FORTINET

FortiSandbox - Administration Guide

Version 3.2.1

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

June 04, 2021
FortiSandbox 3.2.1 Administration Guide
34-321-631294-20210604

TABLE OF CONTENTS

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.

FortiSandbox rating can be performed by either the standard method or by using artificial intelligence (AI) mode. In AI mode, the AI engine uses machine learning technology to analyze the behavior of thousands of known malware. FortiSandbox uses this engine to inspect file behavior inside a VM to detect indicators of new malware.

AI mode can be toggled in the CLI using the command `ai-mode`.

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

Infection Type	Description
Infector	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.
Worm	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.

Infection Type	Description
Botnet	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.
Hijack	Hijack malware attempts to hijack the system by modifying important registry keys or system files.
Stealer	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.
Backdoor	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.
Injector	Injector malware injects malicious code into system processes to perform tasks on its behalf.
Rootkit	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.
Adware	Adware malware is a software package which attempts to access advertising websites. Adware displays these unwanted advertisements to the user.
Dropper	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.
Downloader	Downloader malware attempts to download other malicious programs.
Trojan	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.
Riskware	Riskware malware has security-critical functions which pose a threat to the computer.
Grayware	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.
Unknown	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.

Windows XP is not longer supported. If you currently use Windows XP, migrate to a later Windows version.

About this document

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

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

FortiGate

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

FortiMail

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 or later.

For more information, see the *FortiMail Administration Guide* in the Fortinet Document Library.

FortiClient

To configure your FortiClient to send files to the FortiSandbox and receive results, your FortiClient must be running FortiClient 5.4.0 or later.

For more information, see the *FortiClient Administration Guide* in the Fortinet Document Library.

FortiWeb

To configure your FortiWeb to submit files for FortiSandbox to evaluate, your FortiWeb must be running 5.4.0 or 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.

In version 3.2.0 and higher, the first time you log in using the CLI, you must set the admin password (6–64 characters).

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 console cable provided.
2. Start a terminal emulation program on the management computer.
3. Use the following settings:

Serial line to connect to	COM1
Speed (baud)	9600
Data bits	8
Stop bits	1
Parity	None
Flow Control	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* in the Fortinet Document Library.

Using the GUI

This section describes general information about using the GUI to access FortiSandbox using a web browser. This section also explains common administrator tasks you can do in the GUI.

This section includes the following topics:

- GUI overview
- CLI Console
- Default port information

GUI overview

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

Connecting to the GUI

The FortiSandbox unit is configured and managed using the GUI. This topic covers connecting to the unit via the GUI.

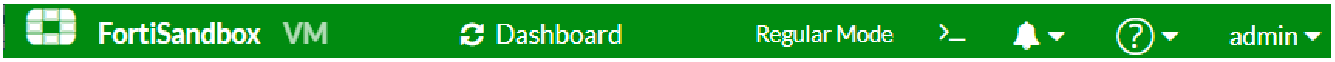
To connect to the FortiSandbox GUI:

1. Connect the port1 (administration) interface or any other administrative port set through the CLI command `set admin-port` to a management computer using an 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, enter the *Password*, 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.

GUI interface

The GUI interface displays a green banner at the top showing system information and command buttons.



The following options are available:

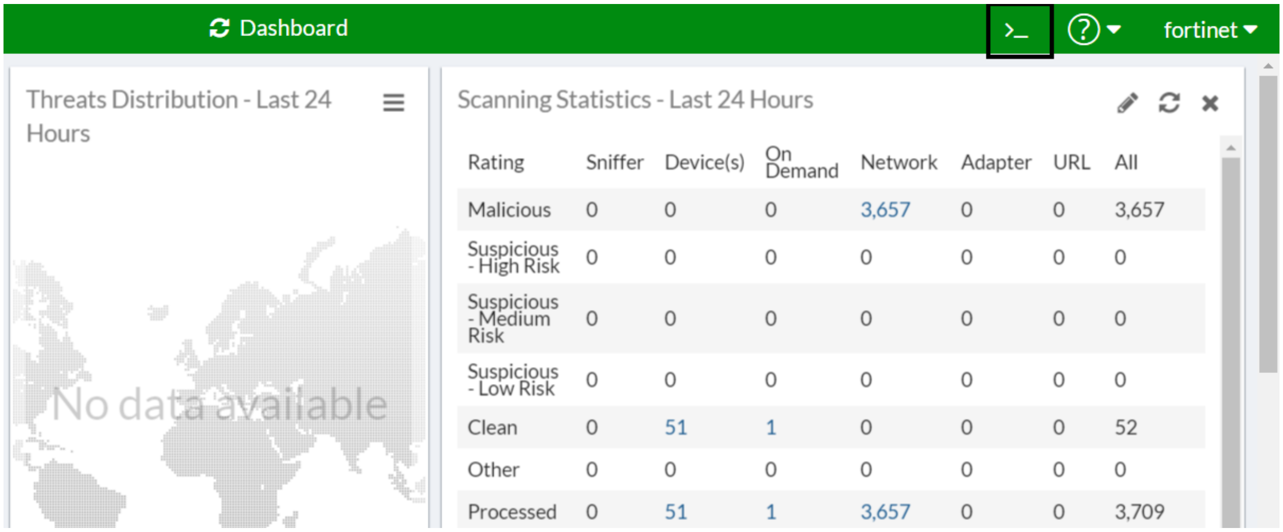
Refresh	Click the *Refresh* icon to refresh the page. For some pages such as *FortiView* > *File Scan Search*, if you click *Refresh*, you lose your current search criteria. Use the *Refresh* icon inside the content pane to continue searching without losing your criteria.
Regular Mode / AI Mode	Shows if FortiSandbox is running in regular mode or AI mode. After changing modes, refresh the page to see the change. To enable AI mode, use the CLI command `ai-mode -e` To disable AI mode, use the CLI command `ai-mode -d`
CLI Console	Click the *CLI Console* button >__ to open the CLI Console pane. See CLI Console on page 13.
Notifications	The bell icon displays messages and notifications that require your attention.
Online Help and Video Tutorials	The question mark icon lets you quickly access the *Online Help* and *Video Tutorials*. *Online Help* links to this Administration Guide in the Fortinet Document Library where you can find information about FortiSandbox and other Fortinet products. *Video Tutorials* links to the Fortinet Video Library for FortiSandbox at https://video.fortinet.com/product/fortisandbox where you can find video tutorials showing how to integrate other Fortinet products, including FortiGates, to FortiSandbox.
User	The user dropdown list lets you change the user password or logout.

CLI Console

You can log into the CLI Console in a window in the GUI. You can issue commands in the CLI Console just like the FortiSandbox CLI.

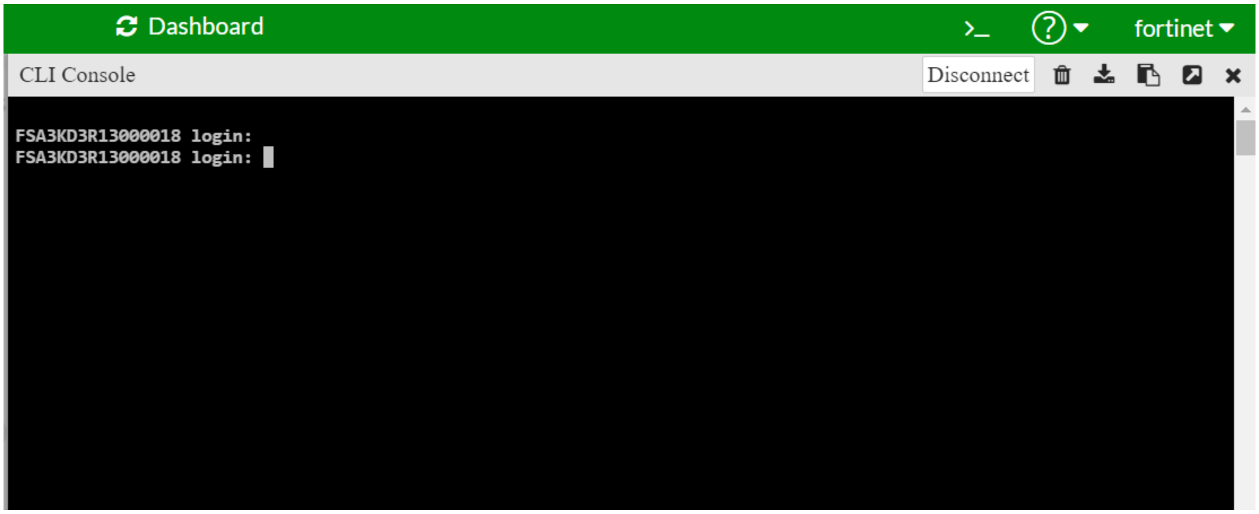
To connect to the CLI Console:

1. In the banner, click the CLI Console button >__ at the top right.


Dashboard
>_
?
fortinet
Threats Distribution - Last 24 Hours
No data available
Scanning Statistics - Last 24 Hours

Rating	Sniffer	Device(s)	On Demand	Network	Adapter	URL	All
Malicious	0	0	0	3,657	0	0	3,657
Suspicious - High Risk	0	0	0	0	0	0	0
Suspicious - Medium Risk	0	0	0	0	0	0	0
Suspicious - Low Risk	0	0	0	0	0	0	0
Clean	0	51	1	0	0	0	52
Other	0	0	0	0	0	0	0
Processed	0	51	1	3,657	0	0	3,709

The CLI Console pane opens.



```
FSA3KD3R13000018 login:
FSA3KD3R13000018 login:
```

2. Click *Connect* to connect to the console.
   The console prompts you for your login information.
   You can issue commands in the CLI Console just like the FortiSandbox CLI. For more information on FortiSandbox CLI commands, see the *FortiSandbox CLI Reference Guide* in the Fortinet Document Library.
3. To disconnect, click *Disconnect* or use *Ctrl+C*.

The CLI Console has the following buttons:

Connect / Disconnect	Toggles the connection to the console.
🗑	Clears the console.

⬇	Downloads the contents of the console to a text file `cliConsole.txt` on your local PC. Maximum is 1000 lines.
⧉	Copies the contents of the console to the clipboard. Maximum is 1000 lines.
↗	Expands and detaches the console from the GUI and opens it in a new browser tab or window.
✖	Closes the CLI Console.

The CLI Console can only connect to a local FortiSandbox.

In HA-Cluster, you cannot use the primary node to open a worker node's CLI Console.

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	TCP ports, 22 (SSH), 23 (Telnet), 80 and 443 (GUI), 514 (OFTP communication with FortiGate, FortiWeb, FortiClient & FortiMail), SNMP local query port. FortiGuard Distribution Servers (FDS) use TCP port 8890 for download. The FortiSandbox will use a random port picked by the kernel. FortiGuard Web Filtering servers use UDP port 53 or 8888. The FortiSandbox will use a random port picked up by the kernel. Fortinet FortiSandbox VM download uses TCP port 443 for download. The FortiSandbox will use a random port picked by the kernel. 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. 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.

Port (Interface)	Type	Default Open Ports
Port2, Port4	RJ-45	No service listens except OFTP. If user specifies it as an administration port through CLI command `set admin-port`, 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 `set admin-port`, TCP ports 80 and 443 will be opened for web UI.

FortiSandbox 3000D default ports:

Port (Interface)	Type	Default Open Ports
Port1	RJ-45	TCP ports, 22 (SSH), 23 (Telnet), 80 and 443 (GUI), 514 (OFTP communication with FortiGate, FortiWeb, FortiClient & FortiMail). SNMP local query port. FortiGuard Distribution Servers (FDS) use TCP port 8890 for download. The FortiSandbox will use a random port picked by the kernel. FortiGuard Web Filtering servers use UDP port 53 or 8888. The FortiSandbox will use a random port picked up by the kernel. 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. 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	RJ-45	No service listens except OFTP (TCP port 514). If user specifies it as an administration port through CLI command `set admin-port`, 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 `set admin-port`, 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 `set admin-port`, TCP ports 80 and 443 will be opened for web UI.

FortiSandbox 1000D default ports:

Port (Interface)	Type	Default Open Ports
Port1	RJ-45	TCP ports 22 (SSH), 23 (Telnet), 80 and 443 (GUI), 514 (OFTP communication with FortiGate, FortiWeb, FortiClient & FortiMail). FortiGuard Distribution Servers (FDS) use TCP port 8890 for download. The FortiSandbox will use a random port picked by the kernel. FortiGuard Web Filtering servers use UDP port 53 or 8888. The FortiSandbox will use a random port picked up by the kernel. 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. 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 `set admin-port`, 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 `set admin-port`, 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.

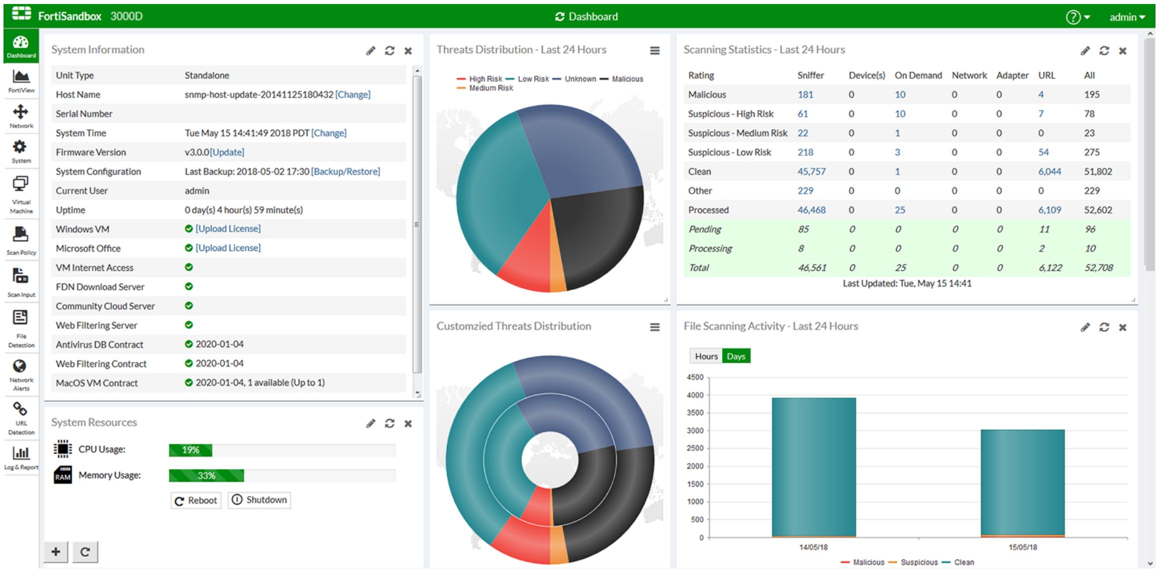
For more information on FortiSandbox 1000D, FortiSandbox 3000D, FortiSandbox 3500D, FortiSandbox 2000E, and FortiSandbox 3000E interfaces, see Interfaces on page 50.

Dashboard

The System Status dashboard displays widgets that provide system information and enable you to configure basic system settings. All widgets appear on a single dashboard, that you can customize.

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

In *Expanded* mode, you can quickly locate a menu item by entering the term in the *Search* bar at the top of the left panel.



System Information

Unit Type	Standalone
Host Name	snmp-host-update-20141125180432 [Change]
Serial Number	
System Time	Tue May 15 14:41:49 2018 PDT [Change]
Firmware Version	v3.0.0[Update]
System Configuration	Last Backup: 2018-05-02 17:30 [Backup/Restore]
Current User	admin
Uptime	0 day(s) 4 hour(s) 59 minute(s)
Windows VM	✓ [Upload License]
Microsoft Office	✓ [Upload License]
VM Internet Access	✓
FDN Download Server	✓
Community Cloud Server	✓
Web Filtering Server	✓
Antivirus DB Contract	✓ 2020-01-04
Web Filtering Contract	✓ 2020-01-04
MacOS VM Contract	✓ 2020-01-04, 1 available (Up to 1)

System Resources

Scanning Statistics - Last 24 Hours

Rating	Sniffer	Device(s)	On Demand	Network	Adapter	URL	All
Malicious	181	0	10	0	0	4	195
Suspicious - High Risk	61	0	10	0	0	7	78
Suspicious - Medium Risk	22	0	1	0	0	0	23
Suspicious - Low Risk	218	0	3	0	0	54	275
Clean	45,757	0	1	0	0	6,044	51,802
Other	229	0	0	0	0	0	229
Processed	46,468	0	25	0	0	6,109	52,602
Pending	*85*	*0*	*0*	*0*	*0*	*11*	*96*
Processing	*8*	*0*	*0*	*0*	*0*	*2*	*10*
Total	*46,561*	*0*	*25*	*0*	*0*	*6,122*	*52,708*

Last Updated: Tue, May 15 14:41

If the unit is the primary node in a cluster, the displayed data shows a summary of all nodes in the cluster.

The following widgets are available:

System Information	Displays basic information about the FortiSandbox system, such as the serial number, system up time, and license status information.
System Resources	Displays the real-time usage status of the CPU and memory.
Scanning Statistics	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.
Scanning Activity	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.
Threats Distribution	Displays threat level distribution over a selected period.
Customized Threats Distribution	Displays threat level distribution over two customized time intervals.

Quick Download	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.
Sniffer Traffic Throughput	Displays sniffed traffic throughput across time.
Top Devices	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.
Top Critical Logs	Displays recent critical logs, including the time they occurred and a brief description.
Pending Job Statistics	Displays pending scan job numbers for a period of time. This widget allows you to monitor the workload trend on your FortiSandbox.
Disk Monitor	Displays the RAID level and status, disk usage, and disk management information. This widget is only available in hardware based models.

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:

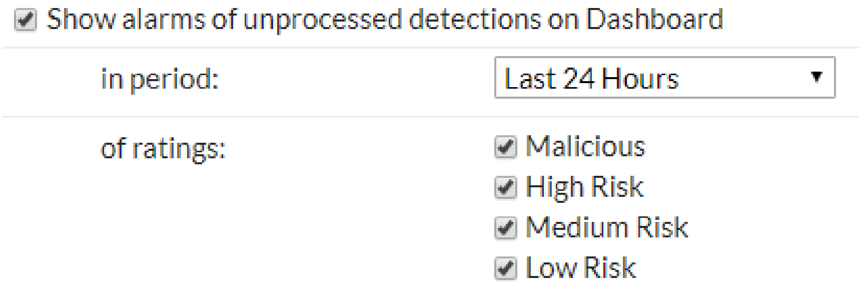
Custom widget title	Optionally, type a custom title for the widget. Leave this field blank to use the default widget title.
Refresh interval	Enter a refresh interval for the widget, in seconds. Some widget have default refresh values: • Scanning Statistics: 600 • Top Devices: 300 • Scanning Activity: 300 • System Resources: 60 • Top Critical Logs: 3600 • Disk Monitor: 300
Top Count	Select the number of entries to display in the widget. The top count can be between 5 to 20 entries. This option is only available in the following widgets: *Top Devices*, *Top Critical Logs*.
Time Period	Select a time period to be displayed from the dropdown list: *Last 24 hours*, *Last 7 days*, *Last 4 weeks*. This option is only available on the following widgets: *Scanning Statistics*, *Top Devices*, *Threats Distribution*, and *Scanning Activity*.

Show unprocessed detection alert notifications on Dashboard

An unprocessed detection alert occurs when a record is in the *Action Required* state in FortiView. These records can also be seen by navigating to *FortiView* > *Operation Center* > *Action* > *Action Required*. FortiSandbox will record these items and display them as an unprocessed detection alert depending on the configuration below.

To show alarms of unprocessed detections on Dashboard:

1. Go to *System* > *Settings*.
2. Enable *Show alarms of unprocessed detections on Dashboard*.



☑ Show alarms of unprocessed detections on Dashboard

in period: Last 24 Hours ▾

of ratings:
☑ Malicious
☑ High Risk
☑ Medium Risk
☑ Low Risk

3. Configure the time period to display unprocessed detections.
4. Select the ratings for unprocessed detections.

After you enable *Show alarms of unprocessed detections on Dashboard*, the banner displays a notification under the bell icon showing *## unprocessed detections in last xx days/hours/weeks*.

In HA-Cluster mode, each node can have its own *Show alarms of unprocessed detections on Dashboard* setting.

System Information

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

Unit Type	The HA cluster status of the device: *Standalone*, *Primary* (formerly *Master*), *Secondary* (formerly *Primary Slave*), or *Worker* (formerly *Regular Slave*). In an HA-Cluster, click *Change* to change the cluster status of the device. If the rating engine is not available or out-of-date, a red blinking *No Rating Engine* message appears.
Host Name	The name assigned to this FortiSandbox unit. Click *Change* to edit the FortiSandbox host name.
Serial Number	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.
System Time	The current time on the FortiSandbox internal clock or NTP server. Select *[Change]* to configure the system time.
Firmware Version	The version and build number of the firmware installed on the FortiSandbox unit. When new firmware is available, a blinking *New firmware available* 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.

System Configuration	The date and time of the last system configuration backup. Select *Backup/Restore* to browse to the *System Recovery* page.
Current User	The administrator that is currently logged on to the system.
Uptime	The duration of time that the FortiSandbox unit has been running since boot up.
Windows VM	Microsoft Windows VM license activation and initialization status. An up icon means the Microsoft Windows VM is activated and initialized. A *Caution* icon means the Microsoft Windows VM is initializing or having issues. Hover the pointer on the status icon to view detailed information. For more information, see *Log & Report* > *VM Events*. 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 *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 might need to purchase Windows 10 license keys from Fortinet. After purchase, the user should download their license file from the Fortinet Customer Service & Support portal. Then, click the *[Upload License]* 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.
Microsoft Office	Microsoft Office product activation status. Select to upload a Microsoft Office license file. An *Up* icon means Microsoft Office is activated and initialized. A *Caution* icon means Microsoft Office is initializing or having issues. The *Up* icon and *Caution* icon can both appear when Microsoft Office software is activated on some enabled VMs but not activated on other enabled VMs. Hover the pointer on the status icon to view detailed information. For more information, see *Log & Report* > *VM Events*.
VM Internet Access	Status of the FortiSandbox guest VM accessing the outside network. An *Up* icon means the VM can access the outside network. A *Caution* icon means the VM cannot access the outside network. Hover the pointer on the status icon to view detailed information. If the VM cannot access the outside network, a simulated network (SIMNET) starts by default. SIMNET provides responses of popular network services, like `http` 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. FortiSandbox guest VM accesses external network through port3. The next-hop gateway and DNS settings can be configured in *Scan Policy* > *General* > *Allow Virtual Machines to access external network through outgoing port3*. If port3 of FortiSandbox is behind a firewall with antivirus inspection enabled, an icon will be displayed.
FDN Download Server	Displays the status of the FDN download server. When the FDN download server is inaccessible, no update packages will be downloaded.

	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.
Community Cloud Server	Displays the status of the Sandbox Community Cloud server. 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.
Web Filtering Server	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.
Antivirus DB Contract	The date that the antivirus database contract expires. If the contract expires within 15 days, a caution icon will appear.
Web Filtering Contract	The date that the web filtering contract expires. If the contract expires within 15 days, a caution icon will appear.
MacOS VM Contract	The date the MacOS contract expires and the number of remote clones reserved in Fortinet MacOS cloud. In cluster mode, the total reserved clone numbers displays on the primary (master) node. All cluster units share a collected pool of reserved clones from each unit. This means that even nodes with no MacOS VM contract can still upload MacOSX files to the cloud for scannning.
Windows Cloud VM Contract	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:

CPU Usage	Gauges the CPU percentage usage.
Memory Usage	Gauges the Memory percentage usage.
RAM Disk Usage	Gauges the RAM Disk percentage usage. RAM Disk is used by the VM clone system.
Reboot/Shutdown	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:

Rating	The file rating refers to the rating categories.
Sniffer, Device(s), On-Demand, Network, Adapter, URL, All	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.
Malicious	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.
Suspicious - High Risk	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.
Suspicious - Medium Risk	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.
Suspicious - Low Risk	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.
Clean	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.
Other	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.
Processed	The total number of files processed for each input type in the selected time period.
Pending	The number of files pending. Pending files are files that are 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.
Processing	The number of files that are being processed.
Total	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 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:

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

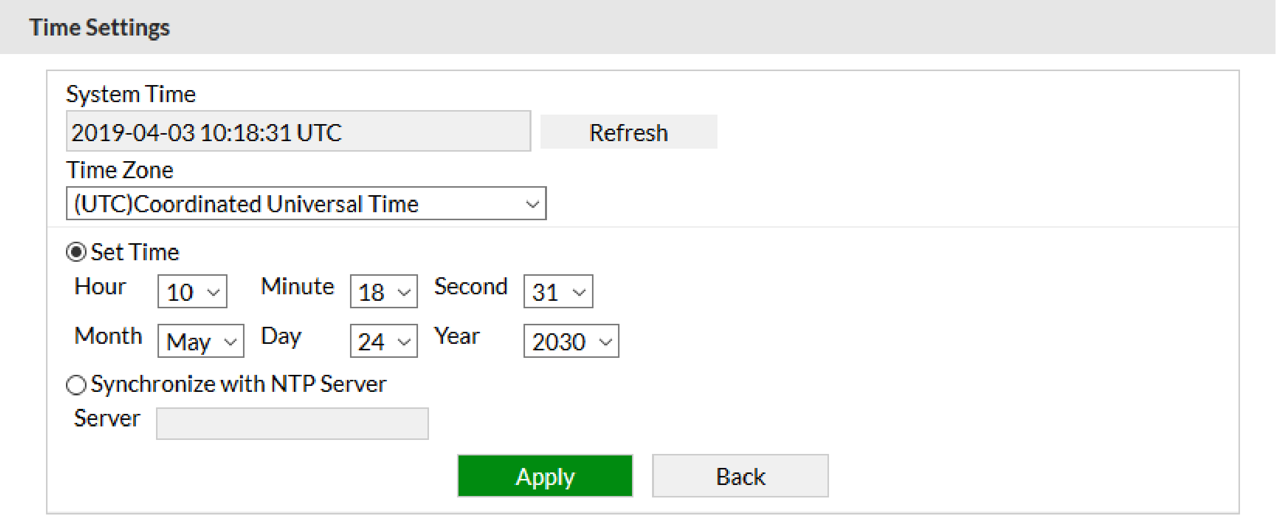
In this page you can also reset all widgets to their default settings.

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 *Change*.



Time Settings

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

Time Zone: (UTC)Coordinated Universal Time

● Set Time

Hour: 10 Minute: 18 Second: 31

Month: May Day: 24 Year: 2030

○ Synchronize with NTP Server

Server:

3. Configure the following settings:

System Time	The date and time according to the FortiSandbox unit's clock at the time that this tab was loaded.
Time Zone	Select the time zone in which the FortiSandbox unit is located.

Set Time	Select this option to manually set the date and time of the FortiSandbox unit's clock, then select the *Hour*, *Minute*, *Second*, *Month*, *Day*, and *Year* fields before you select *Apply*.
Synchronize with NTP Server	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.
Server	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, go to http://www.ntp.org. 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 in 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 or external site 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*.
3. Under Remote Backup, configure the following settings:

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

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

To restore the FortiSandbox configuration:

1. Go to *Dashboard >System Information widget > System Configuration*.
2. Select *Backup/Restore*.
3. Click *Browse...*, locate the backup file on your management computer, then select *Restore* to load the backup file.
4. 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.

To backup the FortiSandbox configuration using SCP or TFTP:

1. Open a CLI console window.
2. Enter the *backup-sysconf* command followed by the following syntax:

```
backup-sysconf [-s|-t[scp|tftp]|-u|-f]
```

The options available are as follows:

-h Help Information

-s Remote SCP/TFTP server IP

-t Protocol type: SCP or TFTP

-u Scp/tftp user name

-f Remote server folder and the backup file name

Example 1:

```
backup-sysconf –s1.2.3.4 –utest –tscp –f/home/test/fsa/backup.conf
```

Example 2:

```
backup-sysconf –s1.2.3.4 –utest –ttftp –f/home/test/fsa/backup.conf
```

To restore the FortiSandbox configuration using SCP, FTP or TFTP:

1. Open a CLI console window.
2. Enter the *restore-sysconf* command followed by the following syntax:

```
restore-sysconf [-s|-t[scp|tfp|tftp]|-u|-f|-o]
```

The options available are as follows:

-h Help Information

-s Remote SCP/FTP/TFTP server IP

-t Protocol type: SCP, FTP or TFTP

-u Scp/ftp/tftp user name

-f Remote server folder and the backup configuration file name

-o [Optional] Restore Administrators, Admin Profiles, Certificates, LDAP Servers and Radius Servers

Example 1:

```
restore-sysconf –s1.2.3.4 –utest –tscp –f/home/test/fsa/backup.conf -o
```

Example 2:

```
restore-sysconf –s1.2.3.4 –utest –ttftp –f/home/test/fsa/backup.conf
```

Example 3:

```
restore-sysconf –s1.2.3.4 –utest –tftp –f/fsa/backup.conf -o
```

FortiView

Use the FortiView pages to view and search threats detected by FortiSandbox.

Operation Center	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.
Threats by Hosts	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.
Threats by Files	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.
Threats by Devices	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.
File Scan Search and URL Scan Search	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:

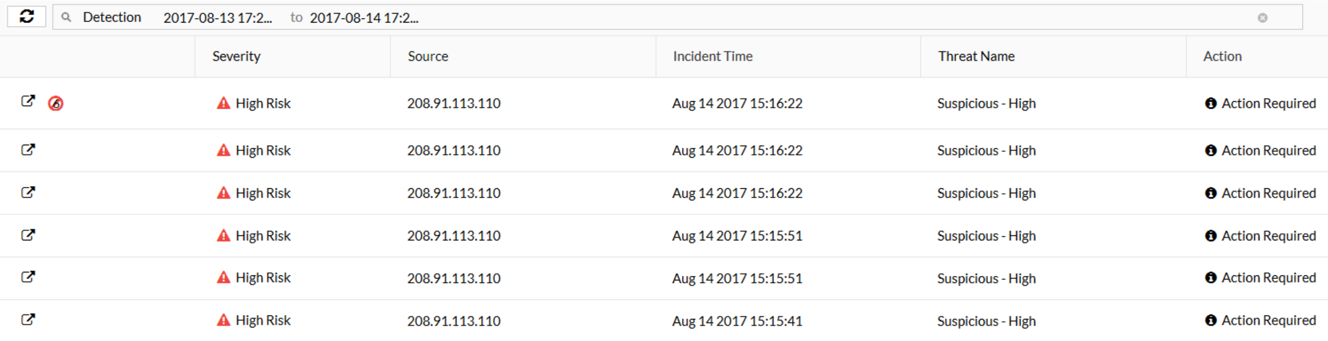
- Operation Center
- Threats by Topology
- Threats by Hosts
- Threats by Files
- Threats by Devices
- File Scan Search
- URL Scan Search

Operation Center

Use this page to view malware that has been detected and its status from a security update perspective.

