.
<b>System Events</b>	Shows logs related to system operation, like user creation and FDN downloads.
<b>VM Events</b>	Shows logs related to guest VM systems, such as VM initialization.
<b>Job Events</b>	Shows logs related to scans. Users can trace the scan flow of each file or URL.
<b>HA-Cluster Events</b>	Shows logs related to cluster configuration and fail overs.
<b>Notification Events</b>	Shows logs related to email alerts and SNMP traps.

#	Date/Time	Level	User	Message
1	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=db726186ae7a48cbc5fdecfb1ed74164eca66cb021c82fed5b186...
2	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=bd781a171f405a5db9daf0b775ba16e3d9d90a9e84abf867...
3	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=f9d1e4ddea48b41df0f3c9cb96939195349c77fb6efd66d1d4a4...
4	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=81cc1b42edcc03e3a335651dc6296ac0f38360c70334d9eee6...
5	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=dc5b2a59fdd3f64b8d8b61dc978af3ba45910e73f0c0c7c32173...
6	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=4388620b7ee1a7d3468fb0bac72ec6800deefd9e2039e9fa4cd68...
7	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=c9d6be39edbf46084af2e6e8f5f06ef00f33217f11dd89d7fb3...
8	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=b399e0631bb16bf6bf1f596c1c16158f3a1e43409d8d2d39fb8f...
9	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=82a321031c0f9c44acf253c7f98f6bada792a0e9fc241f794e66e...
10	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=497bf0734786d19ac7ead2a25dffdcc3584cef26023b3b98c157c...
11	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=160927dbb11b4cc3ec38a25a7a9ae12b1ebddc8bc214312853...

The following options are available:

<b>Download Log</b>	Select to download a file containing the raw logs to the management computer.
<b>History Logs</b>	Enable to include historical logs in Log Search.
<b>Refresh</b>	Select to refresh the log message list.
<b>Add Search Filter</b>	Click the search filter field to add search filters. Users can select different categories to search the logs. The Search feature is not case sensitive.
<b>Pagination</b>	Use these controls to jump or scroll to other pages. The total number of pages and logs is also shown.

The following information is displayed:

#	Log number.
---	-------------

<b>Date/Time</b>	The time that the log message was created.
<b>Level</b>	The level of the log message. The available logging levels are: <ul style="list-style-type: none"> <li>• Alert: Immediate action is required.</li> <li>• Critical: Functionality is affected.</li> <li>• Error: Functionality is probably affected.</li> <li>• Warning: Functionality might be affected.</li> <li>• Information: Information about normal events.</li> <li>• Debug: Information used for diagnosis or debugging.</li> </ul>
<b>User</b>	The user to which the log message relates. User can be a specific user or system.
<b>Message</b>	Detailing log message.

## Log Servers

FortiSandbox logs can be sent to a remote syslog server, common event type (CEF) server, or FortiAnalyzer. Go to *Log & Reports > Log Servers* to create new, edit, and delete remote log server settings. You can configure up to 30 remote log server entries.

The following options are available:

<b>Create New</b>	Select to create a new log server entry.
<b>Edit</b>	Select a log server entry in the list and click <i>Edit</i> in the toolbar to edit the entry.
<b>Delete</b>	Select a log server entry in the list and click <i>Delete</i> in the toolbar to delete the entry.

This page displays the following information:

<b>Name</b>	The name of the server entry.
<b>Server Type</b>	The server type. One of the following options: CEF, syslog, or FortiAnalyzer.
<b>Server Address</b>	The log server address.
<b>Port</b>	The log server port number.
<b>Status</b>	The status of the log server, <i>Enabled</i> or <i>Disabled</i> .