When a dynamic signature is sent back to FortiGate, FortiMail, or FortiClient, check the status information that it has been done.

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



Detection 2017-08-13 17:2... to 2017-08-14 17:2...

	Severity	Source	Incident Time	Threat Name	Action
↗	⚠ High Risk	208.91.113.110	Aug 14 2017 15:16:22	Suspicious - High	ℹ Action Required
↗	⚠ High Risk	208.91.113.110	Aug 14 2017 15:16:22	Suspicious - High	ℹ Action Required
↗	⚠ High Risk	208.91.113.110	Aug 14 2017 15:16:22	Suspicious - High	ℹ Action Required
↗	⚠ High Risk	208.91.113.110	Aug 14 2017 15:15:51	Suspicious - High	ℹ Action Required
↗	⚠ High Risk	208.91.113.110	Aug 14 2017 15:15:51	Suspicious - High	ℹ Action Required
↗	⚠ High Risk	208.91.113.110	Aug 14 2017 15:15:41	Suspicious - High	ℹ Action Required

The following options are available:

Refresh	Refresh the entries after applying search filters.
Search	Show or hide the search filter field.
Time Period	Select the time period from the dropdown list. Select one of the following: 24 Hours, 7 Days, or 4 Weeks.
Clear all removable filters	Click the trash can icon to clear all removable filters.
Export to report	Click *Export to report* to create a PDF or CSV snapshot report. The time to generate the report depends on the number of events. You can wait to view the report or find the report later in *Log & Report > Report Center*.
Add Search Filter	Click the search filter field to add search filters. Use search filters to define what to display in the GUI. For example, you can use a field like source IP address as the search criterion.
View Job	Show the job detail page.
Number of Blocks	After a malware's signature is added to a Malware package and downloaded by FortiGate, FortiGate can block subsequent occurrences. Hover your cursor over the icon to see the number of blocks of this Malware.
In Cloud	An icon appears if the malware is available in the FortiSandbox Community Cloud.
In Signature	An icon appears if the malware is included in the current FortiSandbox generated Malware Package.
Perform Rescan	Rescan the suspicious or malicious entry. In the *Rescan Configuration* dialog box, you can force the file to do Sandboxing scan even if was detected in former steps of Static Scan, AV Scan, Cloud Query, or stopped from entering VM by Sandboxing-prefilter setting. The rescan job is in *File Input > File On-Demand*.
Archived File	An icon appears if the file is an Archived File.
Pagination	Use pagination options to browse entries.

This page displays the following information:

Severity	The severity rating of the malware, including: - Low Risk - Medium Risk - High Risk - Malicious If a file is detected by FortiSandbox first before an antivirus signature is available, the Severity level is Zero-day.
Source	IP address of the client that downloaded the malware. Use the column filter to sort the entries.
Incident Time	Date and time the file was received by FortiSandbox. Use the column filter to sort the entries.
Threat Name	Name of the virus. Use the column filter to sort the entries. If the virus name is not available, the malware's Severity is used as its Threat Name.
Action	Current action applied to the malware. Use this field to track responses to the incident, including: - Action Taken. - Ignore. - Action Required. The user can mark an action against a single job or to all jobs in the same file.

To view file details:

1. Select a file.
2. Click the *View Details* icon to open a new tab.
   For descriptions of the *View Details* page, see Appendix A - View Details page reference on page 202.

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.

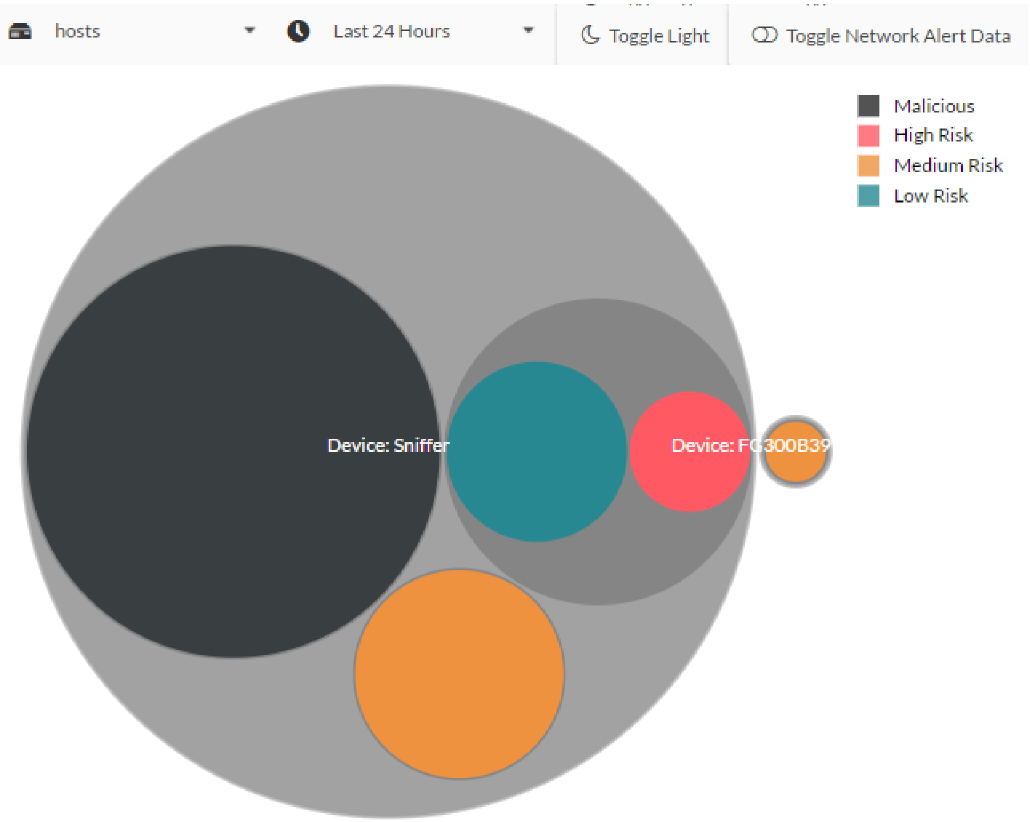
Clicking on the circles will drill down to the host level. At the host level, clicking on a circle will display a new page to show threat details.

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

The following options are available:

Hosts	Select the host.

Time Period	Select the time period from the dropdown list. Select *24 Hours*, *7 Days*, or *4 Weeks*.
Toggle Light	Select *Toggle Light* to change the topology background color.
Toggle Network Alert Data	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 *24 Hours*, *7 Days*, or *4 Weeks*.
Export Data	Click the *Export Data* 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 *Log & Report > Report Center* page.

Search	Show or hide the search filter field.
Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.
Add Search Filter	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. 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.
View Job	Click the *View Jobs* icon to drill down the entry.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

Host/Username	The device and username that is the target of threats. Click the column header to sort the table by this column. **Note**: A duplicate user name or host from a different VDOM is considered a different user.
Device Name	The device name. Click the column header to sort the table by this column.
# of Malicious Files	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.
# of Suspicious Files	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.
# of Network Threats	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.
Timeline	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 *View Details* page will open.
Total Host	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:

Back	Click *Back* button to return to the main landing page.
Threat Timeline Chart	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.

Summary		The following fields are displayed: Device, Threat Target, Time Period, Total Files, number of: Malicious Files, Suspicious Files, and Network Events.
Details		
	Malicious Files	Malicious file information including malware name, Threat Source, and number of detection times. The options are: • Click the *View Jobs* icon to drill down the entry. • Click the malware name to view the related FortiGuard Encyclopedia page.
	Suspicious Files	Suspicious file information including file name, file type, rating, the malware hosting address and number of detection times. Click the *View Jobs* icon to drill down the entry.
	Attacker Events	Attacker event information including backdoor name, attack origin address and port, attack destination address and port, and number of detection times.
	Botnet Events	Botnet event information including botnet name, user IP address, user port, destination IP address, destination IP port and number of detection times.
	URL Events	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:

Back	Click the *Back* button to return to the main landing page.
View Details	Click the *View Details* icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
Perform Rescan	Click the icon to rescan the entry. In the *Rescan Configuration* dialog box, you can force the file to do Sandboxing scan even if was detected in former steps of Static Scan, AV Scan, Cloud Query, or stopped from entering VM by Sandboxing-prefilter setting. Click the *Close* icon 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:

Malicious Files	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.
Suspicious Files	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 202.

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 1000; the maximum number of events you can export to a CSV report is 15000. 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:

Time Period	Select the time period from the dropdown list. Select *24 Hours*, *7 Days*, or *4 Weeks*.
Export Data	Click the *Export Data* 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 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 the *Log & Report* > *Report Center* page.
Search	Show or hide the search filter field.

Refresh	Click the *Refresh* icon to refresh the entries displayed after applying search filters.
Add Search Filter	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 filter *Filename* 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.
View Jobs	Click the *View Jobs* icon to drill down the entry.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

Filename	The threat file name. Click the column header to sort the table by this column.
Rating	The file rating. Click the column header to sort the table by this column.
# of Users	The number of users affected. Click the column header to sort the table by this column.
Timeline	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 *View Details* page will open.
Total Files	The number of files displayed and the total number of files.

Threats by Files - level 2

The following options are available:

Back	Click the *Back* icon to return to the main landing page.
Time Period	Select the time period from the dropdown list. Select *24 Hours*, *7 Days*, or *4 Weeks*.
Search	Show or hide the search filter field.
Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.
Add Search Filter	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.
View Jobs	Click the *View Jobs* icon to drill down the entry.
Pagination	Use the pagination options to browse entries displayed.

The following information is displayed:

Back	Click the *Back* button to return to the main landing page.

Summary of	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.
Details	Detail information including user IP address. destination IP address, and number of detection times. Select the *View Jobs* icon, or double-click on the row, to drill down the entry.

Threats by Files - level 3

The following options are available:

Back	Click the *Back* icon to return to the main landing page.
View Details	Select the *View Details* icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
Perform Rescan	Click the icon to rescan the entry. In the *Rescan Configuration* dialog box, you can force the file to do Sandboxing scan even if was detected in former steps of Static Scan, AV Scan, Cloud Query, or stopped from entering VM by Sandboxing-prefilter setting. Click the *Close* icon 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.

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:

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

Threats by Files - level 4

For more about information in the *View Details* pages for malicious and suspicious files, see Summary Report on page 179

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.

The maximum number of events you can export to a PDF report is 5000. The maximum number of events you can export to a CSV report is 150000.

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:

Time Period	Select the time period from the dropdown list. Select *24 Hours*, *7 Days*, or *4 Weeks*.
Export Data	Click the *Export Data* 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 *Log & Report* > *Report Center* page.
Search	Show or hide the search filter field.
Refresh	Click the *Refresh* icon to refresh the entries displayed after applying search filters.
Add Search Filter	Click the *Search Filter* field to add search filters. Click the *Cancel* icon beside the search filter to remove the specific filter. Click the *S* 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.

View Jobs	Click the *View Jobs* icon to drill down the entry.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

Device	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.
# of Malicious Files	The number of malicious files submitted by the device. Click the column header to sort the table by this column.
# of Suspicious Files	The number of suspicious files submitted by the device. Click the column header to sort the table by this column.
Timeline	View the Threat Timeline Chart of the device. When you hover on any dot, all victim hosts managed by the device appears within five minutes. When you click on any dot in the chart, all events associated displays. When you click on an event, the View Details page opens.
Total Devices	The number of devices displayed and the total number of devices.

Threats by Devices - level 2

The following information is displayed:

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

Threats by Devices - level 3

The following options are available:

Back	Click the *Back* icon to return to the main landing page.
View Details	Select the *View Details* icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.

Perform Rescan	Click the icon to rescan the entry. In the *Rescan Configuration* dialog box, you can force the file to do Sandboxing scan even if was detected in former steps of Static Scan, AV Scan, Cloud Query, or stopped from entering VM by Sandboxing-prefilter setting. Click the *Close* icon 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:

Malicious Files	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.
Suspicious Files	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 information about the malicious and suspicious files in the *View Details* pages, see Appendix A - View Details page reference on page 202.

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 1000; the maximum number of events you can export to a CSV report is 15000. Jobs over that limit will not be included in the report.

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

The following options are available:

Refresh		Click the *Refresh* icon to refresh the entries displayed after applying search filters.
Search Field		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 *Filename*, click the = sign to toggle between the exact and pattern search.
Time Period		Select a time period to apply to the search.
Export to Report		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 *Log & Report* > *Report Center* page.
Customize		Click the *Customize* icon to customize the Job View settings page. For more information, see Job View Settings on page 78.
Action		
	View Details	Click the *View Details* icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
	Archived File	The icon displays that the file as an archived file.
	FortiGuard Advanced Static Scan	The icon displays that the file is rated by user's overridden verdict or FortiGuard advanced static scan.
	File Inside Archive	The icon displays that the file is a file extracted from an archive file.
	Rescan Job	The icon displays that the job is Malicious from an AV Rescan or a rescan of the Malicious file.
	Video	Click the *Video* button to play the video of the scan. Scan videos are available in On-Demand scans if the user has the privilege.
	Perform Rescan	Click the icon to rescan the entry. In the *Rescan Configuration* dialog box, you can skip *Static Scan*, *AV Scan*, *Cloud Query*, and *Sandboxing*. Click *OK* to continue. This feature is only available for files with a *Malicious* rating and the suspicious jobs detected by *Static Scan*, *AV Scan*, *Cloud Query* and the yara engine. The rescan job is in *File Input* > *File On-Demand*.
Pagination		Use the pagination options to browse entries displayed.

The following information is displayed:

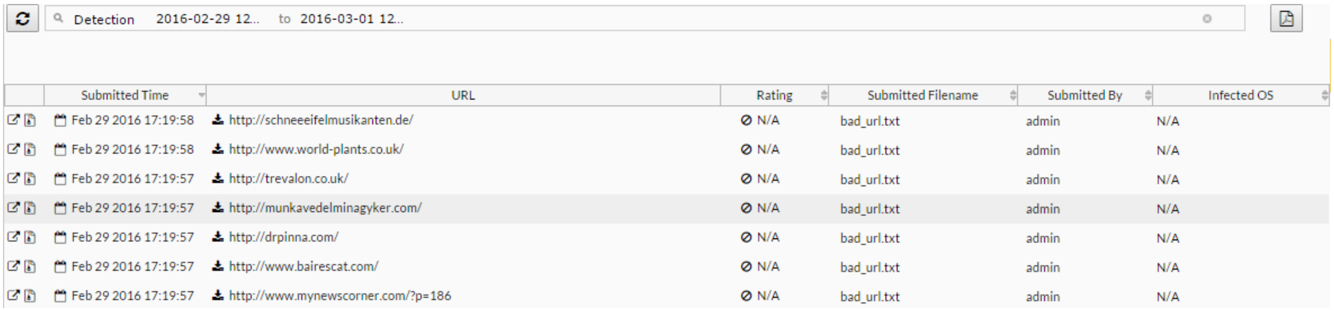
Total Jobs	The number of jobs displayed and the total number of jobs.

The displayed columns are determined by settings defined in *System* > *Job View Settings* > *File Detection Columns* page. For more information, see Job View Settings on page 78.

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 node of a cluster, all jobs processed by the cluster are available to be searched. If the device is a worker 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.mynewscorner.com/?p=186	⊘ N/A	bad_url.txt	admin	N/A

The following options are available:

Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.
Search Field	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 *Submitted Filename*, click the = sign to toggle between the exact and pattern search.
Time Period	Select a time period to apply to the search.
Export to Report	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 *Log & Report* > *Report Center* page.
Customize	Click the *Customize* icon to customize the Job View settings page. For more information, see Job View Settings on page 78.
Action	
View Details	Click the *View Details* icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.

	FortiGuard Advanced Static Scan	The icon displays that the URL is rated by user's overridden verdict, or FortiGuard advanced static scan
	Rescan Job	The icon displays that the job is a customized rescan job of a Malicious URL.
	Video	Click on the *Video* button to play the video of the scan job. Scan videos are available in On-Demand scans if user has the privilege.
	Archive File	The icon displays that the URL is from a file from an On-Demand scan
	File Downloading URL	The icon displays that the URL is from a downloading URL, and its payload is also scanned as a file scan job.
	Perform Rescan	Click the icon to rescan the suspicious or malicious entry except suspicious files rated by the VM. In the *Rescan Configuration* dialog box, you can customize the new scan's depth and timeout value. You can also force the URL to do Sandboxing scan even if was detected in former steps of the allowlist and blocklist check or stopped from entering VM by a Sandboxing-prefilter setting. Click *OK* to continue. The rescan job is in *File Input > URL On-Demand*.
Pagination		Use the pagination options to browse entries displayed.

The following information is displayed by default:

Detection	The date and time that the file was detected by FortiSandbox.
URL	Displays the URL.
Rating	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.
Submitted Filename	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.
Submit User	The user that submitted the URL to be scanned. Click the column header to sort the table by this column.
Infected OS	The OS version of the FortiSandbox VM that was used to make the Suspicious verdict
Total Jobs	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. For more information, see Job View Settings on page 78.

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. The failover IP includes the description: *(cluster external port)*.
port1 (administration port)	port1 is hard-coded as the administration interface. You can enable or disable HTTP, SSH, or Telnet access rights on port1. HTTPS is enabled by default. You can use port1 for Device mode, although a different, dedicated port is recommended.
port2	You can use port2 for Sniffer mode, Device mode, or inter-node communication within a cluster.
port3 (VM outgoing interface)	port3 is reserved for outgoing communication triggered by the execution of the files under analysis. FortiSandbox uses port3 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, ensure that the connection for port3 is isolated but can also access the Internet. Do not allow this connection to 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. FortiSandbox VM accesses external networks through port3. Configure the next hop gateway and DNS settings in *Scan Policy > General > Allow Virtual Machines to access external network through outgoing port3*. This allows files running inside VMs to access the external network. One special type of outgoing communication from a guest VM is to connect to the Microsoft activation server to activate the Windows Sandbox VM product keys. Office licenses are verified through VM machines so internet access via port3 is required to contact Microsoft for license activation.

	If the VM cannot access the outside network, a simulated network (SIMNET) starts by default. SIMNET provides responses to popular network services like `http` where some malware is expected. If the VM internet access is down, the SIMNET status is displayed beside the down icon. Click that icon to go to the VM network configuration page. ⚠ SIMNET is not a real internet. This can affect catch rate. Do not use an IP address from the production IP pool for the IP assignment on port3 because it might get put on the blocklist.
port4	You can use port4 for Sniffer mode, Device mode, or inter-node communication within a cluster.
port5/port6	You can use port5 and port6 for Sniffer mode, Device mode, or 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 or secondary node as communications ports with cluster workers.
port7/port8	You can use port7 and port8 for Sniffer mode, Device mode, or 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 or secondary node as communications ports with cluster workers.
IPv4	IPv4 IP address and subnet mask of the interface.
IPv6	IPv6 IP address and subnet mask of the interface.
Interface Status	State of the interface: • Interface is up • Interface is down • Interface is being used by sniffer
Link Status	Link status: • Link up • Link down
Access Rights	Access rights associated with the interface. HTTPS is enabled by default on port1 and any other administrative port set by the CLI command `set admin-port`. You can select to enable HTTP, SSH, and Telnet access on the administrative port.
PCAP	Click the PCAP icon to sniff the traffic of an interface for up to 60 seconds. Click *Capture & Download* to download the PCAP file as a zip file. Maximum file size is 100MB file size. You can define the tcpdump filter such as host 172.10.1.1 or TCP port 443. You can only run one capture at a time for each port. Sniffing ports are combined and treated as a single port.
Create New	Create an interface.
Edit	Edit the selected interface.

For more information on FSA-1000D, FSA-3000D, FSA-2000E, FSA-3500D, and FSA-3000E ports, see Default port information on page 15.

To set up more administration ports, use the CLI command `set admin-port`.

The following subnets are reserved by FortiSandbox. Do not configure interface IP addresses in this range.

```
192.168.56.0/24
192.168.57.0/24
192.168.250.0/24
```

Edit an interface

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

To edit an IPv4 or IPv6 address:

1. Go to *Network* > *Interfaces*.
2. Select an interface and click *Edit*.
3. Edit the IP address.
4. To change the *Interface Status*, click its icon.
5. Click *OK*.

Edit administrative access

Administrative access rights can only be set on port1. All other administrative ports follow port1 settings.

The port1 interface or any other administrative port set through the CLI command `set admin-port` is used for administrative access to FortiSandbox. HTTPS is enabled by default. You can edit this interface to enable HTTP, SSH, and Telnet support.

To edit administrative access:

1. Go to *Network* > *Interfaces*.
2. Select an administrative interface and click *Edit*.
3. Edit the IP address.
4. To change the *Interface Status*, click its icon.
5. Select the *Access Rights* for *HTTP*, *SSH*, and *Telnet*.
6. Click *OK*.

Create an aggregate interface

You can create an interface that uses IEEE 802.3ad to bind multiple physical networks to form an aggregated, combined link. The aggregate link has the bandwidth of the combined links. If one interface in the group fails, traffic is automatically transferred to the other interfaces. The only noticeable effect is reduced bandwidth.

In *Network* > *Interfaces*, a network interface that is part of an aggregate link is displayed in gray. You cannot configure the interface individually.

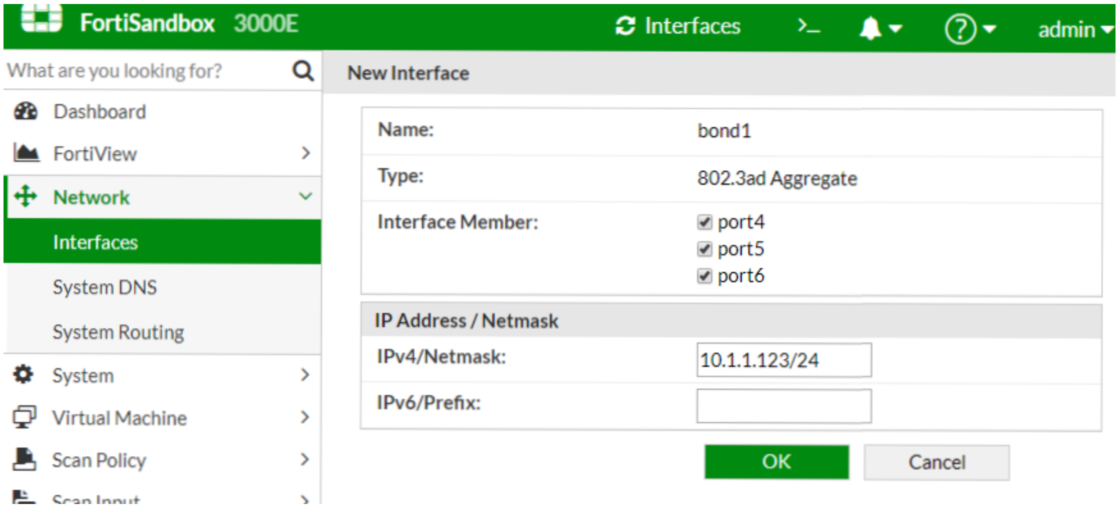
A network interface must meet all the following conditions to be added to an aggregate interface:

- It is not already part of an aggregate interface.
- It does not have the same IP address as another interface.
- It is not an administration port.
- It is not a VM outgoing port.
- It is not a sniffer port.
- It is not an HA-Cluster communication port.

To create an aggregate interface:

This example creates an aggregate interface on ports 4 - 6 with an internal IP address of 10.1.1.123 with administrative access to HTTPS and SSH.

1. Go to *Network > Interfaces* and click *Create New*.
   FortiSandbox sets the *Name* as *bond{n}* and the *Type* as *802.3ad Aggregate*.
2. For *Interface Member*, select the physical interface members. In this example, select ports 4, 5, and 6.
3. Enter the IPv4 IP address for the port. In this example, enter *10.1.1.123/24*.
4. If necessary, enter the IPv6 IP address.



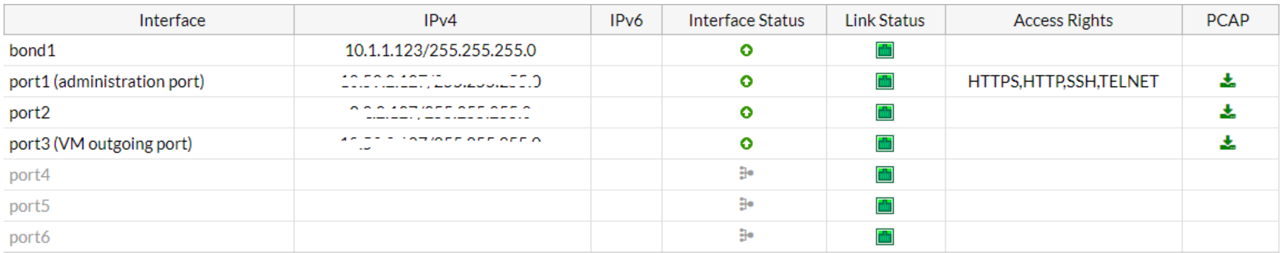
New Interface

Name:	bond1
Type:	802.3ad Aggregate
Interface Member:	☑ port4 ☑ port5 ☑ port6

IP Address / Netmask

IPv4/Netmask:	10.1.1.123/24
IPv6/Prefix:	

5. Click *OK* to display the created bond.



Interface	IPv4	IPv6	Interface Status	Link Status	Access Rights	PCAP
bond1	10.1.1.123/255.255.255.0		●	🟩		
port1 (administration port)	[redacted]		●	🟩	HTTPS,HTTP,SSH,TELNET	⤓
port2	[redacted]		●	🟩		⤓
port3 (VM outgoing port)	[redacted]		●	🟩		⤓
port4			⊪	🟩		
port5			⊪	🟩		
port6			⊪	🟩		

6. Use the CLI command `show` to display the bond information. For example:

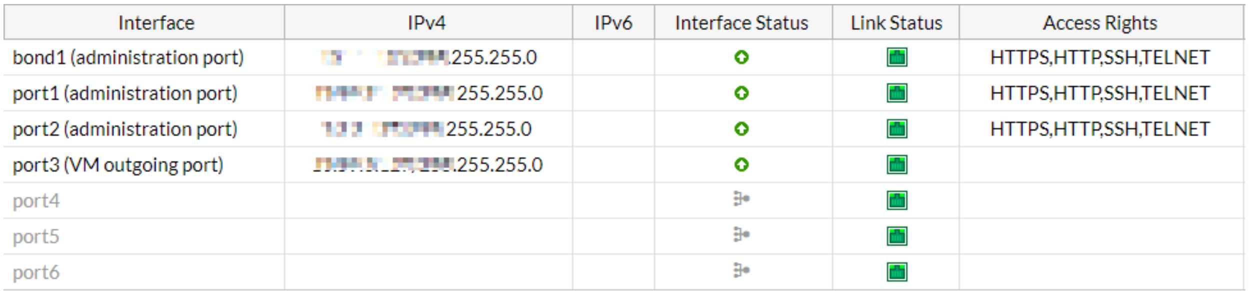
```
Bond 1  IPv4 IP: 10.1.1.123/24  MAC: xx:xx:xx:xx:xx:xx
        MTU: 1500
        Slave Interface:  port4  port5  port6
```

7. Use the following CLI command to add *bond1* as the administration port.

   ```
   set admin-port bond1
   ```

   Network > Interfaces shows that *bond1* has the same access rights as *port1*.

   When you change the *port1* access rights, the *bond1* access right is automatically synchronized.



Interface	IPv4	IPv6	Interface Status	Link Status	Access Rights
bond1 (administration port)	[redacted]255.255.0		●	🟩	HTTPS,HTTP,SSH,TELNET
port1 (administration port)	[redacted]255.255.0		●	🟩	HTTPS,HTTP,SSH,TELNET
port2 (administration port)	[redacted]255.255.0		●	🟩	HTTPS,HTTP,SSH,TELNET
port3 (VM outgoing port)	[redacted]255.255.0		●	🟩	
port4			○	🟩	
port5			○	🟩	
port6			○	🟩	

To set the aggregate interface as the administration port, use the CLI command `set admin-port bond1`.

To change the MTU of an aggregate interface, use the `set port mtu` CLI command. For example, `set port-mtu bond1 1200`.

Additional information

There is no CLI command to create or delete the LACP 802.3ad interface.

The bond interface does not support PCAP.

You cannot delete an admin LCAP bond.

You cannot add a new interface to an existing bond.

You cannot remove an interface member from an existing bond.

For FortiSandbox VM, including KVM, Hyper-V, AWS, and Azure, implement the LCAP support on the virtual server first, then create the aggregate interface.

Failover IP

Users are able to configure a cluster level failover IP, which will be set only on primary node. This failover IP can only be set on current primary 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 node.

The primary and secondary 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:

Create New	Select to create a new static route.
Edit	Select a static route in the list and click *Edit* in the toolbar to edit the entry.
Delete	Select a static route in the list and click *Delete* in the toolbar to delete the entry.

The following information is displayed:

IP/Mask	Displays the IP address and subnet mask.
Gateway	Displays the gateway IP address.
Device	Displays the interface associated with the static route.
Number of Routes	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 fe80:0:0:0:0:0:c0a8:1fe.

The following subnets are reserved for use by FortiSandbox. Do not configure static routes for these IP address ranges:

- `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 are for system use and are not applied to traffic originating from the guest VM during a file's execution.

System

Use the *System* pages to manage and configure the basic system options for the FortiSandbox unit. This includes administrator configuration, mail server settings, and maintenance information.

System provides access to the following pages. Some pages do not display on worker nodes in a cluster.

Administrators	Configure administrator user accounts.
Admin Profile	Configure user profiles to define user privileges.
Device Groups	Add devices to a device group and assign it to multiple device users.
Certificates	Configure CA certificates.
LDAP Servers	Configure LDAP Servers.
RADIUS Servers	Configure RADIUS Servers.
Mail Server	Configure the Mail Server.
SNMP	Configure SNMP.
FortiGuard	Configure FortiGuard.
Login Disclaimer	Configure the Login Disclaimer.
Settings	Configure the idle timeout, the GUI language, and whether the left menu is expanded or compact. You can also reset all widgets to their default state.
Job View Settings	Define columns and orders of job result tables.

Administrators

Use the *Administrators* menu to configure administrator user accounts.

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

Only the default admin account can see and access that account. Other users cannot see the default admin account in the GUI.

The following options are available:

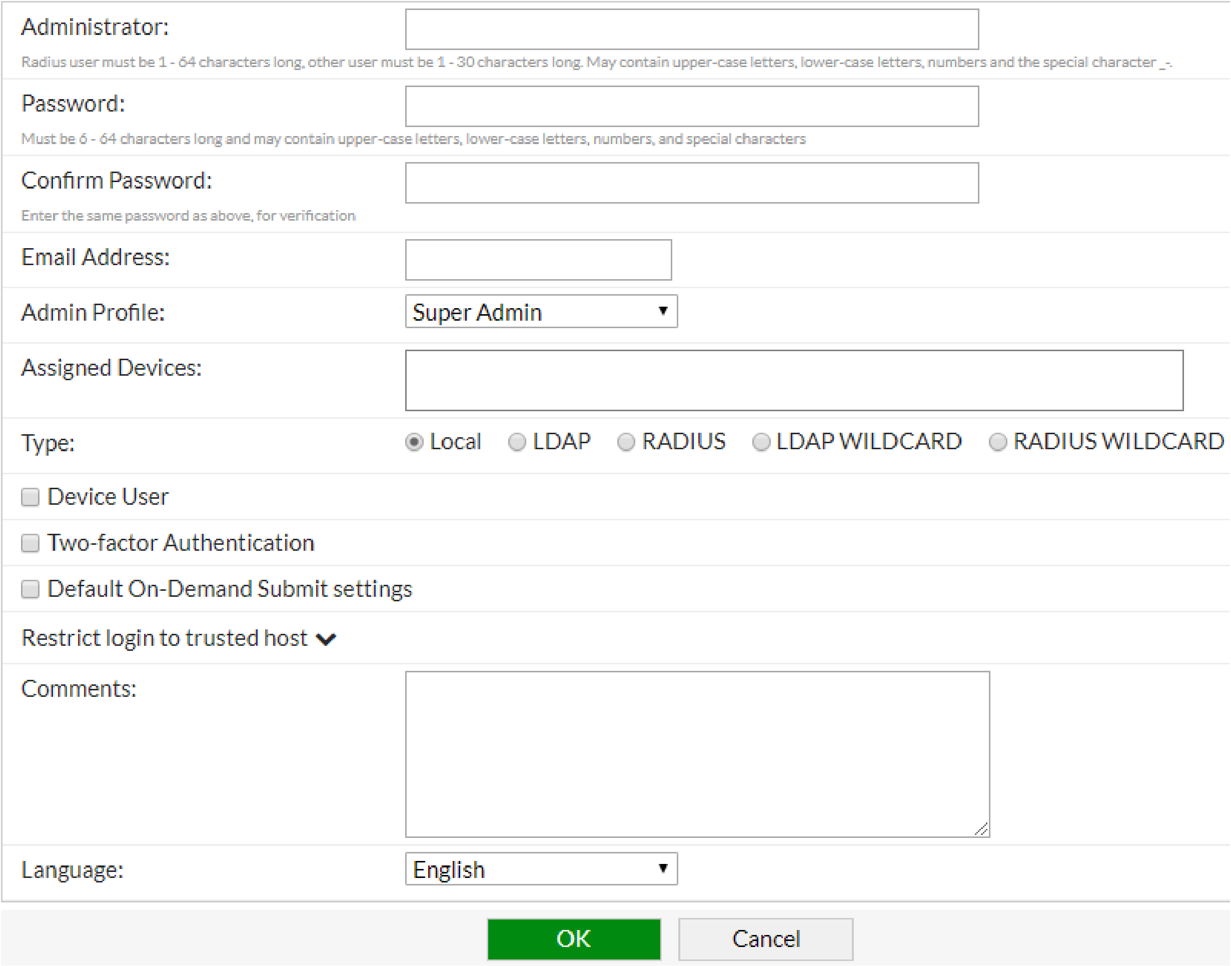
Create New	Create a new administrator account.
Edit	Edit the selected administrator account.
Delete	Delete the selected administrator account.
Test Login	Test the selected LDAP/RADIUS administrator account's login settings. A detailed debug message display any errors.

The following information is displayed:

Name	Administrator account name.
Type	Administrator type: • Local • LDAP • RADIUS • LDAP WILDCARD • RADIUS WILDCARD
Profile	The Admin Profile the user belongs to.

To create a new user:

1. Log in as a user whose Admin Profile has *Read/Write* privileges under *System* > *Admin access*, and go to *System* > *Administrators*.
2. Click *Create New*.



Administrator:

Radius user must be 1 - 64 characters long, other user must be 1 - 30 characters long. May contain upper-case letters, lower-case letters, numbers and the special character _-.

Password:

Must be 6 - 64 characters long and may contain upper-case letters, lower-case letters, numbers, and special characters

Confirm Password:

Enter the same password as above, for verification

Email Address:

Admin Profile: Super Admin

Assigned Devices:

Type: ● Local ○ LDAP ○ RADIUS ○ LDAP WILDCARD ○ RADIUS WILDCARD

□ Device User

□ Two-factor Authentication

□ Default On-Demand Submit settings

Restrict login to trusted host

Comments:

Language: English

3. Configure the following and click *OK*.

Administrator	Name of the administrator account. The administrator name must be 1 to 30 characters using uppercase letters, lowercase letters, numbers, or the underscore character (_).
Password, Confirm Password	This field is only available when *Type* is *Local*. Password of the account. The password must be 6 to 64 characters using uppercase letters, lowercase letters, numbers, or special characters.
Email Address	Email address for contact information.
Phone Number	Phone number for contact information. Phone number must start with *+1*.
Admin Profile	Select the Admin Profile for the user: *Super Admin*, *Read Only*, or *Device*.
Assigned Devices	Assign devices and/or VDOMs/Protected Domains to the user. This applies if you enable *Device User*. Click in the *Assigned Devices* box to display the *Available Devices* panel which lists all available devices and VDOMs/Protected Domains. Use this panel to select or add devices.
Type	Select administrator type.
LDAP	When *Type* is *LDAP*, select the *LDAP Server*. For more information, see LDAP Servers on page 66.
RADIUS	When *Type* is *RADIUS*, select the *RADIUS Server*. For more information, see RADIUS Servers on page 68.
LDAP WILDCARD	When *Type* is *LDAP WILDCARD*, select the *LDAP Server*. The *Administrator* is *LDAP_WILDCARD* and cannot be edited. For more information, see Wildcard Admin Authentication on page 62.
RADIUS WILDCARD	When *Type* is *RADIUS WILDCARD*, select the *Radius Server*. The *Administrator* is *RADIUS_WILDCARD* and cannot be edited. For more information, see Wildcard Admin Authentication on page 62.
Device User	Enable this option to assign devices to the user. When the user logs in, only jobs belonging to the assigned devices or VDOMs/Protected Domains are visible. You can create device groups in *System* > *Device Groups* and then assign them to a device user. You can also assign devices on the fly by selecting *self assigned* in the *Device Group* dropdown list.
Two-factor Authentication	When administrator *Type* is *Local*, you can use two-factor authentication. Select an *Authentication Type* of *Email*, *SMS*, or *FTM* (FortiTokenMobile). Two-factor Authentication is only available for FortiSandbox appliances, not for FortiSandbox VM.
Default On-Demand Submit settings	This option is available to administrators whose *Administrator Profile* > *Scan Input* has *Read Write* access.

	Use this option to set the default settings in *Scan Input* > *File On-Demand* and *URL On-Demand*. Each administrator can have their own default settings. For information on these settings, see File On-Demand on page 120 and URL On-Demand on page 124.
Restrict login to trusted host	Expand to configure trusted hosts.
Trusted Host 1, Trusted Host 2, Trusted Host 3	Enter up to three IPv4 trusted hosts. Only users from trusted hosts can access FortiSandbox.
Trusted IPv6 Host 1, Trusted IPv6 Host 2, Trusted IPv6 Host 3	Enter up to three IPv6 trusted hosts. Only users from trusted hosts can access FortiSandbox.
Comments	Optional description comment for the administrator account.
Language	GUI language for the user: *English*, *Japanese*, or *French*.

Setting trusted hosts for administrators limits which computers an administrator can log into from FortiSandbox. When you configure a trusted host, FortiSandbox only accepts 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 are dropped.

To edit a user account:

1. Login as an user whose Admin Profile has *Read/Write* privileges under *System* > *Admin access*, and go to *System* > *Administrators*.
2. Select the user you want to edit and click *Edit*.
   Only the *admin* account can edit its own settings.

   When editing the *admin* account, you must enter the old password before you can set a new password.
3. Edit the account and then retype the new password in the confirmation field.
4. Click *OK*.

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 an LDAP/RADIUS user to test.
3. Click *Test Login*.
4. In the dialog box, enter the user's password.
5. Click *OK*.
   If an error occurs, a detailed debug message appears.

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. 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 to test login.

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.

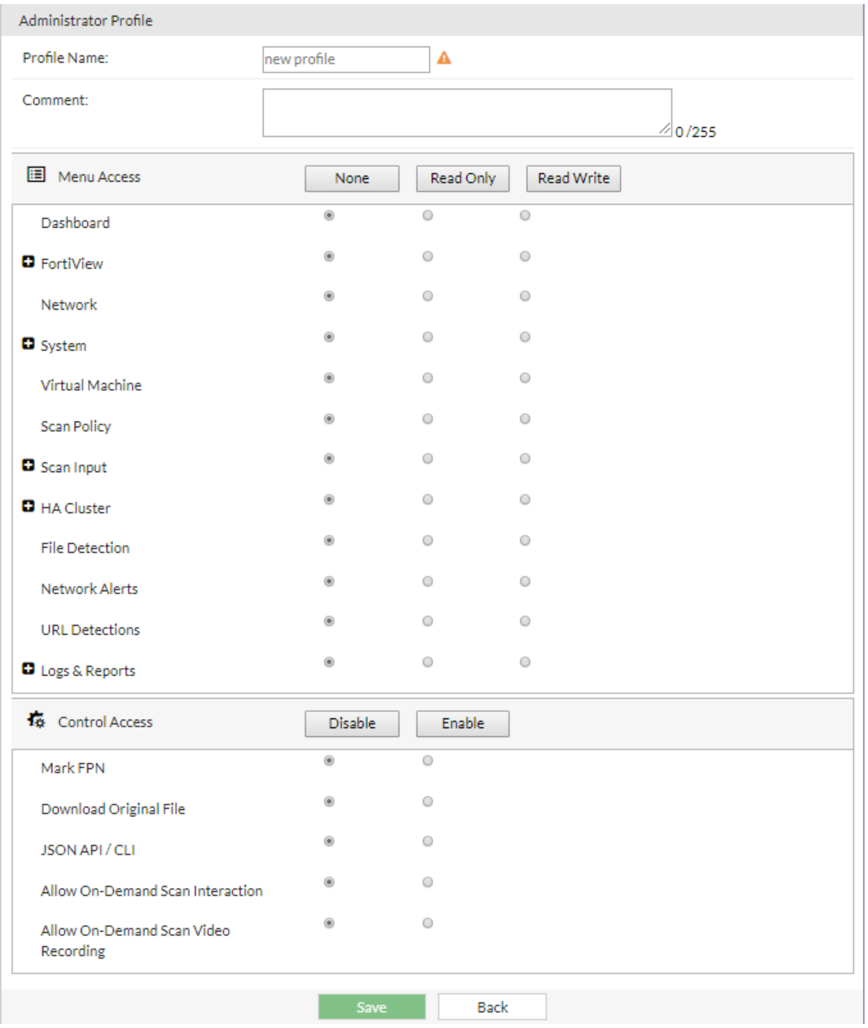
There are three predefined administrator profiles, which cannot be modified or deleted:

- 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: new profile

Comment: 0/255

Menu Access	None	Read Only	Read Write
Dashboard	●	○	○
FortiView	●	○	○
Network	●	○	○
System	●	○	○
Virtual Machine	●	○	○
Scan Policy	●	○	○
Scan Input	●	○	○
HA Cluster	●	○	○
File Detection	●	○	○
Network Alerts	●	○	○
URL Detections	●	○	○
Logs & Reports	●	○	○

Control Access	Disable	Enable
Mark FPN	●	○
Download Original File	●	○
JSON API / CLI	●	○
Allow On-Demand Scan Interaction	●	○
Allow On-Demand Scan Video Recording	●	○

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.

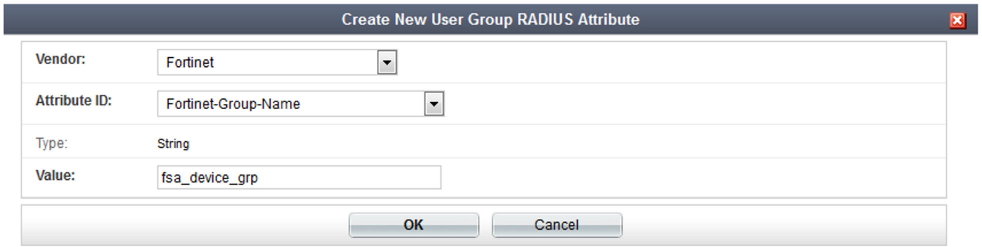
Wildcard Admin Authentication

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

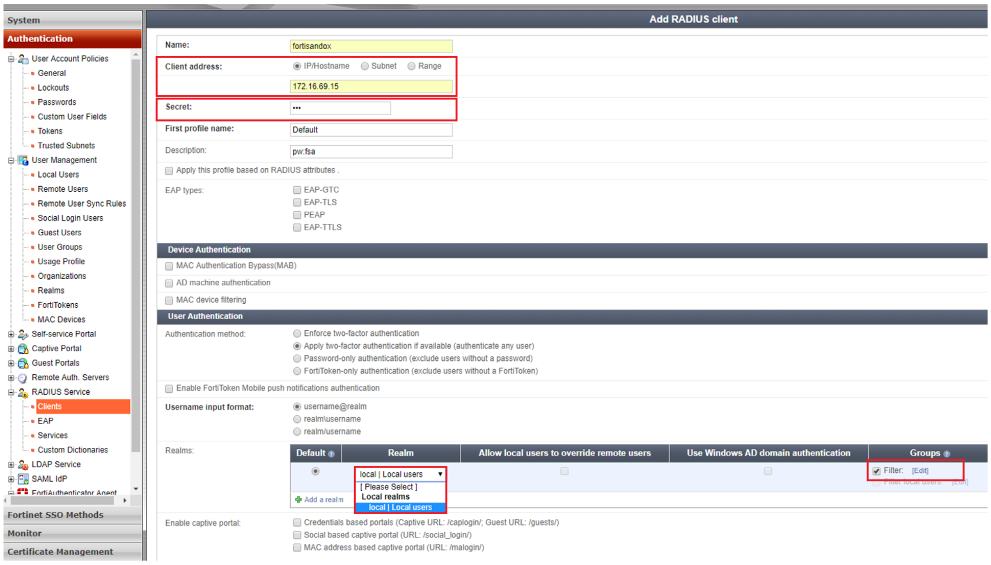
Attribute ID: Fortinet-Group-Name

Type: String

Value: fsa_device_grp

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.



Add RADIUS client

Name: fortisandox

Client address: ● IP/Hostname ○ Subnet ○ Range

172.16.69.15

Secret: •••

First profile name: Default

Description: pw:fsa

□ Apply this profile based on RADIUS attributes .

EAP types: □ EAP-GTC □ EAP-TLS □ PEAP □ EAP-TTLS

Device Authentication

□ MAC Authentication Bypass(MAB)

□ AD machine authentication

□ MAC device filtering

User Authentication

Authentication method:
○ Enforce two-factor authentication
● Apply two-factor authentication if available (authenticate any user)
○ Password-only authentication (exclude users without a password)
○ FortiToken-only authentication (exclude users without a FortiToken)

□ Enable FortiToken Mobile push notifications authentication

Username input format:
● username@realm
○ realm\username
○ realm/username

Realms:

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups
●	local | Local users ▾ [Please Select] Local realms local | Local users	□	□	☑ Filter: [Edit]

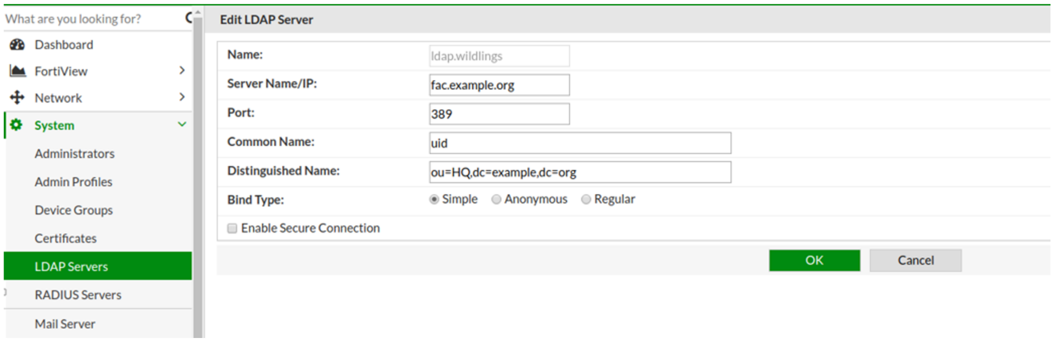
Add a realm

Enable captive portal:
□ Credentials based portals (Captive URL: /caplogin/; Guest URL: /guests/)
□ Social based captive portal (URL: /social_login/)
□ MAC address based captive portal (URL: /malogin/)

4. On FortiSandbox, set up the RADIUS server in *System* > *RADIUS Servers*.
   See RADIUS Servers on page 68.
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 66.
   In this example, all users from OU=HQ under the LDAP tree dc=example, dc=org will be able to login to FortiSandbox.



Edit LDAP Server

Name: ldap.wildlings

Server Name/IP: fac.example.org

Port: 389

Common Name: uid

Distinguished Name: ou=HQ,dc=example,dc=org

Bind Type: ● Simple ○ Anonymous ○ Regular

□ Enable Secure Connection

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 62.

Certificates

In this page you can import, view, download 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:

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

The following information is displayed:

Name	The name of the certificate.
Subject	The subject of the certificate.
Status	The certificate status, active or expired.
Service	HTTPS or SSH service that is using this certificate.
Certificate	Download the server certificate.
Sub Certificate	Download the intermediate CA (Certificate Authority) certificate if you are using a certificate chain.
Cacert	Download the CA (Certificate Authority) 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. Optionally, you can import the intermediate CA certificate by clicking the *Choose File* button for *Sub Certificate*, and locating the intermediate CA certificate file.
6. Click *OK* to import the certificate.

You also 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 the possible password. When checking the *PKCS12 Format* box, the other Certificate file selection boxes disappear and are replaced by the *PKCS12 File* selection option because only this type is valid.

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:

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

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

To download a CA certificate:

1. Go to *System* > *Certificates*.
2. Click the download icon ⬇ in one of the columns: *Certificate*, *Sub Certificate*, or *Cacert*.

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, configure the 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 accepts the connection. If the LDAP server cannot authenticate the user, the FortiSandbox unit refuses the connection.

The following options are available:

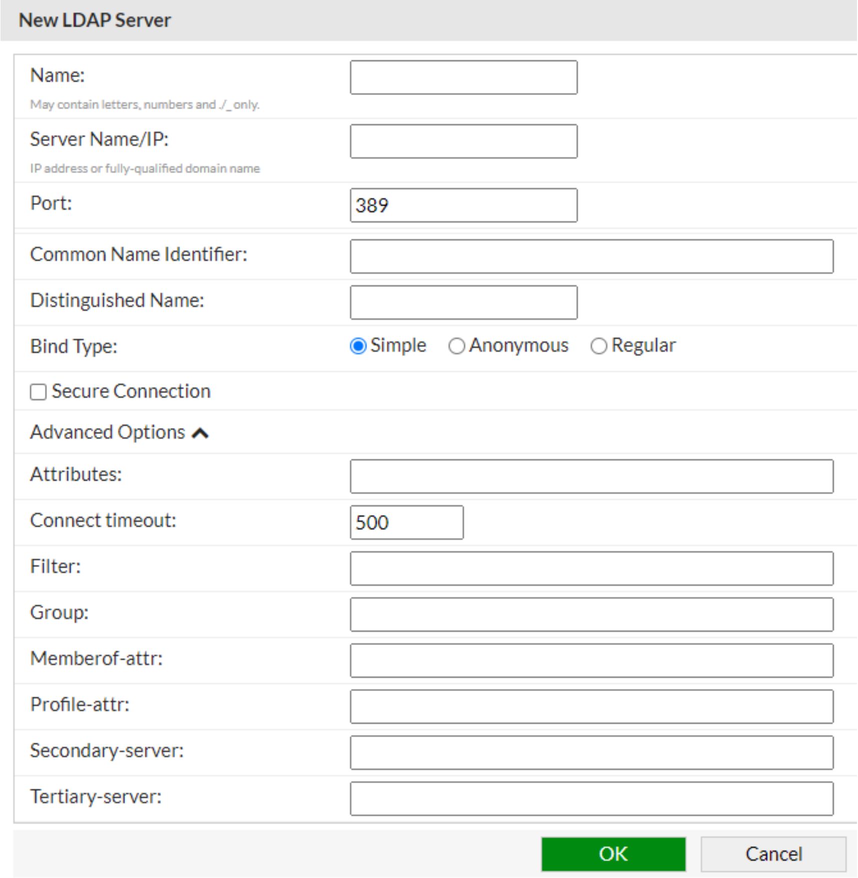
Create New	Add an LDAP server.
Edit	Edit the selected LDAP server.
Delete	Delete the selected LDAP server.

The following information is displayed:

Name	LDAP server name.
Address	LDAP server IP address.
Common Name	LDAP common name.
Distinguished Name	LDAP distinguished name.
Bind Type	LDAP bind type.
Connection Type	LDAP connection type.

To create a new LDAP server:

1. Go to *System* > *LDAP Servers*.
2. Click *Create New*.



New LDAP Server

Name:
May contain letters, numbers and ./_ only.

Server Name/IP:
IP address or fully-qualified domain name

Port: 389

Common Name Identifier:

Distinguished Name:

Bind Type: ● Simple ○ Anonymous ○ Regular

□ Secure Connection

Advanced Options

Attributes:

Connect timeout: 500

Filter:

Group:

Memberof-attr:

Profile-attr:

Secondary-server:

Tertiary-server:

3. Configure the following settings and then click *OK*.

Name	LDAP server name. Use a name unique to FortiSandbox.
Server Name/IP	LDAP server IP address or fully qualified domain name.
Port	Port for LDAP traffic. LDAP default port is 389. LDAPS default port is 636.
Common Name Identifier	LDAP common name. Most LDAP servers use `cn`. Some servers use other common name identifiers such as `uid`.
Distinguished Name	LDAP distinguished name used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. For example, you can follow the format `CN=Users,DC=Example,DC=Com`.
Bind Type	LDAP bind type for authentication, including: • Simple • Anonymous • Regular

Username	If *Bind Type* is *Regular*, enter the user distinguished name.
Password	If *Bind Type* is *Regular*, enter the password.
Secure Connection	LDAP connection type.
Protocol	If *Secure Connection* is enabled, select *LDAPS* or *STARTTLS*.
CA Certificate	If *Secure Connection* is enabled, select the CA certificate.
Advanced Options	Expand to configure advanced options.
Attributes	Attributes such as *member*, *uniquemember*, or *memberuid*.
Connect timeout	Connection timeout in milliseconds. Default is 500.
Filter	Filter in the format such as `(&(objectClass=*)`.
Group	Name of the LDAP group. For example, you can follow the format `CN=Group1,DC=Example,DC=Com`.
Memberof-attr	Specify the value for this attribute. This value must match the attribute of the group in LDAP server. All users of the LDAP group with the attribute matching the *memberof-attr* inherit the administrative permissions of the group.
Profile-attr	Specify the attribute for this profile.
Secondary-server	Specify a secondary server for failover in case the primary LDAP server fails. The *Distinguished Name* must be the same.
Tertiary-server	Specify a tertiary server for failover in case the primary and secondary servers fail. The *Distinguished Name* must be the same.

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:

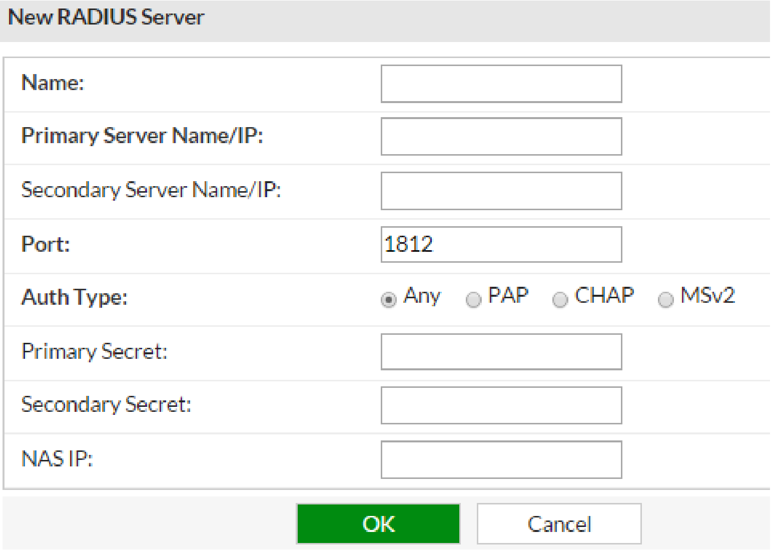
Create New	Select to add a RADIUS server.
Edit	Select a RADIUS server in the list and click *Edit* in the toolbar to edit the entry.
Delete	Select a RADIUS server in the list and click *Delete* in the toolbar to delete the entry.

The following information is displayed:

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

To add a RADIUS server:

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



New RADIUS Server

Name:	
Primary Server Name/IP:	
Secondary Server Name/IP:	
Port:	1812
Auth Type:	● Any ○ PAP ○ CHAP ○ MSv2
Primary Secret:	
Secondary Secret:	
NAS IP:	

3. Configure the following settings:

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

SMTP Server Address	Enter the SMTP server address.
Port	Enter the SMTP server port number. If port 587 is used, the SMTP process will use STARTTLS to encrypt the credentials and the email.
E-Mail Account	Enter the mail server email account. This will be used as the *from* address.
Login Account	Enter the mail server login account.
Password	Enter the password.
Confirm Password	Confirm the password.

Send a notification email to the global email list when Files/URLs with selected rating are detected	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.
What rating of job to send alert email	Select the rating of jobs that are included in the email alerts. Options include: *Malicious*, *High Risk*, *Medium Risk*, and *Low Risk*.
Global notification mail receivers list (separated by comma)	Enter the email addresses that comprise the global email list.
Notification mail subject template	Enter the subject line for the notification emails.
Send a notification email to the Device/Domain/VDOM email list when Files/URLs with selected ratings are detected	When a malware from an input device is detected, send a notification email to its admin email address.
What rating of job to send alert email	Select the rating of jobs that will trigger email notification. Options include: *Malicious*, *High Risk*, *Medium Risk*, and *Low Risk*.
Notification mail subject template	Enter the subject line for the notification emails.
Send a notification email to the below email list when malicious/suspicious verdict is returned to client device.	When enabled, a notification email is sent to an email list when a malicious/suspicious rating is retrieved by a client device.
Use FQDN as unit address for job detail link (default is IP address of Port1)	Use FQDN instead of port1 IP for a job detail link inside alert emails and reports.
FQDN Name	Enter FQDN name.
Send scheduled PDF report to global email receiver	Select to send a report email to the global email list.
Global email list to receive summary/detail report (separated by comma)	Enter the email addresses that comprise the global email list.
Send scheduled PDF report to Device/Domain/VDOM email address	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.
Report Schedule Type:	Select the report schedule type: *Hourly*, *Daily*, or *Weekly*. For different schedule types, different frequency options are displayed. If the schedule type is *Daily*, the user can set the hour for which the report is generated.
Week Day:	Select the day the report is to be sent.
At hour:	Select the hour interval the report is to be sent.
Include job data before Days (0-28) days:	Select the job data before *0-28* days.
Hours (0-23):	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.
	What rating of job to be included in the detail report	Select the rating of jobs that are included in the reports. Options include: *Malicious*, *High Risk*, *Medium Risk*, *Low Risk*, and *Clean*. Because there is a large amount of jobs with a Clean rating, it is recommended to exclude the Clean rating from the detail report.
OK		Select *OK* to apply any changes made to the mail server configuration.
Send Test Email		Select *Send Test* 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.
Restore Default		Select *Restore Default* 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 your FortiSandbox system on your local computer. You will need an SNMP agent on your computer to read the SNMP information.

Using SNMP, your FortiSandbox system monitors for system events including CPU usage, memory usage, log disk space, interface changes, and malware detection. Go to *System* > *SNMP* to configure your FortiSandbox system's 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 also download FortiSandbox and Fortinet core MIB files.

For all models other than FSA-1000D, when one plug is cut off, the unit will send out SNMP trap and generate a log.

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 there are any critical events occurring. The description, location, and contact information for this FortiSandbox system will be part of the information an SNMP manager will have. 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* to configure the SNMP agent.
2. Configure the following settings:

SNMP Agent	Select to enable the FortiSandbox SNMP agent. When this is enabled, it sends FortiSandbox SNMP traps.
Description	Enter a description of this FortiSandbox system to help uniquely identify this unit.
Location	Enter the location of this FortiSandbox system to help find it in the event it requires attention.
Contact	Enter the contact information for the person in charge of this FortiSandbox system.
SNMP v1/v2c	Create new, edit, or delete SNMP v1 and v2c communities. You can select to enable or disable communities in the edit page. The following columns are displayed: Community Name, Queries, Traps, Enable.
SNMP v3	Create new, edit, or delete SNMP v3 entries. You can select to enable or disable queries in the edit page. The following columns are displayed: User Name, Security Level, Notification Host, Queries.