### To create a new server entry:

1. Go to *Log & Reports > Log Servers*.
2. Select + *Create New* from the toolbar.

## 3. Configure the following settings:

<b>Name</b>	Enter a name for the new server entry.
<b>Type</b>	Select <i>Log Server Type</i> from the dropdown list.
<b>Log Server Address</b>	Enter the log server IP address or FQDN.
<b>Port</b>	Enter the port number. The default port is 514.
<b>Status</b>	Select to enable or disable sending logs to the server.
<b>Log Level</b>	<p>Select to enable the logging levels to be forwarded to the log server. The following options are available:</p> <ul style="list-style-type: none"> <li>• Enable Alert Logs. By default, only logs of non-Clean rated jobs are sent. Users can choose to send Clean Job Alert Logs by selecting <i>Include job with Clean Rating</i>.</li> <li>• Enable Critical Logs</li> <li>• Enable Error Logs</li> <li>• Enable Warning Logs</li> <li>• Enable Information Logs</li> <li>• Enable Debug Logs</li> </ul>

4. Select *OK* to save the entry.

You can forward FortiSandbox logs to a FortiAnalyzer running 5.2.0 or later.

**To edit or delete a log server:**

1. Go to *Log and Report > Log Servers*.
2. Select a syslog server, FortiAnalyzer, or new common event entry.
3. Click the *Edit* or *Delete* button from the toolbar.

## Local Log

As there is a size limit of total logs that FortiSandbox can save locally, you can choose to turn off logs from specified severity levels.

**To turn off logs from specific severity levels:**

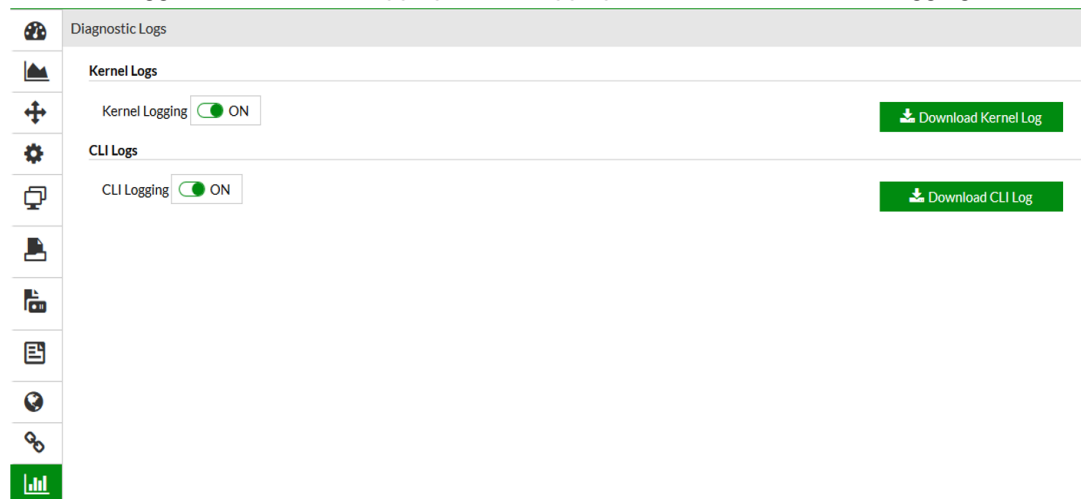
1. Go to *Log & Report > Local Log*.
2. Uncheck a level to turn off logs from that severity level.

## Diagnostic Logs

Diagnostic logs allow the FortiSandbox support team to collect information for troubleshooting purposes. When enabled, users can record and view system internal logs and CLI histories.

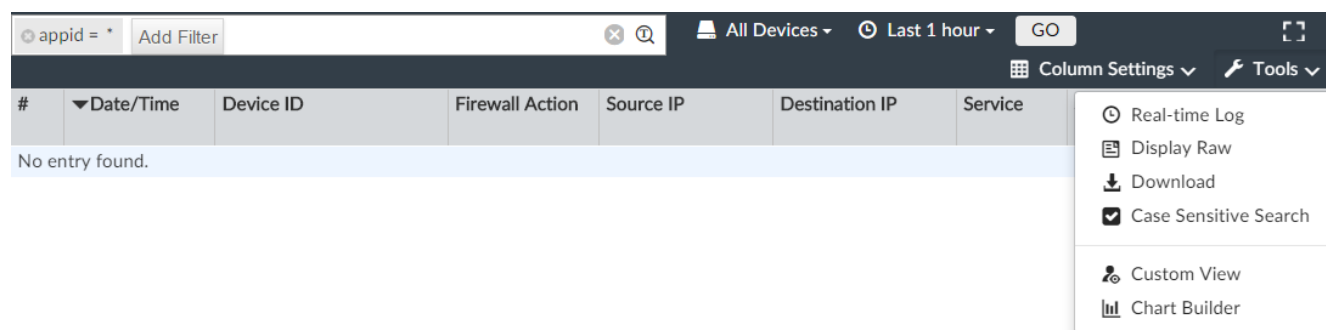
### To enable or disable Diagnostic Logs:

1. Go to *Logs & Report > Diagnostic Logs*.
2. Select the toggle next to *Kernel Logging* or *CLI Logging* to enable or disable that logging.



## Viewing logs in FortiAnalyzer

### To view FortiSandbox logs in your FortiAnalyzer:



1. Log into your FortiAnalyzer.
2. Select FortiSandbox from the *Select an ADOM* prompt.
3. Click the *Log View* tile.

The following options are available:

<b>Add Filter</b>	Enter a search term to search the log messages. You can also right-click an entry in one of the columns and select to add a search filter. Select <b>GO</b> in the toolbar to apply the filter. Not all columns support the search feature.
<b>Device</b>	Select the device in the dropdown list.
<b>Time Period</b>	Select a time period from the dropdown list. Options include: <i>Last 30 mins</i> , <i>Last 1 hour</i> , <i>Last 4 hours</i> , <i>Last 12 hours</i> , <i>Last 1 day</i> , <i>Last 7 days</i> , <i>Last N hours</i> , <i>Last N days</i> , or <i>Custom</i> .
<b>GO</b>	Select to apply the time period and limit to the displayed log entries. A progress bar is displayed in the lower toolbar.
<b>Column Settings</b>	Select specific columns to be displayed. You can also reset the columns to its default.
<b>Tools</b>	The <i>Tools</i> button provides options for changing the manner in which the logs are displayed, and search and column options.
<b>Real-time Log</b>	FortiSandbox does not support <i>Real-time Log</i> .
<b>Display Raw</b>	Select to change view from formatted display to raw log display.
<b>Download</b>	Select to download logs. A download dialog box is displayed. Select the log file format, compress with gzip, the pages to include and select <i>Apply</i> to save the log file to the management computer. This option is only available when viewing logs in formatted display.
<b>Case Sensitive Search</b>	Select to enable case sensitive search.
<b>Chart Builder</b>	Select to create a custom chart.
<b>Display Details button</b>	Detailed information on the log message selected in the log message list. The item is not available when viewing raw logs. <i>Log Details</i> are only displayed when enabled in the <i>Tools</i> menu.
<b>Search Scope</b>	Select the maximum number of log entries to be displayed from the dropdown list. Options include: <i>1000</i> , <i>5000</i> , <i>10000</i> , <i>50000</i> , or <i>All</i> .

This page displays the following information:

<b>Logs</b>	The columns and information shown in the log message list will vary depending on the selected log type and the view settings. Right-click on various columns to add search filters to refine the logs displayed. When a search filter is applied, the value is highlighted in the table and log details.
<b>Status Bar</b>	Displays the log view status as a percentage.
<b>Pagination</b>	Adjust the number of logs that are listed per page and browse through the pages.

## Customizing the log view

The message column can display raw or formatted logs. The columns in the log message list can be customized to show only relevant information in your preferred order.

## To View Raw and Formatted Logs

By default, formatted logs are displayed. The selected log view will affect available view options. You cannot customize the columns when viewing raw logs.

### To view raw logs:

Go to *Tools* and select *Display Raw* from the dropdown menu from the toolbar.

### To view formatted logs:

Go to *Tools* and select *Display Formatted* from the dropdown menu from the toolbar.

## Columns

The columns displayed in the log message list can be customized and reordered as needed. Filters can also be applied to the data in a column.

### To customize the displayed columns:

1. In the log message list view, click *Column Settings* in the toolbar.
2. From the dropdown list that is displayed, select a column to hide or display.



The available column settings will vary based on the device and log type selected.

---

3. To add more columns, select *More Columns*. In the *Column Settings* dialog box that opens, you can show or hide columns by selecting and deselecting the columns.
4. To reset to the default columns, click *Reset to Default*.
5. Click *OK* to apply your changes.