To create a new SNMP v1/v2c community:

1. Go to *System* > *SNMP*.
2. In the SNMP v1/v2c section of the screen select *Create New* from the toolbar.

3. Configure the following settings:

Enable	Select to enable the SNMP community.
Community Name	Enter a name to identify the SNMP community.
Hosts	The list of hosts that can use the settings in this SNMP community to monitor the FortiSandbox system.
IP/Netmask	Enter the IP address and netmask of the SNMP hosts. Select the *Add* button to add additional hosts.
Queries v1	Enter the port number and select to enable. Enable queries for each SNMP version that the FortiSandbox system uses.
Queries v2c	Enter the port number and select to enable. Enable queries for each SNMP version that the FortiSandbox system uses.
Traps v1	Enter the local port number, remote port number, and select to enable. Enable traps for each SNMP version that the FortiSandbox system uses.
Traps v2c	Enter the local port number, remote port number, and select to enable. Enable traps for each SNMP version that the FortiSandbox system uses.
SNMP Events	Enable the events that will cause the FortiSandbox unit to send SNMP traps to the community. • CPU usage is high • Memory is low • Hard disk usage is high • RAID disk information • Average scan time • Topology map and health check status for cluster has changed • Interface is up or down • Power Supply failure (not available on FSA-500F model) • Malware is detected

4. Click *OK* to create the SNMP community.

To create a new SNMP v3 user:

1. Go to *System* > *SNMP*.
2. In the SNMP v3 section of the screen, select *Create New* from the toolbar.

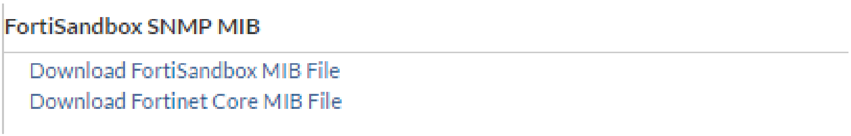
3. Configure the following settings:

Username	Enter the name of the SNMPv3 user.
Security Level	Select the security level of the user. Select one of the following: • None • Authentication only • Encryption and authentication
Authentication	Authentication is required when *Security Level* is either *Authentication only* or *Encryption and authentication*.
Method	Select the authentication method. Select either: • MD5 (Message Digest 5 algorithm) • SHA1 (Secure Hash algorithm)
Password	Enter the authentication password. The password must be a minimum of 8 characters.
Encryption	Encryption is required when *Security Level* is *Encryption and authentication*.
Method	Select the encryption method, either DES or AES.
Key	Enter the encryption key. The encryption key value must be a minimum of 8 characters.
Notification Hosts (Traps)	
IP/Netmask	Enter the IP address and netmask. Click the *Add* button to add additional hosts.
Query	
Port	Enter the port number. Select to *Enable* the query port.
SNMP v3 Events	Select the SNMP events that will be associated with that user. • CPU usage is high • Memory is low • Hard disk usage is high • RAID disk information • Average scan time • Topology map and health check status for cluster has changed • Interface is up or down • Power Supply failure (not available on FSA-500F model) • Malware is detected

4. Click *OK* to create the SNMP community.

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:

Module Name	FortiGuard module name such as *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 Rating Engine*, *Linux Analytic Engine*, *Linux Rating Engine*, *Industry Security Signature*, and *Traffic Sniffer*. All modules automatically install update packages when they are available on FDN.
Current Version	Current version of the module.
Last Check Time	Date and time that module last checked for an update.
Last Update Time	Date and time that module was last updated.
Last Check Status	Status of the last update attempt.
Upload Package File	Click *Choose File* to select a package file on the management computer, then click *Submit* to upload the package file to FortiSandbox. If the unit has no access to Fortinet FDN servers, go to the Customer Service and Support site to download package files manually.
FortiGuard Server Location	Select FDN servers for package update and Web Filtering query. The default selection is *Nearest* which is the FDN server nearest the unit's time zone. Selecting *US Region* means using only servers in the USA.
FortiGuard Server Settings	
Use override FDN server to download module updates	Enable this option to use an override FDN server or FortiManager to download module updates. Enter the override server IP address or FQDN in the text box. Enabling this option disables *FortiGuard Server Location*. Click *Connect FDN Now* to schedule an immediate update check.
Use Proxy	Enable this option to use a proxy. Configure the *Proxy Type* (*HTTP Connect*, *SOCKS v4*, or *SOCKS v5*), *Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
Connect FDN Now	Click *Connect FDN Now* to connect to the override FDN server/proxy.
FortiGuard Web Filter Settings	

Secure Connection	FortiSandbox supports secure XOR encrypted connection for FortiGuard web filter settings. When enabled, the system uses secure XOR encrypted mode for the connection.
Use override server for web filtering query	Enable this option to use an override server address for web filtering query using the server IP address or FQDN in the text box. The default is the web filtering server nearest the unit's time zone.
Use Proxy	Enable this option to use a proxy. Configure the *Socks5 Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
VM Image Download Proxy Settings	
Use Proxy	Enable this option to use a proxy. Configure the *Proxy Type* (*HTTP Connect*, *SOCKS v4*, or *SOCKS v5*), *Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
FortiSandbox Community Cloud & Threat Intelligence Settings	
Use override server for community cloud server query	Enable this option when using FortiManager for FortiGuard upgrades in your environment. When using FortiManager for FortiGuard upgrades, only verdict information is available for malware. The malware's behavior information is not available.
Use Proxy	Enable this option to use a proxy. Configure the *Socks5 Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
FortiSandbox WindowsCloud VM Settings	
Server Regions	This option requires a Windows Cloud VM contract. Select the region where Windows Cloud VMs are used to scan files. You can override the APT server and manually enter the IP address of the APT server which hosts the Windows Cloud VM.

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 settings.

Idle timeout	Length of time before FortiSandbox logs out an inactive user, from 1 to 480 minutes.

Menu Type	Set the left menu to be *Compact* or *Expanded*. In compact mode, click an icon in the left menu to expand and display the menu items.
Language	Temporarily change the GUI language until the next login.
Report Saving Days	Length of time to keep reports, from 1 to 28 days.
Show alarms of unprocessed detections on Dashboard	Enable this option to show notifications in the top banner. Select the time period and rating of notifications. You must log out and log back in to show notifications. Click the notification to go to *FortiView* > *Operation Center* to see the details.
Reset all widgets	Reset all widgets in *Dashboard*, *File Detection* > *Summary Report*, *Network Alerts* > *Summary Report*, and *URL Detection* > *Summary Report*.

Job View Settings

Go to *System* > *Job View Settings* to define columns and their order for every job result. You can set the number of jobs shown on each page for view types that support pagination.

You can configure how to load the next set of jobs:

- Pagination
- Infinite Scroll

Job Result pages show job data, including:

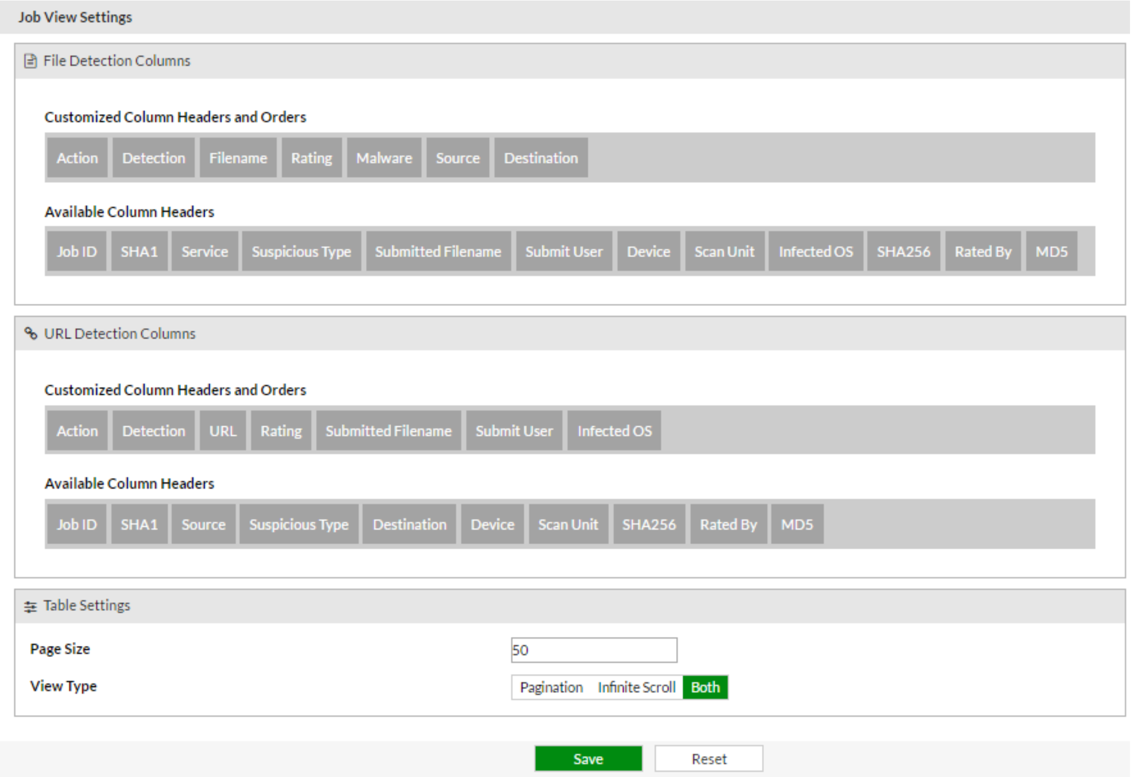
- *FortiView* > *File Scan Search*
- *FortiView* > *URL Scan Search*
- *File Detection* > *File Scan*
- *URL Detection* > *URL Scan*
- Job links in *Dashboard* > *Scanning Statistics* widget

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

Action | Detection | Filename | Rating | Malware | Source | Destination

Available Column Headers

Job ID | SHA1 | Service | Suspicious Type | Submitted Filename | Submit User | Device | Scan Unit | Infected OS | SHA256 | Rated By | MD5

URL Detection Columns

Customized Column Headers and Orders

Action | Detection | URL | Rating | Submitted Filename | Submit User | Infected OS

Available Column Headers

Job ID | SHA1 | Source | Suspicious Type | Destination | Device | Scan Unit | SHA256 | Rated By | MD5

Table Settings

Page Size: 50

View Type: Pagination | Infinite Scroll | [✓ Both]

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

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

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

Virtual Machine

The FortiSandbox VM host is based on a modified hypervisor.

Model, License, and VM Information

Model	Windows License	Default Windows VMs	Number of VM Hosts Supported
FSA-1000D	Windows 7 Microsoft Office	WIN7X86VM (with Office) WIN7X64VM	8
FSA-2000E	Windows 7 Windows 8.1 Windows 10 Microsoft Office	WIN7X86SP1O16 (with Office)	Supports 4 VM hosts by default, maximum up to 24 VM hosts.
FSA-3000E	Windows 7 Windows 8.1 Windows 10 Microsoft Office	WIN7X86VM (with Office) WIN7X64VM	Supports 8 VM hosts by default, maximum up to 56 VM hosts.
FSA-3000D			28
FSA-3500D	Windows 7 Windows 8.1 Windows 10 Microsoft Office	WIN7X86VM (with Office) WIN7X64VM	8 on each blade
FSA-500F	Windows 7 Windows 10 Office	WIN7X64SP1O16 (with Office)	Supports 2 VM hosts by default, maximum up to 6 VM hosts.
FSA-1000F	Windows 7 Windows 10 Office	WIN7X64SP1O16 (with Office)	Supports 2 VM hosts by default, maximum up to 14 VM hosts.
FSA-3000F	Windows 7 Windows 10 Office	WIN7X64SP1O16 (with Office)	Supports 2 VM hosts by default, maximum up to 74 VM hosts.
FSAVM00			No VM host by default, maximum up to 8 VM hosts. To expand the unit's scan power, you can purchase a Cloud Windows VM subscription. Files can be sent to Fortinet Cloud Sandboxing to scan.

FortiSandbox devices purchased after March 17, 2017 do not support WINXP VM type and its licenses due to Microsoft EOL.

The number of supported VM hosts for each model is only for images published by Fortinet. This number might be lower for custom images with high resource requirements.

You can download and use optional images from *VM Images* > *Optional VMs*. The VM name shows the OS type. *O16* in the name means Microsoft Office 2016 is installed. You might need extra Windows OS licenses. For example, if you want to use a Windows 10 image on a FSA-1000D unit, you must purchase a Windows 10 license key from Fortinet.

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

Android VM is free to download and use.

You can build custom VM images but you must have software licenses for your custom 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 the running scan. If the scan allows VM interaction, users can click the VM Interact icon to interact with the scan.

To take snapshots of scans or initiate interactions with the VM, your admin profile must have *Read/Write* privilege for *All On-Demand Scan Interactions*.

VM Images

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

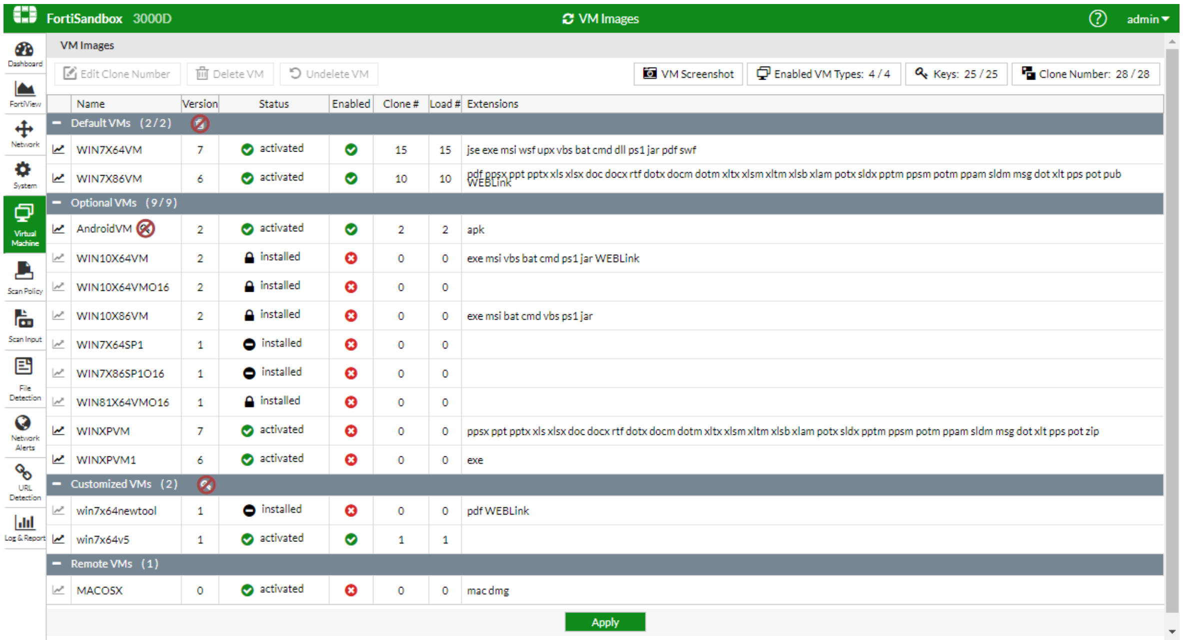
VM images are grouped into the following categories:

Default VMs	Basic set of images installed on FortiSandbox by default. The FSA-AWS models are the Windows VMs installed on AWS.
Optional VMs	Optional VM images published by Fortinet.
Customized VMs	User created images and uploaded to FortiSandbox.

Remote VMs	Fortinet supports *MACOSX* and *WindowsCloudVM* as remote VMs. You can purchase subscription services from Fortinet to reserve clone numbers in the FortiSandbox Cloud. There is no trial license for MACOSX VM. In cluster mode for MACOSX remote VMs, all cluster nodes share a collected pool of reserved clones from each unit. This means that even if a node has no remote VM contract, it can still upload files to the cloud for scanning. For the cluster as a whole, the number of files being scanned on the cloud cannot exceed the total number of reserved clone numbers at any given moment. In cluster mode for WindowsCloudVM, VM00 units in the cluster can purchase WindowscloudVM seat counts. These cloud VM clones are local to the VM00 unit and are not shared.
Simulator VMs	For v3.1.1 and later, *LinuxOT* is supported as a simulator Linux VM for the OT industry to detect malware. You can purchase the Industry Security Signature Contract from Fortinet to enable LinuxOT. To scan files with the simulator VM, submit files through the Ubuntu VM which simulates protocols such as Modbus, SNMP, IPMI, FTP, and TFTP to detect malware. Currently, SIEMENS is supported inside the simulator VM. OT image is not supported on EOL like FSA 1000-D, 3000-D, and 3500-D. OT images use one VM license. The clone number does not change when enabled.

When Fortinet publishes a new version of VM image on its image server, the image appears in the *Optional VMs* group with a download button in the *Status* column. Click the button to start downloading. After downloading all the images, click the *Ready to Install* button to install all downloaded images. No reboot is necessary for installation.

After an image is installed, its license key is checked. If no keys are available, the image status is *installed* but disabled until the key is imported and the image is activated. After the image is activated, you can start using it by setting its clone number to be greater than 0. Then the image status changes to *activated*.



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 xltx xlsm xltm xlsb xlam potx sldx pptm ppsm potm ppam sldm msg dot xlt pps pot pub WEBLink
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 xltx xlsm xltm xlsb xlam potx sldx pptm ppsm potm ppam sldm 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

The following options are available:

Edit Clone Number	Edit the selected entry. Click the green checkmark to save the new number and then click *Apply*.
Delete VM	Delete the selected entry. VMs deleted in the GUI are deleted when the system reboots. You cannot delete the default set of four Windows VMs.
Undelete VM	After deleting a VM, you can use *Undelete the VM* to recover it. After the system reboots and the delete action is completed, you cannot undelete a VM.
VM Screenshot	Take a screenshot of a running VM and view the filename the VM is scanning. This is only available for a admin users.

The following information is displayed:

Enabled VM Types	The maximum number of VM types that can concurrently run. The maximum is four on models other than FSA-3000E. The maximum is six on FSA-3000E.
Keys	Maximum number of keys including used key numbers and installed key numbers.
Clone Number	Maximum clone number and 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. • FSA-2000E, the maximum clone number is 24. • 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.
Name	Name of the VM image. The name is unique in the system. If you upload a new VM image of the same name, the current installation is replaced. To see the VM’s usage chart, click the *Chart* icon beside the *Name*.
Version	VM image version. If there is a new version of an image on the Fortinet Image Server, a *New Version Available* icon appears. You can download, install, and activate it.
Status	VM image status such as: • Ready to Download • Ready to Upgrade • Downloading (shows a progress bar) • Ready to Install (Install or Remove downloaded image) • Installing • Installed (Disabled) • Installed (No Keys Available) • Activated
Enabled	If an image's clone number is 0, it is disabled. Otherwise it is enabled.
Clone#	VM clone number. Double-click the number to edit it and then click the green checkmark to save the new number. Click *Apply* to apply the change. The VM system re-initializes.

	The total clone number of all VM images cannot exceed the number of installed Windows licenses. For example, for FSA-3000D, the maximum clone number is 28. We recommend applying more than 8+clone_number*3 of memory on your FSA unit.
Load#	The used VM clone number. For example, if a cluster primary node is set to use 50% of sandboxing scan power, the load # is half of clone #.
Extensions	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. If the sandbox prefiltering is turned off for a file type, it will be scanned inside each associated VM type. 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 types. You can define file type and VM association in *Scan Policy > Scan Profile*. You can double-click the value to access the *Scan Profile* page to edit the list.

Enabled clone numbers are checked against allocated CPU and memory resources. If there are not enough resources, a warning message appears and the setting is denied.

Clone Number for VM Image

The following is the default clone number for VM images:

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.

You can change the default settings to suit the majority of file types in your environment. For example, if most file types are Office files and WIN7X86VM is associated with Office files, you 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.

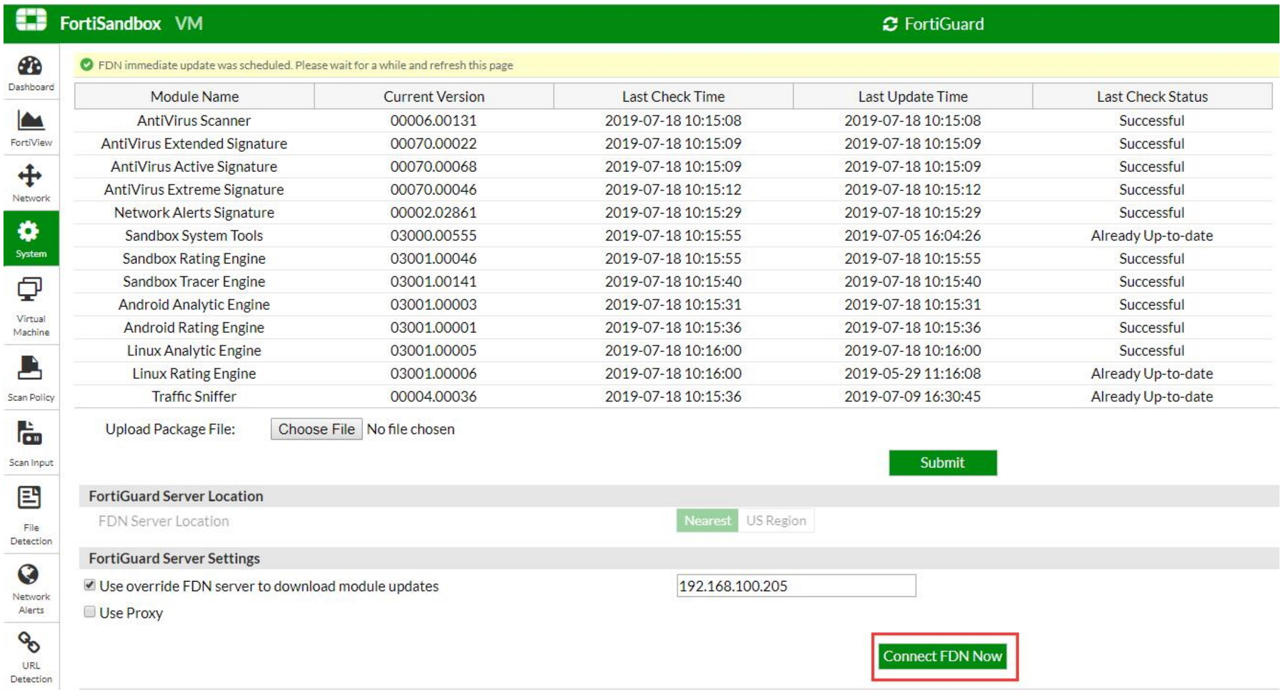
This button is only available when login user is *admin*.

OT Simulation

OT Simulation is a simulated Linux VM developed by Fortinet to address the OT industry’s need to detect malware which sends commands or collects data from their Industrial Control systems (ICS). The implementation in FortiSandbox uses an Industrial Security Signature contract in a Linux VM that simulates protocols such as Modbus, SNMP, IPMI, FTP and TFTP to detect the malware.

Preparing the OT Simulator VM on FortiSandbox

1. First, log in to Fortinet One, select *Manage/View Products*, and ensure the unit's Serial Number contains the "ISSS" contract and that it is not expired.
2. On the FortiSandbox *System -> FortiGuard* page, click the *Connect FDN Now* button to download the latest contracts and engines.



FDN immediate update was scheduled. Please wait for a while and refresh this page

Module Name	Current Version	Last Check Time	Last Update Time	Last Check Status
AntiVirus Scanner	00006.00131	2019-07-18 10:15:08	2019-07-18 10:15:08	Successful
AntiVirus Extended Signature	00070.00022	2019-07-18 10:15:09	2019-07-18 10:15:09	Successful
AntiVirus Active Signature	00070.00068	2019-07-18 10:15:09	2019-07-18 10:15:09	Successful
AntiVirus Extreme Signature	00070.00046	2019-07-18 10:15:12	2019-07-18 10:15:12	Successful
Network Alerts Signature	00002.02861	2019-07-18 10:15:29	2019-07-18 10:15:29	Successful
Sandbox System Tools	03000.00555	2019-07-18 10:15:55	2019-07-05 16:04:26	Already Up-to-date
Sandbox Rating Engine	03001.00046	2019-07-18 10:15:55	2019-07-18 10:15:55	Successful
Sandbox Tracer Engine	03001.00141	2019-07-18 10:15:40	2019-07-18 10:15:40	Successful
Android Analytic Engine	03001.00003	2019-07-18 10:15:31	2019-07-18 10:15:31	Successful
Android Rating Engine	03001.00001	2019-07-18 10:15:36	2019-07-18 10:15:36	Successful
Linux Analytic Engine	03001.00005	2019-07-18 10:16:00	2019-07-18 10:16:00	Successful
Linux Rating Engine	03001.00006	2019-07-18 10:16:00	2019-05-29 11:16:08	Already Up-to-date
Traffic Sniffer	00004.00036	2019-07-18 10:15:36	2019-07-09 16:30:45	Already Up-to-date

Upload Package File: No file chosen

FortiGuard Server Location

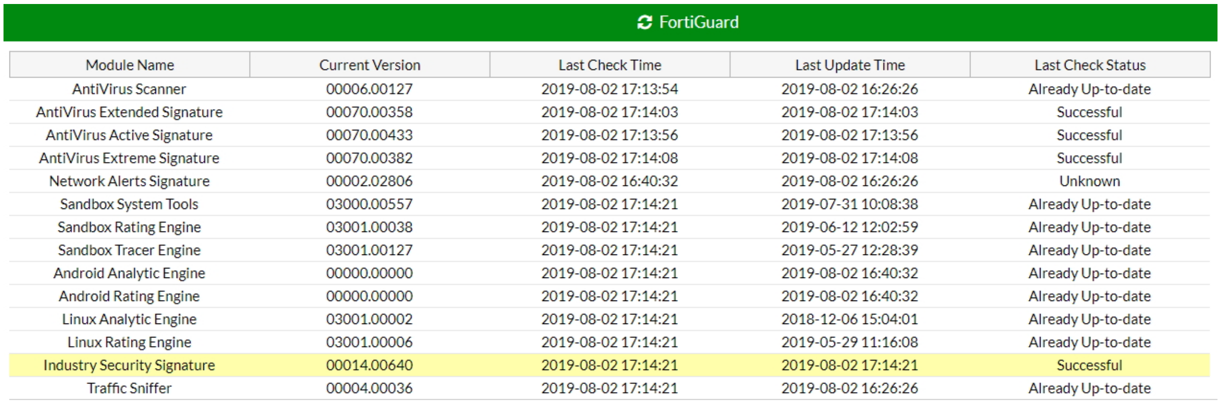
FDN Server Location: Nearest | US Region

FortiGuard Server Settings

☑ Use override FDN server to download module updates 192.168.100.205

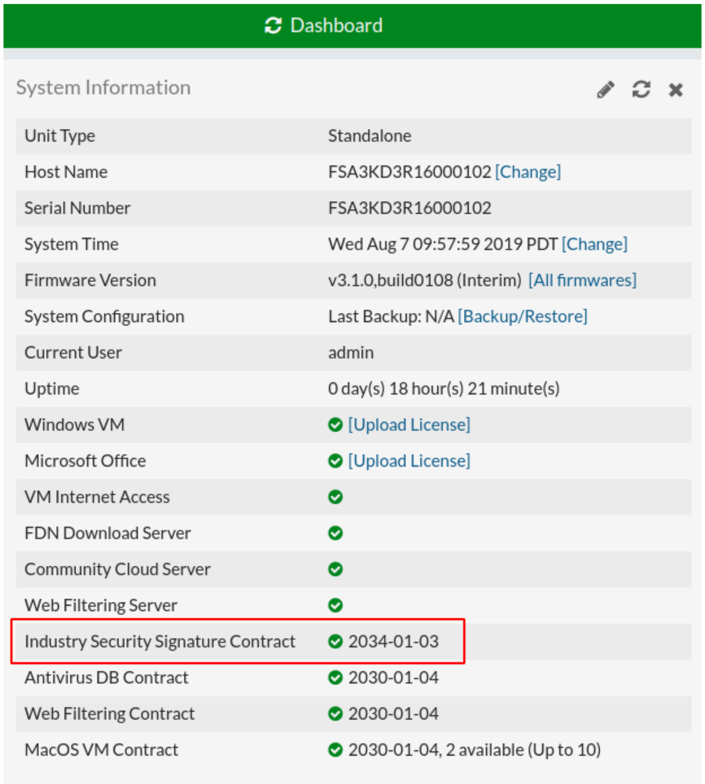
□ Use Proxy

3. Wait for a while then refresh the FortiGuard page. There is a new entry for *Industry Security Signature*.



Module Name	Current Version	Last Check Time	Last Update Time	Last Check Status
AntiVirus Scanner	00006.00127	2019-08-02 17:13:54	2019-08-02 16:26:26	Already Up-to-date
AntiVirus Extended Signature	00070.00358	2019-08-02 17:14:03	2019-08-02 17:14:03	Successful
AntiVirus Active Signature	00070.00433	2019-08-02 17:13:56	2019-08-02 17:13:56	Successful
AntiVirus Extreme Signature	00070.00382	2019-08-02 17:14:08	2019-08-02 17:14:08	Successful
Network Alerts Signature	00002.02806	2019-08-02 16:40:32	2019-08-02 16:26:26	Unknown
Sandbox System Tools	03000.00557	2019-08-02 17:14:21	2019-07-31 10:08:38	Already Up-to-date
Sandbox Rating Engine	03001.00038	2019-08-02 17:14:21	2019-06-12 12:02:59	Already Up-to-date
Sandbox Tracer Engine	03001.00127	2019-08-02 17:14:21	2019-05-27 12:28:39	Already Up-to-date
Android Analytic Engine	00000.00000	2019-08-02 17:14:21	2019-08-02 16:40:32	Already Up-to-date
Android Rating Engine	00000.00000	2019-08-02 17:14:21	2019-08-02 16:40:32	Already Up-to-date
Linux Analytic Engine	03001.00002	2019-08-02 17:14:21	2018-12-06 15:04:01	Already Up-to-date
Linux Rating Engine	03001.00006	2019-08-02 17:14:21	2019-05-29 11:16:08	Already Up-to-date
Industry Security Signature	00014.00640	2019-08-02 17:14:21	2019-08-02 17:14:21	Successful
Traffic Sniffer	00004.00036	2019-08-02 17:14:21	2019-08-02 16:26:26	Already Up-to-date

4. On the Dashboard page, under the *System Information* widget, check that the ISSS contract is downloaded and valid.

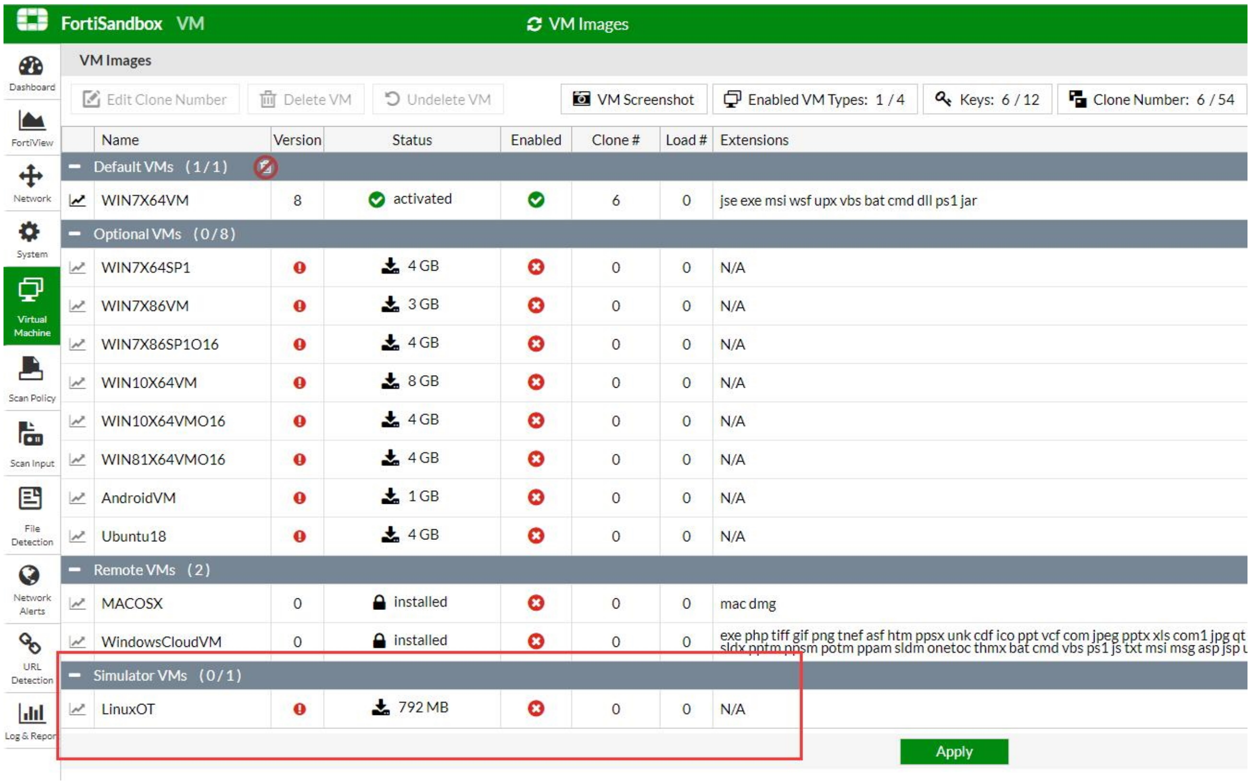


Dashboard

System Information

Unit Type	Standalone
Host Name	FSA3KD3R16000102 [Change]
Serial Number	FSA3KD3R16000102
System Time	Wed Aug 7 09:57:59 2019 PDT [Change]
Firmware Version	v3.1.0,build0108 (Interim) [All firmwares]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 18 hour(s) 21 minute(s)
Windows VM	✓ [Upload License]
Microsoft Office	✓ [Upload License]
VM Internet Access	✓
FDN Download Server	✓
Community Cloud Server	✓
Web Filtering Server	✓
Industry Security Signature Contract	✓ 2034-01-03
Antivirus DB Contract	✓ 2030-01-04
Web Filtering Contract	✓ 2030-01-04
MacOS VM Contract	✓ 2030-01-04, 2 available (Up to 10)