### To change the order of the displayed columns:

Place the cursor in the column header area, and then move a column by dragging and dropping.

### To filter column data:

1. You can filter log summaries by using the *Add Filter* box in the toolbar or by right-clicking an entry and selecting a context-sensitive filter.
2. Specify filters in the *Add Filter* box.  
Use Regular Search. In the selected summary view, click in the *Add Filter* box, select a filter from the dropdown list, and type a value. You can click on an operator to use it, such as greater than (>), less than (<), OR, and NOT. You can add multiple filters at a time, and connect them with "and" or "or".  
Use Advanced Search. Click the Switch to Advanced Search icon at the end of the *Add Filter* box. In Advanced Search mode, you provide the whole search criteria (log field names and values) by typing. Click Switch to Regular Search icon to go back to regular search.



From the *Tools* dropdown menu in the tool bar, you can use the Case Sensitive Search check box to specify whether you want Log View to treat the filter value that you type case-sensitive or not.

3. In the Device list, select a device.
4. In the Time list, select a time period.
5. Click *Go*.

#### To filter log summaries by using the right-click menu:

In a log message list view, right-click an entry, and select a filter criteria. The search criteria with a icon will return entries that match the filter values, while the search criteria with a icon will return entries that negate the filter values.

Depending on the column in which your mouse is located when you right-click, Log View will use the column value of the selected entry as the filter criteria. This context-sensitive filter is only available for certain columns.



For additional information, see the *FortiAnalyzer Administration Guide* in the [Fortinet Document Library](#).

## Summary Reports

The *Summary Reports* page lists all Executive Summary and Threat Activity reports including their statuses and the user that generated the report. You can download and delete the PDF reports in this page.



Report pages are not visible on the worker node in a cluster.

## Generate reports

To generate a summary report on demand, go to *Logs & Reports > Summary Report*.

You can generate executive summary and threat activity reports for a specified time period.

The following options are available:

<b>Generate Report</b>	Generate a report.
<b>Download Report</b>	Download a report.
<b>Refresh</b>	Click the button to refresh the entries displayed.
<b>Delete</b>	Delete a report.

This page displays the following information:



<b>Time Period</b>	Time period of data the report includes.
<b>Report Type</b>	Type of report.
<b>Size</b>	Report size.
<b>Status</b>	Status of the report.
<b>User</b>	Who generated the report.

## Report Center

On FortiSandbox, when a user generates a report, they can wait until the report is ready to view, or navigate away and find the report later on the Report Center page.

This page displays the following information:

<b>Status</b>	The status of report generation process: Done, Stopped, or In Progress.
<b>Start Time</b>	The time report generation starts.
<b>Finish Time</b>	The time report is ready.
<b>Report Type</b>	The type of report: PDF or CSV.
<b>Report Size</b>	The size of the report, in kilobytes.
<b>Download Count</b>	The number of times that the report has been downloaded.
<b>Progress</b>	Percentage that the report has finished
<b>Source</b>	The location that the report is scheduled to generate.
<b>Detection Period</b>	The time range of the jobs that this report contains.
<b>Actions</b>	You can view, delete, and download a report.
<b>Pagination</b>	Adjust the number of reports that are listed per page and browse through the pages. When you click on any entry on this page, detailed information about the report is displayed, including the job filtering criteria.

# Appendix A - View Details Page Reference

When you click on the *View Details* icon, a new tab will open in your browser.

The following information are descriptions of the *View Details* page for:

- *Last drill-down level of the FortiView pages*
- *Scan Input > File and URL On Demand*
- *File Detection > Malicious Files*
- *File Detection > Suspicious Files*
- *File Detection > Clean Files*
- Job lists from Network Share scans and drill-down of Dashboard widget

FortiSandbox shows detailed forensic information of a job. They are grouped in three parts: *Overview*, *Tree view*, and *Details*.

The *Overview* tab shows overview information of a job, including input source, scan conditions, file type, etc. A global map is displayed to show the source and destination of the file or URL.

Item	Description
<b>File type</b>	The file type, <i>High Risk Downloader</i> for example.
<b>Virus Name</b>	The name of the virus.
<b>FortiGuard Encyclopedia Analysis</b>	Select to view the FortiGuard Encyclopedia analysis of the file if the file has a Malicious rating. This page provides analysis details, detection information, and recommended actions.
<b>Mark as clean (false positive) / Mark as suspicious (false negative)</b>	<p>Select to mark the file as clean (false positive) or suspicious (false negative). This field is dependent on the file risk type. In the <i>Apply Override Verdict</i> dialog box type a comment and select <i>Submit</i> or <i>Submit feedback to Cloud</i> to send the file to the FortiGuard team for analysis.</p> <p>After a file has an overridden verdict, its future rating will be the overridden one until you reset the verdict.</p> <p>After a file's verdict is overridden, the job will be listed in the <i>Scan Profile &gt; Overridden Verdicts</i> page for easy tracking.</p>
<b>Export Job Details to Page</b>	Export the job details to a PDF report.
<b>Download Original File</b>	<p>Download the password protected original file (.zip format) to your management computer for further analysis. The default password for this file is <i>fortisandbox</i>.</p> <p><b>Caution:</b> The original file should only be unzipped on a management computer in an analysis environment.</p>
<b>Received</b>	The date and time the file was received by FortiSandbox.
<b>Started</b>	The date and time the scan started and the timezone.
<b>Status</b>	The status of the scan. Status: <i>Done</i> , <i>Canceled</i> , <i>Skipped</i> , and <i>Timed Out</i> .

Item	Description
<b>Rated by</b>	Which scan module made the rating decision, such as the AV Scanner, FortiSandbox Community Cloud, Static File Scan or VM Engine.
<b>Submit Type</b>	The input source of the file such as FortiMail.
<b>Source IP</b>	The malware host IP address.
<b>Destination IP</b>	The IP address of the client that downloaded the virus.
<b>Digital Signature</b>	The digital signature availability status of the scanned file.
<b>Scan Bypass Configuration</b>	When available, the scan bypass configuration will be displayed.
<b>SIMNET</b>	When the scan was done, its SIMNET is on.
<b>Virus Total</b>	By clicking the Virus Total link, a new page will open to query <a href="https://www.virustotal.com">https://www.virustotal.com</a> . Only a limited number of queries per minute is allowed without manual interaction with the Virus Total website.
<b>The Original Job of this Rescan Job</b>	Click the link to view the original job if this one is an AV rescan or On-Demand rescan job.
<b>Details Information</b>	View additional file information including the following: Packers, File Type, Downloaded From, File Size, Service, MD5, SHA1, SHA256, ID, Submitted By, Submitted Filename, Filename, Received, Scan Start Time, VM Scan Start Time, VM Scan End Time, VM Scan Time, Scan End Time, Total Scan Time, Scan Unit, Launched OS, and Infected OS.  If the file is from FortiMail, Email related information, such as the Email Sender, Receiver, and Subject will also be shown.
<b>Indicators</b>	A summary of the Malware's behavior indicators if there are any.
<b>Behavior Summary</b>	View the file behavior summary.

The *Tree View* shows a tree for file's static structure or file's parent-child process relationship when it executes inside a guest VM. You can drag the tree using the mouse and zoom in or out using the mouse wheel. If there is suspicious activity with one tree node, its label will be colored red. Clicking a node in the tree will open more information in tab format. Suspicious information is shown in the color red, so you can quickly locate it.

The *Details* part shows analysis details for each detection OS that is launched during the scan. It shows information in a different way from *Tree View* part. The following are details of information displayed:

Item	Description
<b>Analysis Details</b>	View the following analysis details for each Detection OS that is launched during the scan. Each Detection OS's detail will be shown in a separate tab. The Infected OS will have a VM Infected icon in its tab title.  If the Malware is detected by non-Sandboxing scan, such as FortiGuard static scan, the tab title is displayed as <i>N/A</i> .
<b>Behavior Chronology Chart</b>	View the file's behavior over time and its density during its execution. Clean behaviors: green bubble.