5. Go to the VM Image page and find *LinuxOT* under the *Simulator VMs* table.



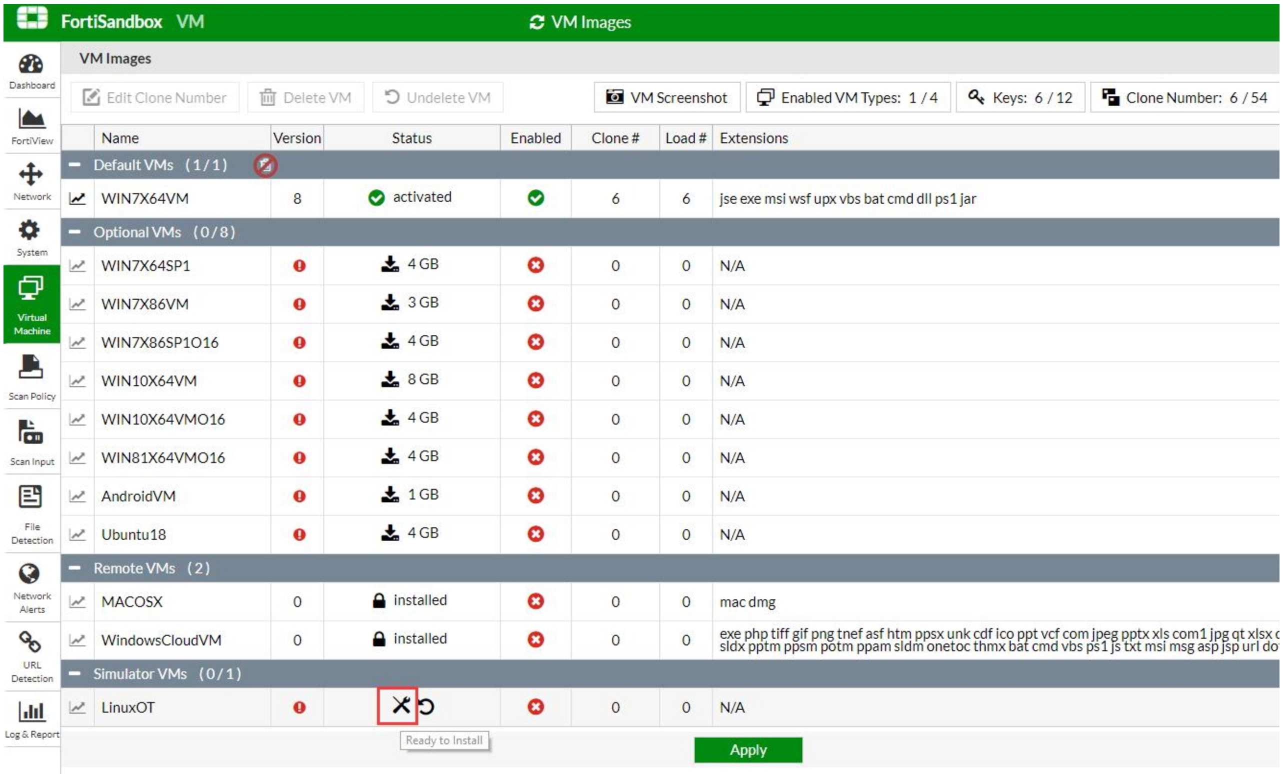
VM Images

Enabled VM Types: 1 / 4 · Keys: 6 / 12 · Clone Number: 6 / 54

Name	Version	Status	Enabled	Clone #	Load #	Extensions
Default VMs (1/1)						
WIN7X64VM	8	✓ activated	✓	6	0	jse exe msi wsf upx vbs bat cmd dll ps1 jar
Optional VMs (0/8)						
WIN7X64SP1	!	4 GB	✖	0	0	N/A
WIN7X86VM	!	3 GB	✖	0	0	N/A
WIN7X86SP1O16	!	4 GB	✖	0	0	N/A
WIN10X64VM	!	8 GB	✖	0	0	N/A
WIN10X64VMO16	!	4 GB	✖	0	0	N/A
WIN81X64VMO16	!	4 GB	✖	0	0	N/A
AndroidVM	!	1 GB	✖	0	0	N/A
Ubuntu18	!	4 GB	✖	0	0	N/A
Remote VMs (2)						
MACOSX	0	installed	✖	0	0	mac dmg
WindowsCloudVM	0	installed	✖	0	0	exe php tiff gif png tnef asf htm ppsx unk cdf ico ppt vcf com jpeg pptx xls com1 jpg qt sldx pptm ppsm potm ppam sldm onetoc thmx bat cmd vbs ps1 js txt msi msg asp jsp
Simulator VMs (0/1)						
LinuxOT	!	792 MB	✖	0	0	N/A

6. Click the download icon in the status column of the *LinuxOT* row.

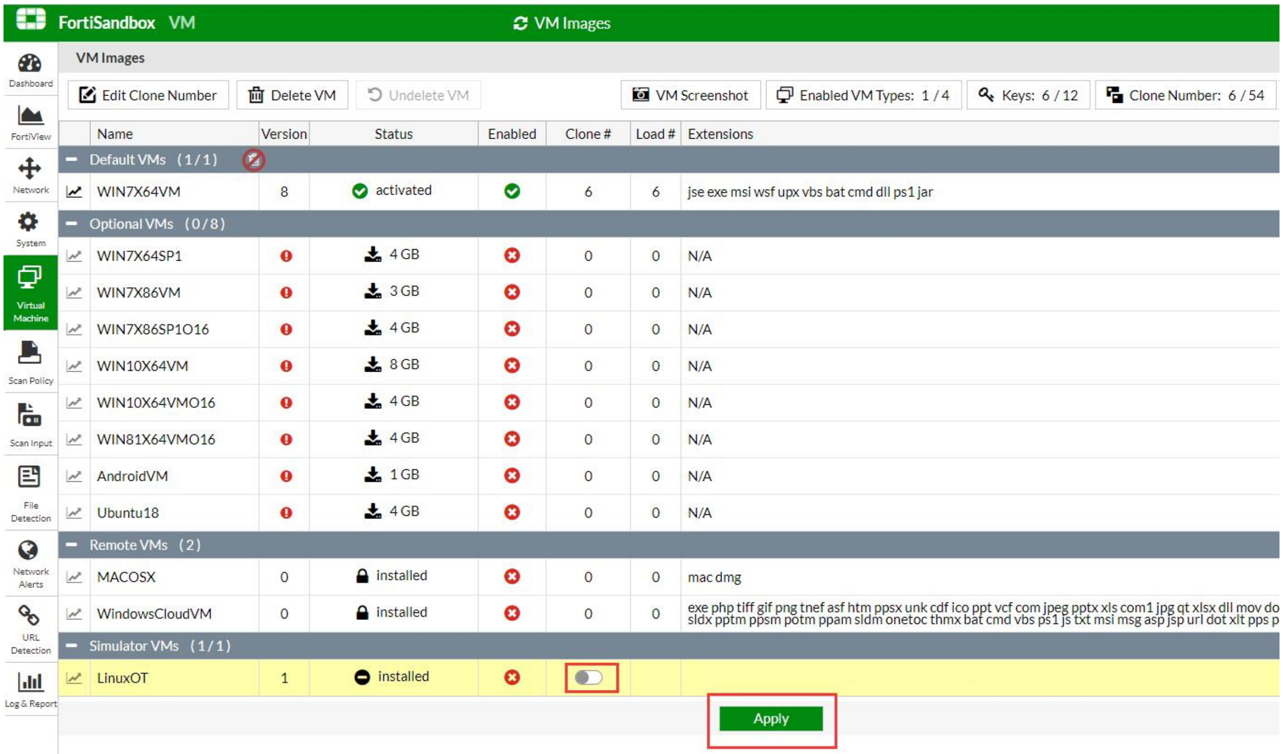
7. Click the *Install* button as below and wait for the installation to complete and the FortiSandbox to reboot.



Name	Version	Status	Enabled	Clone #	Load #	Extensions
Default VMs (1/1)						
WIN7X64VM	8	✓ activated	✓	6	6	jse exe msi wsf upx vbs bat cmd dll ps1 jar
Optional VMs (0/8)						
WIN7X64SP1	!	⬇ 4 GB	✗	0	0	N/A
WIN7X86VM	!	⬇ 3 GB	✗	0	0	N/A
WIN7X86SP1O16	!	⬇ 4 GB	✗	0	0	N/A
WIN10X64VM	!	⬇ 8 GB	✗	0	0	N/A
WIN10X64VMO16	!	⬇ 4 GB	✗	0	0	N/A
WIN81X64VMO16	!	⬇ 4 GB	✗	0	0	N/A
AndroidVM	!	⬇ 1 GB	✗	0	0	N/A
Ubuntu18	!	⬇ 4 GB	✗	0	0	N/A
Remote VMs (2)						
MACOSX	0	🔒 installed	✗	0	0	mac dmg
WindowsCloudVM	0	🔒 installed	✗	0	0	exe php tiff gif png tnef asf htm ppsx unk cdf ico ppt vcf com jpeg pptx xls com1 jpg qt xlsx d sldx pptm ppsm potm ppam sldm onetoc thmx bat cmd vbs ps1 js txt msi msg asp jsp url do
Simulator VMs (0/1)						
LinuxOT	!	✗ ↺	✗	0	0	N/A

8. After rebooting, the *LinuxOT VM* is installed with clone disabled.

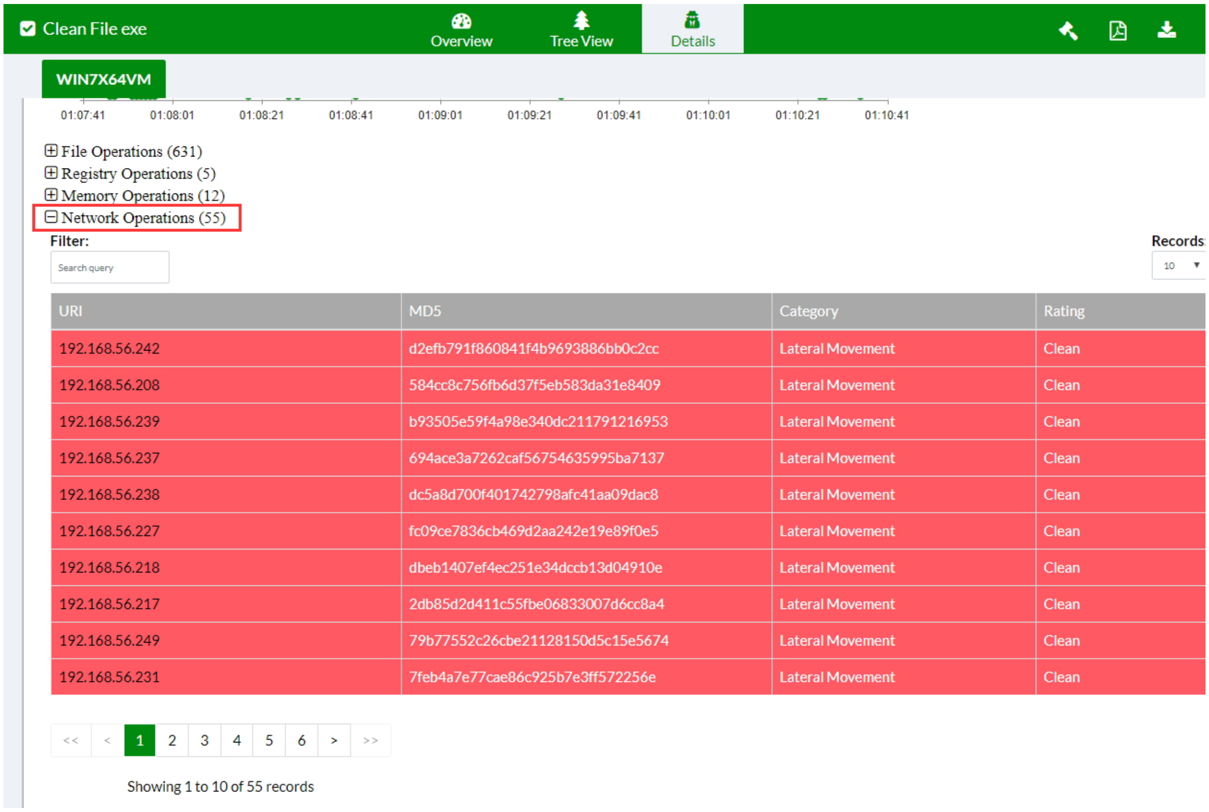
9. Toggle the switch in the *Clone #* column to enable it then press *Apply* to save the changes.



Name	Version	Status	Enabled	Clone #	Load #	Extensions
Default VMs (1/1)						
WIN7X64VM	8	✓ activated	✓	6	6	jse exe msi wsf upx vbs bat cmd dll ps1 jar
Optional VMs (0/8)						
WIN7X64SP1	!	⬇ 4 GB	✗	0	0	N/A
WIN7X86VM	!	⬇ 3 GB	✗	0	0	N/A
WIN7X86SP1O16	!	⬇ 4 GB	✗	0	0	N/A
WIN10X64VM	!	⬇ 8 GB	✗	0	0	N/A
WIN10X64VMO16	!	⬇ 4 GB	✗	0	0	N/A
WIN81X64VMO16	!	⬇ 4 GB	✗	0	0	N/A
AndroidVM	!	⬇ 1 GB	✗	0	0	N/A
Ubuntu18	!	⬇ 4 GB	✗	0	0	N/A
Remote VMs (2)						
MACOSX	0	🔒 installed	✗	0	0	mac dmg
WindowsCloudVM	0	🔒 installed	✗	0	0	exe php tiff gif png tnef asf htm ppsx unk cdf ico ppt vcf com jpeg pptx xls com1 jpg qt xlsx dll mov do sldx pptm ppsm potm ppam sldm onetoc thmx bat cmd vbs ps1 js txt msi msg asp jsp url dot xlt pps p
Simulator VMs (1/1)						
LinuxOT	1	⊖ installed	✗	○		

Scanning the files with the Simulator VM enabled

1. To Scan a file using the Simulator VM, submit a scan job to the Windows VMs. The Simulator VM will detect network operations automatically.
2. After the scan is finished, check the job detail to confirm the following:
    - There should be more than one .pcap file in the *PCAP Information* section.
    - There should be at least one item containing the *Lateral Movement* category in the *Network Operations* section.



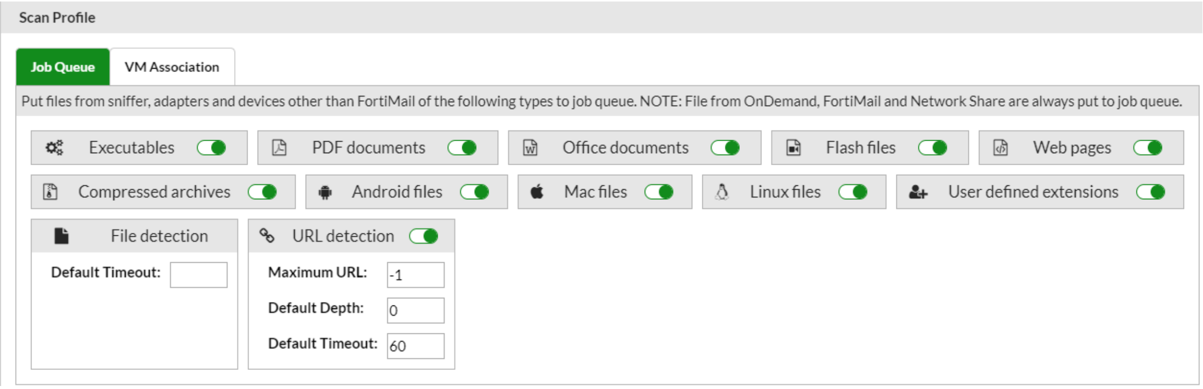
URI	MD5	Category	Rating
192.168.56.242	d2efb791f860841f4b9693886bb0c2cc	Lateral Movement	Clean
192.168.56.208	584cc8c756fb6d37f5eb583da31e8409	Lateral Movement	Clean
192.168.56.239	b93505e59f4a98e340dc211791216953	Lateral Movement	Clean
192.168.56.237	694ace3a7262caf56754635995ba7137	Lateral Movement	Clean
192.168.56.238	dc5a8d700f401742798afc41aa09dac8	Lateral Movement	Clean
192.168.56.227	fc09ce7836cb469d2aa242e19e89f0e5	Lateral Movement	Clean
192.168.56.218	dbeb1407ef4ec251e34dccb13d04910e	Lateral Movement	Clean
192.168.56.217	2db85d2d411c55fbe06833007d6cc8a4	Lateral Movement	Clean
192.168.56.249	79b77552c26cbe21128150d5c15e5674	Lateral Movement	Clean
192.168.56.231	7feb4a7e77cae86c925b7e3ff572256e	Lateral Movement	Clean

Showing 1 to 10 of 55 records

Scan Policy

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.



Scan Profile

Job Queue | VM Association

Put files from sniffer, adapters and devices other than FortiMail of the following types to job queue. NOTE: File from OnDemand, FortiMail and Network Share are always put to job queue.

Executables ● | PDF documents ● | Office documents ● | Flash files ● | Web pages ●

Compressed archives ● | Android files ● | Mac files ● | Linux files ● | User defined extensions ●

File detection
Default Timeout:

URL detection ●
Maximum URL: -1
Default Depth: 0
Default Timeout: 60

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. You can enable pre-filtering with the following CLI command: `sandboxing-prefilter -e -tdll` Only the DLL files which can be executed inside a VM are put into the Job Queue.
Archives	7Z, ARB, BZIP, BZIP2, CAB, ISO, EML, GZIP, LZW, RAR, TAR, XZ, ZIP, and more. Archive files are extracted up to six levels and each file inside are scanned according to the Scan Profile settings. The maximum number of files extracted are: • On-Demand input: 10000 • JSON API: 1000 • All other input sources: 100
Microsoft Office	Word, Excel, PowerPoint, Outlook, and more.
Adobe	PDF, SWF, and Flash.
Static Web Files	HTML, JS, URL, and LNK.
Android File	APK.

MACOSX Files	MACH_O, FATMACH, DMG, XAR, Linux, and APP.
WEBLink	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 FortiSandbox when the `.eml` file is attached inside an email. FortiSandbox parses the `.eml` file to extract its attachments and perform file scans.

When `sandboxing-embeddedurl` is enabled, the top three URLs inside the email body are extracted and scanned along with the .eml inside the same VM. If the URL is a direct download link, the file is downloaded and sent with the URL to be scanned.

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

By default, FortiMail holds a mail item for a time to wait for the FortiSandbox verdict. Before FortiSandbox scans a file or URL sent from FortiMail, it checks if FortiMail still needs the verdict as FortiMail might have already released the email after time out. If not, FortiSandbox gives the job an *Unknown* rating and skipped status.

Use the 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 are uploaded to Fortinet Sandboxing cloud to scan according to *Scan Profile* settings.

Scan Profile Job Queue Tab

Use the *Job Queue* to define file types and URLs that are allowed to enter the job queue if they are from a sniffer, adapter, or device other than FortiMail.

Files or URLs submitted through On-Demand, RPC JSON API, network share, or FortiMail are always 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.

File Detection

FortiSandbox supports a customized timeout value to control the tracer running time in VM.

Currently, MAC OSX and Windows Cloud VM do not support *File detection*.

To configure File Detection:

1. Select *Scan Policy* > *Scan Profile*
2. In the *File detection* window, enter a *Default Timeout* value between 60 and 180 seconds.
   A shorter *Default Timeout* value gives better performance and faster scan speed, but lower accuracy. For a balance of speed and accuracy, use a value that falls in the middle of the 60-180 second range.
3. Click *Apply* to save.
   The Scan results shows the VM Scan time.

URL Detection

When URL detection is enabled, FortiSandbox scans URLs (WEBLinks). You can also define the Default Depth setting (from 0 to 5) of the URL and the Default Timeout.

If there is a long queue of pending jobs, consider turning off some file types to job queue. For example, in most networks, static web files (JavaScript, html, aspx files) 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 that type already in the job queue will still be processed. You can use the `pending-jobs` command or *Scan Input* > *Job Queue* page to purge them.

To determine the number of each file type and its input source, use the 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 are sandboxed by the associated VM type. This page displays all installed VM image(s), their clone numbers, versions, and status.

To configure association:

Click the edit icon. The left panel shows installed applications and the right 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 the 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 3.2.1 CLI Reference Guide*.

To edit an 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 width, 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.

   FortiSandbox provides default scan profile settings.

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.

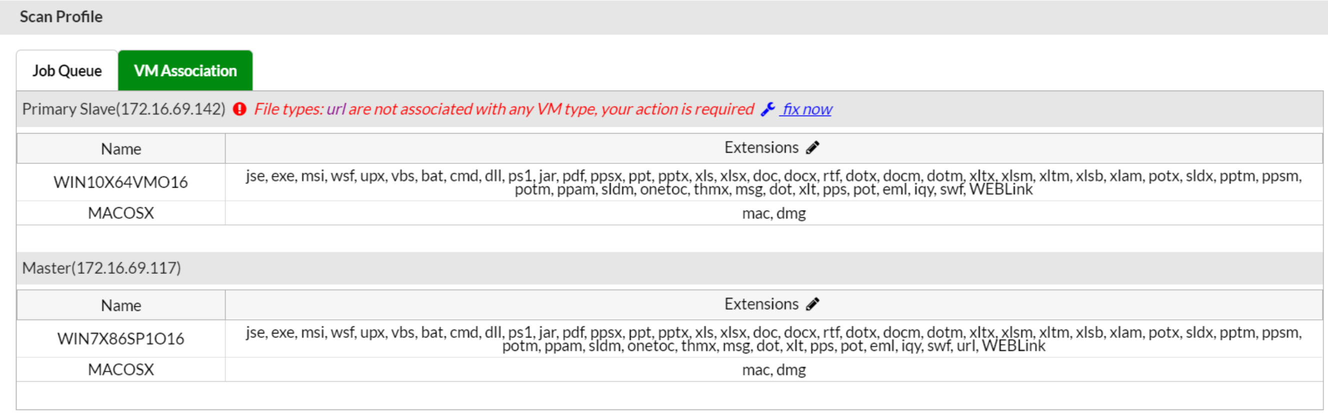
HA-Cluster

In an HA cluster environment, it is highly recommended that all cluster nodes have the same enabled VM. The Scan Profile can only be configured on the primary node, and these configurations are synchronized to the worker nodes. The primary node will collect all enabled VM image information. If a unique VM image is only installed on a worker node, you can still configure the primary node and the result will be synchronized to that worker node.

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 node and the configurations will be synced to worker nodes. The primary node will collect all installed VM image information. If a unique VM image is only installed on a worker node, you can still configure on the primary node and the result will be synchronized to that worker node.

HA-Cluster Scan Profile VM Association Tab



Scan Profile

Primary Slave(172.16.69.142) *File types: url are not associated with any VM type, your action is required* *fix now*

Name	Extensions
WIN10X64VMO16	jse, exe, msi, wsf, upx, vbs, bat, cmd, dll, ps1, jar, pdf, ppsx, ppt, pptx, xls, xlsx, doc, docx, rtf, dotx, docm, dotm, xltx, xlsm, xltm, xlsb, xlam, potx, sldx, pptm, ppsm, potm, ppam, sldm, onetoc, thmx, msg, dot, xlt, pps, pot, eml, iqy, swf, WEBLink
MACOSX	mac, dmg

Master(172.16.69.117)

Name	Extensions
WIN7X86SP1O16	jse, exe, msi, wsf, upx, vbs, bat, cmd, dll, ps1, jar, pdf, ppsx, ppt, pptx, xls, xlsx, doc, docx, rtf, dotx, docm, dotm, xltx, xlsm, xltm, xlsb, xlam, potx, sldx, pptm, ppsm, potm, ppam, sldm, onetoc, thmx, msg, dot, xlt, pps, pot, eml, iqy, swf, url, WEBLink
MACOSX	mac, dmg

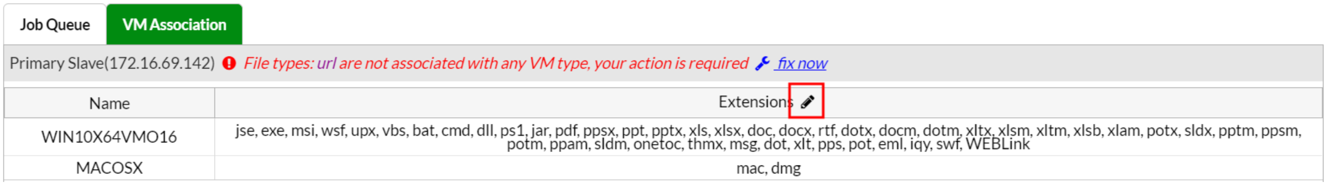
This page displays all cluster nodes enabled VM images and their enabled extensions. If the clone number is 0, the VM type is disabled. In this case, the enabled simulator VM is not listed.

The tips beside each cluster nodes display the unassociated file types on this node. The *fix now* link opens a configuration page for the file type associations. It is highly recommended that all cluster nodes have the same associated file types as the enabled VM.

Cluster nodes will be grouped with same enabled VM image. The tips and *fix now* link disappear when there are no longer any unassociated file types.

To configure associations for the HA-Cluster:

Click the pencil icon or the *fix now* link to edit the corresponding HA node.



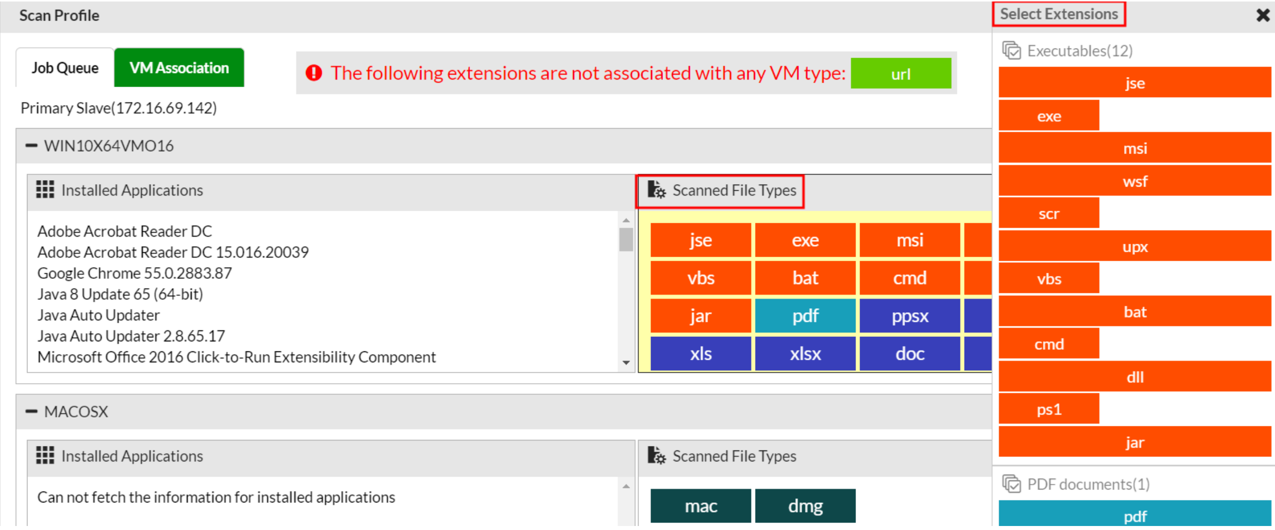
Primary Slave(172.16.69.142) *File types: url are not associated with any VM type, your action is required* *fix now*

Name	Extensions
WIN10X64VMO16	jse, exe, msi, wsf, upx, vbs, bat, cmd, dll, ps1, jar, pdf, ppsx, ppt, pptx, xls, xlsx, doc, docx, rtf, dotx, docm, dotm, xltx, xlsm, xltm, xlsb, xlam, potx, sldx, pptm, ppsm, potm, ppam, sldm, onetoc, thmx, msg, dot, xlt, pps, pot, eml, iqy, swf, WEBLink
MACOSX	mac, dmg

A new page will appear, with the left side panel displaying the installed applications and the right side panel displaying the currently associated file types.

To edit the associated file type for the HA-Cluster:

1. Click the *Scanned File Types* area. The *Select Extensions* pane is displayed.



Scan Profile

The following extensions are not associated with any VM type: url

Primary Slave(172.16.69.142)

WIN10X64VMO16

Installed Applications

Adobe Acrobat Reader DC
Adobe Acrobat Reader DC 15.016.20039
Google Chrome 55.0.2883.87
Java 8 Update 65 (64-bit)
Java Auto Updater
Java Auto Updater 2.8.65.17
Microsoft Office 2016 Click-to-Run Extensibility Component

Scanned File Types

MACOSX

Installed Applications

Can not fetch the information for installed applications

Scanned File Types

Select Extensions

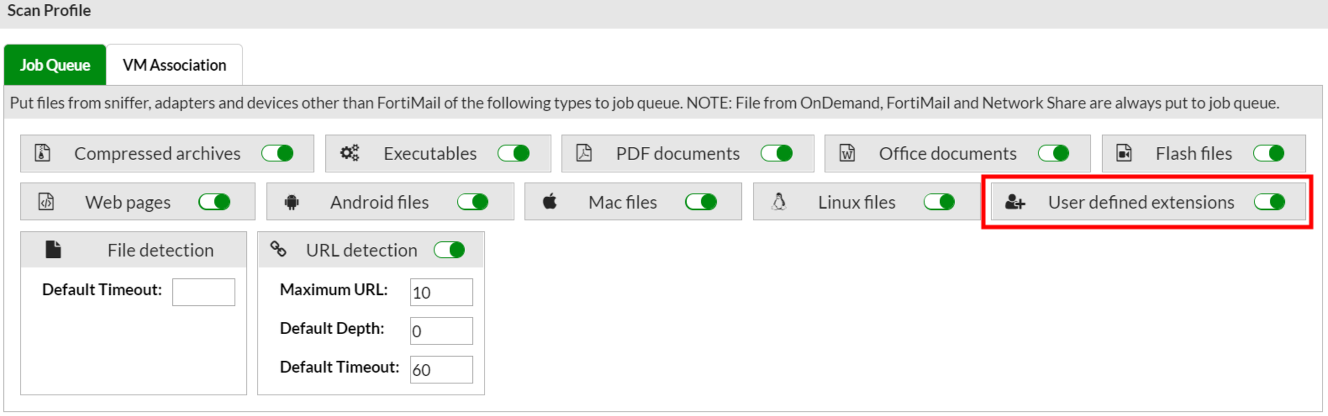
Executables(12)

PDF documents(1)

2. Click the name of the extension to toggle associations of grouped file types. The file types are grouped in different categories. Click an individual file type to toggle the corresponding association on or off.
   When the file type is displayed in the full width of the *Select Extensions* pane, it means the file type is associated (for example, the .jse extension above). When the file type is displayed in partial width, it means the file type is not currently associated (for example, the .exe extension above).

To add a user-defined extension for the HA-Cluster:

First, make sure the user-defined extension is enabled in the *Job Queue* tab.



Scan Profile

Put files from sniffer, adapters and devices other than FortiMail of the following types to job queue. NOTE: File from OnDemand, FortiMail and Network Share are always put to job queue.

Default Timeout:

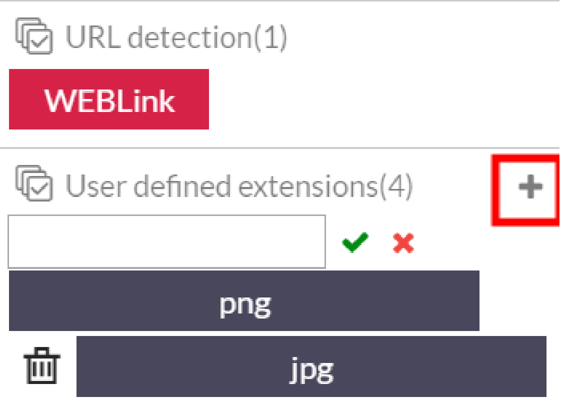
Maximum URL: 10

Default Depth: 0

Default Timeout: 60

To create a new user defined extension for the HA-Cluster:

1. Scroll to the bottom of the *Select Extensions* pane and click the + icon next to *User defined extensions*.



2. Enter a new extension in the text window.
3. Click the green check mark to confirm.
4. You can then click the new extension to toggle its association.

To add a user defined extension defined by other cluster nodes:

1. Click the + icon.
2. Enter the extension defined by other cluster nodes in the text window.
3. Click the green check mark to confirm.
4. You can then click on the new extension to toggle its association.

Finalizing the list of Scanned File Types in the HA-Cluster:

1. After you have finished the VM association, click *Scanned File Types* to finalize the list.
2. Click the Apply button to apply the changes. The configuration on the primary node will be synchronized with the edited node in real-time. Files will then be scanned by the associated VM images.
3. On the primary node, an alert message may appear in the bell icon in the upper right corner after updating the configuration. Click this, and the bell icon shows *Scan Profile requires your action*. Clicking the alert message redirects to the *Scan Profile* > *VM Association* page where you can use the *fix now* links to resolve issues with file extensions..

The `url`, `htm`, and `lnk` file types in the *Web pages* group are for the file types containing shortcuts of a web link, while the *WEBLink* type in the *URL detection* group is for URL addresses. The *WEBLink* type follows the depth and timeout settings in the *Job Queue* tab.

There might be malicious URLs, including direct download links, inside Office files and PDF files. You can scan selected URLs along with the original file inside files' associated VM. To turn on this feature, use the `sandboxing-embeddedurl` CLI command. For more information, see the FortiSandbox CLI Reference Guide.

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 and Linux 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 stops.

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 compared with the *Scan Profile page* > *Job Queue* tab settings to decide if it should be put in the job queue. If yes, it is compared with the allowlist and blocklist and overridden verdict list.

   For certain 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 a malicious website.
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 are 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 is 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 stops.

1. Static Scan.
   In this step, the URL is checked against the user uploaded *Allow/Block* or *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 is 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* is scanned inside a VM.

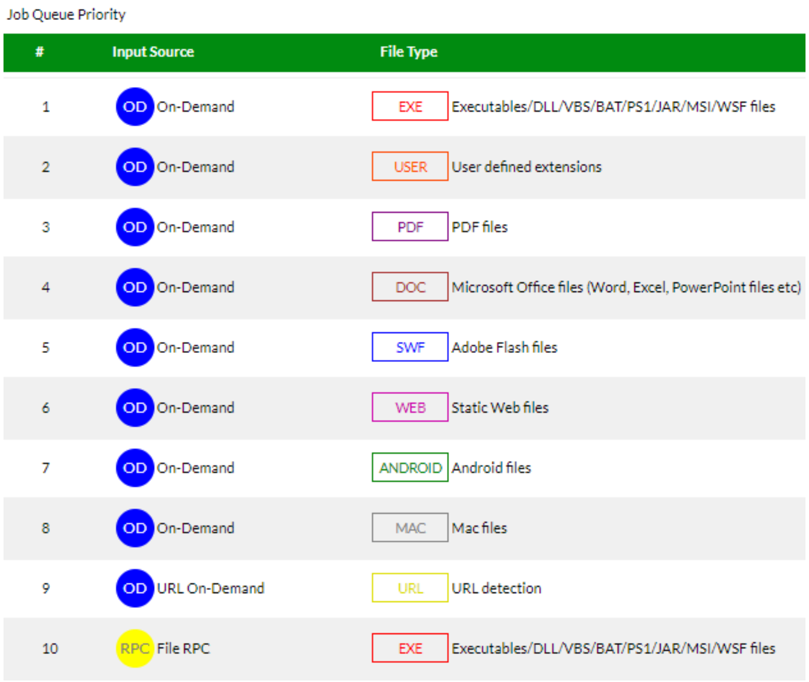
   For more information, see the the `sandboxing-prefiltering` command in the *FortiSandbox CLI Guide*.

In the Static Scan step, URLs are checked against the user uploaded allowlist and blocklist in this order and rated as *Clean* or *Malicious*: *Domain black list* > *URL REGEX black list* > *URL black list* > *Domain white list* > *URL REGEX white list* > *URL 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/1abc/bad.html` is 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.

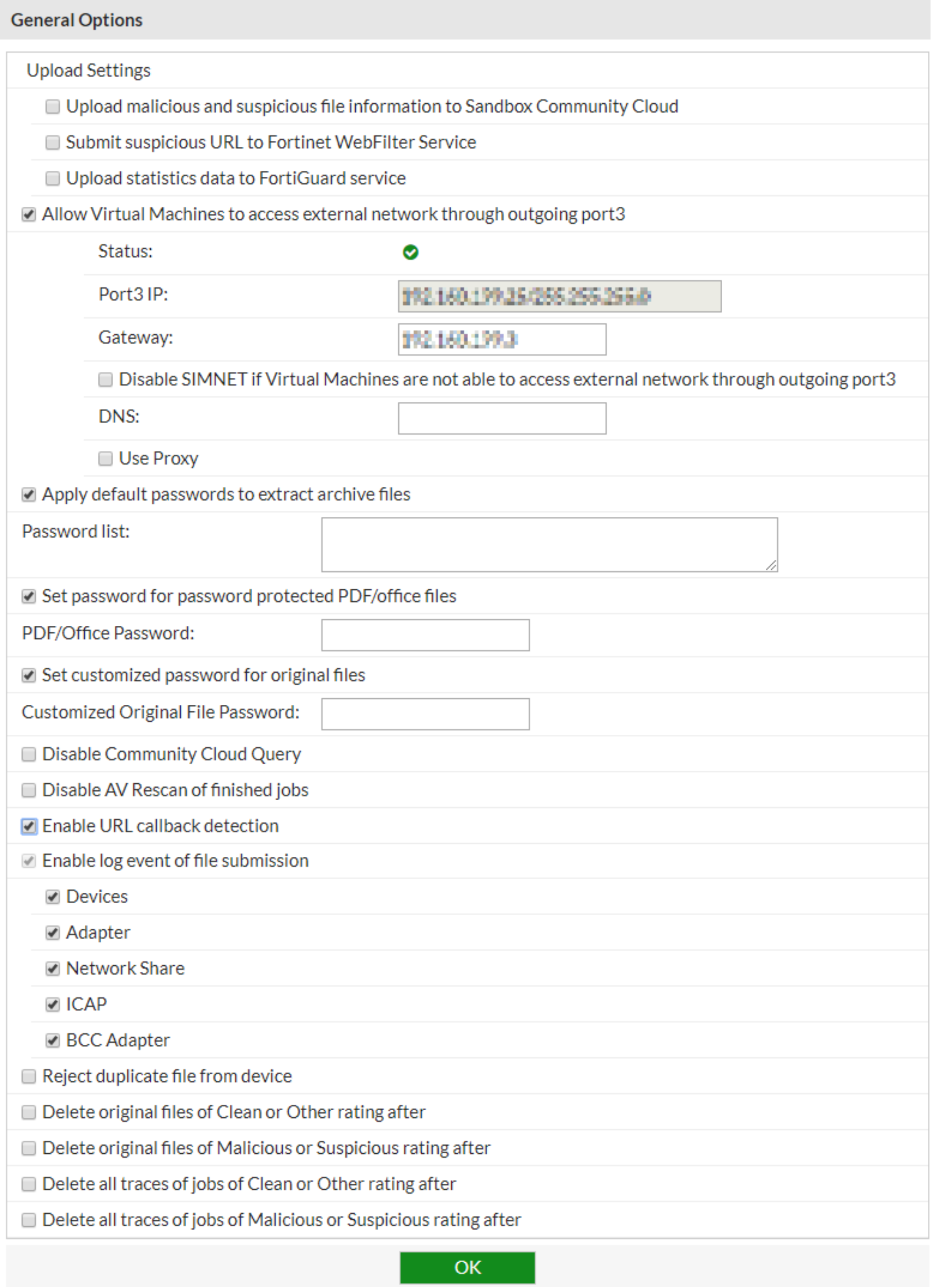


Job Queue Priority

#	Input Source	File Type
1	OD On-Demand	EXE Executables/DLL/VBS/BAT/PS1/JAR/MSI/WSF files
2	OD On-Demand	USER User defined extensions
3	OD On-Demand	PDF PDF files
4	OD On-Demand	DOC Microsoft Office files (Word, Excel, PowerPoint files etc)
5	OD On-Demand	SWF Adobe Flash files
6	OD On-Demand	WEB Static Web files
7	OD On-Demand	ANDROID Android files
8	OD On-Demand	MAC Mac files
9	OD URL On-Demand	URL URL detection
10	RPC File RPC	EXE 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: [redacted]
- Gateway: [redacted]
- □ 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:

☑ Set password for password protected PDF/office files

PDF/Office Password:

☑ Set customized password for original files

Customized Original File Password:

□ Disable Community Cloud Query

□ Disable AV Rescan of finished jobs

☑ Enable URL callback detection

☑ Enable log event of file submission

- ☑ Devices
- ☑ Adapter
- ☑ Network Share
- ☑ ICAP
- ☑ BCC Adapter

□ 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

□ Delete all traces of jobs of Malicious or Suspicious rating after

The following options are available:

Upload malicious and suspicious file information to Sandbox community Cloud	Enable to upload malicious and suspicious file information to the Sandbox community Cloud. If enabled, the original file, file checksum, tracer log, verdict, submitting device serial number, and downloading URL are uploaded.
Submit suspicious URL to Fortinet WebFilter Service	Enable to submit malware downloading URL to the FortiGuard Web Filter Service.
Upload statistics data to FortiGuard service	Enable to upload statistics to FortiGuard. If enabled, the following are uploaded: submitting device serial number and firmware, job-related results and statistics.
Allow Virtual Machines to access external network through outgoing port3	Enable to allow Virtual Machines to access external network through the outgoing port3. For further details, refer to the *port3 (VM outgoing interface)* topic in Interfaces on page 50.
Status	Port3 status to access the Internet.
Gateway	Enter the next hop gateway IP address.
Disable SIMNET if Virtual Machines are not able to access external network through outgoing port3	Enable to disable SIMNET when Virtual Machines are not able to access external network through the outgoing port3.
DNS	DNS server used by VM images when a file is scanned.
Use Proxy	Enable to use the proxy. Configure the Proxy Type, Server Name/IP, Port, Proxy Username, and Proxy Password. When the proxy server is enabled, all the non UDP outgoing traffic started from Sandbox VM will be directed to the proxy server. 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. For other traffic started by FortiSandbox firmware, such as FortiGuard Distribution Network (FDN) upgrades, the configurations should be done under the *Network* menu.
Proxy Type	Select the proxy type from the dropdown list. The following options are available: • HTTP Connect • HTTP Relay • SOCKS v4 • SOCKS v5; requires DNS UDP protocol is not supported.
Server Name/IP	Enter the proxy server name or IP address.
Port	Enter the proxy server port number.
Proxy Username	Enter a proxy username.

Proxy Password	Enter the proxy password.
Apply default passwords to extract archive files	User can define a list of passwords that can be tried to extract archive files. Input passwords line by line.
Set password for password protected PDF and office files	User can define one password for PDF and Office files.
Set customized password for original files	User can define their own password for the original sample when downloaded from FortiSandbox.
Disable Community Cloud Query	By default the Cloud Query is enabled. Disable the Cloud Query in the following scenarios: • You have an enclosed environment. Disabling the Cloud Query will improve the scan speed. • You receive an incorrect verdict from the Cloud Query and before Fortinet fixes it, you can turn it off temporarily.
Disable AV Rescan of finished Jobs	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.
Enable URL call back detection	Enable URL call back detection. When enabled, previously detected clean URLs in sniffered traffic are frequently queried against Web Filtering service.
Enable log event of file submission	Enable to log the file submission events of an input source.
Devices	Select to log the file submission events of a device, like FortiGate, FortiMail, or FortiClient.
Adapter	Select to log the file submission events from an adapter like a Carbon Black server.
Network Share	Select to log the file submission events when they are from a network share.
ICAP	Select to log the file submission events from an ICAP client.
BCC Adapter	Select to log the file submission events from a BCC client.
Reject duplicate file from device	Enable to reject duplicate files from devices.
Delete original files of Clean or Other rating after	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.
Day	Enter the day.
Hour	Enter the hour.
Minute	Enter the minute.
Delete original files of Malicious or Suspicious rating after	Enable to delete original files of Malicious or Suspicious ratings after a specified time.
Day	Enter the day.

Hour	Enter the hour.
Minute	Enter the minute.
Delete all traces of jobs of Clean or Other rating after	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.
Day	Enter the day.
Hour	Enter the hour.
Minute	Enter the minute.
Delete all traces of jobs of Malicious or Suspicious rating after	Enable to delete all traces of jobs of Malicious or Suspicious ratings after a specified time.
Day	Enter the day.
Hour	Enter the hour.
Minute	Enter the minute.

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

Allowlist and blocklist (whitelist and blacklist)

Allowlist and blocklist 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/URL/URL REGEXs. Domain/URL/URL REGEX 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_URL, 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 allowlist and blocklist manually:

1. Go to *Scan Policy > White / Black List*.
2. Click the menu icon beside *White Lists* or *Black Lists* to see its menu items.

3. Click the + button to add a new entry.

> The URL pattern has 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/1abc/bad.html` will be rated as `Malicious`.

4. Click *OK*.

To manage the allowlist and blocklist through files:

1. Go to *Scan Policy* > *White / Black List*.
2. Beside *White Lists* or *Black Lists*, click the menu icon and select the *Manage lists by uploading files* icon.
3. Select the list type from the dropdown menu:
   - *MD5*
   - *SHA1*
   - *SHA256*
   - *Domain*
   - *URL*
   - *URL REGEX*
4. Select the *Action* 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.

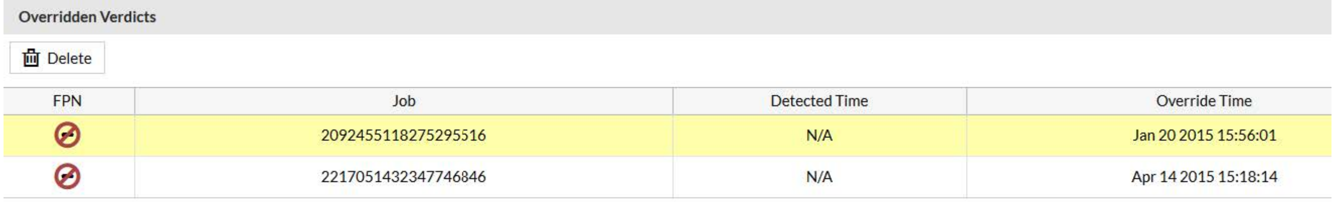
> In a cluster setting, create allowlist and blocklist on the primary node. Lists are synchronized with other nodes.

> The total number of URL REGEXs in allowlist and blocklist must be less than 1000.
> The total number of domains plus URLs in allowlist and blocklist must be less than 50000.
> The total number of MD5+SHA1+SHA256 in allowlist and blocklist must 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

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:

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

The following information is displayed:

Name	The name of the YARA rule set.
File Type	The file types the YARA rule is applied to.
Modify Time	The date and time the YARA rule set was last modified.
Size	The size of the YARA rule file.
Sha256	The Sha256 checksum of the YARA rule file.
Status	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:

YARA Rule Name	Enter a name for the YARA rule set.
Default Description	Enter a description of the YARA rule set.
Rules Risk Level	Select a rule risk level between 1-10.

	• *0-1*: Clean • *2-4*: Low Risk • *5-7*: Medium Risk • *8-10*: High Risk All the YARA rules inside the YARA rule file will share the same risk level.
File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
YARA Rule File	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:

ID	YARA ID number. You cannot edit this field.
Yara Rule Name	Enter a name for the YARA rule set.
Default Description	Enter a description of the YARA rule set.
Rules Risk Level	Select a rule risk level between 1-10. • *0-1*: Clean • *2-4*: Low Risk • *5-7*: Medium Risk • *8-10*: High Risk All the YARA rules inside the YARA rule file will share the same risk level.
File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
YARA Rule File	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.

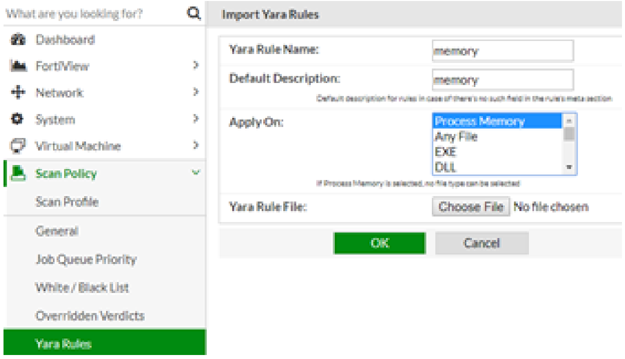
To change the status of a YARA rule set:

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.

To import a process memory YARA Rule:

A process memory YARA Rule differs slightly from other YARA rules. It is used by the VM Engine and is only applied in the VM Engine scan stage, whereas a regular YARA rule is applied in the Static Scan stage.

1. Go to *Scan Policy* > *YARA Rules*.
2. Click the *Import* button.
3. Input a YARA rule name in the *Yara Rule Name* field.
4. Add a description for the YARA Rule if there is no corresponding field contained in the rule's *meta* section.
5. In the *Apply On:* field, click *Process Memory*. The *Rules Risk Level* field will be hidden upon click because it is not required for *Process Memory*.



Import Yara Rules

Yara Rule Name: memory

Default Description: memory

Default description for rules in case of there's no such field in the rule's meta section

Apply On: Process Memory (selected), Any File, EXE, DLL

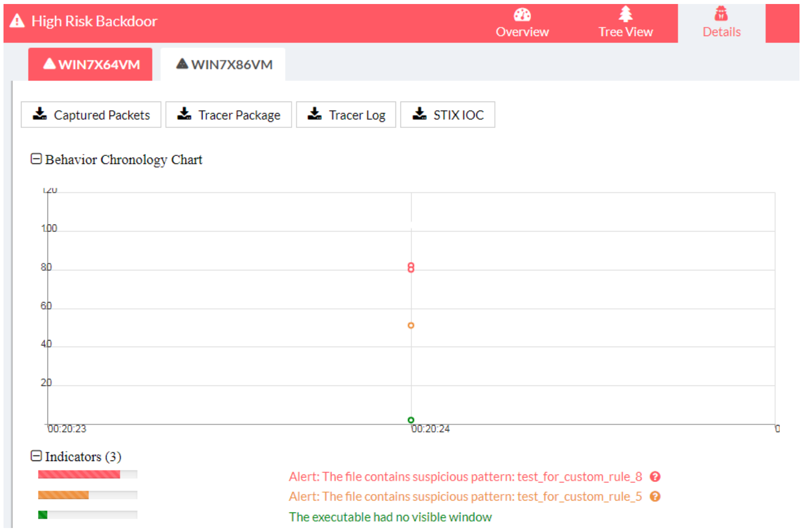
If Process Memory is selected, no file type can be selected

Yara Rule File: Choose File No file chosen

6. Click *Choose File* and select the YARA Rule file.
7. Click “OK” to upload the file.

To verify when a sample is detected by a process memory YARA rule:

If a sample is detected by a process memory YARA rule, FortiSandbox will show the following information in the FortiView job details:



Alert: The file contains suspicious pattern: test_for_custom_rule_8

Alert: The file contains suspicious pattern: test_for_custom_rule_5

The executable had no visible window

- The Indicators section shows that the sample contains a suspicious pattern with the YARA rule name.
- The YARA rule and rating are displayed as Behaviors.

If a sample is detected by multiple process memory YARA rules,FortiSandbox shows all hits and takes the highest scoring YARA rule as the final scan score if no other suspicious behavior is detected.

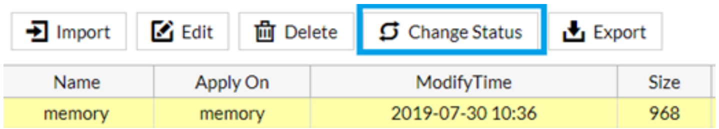
Format guidelines for process memory YARA Rules:

- A rule file must be in plain text format
- A rule file can contain many rules
- A rule name must be unique
- A rule should be in the following format:

```
rule Andromeda29_Memory_Pattern
{
meta:
description = "Andromeda29"
impact = 8
condition:
...
}
description: description of the rule, it will show in the indicator if matched
impact: the impact level of the pattern, range: 0-10, 0-1:clean,2-4: Low Risk,5-7: Medium
     Risk,8-10:High Risk
```

To activate the process memory YARA Rule

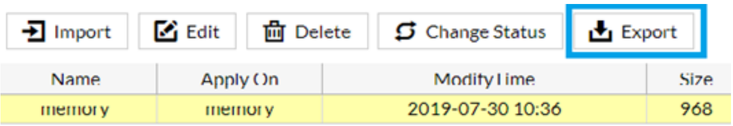
1. Select the YARA Rule in *Scan Policy* > *Yara Rules*, then click *Change Status* to activate the YARA rule. Clicking the *Change Status* button again will toggle the *Status* between Active and Inactive.



Name	Apply On	ModifyTime	Size
memory	memory	2019-07-30 10:36	968

To export a YARA rule:

1. From *Scan Policy* > *Yara Rules*, click *Export* to export this YARA rule in plain text format.

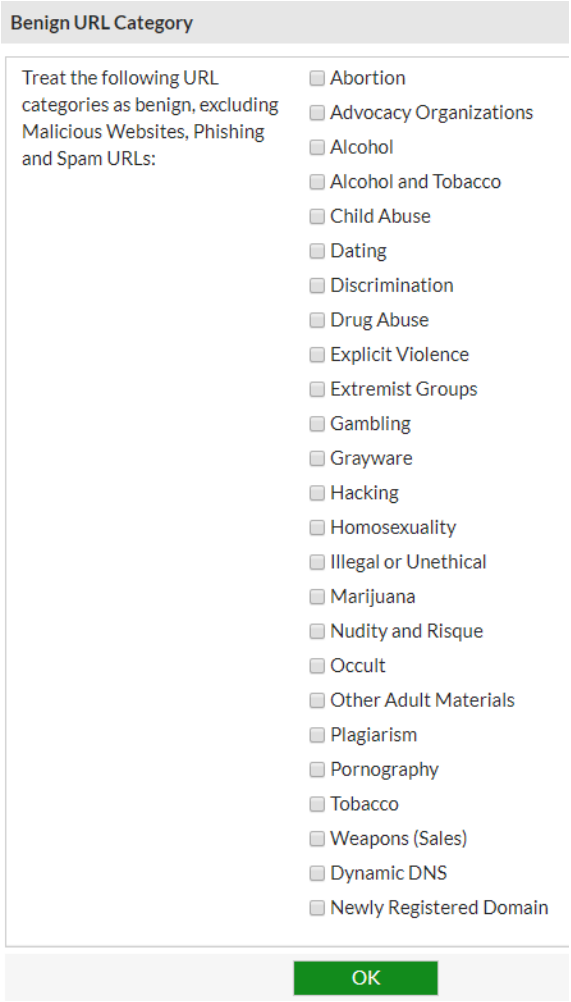


Name	Apply On	Modify Time	Size
memory	memory	2019-07-30 10:36	968

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)
- Dynamic DNS
- Newly Registered Domain



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)
- □ Dynamic DNS
- □ Newly Registered Domain

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.

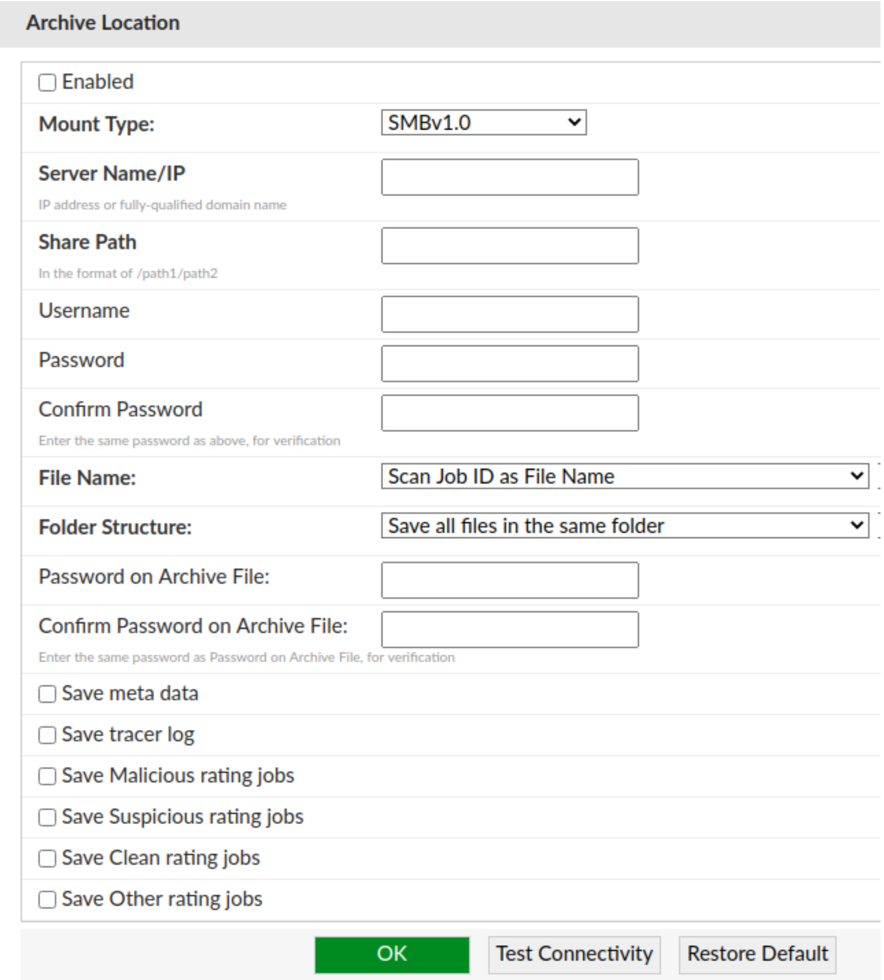
The following options can be configured:

VM Timeout	Windows VM cannot be launched properly. This usually occurs on FSA-VM model running on hardware with limited resources. Select one of the following ratings: • Unknown • Clean • Malicious • Low Risk • Medium Risk • High Risk
Tracer Engine Timeout	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. Select one of the following ratings: • Unknown • Clean • Malicious • Low Risk • 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

□ Enabled

Mount Type: SMBv1.0

Server Name/IP
IP address or fully-qualified domain name

Share Path
In the format of /path1/path2

Username

Password

Confirm Password
Enter the same password as above, for verification

File Name: Scan Job ID as File Name

Folder Structure: Save all files in the same folder

Password on Archive File:

Confirm Password on Archive File:
Enter the same password as Password on Archive File, for verification

□ Save meta data

□ Save tracer log

□ Save Malicious rating jobs

□ Save Suspicious rating jobs

□ Save Clean rating jobs

□ Save Other rating jobs

The following options can be configured:

Enabled	Select to enable the job archive feature.
Mount Type	Select the mount type of the network share folder: • SMB v1.0 • SMB v2.0 • SMB v2.1 • SMB v3.0 • NFSv2 • NFSv3 • NFSv4

	• Azure File Share • AWS S3 • AWS S3 BJ • AWS S3 NX
Server Name/IP	Enter the server fully qualified domain name (FQDN) or IP address.
Share Path	Enter the file share path in the format of `/path1/path2`.
Username	Enter a user name. The username should have the write privilege of the remote network share folder.
Password	Enter the password.
Confirm Password	Enter the password a second time for verification.
File Name	Select the file name from the dropdown list. The following options are available: • Scan Job ID as File Name • Original File Name
Folder Structure	Select the folder structure from the dropdown list. The following options are available: • Save all files in the same folder • Save file in folders of the scan finish time • Save file in folders of ratings
Password on Archive File	Enter the password for saved jobs.
Confirm Password on Archive File	Enter the password a second time for verification.
Save meta data	When selected, the job summary information will be saved.
Save tracer log	When selected, the job's tracer log will be saved.
Save Malicious rating jobs	When selected, files of Malicious rating will be saved.
Save Suspicious rating jobs	When selected, files of Suspicious rating will be saved.
Save Clean rating jobs	When selected, files of Clean rating will be saved.
Save Other rating jobs	When selected, files of Other rating will be saved.