Item	Description
	<p>Suspicious behaviors: red, blue, or orange bubble.</p> <p>The higher the bubble, the more serious the event is.</p> <p>To view the event details, hover the mouse on top of the bubble.</p> <p>If a file scan is scanned with more than one VM type, the VM tab will dynamically switch to the chart for that type.</p> <p>If the file hits any imported YARA rule, a YARA tab will appear with detailed information. including:</p> <ul style="list-style-type: none"> <li>• The hit rule</li> <li>• Rule's risk level</li> <li>• Rule set name</li> <li>• Link to original YARA rule file</li> </ul>
<b>Captured Packets</b>	<p>Select the <i>Captured Packets</i> button to download the tracer PCAP file to your management computer. The packet capture (PCAP) file contains network traffic initiated by the file. You must have a network protocol analyzer installed on your management computer to view this file.</p> <p>The <i>Captured Packets</i> button is not available for all file types.</p>
<b>Tracer Package</b>	<p>Download the compressed .tar file containing the tracer log and related files. The password protected /backup folder in the tracer log contains information about the program's execution. The default password for this file is <i>fortisandbox</i>.</p> <p><b>Caution:</b> The tracer log should only be unzipped on a management computer in an analysis environment.</p>
<b>Tracer Log</b>	A text file containing detailed information collected inside the Sandbox VM.
<b>STIX IOC</b>	Download the IOC in STIX2 format.
<b>Screenshot</b>	Download a screenshot image when the file was running in the sandbox. This image is not always available.
<b>YARA Hits</b>	If the file hits FortiSandbox internal YARA rules, detailed information is displayed.
<b>Office Behaviors</b>	Suspicious indicators detected by FortiGuard advanced Office file static scan engine.
<b>Virtual Simulator</b>	Suspicious indicators detected by FortiGuard advanced Web file static scan engine.
<b>Indicators</b>	<p>A summary of behavior indicators, if available.</p> <p>When detailed information is available below, a question mark icon is displayed. When clicked, detailed information is displayed. For some operations, such as File Operations, users can download files in a password protected ZIP format.</p>
<b>MITRE ATT&amp;CK MATRIX</b>	<p>Displays malware's attack techniques and tactics.</p> <p>By default, a light version is displayed. Click the toggle button to swap between the Lite Matrix and Full Matrix.</p>
<b>Botnet Info</b>	The botnet name and target IP address.
<b>Files Created</b>	The executable has been observed to drop some files.

Item	Description
	Click the <i>Files Created</i> dropdown icon to view the files created by the file. This field may not be available for all file types.
<b>Files Deleted</b>	This executable has been observed to delete some files. Click the <i>Files Deleted</i> dropdown icon to view the files deleted by the file. This field may not be available for all file types.
<b>File Modified</b>	The executable file has been observed to modify some files.
<b>Launched Processes</b>	The executable spawns some processes. Click the <i>Launched Processes</i> dropdown icon to view the processes launched by the file. This field may not be available for all file types.
<b>Registry Changes</b>	The executable applies autostart registry modifications to be able to start itself automatically. Click the <i>Registry Changes</i> dropdown icon to view the registry changed made by the file. This field may not be available for all file types.
<b>Network Behaviors</b>	Users that are infected by this executable will notice HTTP connections with certain URL/IP addresses. Click the <i>Network Behaviors</i> dropdown icon to view the network behavior of the file. This field may not be available for all file types. For certain document files, if they contain malicious URLs, those URLs are displayed here. Users can select a URL to display its detailed information, like rating history and visit volume history.
<b>Behaviors In Sequence</b>	The executable file's behavior during execution, in time sequence.
<b>Tracer/Rating Engine Version</b>	The tracer/rating package version is displayed at the bottom of the job detail page and in the PDF Report.
<b>Print</b>	Click the print icon to print the malware details page information.
<b>Open in New Window</b>	Click the icon to open the page in a new web browser window.

## Appendix B - FortiCloud Sandbox

In addition to physical and virtual deployments, FortiSandbox is also available as a cloud-based advanced threat protection service, integrated with FortiGate, FortiMail, and FortiWeb, called FortiCloud Sandbox. FortiCloud Sandbox requires an active FortiCloud account for use with FortiGate, FortiMail, and FortiWeb. Below, you can see a comparison of the features, deployments, and capabilities of the FortiCloud Sandboxing service compared to a physical or virtual deployment set up on-premises (FortiSandbox Appliance).