Global Network

FortiSandbox can generate antivirus database packages (malware packages) and add URL packages from scan results into the blocklist, and distribute them to FortiGate devices and FortiClient endpoints for antispyware/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.

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 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 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:

Alias	Enter the network Alias name.
Authentication Code	Enter the authentication code for Contributor to join the network.
Contributors	List the units who are in the network.
Local Malware Package Options	These options define how each unit generates local packages after it has threat information. For more information, see Local Packages on page 115.
Local URL Package Options	
Enable Local STIX IOC Package	

   b. *Work as threat information contributor. Scan profile is managed by manager.*
      If the unit works as a *Contributor*, configure the following:

Collector IP Address	Enter the Collector's IP address.
Alias	Enter the global network Alias name.
Authentication Code	Enter the authentication code to join the network.
Local Malware Package Options	These options define how each unit generates local packages after it has threat information. For more information, see Local Packages on page 115.
Local URL Package Options	

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 you configure a scan profile on the Collector, the configurations will be downloaded by each Contributor. 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 a standalone unit or primary node in a cluster can join the network.

4. 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 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.
Medium Risk	Include malware with medium risk ratings and URLs sent by FortiMail devices of medium risk ratings and whose scan depth is 0.
Local URL Package Option	
Include past __ day(s) of data. (1-365 days)	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.
Include the job data of the following ratings	
Malicious	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.
High Risk	Include downloaded URLs of malware with high risk ratings.
Medium Risk	Include downloaded URLs of malware with medium risk ratings.
Enable STIX IOC	Enable to generate STIX IOC packages.
STIX Malware Package Options	
Include past __ day(s) of data. (1-365 days)	Enter the number of days.
Include the job data of the following ratings	
Malicious	Include malware with malicious ratings.
High Risk	Include malware with high risk ratings.
Medium Risk	Include malware with medium risk ratings.
Generate STIX file with behaviour	Include behavior information of each malware or suspicious URL.
Download STIX	Download most recently generated Malware STIX IOC package.
STIX URL Package Options	
Include past __ day(s) of data. (1-365 days)	Enter the number of days.
Include the job data of the following ratings	
Malicious	Include malware with malicious ratings.
High Risk	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.
Medium Risk	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.
Download STIX	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
                    e433e0229c2accec5d</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

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 endpoints 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 for details and apply search filters. You can select to create a PDF or CSV format report for on-demand files.

Use *File On-Demand* to upload different file types directly to FortiSandbox. You can then view the results and decide whether 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 when run on the Microsoft Windows host. You can force the file to do Sandboxing scan even if was detected in former steps of Static Scan, AV Scan, Cloud Query, or stopped from entering VM by Sandboxing-prefilter setting. All rescanned jobs are listed on the *File On-Demand* page.

You can select VM types to do the sandboxing by overwriting what is defined in the Scan Profile. When you select MACOSX or WindowsCloud, the file is 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 in the *Scan Policy* > *General* page is also used to extract the archive files.

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

File On-Demand page - level 1

The following options are available:

Submit File	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.
Show Rescan Job	Jobs generated from manual rescan can be shown/hidden by this option.
Search	Show or hide the search filter field.
Add Search Filter	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.
Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.
Clear all removable filters	Click the *trash can* icon to clear all removable filters.
Export Data	Click the *Export Data* 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 *Log & Report* > *Report Center*.

View Jobs	Click the icon to view the scan jobs associated with the entry. 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.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

Submission Time	The date and time that the file was submitted to FortiSandbox. Use the column filter to sort the entries in ascending or descending order.
Submitted Filename	The file name.
Submitted By	The name of the administrator that submitted the file. Use the column filter to sort the entries in ascending or descending order.
Rating	Hover over the icon 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 are displayed. 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.
Status	The scan status can be *Queued*, *In-Process*, or *Done*.
File Count	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 *In-Progress*. When the scan is done, it will display the total number of files in this submission.
Comments	The comments user enters when submitting the file.
Rescan Job	This icon indicates that this file is a rescanned version of another file.
Archive Submission	This icon indicates that an archived file has been submitted for scanning.
Total Jobs	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:

Back	Click the *Back* button to return to the On-Demand page.

Search	Show or hide the search filter field.
Refresh	Click the *Refresh* icon to refresh the entries displayed after applying search filters.
Add Search Filter	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. When the search filter is Filename, select the *Equal* icon to toggle between exact search and pattern search.
View Details	Click the *View Details* icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
Scan Video	When the scan is submitted, if *Record scan process in video* 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 *System* > *Job View Settings* > *File Detection Columns* page. For more information, see Job View Settings on page 78.
Pagination	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. For information on the *View Details* page, see Appendix A - View Details page reference on page 202.
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 PDF or CSV.
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 1000; the maximum number of events you can export to a CSV report is 15000. 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:

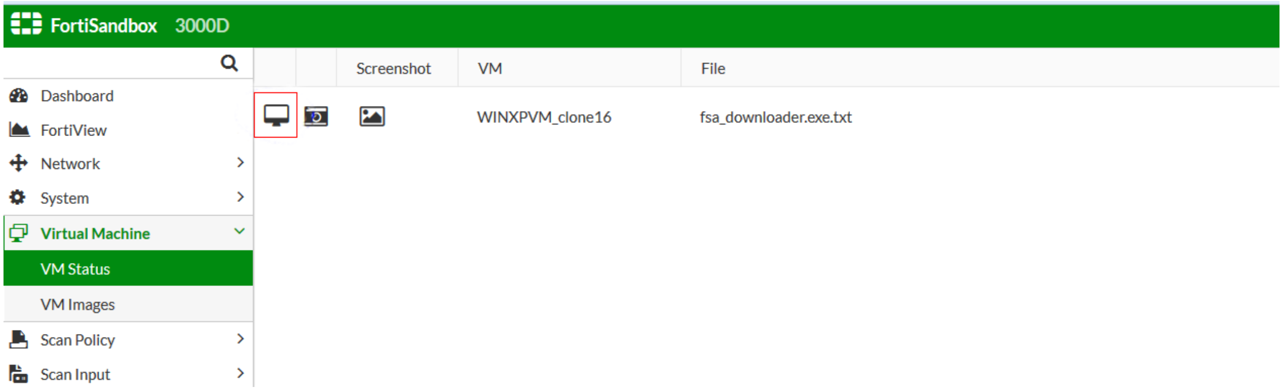
Select a File	Click the *Browse* button and locate the sample file or archived sample file on your management computer.
Possible password(s) for archive/office file	List all possible passwords to extract password protected archive file, or open password protected Microsoft Office file. One password per line. Default password list set in the Scan Policy > General page will also be used to extract the archive files.
Comments	Optional comments for future reference.
Force to scan the file inside VM	Enable to select advanced options.
Follow VM Association Settings in Scan Profile	If the sandboxing step is not skipped, the file will be sent to its associated VMs defined in Scan Profile.
Force to Scan Inside the Following VMs	Overwrite VM association settings in Scan Profile by selecting one or more of the enabled VMs.
Allow Interaction	Select the *Allow Interaction* checkbox to interact with the Windows VM. For more information, see To use the Allow Interaction Feature: on page 123.
Record scan process in video if VMs involve	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.
Add sample to threat package	If result matches malware package requirement, add scan result to threat package.
Enable AI	Use AI engine to scan the file.

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.

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:

Submit File/URL	Click the button to submit a file containing a list of scanned URLs, or submit an individual URL.

Show Rescan Job	Jobs generated from a customized rescan of a URL can be shown/hidden by this option.
Refresh	Click the *Refresh* icon to refresh the entries displayed after applying search filters.
Search	Show or hide the search filter field.
Add Search Filter	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.
Clear all removable filters	Click the *Trash can* icon to clear all removable filters.
Export Data	Click the *Export Data* 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 *Log & Report > Report Center*.
View Jobs	Click the icon to view the scan job(s) associated with the entry. Click the *Back* button to return to the on-demand page.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

Submission Time	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.
Submitted Filename	The submitted URL file name. If the scan is about an individual URL, the name is `scan_of_URL.`
Submitted By	The name of the administrator that submitted the file scan.
Rating	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.
Status	The scan status can be *Queued*, *In-Process*, or *Done*.
URL Count	The number of URLs associated with the submission when the scan is done. When the scan is *In-Progress*, it shows (finished scan)/(total URLs of this submission).
Comments	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:

Back	Click the *Back* button to return to the on-demand page.
Search	Show or hide the search filter field.
Refresh	Click the *Refresh* icon to refresh the entries displayed after applying search filters.
Add Search Filter	Click the search filter field to add search filters. 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.
View Details	Select the *View Details* icon to view file information.
Scan Video	When the scan is submitted, if *Record scan process in video* 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.
Pagination	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, see Job View Settings on page 78.
3. Click the *View Details* icon to view file details. The *View Details* page will open a new tab. For information on the *View Details* page, see Appendix A - View Details page reference on page 202.
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:

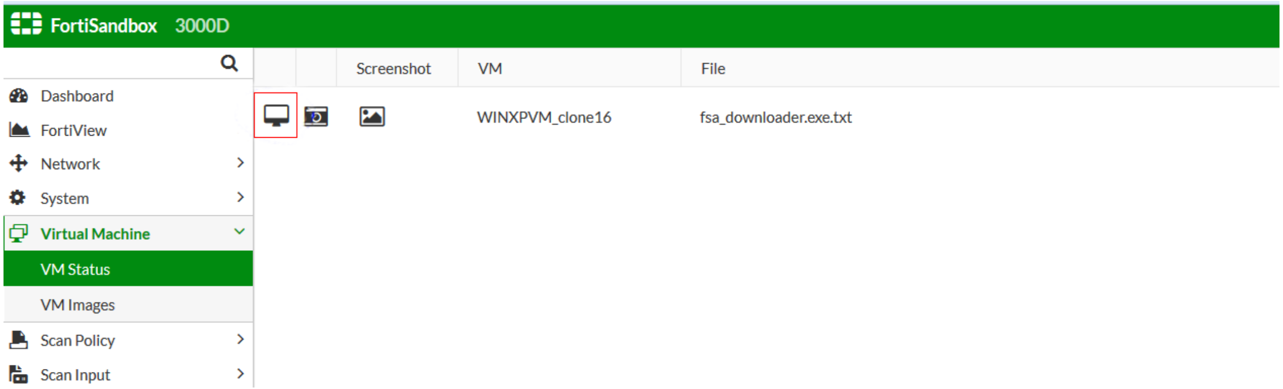
Depth	Enter the *Recursive Depth* in which URLs are examined. The original URL is considered level `0`. A depth of `1` will open all links on the original URL page and crawl into them. The default value is define in the *Scan Policy > Scan Profile* page.
Timeout	Enter the *Timeout Value*. The Timeout 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 *Scan Policy > Scan Profile* page.
Direct URL	To scan only a single URL, check the *Direct URL* checkbox. Enter the URL in the *Enter a URL* field.
Select a File	Click the *Browse* button and locate the plain-text file on your management computer. The maximum number of URLs in this file is determined by *Maximum URL Value* in *Scan Policy > Scan Profile* page.
Comments	You can choose to enter optional comments for future reference.

Debug Options	To display the advanced options, check the *Debug Options* toggle. Users can choose to follow scan profile settings or specify the VMs.
Follow VM Association settings in Scan Profile	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`. **Note**: To use WindowsCloud VM, you need to purchase the subscription service. URL will be sent to Fortinet Sandboxing cloud to scan.
Force to Scan the URL Inside VM	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.
Allow Interaction	Select the *Allow Interaction* checkbox to interact with the Windows VM. For more information, see To use the Allow Interaction Feature: on page 127.
Record scan process in video	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.
Add URL sample to threat package	Select to add the sample to malware package, if the result meets settings in Package Options
Enable AI	Use AI engine to scan the file.

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.



		Screenshot	VM	File
🖥	📷	🖼	WINXPVM_clone16	fsa_downloader.exe.txt

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.

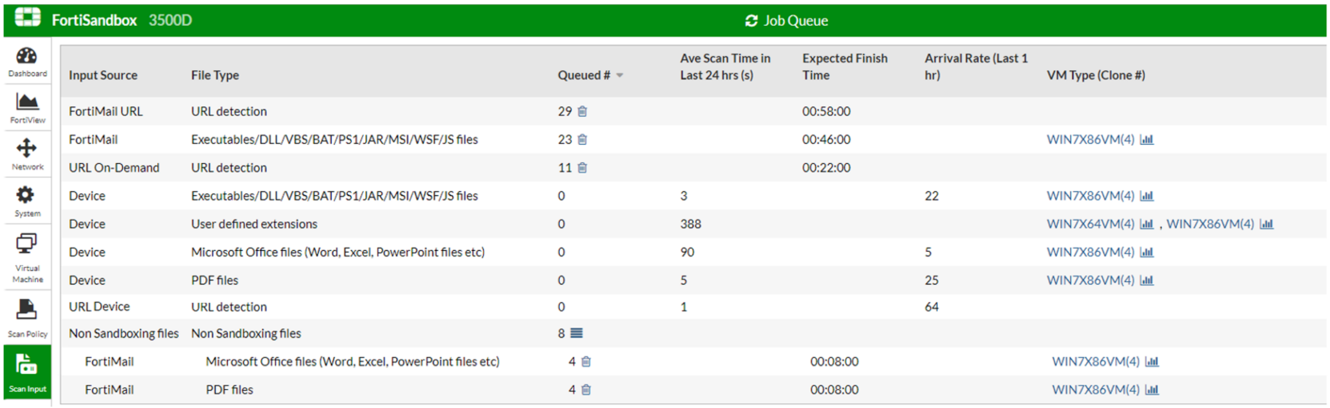
VM Interaction and Scan video recording features are only available to users whose admin profile has *Allow On-Demand Scan Interaction* enabled.

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.



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:

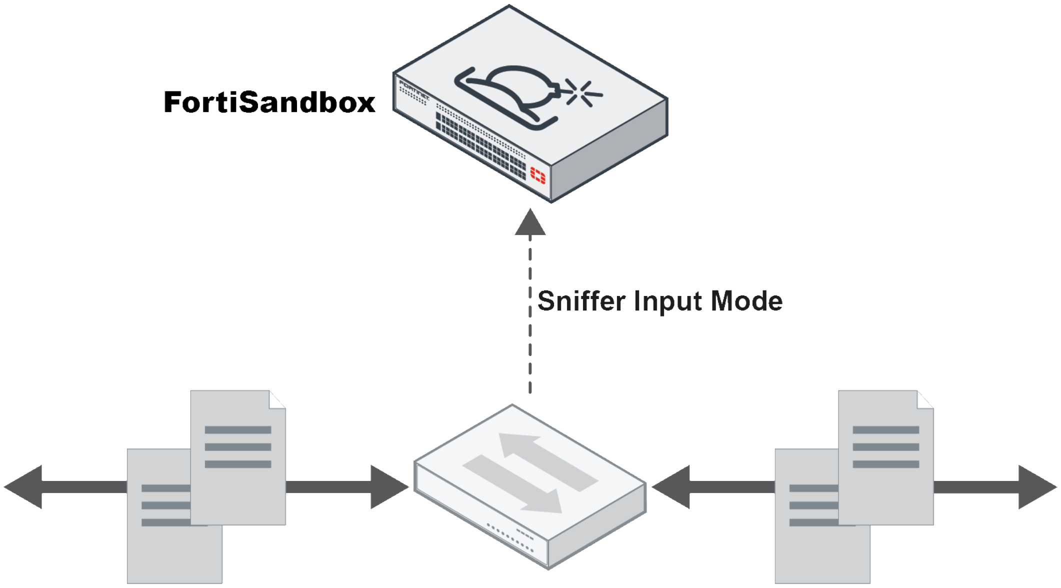
Chart icon	Click the *Chart* icon beside the VM Type to display the *VM's Usage Chart*.
Trash icon	Click the *Trash* icon beside the Pending Job Number purges the job queue.
Prioritize	Click the *Prioritize* button takes you to the *Job Queue Priority List* page where you can adjust the list.

The following information is displayed:

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

	• On-Demand • File RPC • Device • Sniffer • Adapter • Network Share • URL On-Demand • URL RPC • URL Device • URL Adapter
File Type	File types can be one of the following values: • Executables /DLL/VBS/BAT/PS1/JAR/MSI/WSF files • Microsoft Office files (Word, Excel, Powerpoint etc) • Adobe Flash files • Archive files (extensions: .7z, xz, .bz2, .gz, .tar, .zip, .Z, .kgb, .ace, etc.) • PDF files • Static Web files • Android files • MACOSX files • URL detection • User defined extensions • Job Queue Assignment Pending files (files received from input sources and not yet processed) • 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.)
Queued #	Current pending job number. A *Trash Can* appears beside the pending job number. Clicking on the *Trash Can* icon purges the job queue. Select the icon next to the *Non Sandboxing files* Input Source to expand the selection to view and purge non-sandboxing files separately.
Ave Scan Time in Last 24 hrs (s)	Average scan time of one file in the last 24 hours, in seconds.
Expected Finish Time	The expected time when the pending jobs will finish.
Arrival Rate (Last 1 hr)	Files put in the Job Queue in the last hour.
VM Type (Clone #)	The VM type with its clone number. A *Chart* icon appears beside the VM Type (Clone#). If you click on the *Chart* 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.

Sniffer

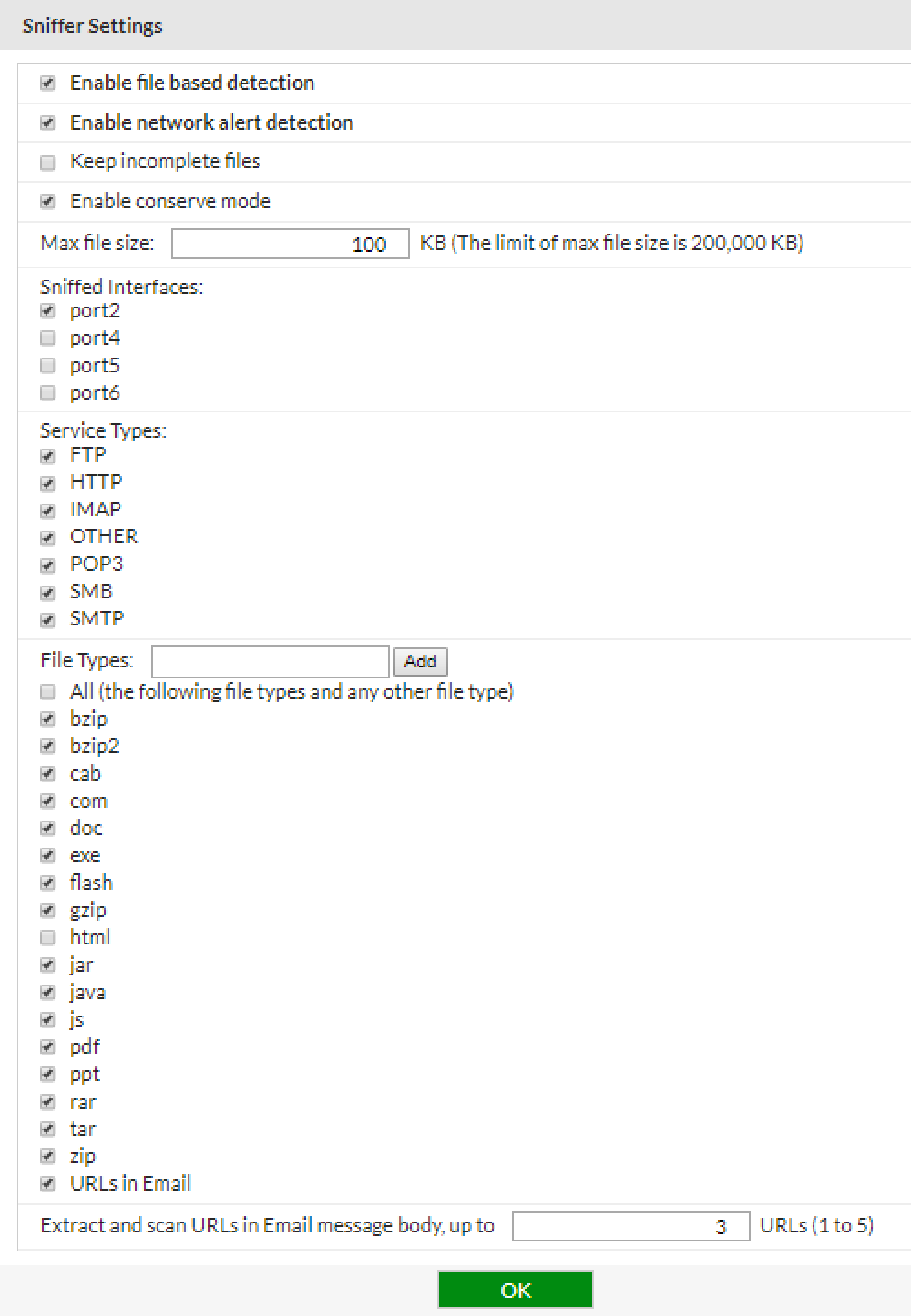


Sniffer mode relies on inputs from spanned switch ports. It is the most suitable infrastructure for adding protection capabilities to existing threat protection systems from various vendors.

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

You can 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.

FortiSandbox reserves port1 for device management and port3 for scanned files to access the Internet. You cannot use these ports as a sniffed interface: port1, the admin port, and the port used for cluster internal communication.



Sniffer Settings

☑ Enable file based detection

☑ Enable network alert detection

☐ Keep incomplete files

☑ Enable conserve mode

Max file size: 100 KB (The limit of max file size is 200,000 KB)

Sniffed Interfaces:
☑ port2
☐ port4
☐ port5
☐ port6

Service Types:
☑ FTP
☑ HTTP
☑ IMAP
☑ OTHER
☑ POP3
☑ SMB
☑ SMTP

File Types:
☐ All (the following file types and any other file type)
☑ bzip
☑ bzip2
☑ cab
☑ com
☑ doc
☑ exe
☑ flash
☑ gzip
☐ html
☑ jar
☑ java
☑ js
☑ pdf
☑ ppt
☑ rar
☑ tar
☑ zip
☑ URLs in Email

Extract and scan URLs in Email message body, up to 3 URLs (1 to 5)

Configure the following settings:

Enable file based detection	Select the checkbox to enable file based detection.
Enable network alert detection	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 *Network Alerts* page.

	For URL visits, certain categories can be treated as benign in *Scan Policy > URL Category*.
Keep incomplete files	Keep files without completed TCP sessions. Select the checkbox to keep incomplete files. Sometimes incomplete files can be useful to detect known viruses.
Enable Conserve mode	When conserve mode is enabled, the sniffer might enter conserve mode if it is too busy, such as when there are too many jobs in the pending queue (250K), sniffed traffic exceeds optimal throughput, or HDD/RAM disk usage is too high. In conserve mode, the sniffer only extracts executable (.exe) and MS Office files. Optimal traffic throughput: • FSA-1000D: 1Gbps • FSA-2000E: 4 Gbps • FSA-3000D: 4.6 Gbps • FSA-3000E: 8 Gbps • FSA-3500D: 2 Gbps • FSA-VM00: 1Gbps • FSA-VM-BASE: 4.6Gbps
Max file size	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 200000kB. Files that exceed the maximum file size are not sent to FortiSandbox.
Sniffed Interfaces	Select the interface to monitor.
Service Types	Select the traffic protocol that the sniffer will work on. Options include: *FTP*, *HTTP*, *IMAP*, *POP3*, *SMB*, *OTHER* and *SMTP*. The *OTHER* service type is for raw TCP protocol traffic.
File Types	Select the file types to extract from traffic. When *All* is checked. all files in the traffic will be extracted. Users can also add extra file extensions by putting it in *File Types* field and clicking *Add* > *OK*. The user can delete it later by clicking the *Trash* can icon beside it and clicking *OK*. When *URLs in Email* type is selected, URLs embedded inside Email body will be extracted and scanned as WEBLink type. User can define the number of URLs to extract for each Email, from 1 to 5.

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, or FortiMail devices to send files to FortiSandbox. For FortiGate, you can send all files for inspection. For FortiMail, you can send email attachments or URLs in the email body to FortiSandbox for inspection, or just send the suspicious ones. When FortiSandbox receives the files or URLs, they are executed and scanned within the VM modules. FortiSandbox sends statistics back to the FortiGate, FortiWeb, and FortiMail. When integrated with FortiGate, supported protocols include: HTTP, FTP, POP3, IMAP, SMTP, MAPI, IM, and their equivalent SSL encrypted versions.

A FortiSandbox system, either a standalone unit or in a cluster, has no limit on the number of authorized devices and FortiClients. However, the concurrent connections of all client devices is limited to 30000.

Use the *Scan Input* > *Device* page to view, edit, and authorize devices.

Devices such as FortiGate can query a file's verdict and retrieve detailed information from FortiSandbox. FortiGate can also download malware 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 size depends on the FortiGate memory size. To change the file size on the FortiGate side, use the following CLI commands:

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

The `profile-protocol-options` setting controls the maximum file size that is AV scanned on the FortiGate. After a virus scan verdict has been made (clean or suspicious), if the file size is less than the `analytics-max-upload` size, it is sent to FortiSandbox using the *Send All/Suspicious Only* setting on the FortiGate.

For information on configuring the oversize limit for `profile-protocol-options` and `analytics-max-upload`, see the FortiOS CLI Reference in the Fortinet Document Library.

In *Scan Input* > *Device*, the following options are available:

Refresh	Refresh display after applying search filters.
Device Filter	Filter devices by entering part of device name or serial number.
Clear all removable filters	Click the trash can icon to remove all filters.

This page displays the following:

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

Others	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.
Mal Pkg	Malware package version currently on the device.
URL Pkg	URL package versions currently on the device.
Auth	Shows if the device or VDOM/Protected Domain is authorized to submit files. Only authorized device or VDOM/Protected Domain can submit files to FortiSandbox.
Limit	Shows if this device has a submission limit.
Status	Status of the device. An icon shows that the device is up or connected, down, or disconnected. If a device, its VDOM, or protected domain does not contact FortiSandbox for more than 15 minutes, the status changes to disconnected.
Delete	Click to delete the device, VDOM, or protect domain. When you delete a device, all its VDOMs and protected domains are also deleted. If the device is FortiClient EMS, its managed FortiClient endpoints are kept. If the device connects to FortiSandbox again, it appears as a new device.

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

Supported Devices

FortiSandbox supports the following devices:

FortiGate	FortiSandbox can perform additional analysis on files that have been AV scanned by FortiGate. You can configure FortiGate to send all files or only suspicious files passing through the AV scan. FortiGate can retrieve scan results and details from FortiSandbox, and also receive antivirus and web filtering signatures to supplement the current signature database. When FortiGate learns from FortiSandbox that a terminal is infected, the administrator can push instruction for self-quarantine on a registered FortiClient host.
FortiMail	You can configure FortiMail to send suspicious, high risk files and suspicious attachments to FortiSandbox. FortiSandbox can perform additional analysis on files that have been scanned by your FortiMail email gateway. Suspicious email attachments include: • Suspicious files detected by heuristic scan of the AV engine. • Executable files and executable files embedded in archive files. • Type 6 hashes (binary hashes) of spam email detected by FortiGuard AntiSpam service. FortiMail can send suspicious URLs in the email body to FortiSandbox for URL scans and then block suspicious emails based on the scan result.

FortiWeb	You can use a file upload restriction policy to submit uploaded files to FortiSandbox for evaluation. If FortiSandbox determines that the file is malicious, FortiWeb performs the following tasks: • Generate an attack log message that contains the result, for example, messages with the Alert action. • For 10 minutes after it receives the FortiSandbox results, take 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.
FortiClient EMS	You can configure a FortiSandbox IP address in an endpoint profile. FortiClient EMS attempts to submit an authorization request to 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 can also receive additional antivirus signatures from FortiSandbox, generated from scan results, to supplement current signatures.

FortiGate devices

You can add FortiSandbox as a Security Fabric device in FortiGate. For information on how to configure FortiGate to send files to FortiSandbox, see the FortiGate guides in the Fortinet Document Library.

On FortiSandbox, go to *Scan Input* > *Device* to see the FortiGate devices and VDOMs.

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 from FortiGate are marked with *vdom=root*.

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

If VDOMs are enabled on 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*.
   This page lists all devices and VDOMs.
2. Click the FortiGate device name to open the *Edit Device Settings* page.
3. Edit the following settings and then click *OK*.

Device Status	
Serial Number	Device serial number.

Hostname	FortiGate host name.
IP	IP address of the FortiGate.
Status	Status of the device.
Last Modified	Date and time the FortiGate settings were last changed.
Last Seen	Date and time the FortiGate last connected to FortiSandbox.
Permissions & Policy	
Authorized	Enable to authorize the FortiGate device. If disabled, files sent from FortiGate are dropped.
New VDOMs/Domains Inherit Authorization	Enable to have new VDOMs inherit the authorization setting configured at the device level.
Email Settings	
Administrator Email	Email address in *Notifier email* in FortiGate at *Security Fabric* > *Settings* > *Sandbox Inspection*.
Send Notifications	Enable to send notifications. When enabled, you receive email notifications when a file from your environment is detected as potential malware. The email contains a link to the scan job details page. To receive notification emails, configure a mail server in *System* > *Mail Server* and enable *Send a notification email to the Device/Domain/VDOM email list when Files/URLs with selected rating are detected*. Otherwise, a warning icon displays.
Send PDF Reports	Enable to send PDF reports of job details. To receive reports and define report generation frequency, configure a mail server in *System* > *Mail Server* and enable *Send scheduled PDF report to Device/Domain/VDOM email address*. Otherwise, a warning icon displays.

To edit VDOM settings:

1. On your FortiSandbox device, go to *Scan Input* > *Device*.
   This page lists all devices and VDOMs.
2. Click the VDOM name to open the *Edit Domain Settings* page.
3. Edit the following settings and then click *OK*.

Device Status	
Domain/VDOM	Device VDOM name.
Serial Number	Device serial number.
Hostname	VDOM name in the format of `Device-Name:VDOM-name`.
IP	IP address of the FortiGate.
Status	Status of the device.
Files Transmitted	Number of files and URLs transmitted to FortiSandbox in the last seven days.

Last Modified	Date and time the authorization status was changed.
Last Seen	Date and time the FortiGate VDOM last connected to FortiSandbox.
Permissions & Policy	
Authorized	Enable to authorize the FortiGate VDOM.
Submission Limitation	Limit the VDOM submission speed. Select *Unlimited* or specify the number of submissions per *Hour* or *Day*. When the limit is reached, FortiSandbox sends a signal to FortiGate to stop file submission to save resources on both devices.
Email Settings	
Email	Enter the administrator email addresses for the VDOM, separated by commas.
Send Notifications	Enable to send notifications when viruses or malware from this VDOM is detected. To receive notification emails, configure a mail server in *System > Mail Server* and enable *Send a notification email to the Device/Domain/VDOM email list when Files/URLs with selected rating are detected*. Otherwise, a warning icon displays.
Send PDF Reports	Enable to send PDF reports of job details. To receive reports and define report generation frequency, configure a mail server in *System > Mail Server* and enable *Send scheduled PDF report to Device/Domain/VDOM email address*. Otherwise, a warning icon displays.
Send Reach Limit Alert Email	Enable to send an alert email to the VDOM email address when *Submission Limitation* is reached.