### Deployment

Deployment options	FortiSandbox Appliance	FortiCloud Sandbox
FortiGate integration	Yes	Yes
FortiMail and FortiWeb integration	Yes	Yes
Fabric integration (FortiClient, FortiWeb, FortiADC, FortiManager, FortiAnalyzer, FortiSIEM)	Yes	
Multiple appliance options (500F, 1000D, 1000F, 2000E, 3000E, and FSA-VM)	Yes	
On-site deployment (centralized or distributed)	Yes	
Third-party products NetworkShare integration (CarbonBlack, BBC Mode, ICAP Client, API)	Yes	

### Detection

Detection capabilities	FortiSandbox Appliance	FortiCloud Sandbox
Device input (FortiGate, FortiMail, FortiWeb, FortiClient, and others)	Yes	Yes
File based detection	Yes	Yes
On-demand scanning - manual upload of suspicious files	Yes	Yes
URL detection - host traffic to malicious sites	Yes	Yes*
Adapters for third-party products	Yes	
API input (REST API)	Yes	

Detection capabilities	FortiSandbox Appliance	FortiCloud Sandbox
BotNet detection via sniffer	Yes	
Network attack detection via sniffer	Yes	
Network share input (file share scanning CIFS and NFS)	Yes	
On-demand scanning - manual upload of URL list	Yes	
Sniffer input via TAP or Mirror/Span port	Yes	
URL detection - ICAP client integration	Yes	
URL detection - REST API integration for web scanning	Yes	

\*Available with FortiCloud 3.1.x onwards.

## File type and protocol support

Profiling, file type, and protocol support	FortiSandbox Appliance	FortiCloud Sandbox
A/V and CPRL pre-filter support for all file types regardless of operating system	Yes	Yes
Archived - .tar, .gz, .tar.g, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .and arj	Yes	Yes
Executable - .exe, .dll, PDF, Windows Office, and Javascript	Yes	Yes
FortiGate integrated - HTTP, SMTP, POP3, IMAP, MAPI, FTP, SMB, IM and SSL and encrypted equivalent	Yes	Yes
Media - .avi, .mpeg, .mp3, and .mp4	Yes	Yes
Share threat intelligence among distributed installations	Yes	Yes
Virtual machine sandboxing	Yes	Yes
FortiMail integrated - SMTP, POP3, and IMAP	Yes	Yes*
Ability to fine tune the scanning environment	Yes	
Scan user-defined file types	Yes	
Utilize customized virtual machines	Yes	

\*FortiMail integration supported from version 5.3.x onwards.

## Alerting, reporting and monitoring

Alerting, reporting, monitoring and logging	FortiSandbox Appliance	FortiCloud Sandbox
Filter by rating (Malicious, Suspicious - Low, Medium, High Risk, Clean)	Yes	Yes
On-demand summary and threat detail reporting by date range	Yes	Yes
FortiAnalyzer integration	Yes	Yes *
Syslog to remote log server	Yes	Yes *
At-a-glance view submission by device (easily see if one site is submitting more than others)	Yes	
Common event format to remote log server	Yes	
Consolidated or separate views of input by device, network, sniffer, or on-demand submission	Yes	
Detailed alerting with source, destination, protocol, file name and forensic/incident response info	Yes	
Filtering and search capabilities - granular drill down and export to detailed report in .PDF format	Yes	
Scheduled summary and threat detail reporting delivered via email	Yes	
File submission summary web view		Yes
Limited daily canned report		Yes
Separate views for each device (not reportable or monitored in aggregate)		Yes
Summary email alerting with source, destination, protocol, and file name		Yes

\*Available through FortiGate.

## Forensic, auditing, and third-party tools

Forensic, auditing, and third-party tools	FortiSandbox Appliance	FortiCloud Sandbox
Forensic/incident response information	Yes	Yes
Source and destination IP address for tracking IOC	Yes	Yes



Forensic, auditing, and third-party tools	FortiSandbox Appliance	FortiCloud Sandbox
Export suspicious files for further analysis or inspection by third-party applications	Yes	
PCAP, TracerLog, and screen captures	Yes	

## Change Log

Date	Change Description
2020-07-27	Initial release.



**FORTINET®**



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.