FortiMail Devices

You can configure FortiMail to send suspicious files, URLs, and suspicious attachments to FortiSandbox for inspection and analysis. FortiSandbox statistics for total detected and total clean are displayed in FortiMail.

If FortiMail sends protected domain information, the domain names and jobs counts from them are listed. For each protected domain, you 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 are grouped in the Unprotected domain name.

For information on how to configure FortiMail to send files to FortiSandbox, see the *FortiMail Administration Guide* in the Fortinet Document Library.

To edit FortiMail Settings in FortiSandbox:

1. On your FortiSandbox device, go to *Scan Input > Device*.
This page lists all devices and protected domains. Since FortiMail does not explicitly send a list of possible protected domains to FortiSandbox, FortiSandbox only knows about a domain after it receives a file or URL. Domains on this page are displayed after the first file or URL is received on that domain.
2. Click the FortiMail device name to open the *Edit Device Settings* page.
3. Edit the following settings and then click *OK*.

Device Status	

Serial Number	Device serial number.
Hostname	FortiMail host name.
IP	IP address of the FortiMail.
Status	Status of the device.
Last Modified	Date and time the FortiMail settings were last changed.
Last Seen	Date and time the FortiMail last connected to FortiSandbox.
Permissions & Policy	
Authorized	Enable to authorize the FortiMail device. If disabled, files sent from FortiMail are dropped.
New VDOMs/Domains Inherit Authorization	Enable to have new protected domains inherit the authorization setting configured at the device level.
Email Settings	
Administrator Email	Email address in *Notifier email* in FortiMail.
Send Notifications	Enable to send notifications. When enabled, you receive email notifications when a file inside an email is detected as potential malware. The email contains a link to the scan job details page. To receive notification emails, configure a mail server in *System* > *Mail Server* and enable *Send a notification email to the Device/Domain/Vdom email list when Files/URLs with selected rating are detected*. Otherwise, a warning icon is displays.
Send PDF Reports	Enable to send PDF reports of job detail. To receive reports and define report generation frequency, configure a mail server in *System* > *Mail Server* and enable *Send scheduled PDF report about an individual VDOM/Domain to its email address*. Otherwise, a warning icon is displays.

To edit Domain settings:

1. On your FortiSandbox device, go to *Scan Input* > *Device*.
2. Click the domain name.
3. Edit the following settings and then click *OK*.

Device Status	
Domain/VDOM FQDN	Protected domain name.
Hostname	Domain/VDOM name in the format of `FortiMail Device Name: Domain name`.
IP	IP address of the FortiMail.
Status	Status of the device.
Files/URLs Transmitted	Number of files and URLs sent to the domain in the last seven days.
Last Modified	Date and time the authorization status was changed.

Last Seen	Date and time last file/URL was sent to this domain.
Permissions & Policy	
Authorized	Enable to authorize the FortiMail domain.
Submission Limitation	Limit the protected domain submission speed. Select *Unlimited* or specify the number of submissions per *Hour* or *Day*. When the limit is reached, FortiSandbox rejects files and URLs sent to this domain.
Email Settings	
Email	Enter the administrator email addresses for the domain, separated by commas.
Send Notifications	Enable to send notifications when viruses or malware to this domain is detected. To receive notification emails, configure a mail server in *System > Mail Server* and enable *Send a notification email to the Device/Domain/VDOM email list when Files/URLs with selected rating are detected*. Otherwise, a warning icon is displays.
Send PDF Reports	Enable to send PDF reports of jobs. To receive reports and define report generation frequency, configure a mail server in *System > Mail Server* and enable *Send scheduled PDF report about an individual VDOM/Domain to its email address*. Otherwise, a warning icon is displays.
Send Reach Limit Alert Email	Enable to send an alert email to the domain email address when *Submission Limitation* is reached.

Upload suspicious attachments to FortiSandbox

For information on how to configure FortiMail to send files to FortiSandbox, see the *FortiMail Administration Guide* in Fortinet Document Library.

Device and VDOM/Domain level notifications

If you enable *Send notifications* in the *Edit Device Settings* or *Edit VDOM/Domain Settings* page, you receive an email every time a file from your environment is detected as potential malware.

Device and VDOM/Domain level PDF reports

If you enable *Send PDF reports* in *Edit Device Settings* or *Edit VDOM/Domain Settings*, you receive a PDF report by email as defined in *System > Mail Server*. This FortiSandbox Summary Reports PDF lists statistics of scan jobs in the time period in *System > Mail Server* and includes the following information:

- Scanning Statistics: The number of files processed by FortiSandbox and a breakdown of files by rating.
- Scanning Statistics by Type: 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: The top targeted hosts.
- Top Malware Files: The top malware programs detected by FortiSandbox.
- Top Infectious URLs: The top infectious URLs detected by FortiSandbox.
- Top Callback Domains: The top callback domains detected by FortiSandbox.

FortiWeb Devices

For information on how to configure FortiWeb to send files to FortiSandbox, see the *FortiWeb Administration Guide* in the Fortinet Document Library.

FortiClient EMS Devices

For information on how to configure FortiClient EMS to send files to FortiSandbox, see the *FortiClient EMS Administration Guide* 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 to open the *Edit Device Settings* page.
3. Edit the following and then click *OK*.

Device Status	
Serial Number	Device serial number.
Hostname	EMS host name.
IP	IP address of the EMS.
Status	Status of the device.
Last Modified	Date and time the EMS settings were last changed.
Last Seen	Date and time the EMS last connected to FortiSandbox.
Permissions & Policy	
Authorized	Enable to authorize the EMS device. All FortiClient endpoints managed by EMS inherit this authorization setting.
Submission Limitation	Limit the submission speed of FortiClient endpoints managed by EMS. Select *Unlimited* or specify the number of submissions per *Hour* or *Day*. When the limit is reached, FortiSandbox sends a signal to FortiClient to stop file submission to save resources on both devices.

FortiClient

FortiClient 5.4 and earlier versions can silently connect to FortiSandbox without the need to be authorized. You can de-authorize a FortiClient host manually. If a FortiClient endpoint is managed by EMS, it follows the authorization status and file submission speed setting of EMS. You can manually change these settings.

For information on how to configure FortiClient to send files to FortiSandbox, see the *FortiClient Administration Guide* in the Fortinet Document Library.

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

The following options are available:

Refresh	Refresh display after applying search filters.
Device Filter	Filter devices by entering part of device name or serial number.
Clear all removable filters	Click the trash can icon to remove all filters.

This page displays the following:

FCT Serial	The FortiClient serial number.
Hostname	FortiClient host name.
User	Current user logged into the FortiClient host, if available.
IP	Host IP Address.
Malicious, High, Medium, Low	The number of malicious, high risk, medium risk, or low risk files submitted by 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.
Clean	Number of clean files submitted by the device to FortiSandbox in the last seven days.
Others	Number of other files submitted by the device to FortiSandbox in the last seven days.
Mal Pkg	Malware package version currently on the device.
Auth	If the FortiClient is authorized, you can click the FortiClient serial number and modify its authorization status.
Limit	Shows if this device has a submission limit.
Status	Status of the FortiClient host. An icon shows that the device is connected (up) or down.
Delete	Click to delete the FortiClient. If the device connects to FortiSandbox again, it appears as a new device.

To edit FortiClient settings in FortiSandbox:

1. On your FortiSandbox device, go to *Scan Input > FortiClient*.
2. Click the device name to open the *Edit FortiClient Settings* page.
3. Edit the following settings and then click *OK*.

FortiClient Status	
Serial Number	Device serial number.
Hostname	FortiClient host name.
IP	IP address of the FortiClient.
Status	Status of the device.
Files Transmitted	Number of files transmitted to FortiSandbox in the last seven days.

Last Seen	Date and time that FortiClient last connected to FortiSandbox.
Permissions & Policy	
Authorized	Enable to authorize the device.
Submission Limitation	Limit the submission speed. Select *Unlimited* or specify the number of submissions per *Hour* or *Day*. When the limit is reached, FortiSandbox sends a signal to FortiClient to stop file submission to save resources on both devices.

Adapter

FortiSandbox uses adapters to connect to third-party products such as Carbon Black/Bit9 server, ICAP, and mail gateway clients.

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 messages from an ICAP client and return a response to it.

FortiSandbox supports mail adapters to receive forwarded emails from an upstream email gateway and scan them. FortiSandbox extracts email attachments and URLs in an email body and sends them to the job queue.

You can use the MTA adapter to inspect and quarantine suspicious emails. For more information, see Configure MTA adapter on page 145 and the FortiSandbox user guide in the AWS marketplace.

The BCC adapter is for information only, it does not block emails.

FortiSandbox creates the ICAP, BCC, and MTA adapters which cannot be deleted. They are disabled by default.

The following options are available:

Create New	Create a new adapter.
Edit	Edit an adapter.
Delete	Delete an adapter. You cannot delete the ICAP, BCC, or MTA adapter.
Test Connection	If available, click this button to test the selected entry's connection. The banner at the top displays the result.

This page displays the following information:

Adapter Name	Adapter name.
Vendor Name	Vendor name.
Serial	Serial number.
FQDN/IP	FQDN/IP address. This field is empty when for the ICAP, BCC, and MTA adapter.
Malicious	File and URL count of Malicious rating from this adapter in the last seven days.

High	File and URL count of High Risk rating from this adapter in the last seven days.
Medium	File and URL count of Medium Risk rating from this adapter in the last seven days.
Low	File and URL count of Low Risk rating from this adapter in the last seven days.
Clean	File and URL count of Clean rating from this adapter in the last seven days.
Other	File and URL count of Other rating from this adapter in the last seven days.

To create an adapter:

1. Go to *Scan Input > Adapter*.
2. Click the *Create New* button from the toolbar.
3. Configure the following and click *OK*.

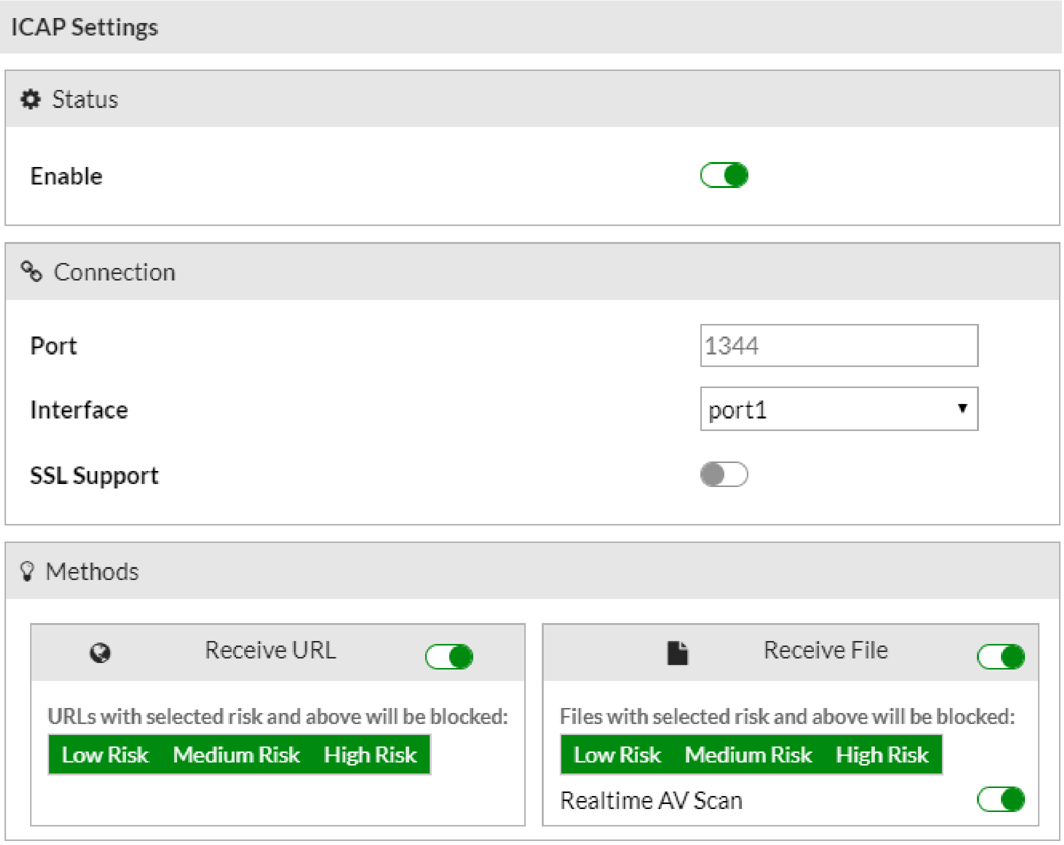
Vendor Name	Select *Carbon Blaclk/Bit9*.
Adapter Name	Enter the adapter name.
Server FQDN/IP	Enter the FQDN/IP address of the Carbon Black server.
Token	Enter the token string. Authentication token is assigned by the Carbon Black or ICAP server.
Timeout (seconds)	Enter the timeout value.
Serial	Auto-generated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

After you create a Carbon Black adapter, FortiSandbox tries to communicate with the Carbon Black server. If the connection and authentication is successful, the status column shows a green icon, otherwise it shows a red icon.

To configure the ICAP adapter:

1. Go to *Scan Input > Adapter*.
2. Select the *ICAP* adapter and click *Edit*.
3. Enable the adapter.
4. Configure the *Connection* settings.
5. You can select the interface port that FortiSandbox listens to. The default is *port1*.
6. In the *Methods* section, you can enable *Receive URL* and *Receive File* and set the rating to block files and URLs.

7. For faster response of a known virus before a file is put into the job queue, enable *Realtime AV Scan*.



ICAP Settings

Status

Enable: ●

Connection

Port: 1344

Interface: port1 ▾

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: ●

8. Click *Apply*.
9. To enable file submission from the ICAP adapter to create log events:
   a. Go to *Scan Policy > General*.
   b. Under *Enable log event of file submission*, select *ICAP*.
   c. Click *OK*.
10. To view ICAP adapter debug logs in run time, execute the following CLI command:

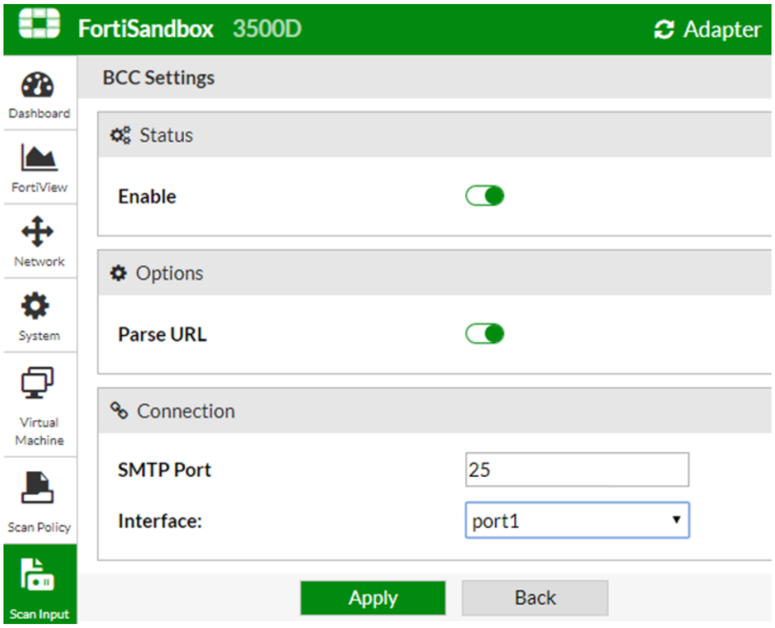
    ```
    diagnose-debug adapter_icap
    ```

    For more information about the `diagnose-debug` command, see the *FortiSandbox CLI Reference*.

To configure the BCC adapter:

1. Go to *Scan Input > Adapter*.
2. Select the *BCC* adapter and click *Edit*.
3. Enable the adapter.
4. Enable *Parse URL* to allow FortiSandbox to extract the first three URLs in an email.

5. Configure the *Connection* settings.



BCC Settings

Status

Enable: on

Options

Parse URL: on

Connection

SMTP Port: 25

Interface: port1

6. Click *Apply*.

To troubleshoot communication problems with an adapter, use this CLI command:

```
diagnose-debug [adapter_cb | adapter_icap | adapter_bcc | adapter_mta_relay | adapter_mta_
    mail]
```

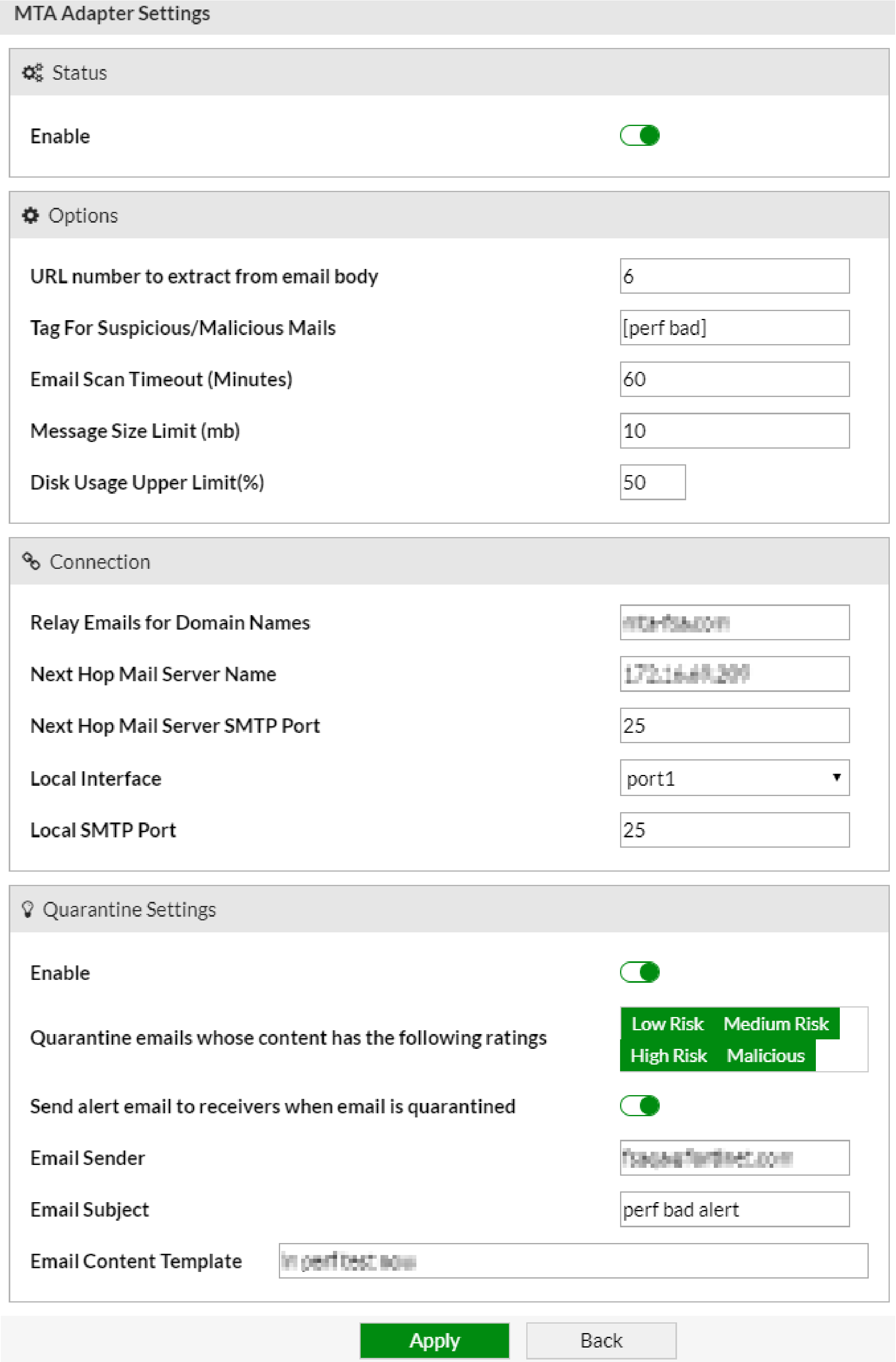
Configure MTA adapter

The MTA adapter requires a contract. The *Dashboard System Information* widget shows the *MTA Contract* status.

To configure the MTA adapter:

1. Go to *Scan Input > Adapter*.
2. Select the *MTA* adapter and click *Edit*.

3. Enable the adapter.



MTA Adapter Settings

Status

Enable	●

Options

URL number to extract from email body	6
Tag For Suspicious/Malicious Mails	[perf bad]
Email Scan Timeout (Minutes)	60
Message Size Limit (mb)	10
Disk Usage Upper Limit(%)	50

Connection

Relay Emails for Domain Names	[redacted]
Next Hop Mail Server Name	[redacted]
Next Hop Mail Server SMTP Port	25
Local Interface	port1 ▼
Local SMTP Port	25

Quarantine Settings

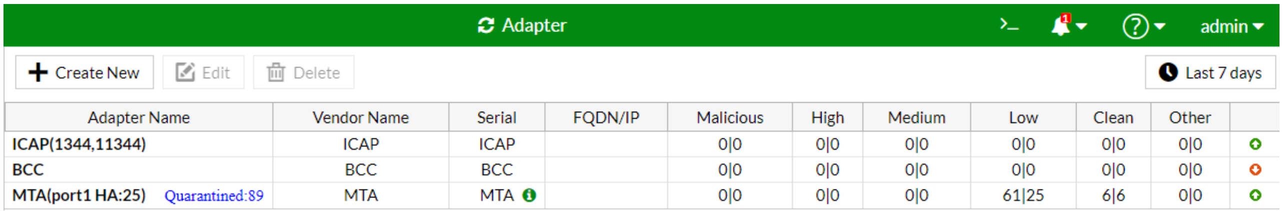
Enable	●
Quarantine emails whose content has the following ratings	Low Risk Medium Risk High Risk Malicious
Send alert email to receivers when email is quarantined	●
Email Sender	[redacted]
Email Subject	perf bad alert
Email Content Template	[redacted]

4. Configure the following settings and then click *Apply*.

URL number to extract from email body	Maximum number of URLs to be extracted from one email body.
Tag For Suspicious/Malicious Mails	If the email scan result is malicious or suspicious, this text is prefixed to the email subject line. The next hop email server can act accordingly.
Email Scan Timeout (Minutes)	Maximum time FortiSandbox waits for scan result. If there is no result after timeout, the email is released to recipient.
Message Size Limit (mb)	Maximum size of email to accept to scan.
Disk Usage Upper Limit(%)	Maximum percentage disk space used before MTA stops scanning emails and only routes emails.
Relay Emails for Domain Names	Domain names of email server to be relayed from this FortiSandbox. When FortiSandbox receives these emails and finishes scan, FortiSandbox relays these emails if they are clean, or quarantines them if malicious.
Next Hop Mail Server Name	IP address or domain name of email server to relay to for relayed emails.
Local Interface	Select the local interface.
Local SMTP Port	Specify the local SMTP port.
Quarantine emails whose content has the following ratings	Select the ratings of emails to quarantine.
Send alert email to receivers when email is quarantined	When email is quarantined, send alert email as configured.
Email Sender	The *From* field of alert email sent.
Email Subject	Email subject line of alert email sent.
Email Content Template	Text in alert email body.

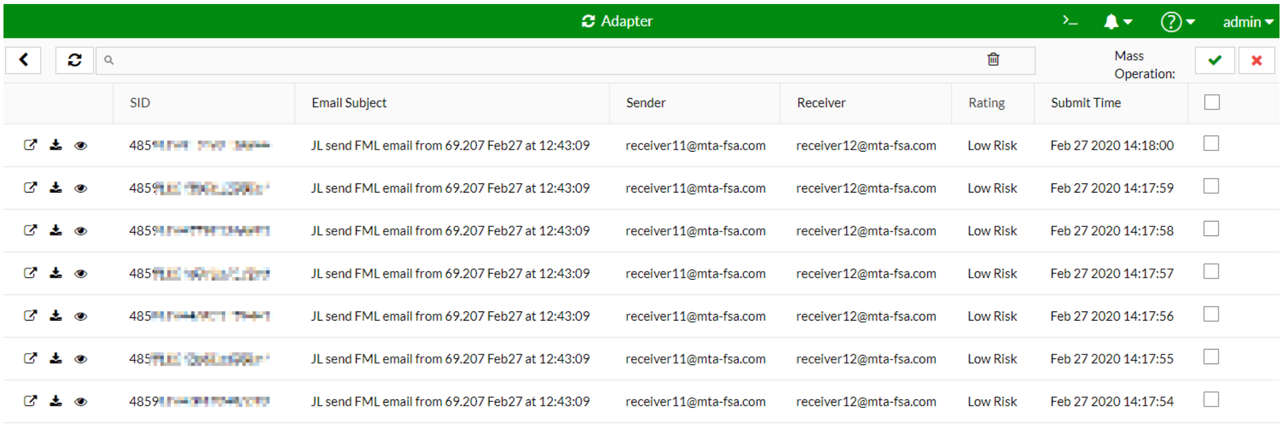
To process quarantined emails:

1. Go to *Scan Input > Adapter*.
   If there are malicious and suspicious emails, the number of quarantined emails is displayed beside the MTA adapter name.



Adapter Name	Vendor Name	Serial	FQDN/IP	Malicious	High	Medium	Low	Clean	Other	
ICAP(1344,11344)	ICAP	ICAP		0|0	0|0	0|0	0|0	0|0	0|0	●
BCC	BCC	BCC		0|0	0|0	0|0	0|0	0|0	0|0	●
MTA(port1 HA:25) Quarantined:89	MTA	MTA ℹ		0|0	0|0	0|0	61|25	6|6	0|0	●

2. Click the *Quarantined* link to display the list of quarantined emails.



	SID	Email Subject	Sender	Receiver	Rating	Submit Time	□
	485[redacted]	JL send FML email from 69.207 Feb27 at 12:43:09	receiver11@mta-fsa.com	receiver12@mta-fsa.com	Low Risk	Feb 27 2020 14:18:00	□
	485[redacted]	JL send FML email from 69.207 Feb27 at 12:43:09	receiver11@mta-fsa.com	receiver12@mta-fsa.com	Low Risk	Feb 27 2020 14:17:59	□
	485[redacted]	JL send FML email from 69.207 Feb27 at 12:43:09	receiver11@mta-fsa.com	receiver12@mta-fsa.com	Low Risk	Feb 27 2020 14:17:58	□
	485[redacted]	JL send FML email from 69.207 Feb27 at 12:43:09	receiver11@mta-fsa.com	receiver12@mta-fsa.com	Low Risk	Feb 27 2020 14:17:57	□
	485[redacted]	JL send FML email from 69.207 Feb27 at 12:43:09	receiver11@mta-fsa.com	receiver12@mta-fsa.com	Low Risk	Feb 27 2020 14:17:56	□
	485[redacted]	JL send FML email from 69.207 Feb27 at 12:43:09	receiver11@mta-fsa.com	receiver12@mta-fsa.com	Low Risk	Feb 27 2020 14:17:55	□
	4859[redacted]	JL send FML email from 69.207 Feb27 at 12:43:09	receiver11@mta-fsa.com	receiver12@mta-fsa.com	Low Risk	Feb 27 2020 14:17:54	□

- To view job details, click the *View Details* icon.
- To download the job files as a zip file, click the *Download Email File* icon.
- To preview the original email, click the *Preview Email* icon.
- To release the quarantined email to recipient, select the emails and click the *Release Email* icon.
- To delete the quarantined email, select the emails and click the *Delete Email* icon.

Using MTA in HA-Cluster

In HA-Cluster, the MTA adapter is only available in the primary node.

Configuration is the same as on a standalone device. When the primary node receives MTA jobs, depending on workload and VM association, it distributes the jobs to itself or worker nodes.

In a cluster, configure the *Local Interface* to the interface of the cluster IP address so that the secondary can take over the configuration in a failover.

To view jobs in a cluster, go to *HA-Cluster > Job Summary*.

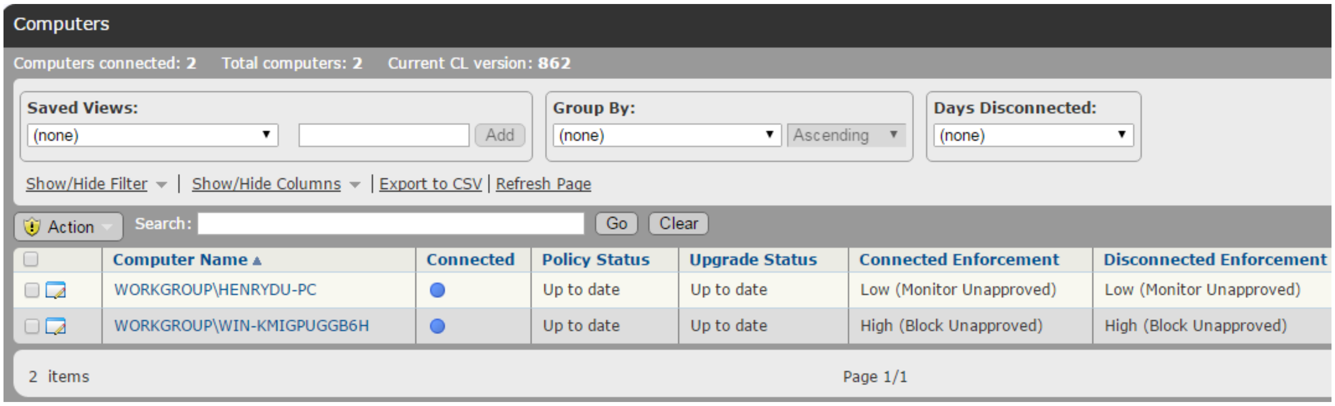
To view logs in the primary node, go to *Log & Report > Job Events*.

To view logs in a worker node, go to *Log & Report > All Events*.

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

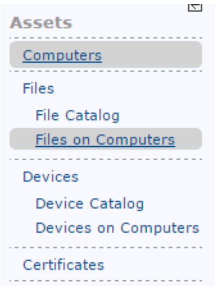
Days Disconnected: (none)

Show/Hide Filter | Show/Hide Columns | Export to CSV | Refresh Page
Action
Search:
Go
Clear

□	Computer Name ▲	Connected	Policy Status	Upgrade Status	Connected Enforcement	Disconnected Enforcement
□	WORKGROUP\HENRYDU-PC	●	Up to date	Up to date	Low (Monitor Unapproved)	Low (Monitor Unapproved)
□	WORKGROUP\WIN-KMIGPUGGB6H	●	Up to date	Up to date	High (Block Unapproved)	High (Block Unapproved)

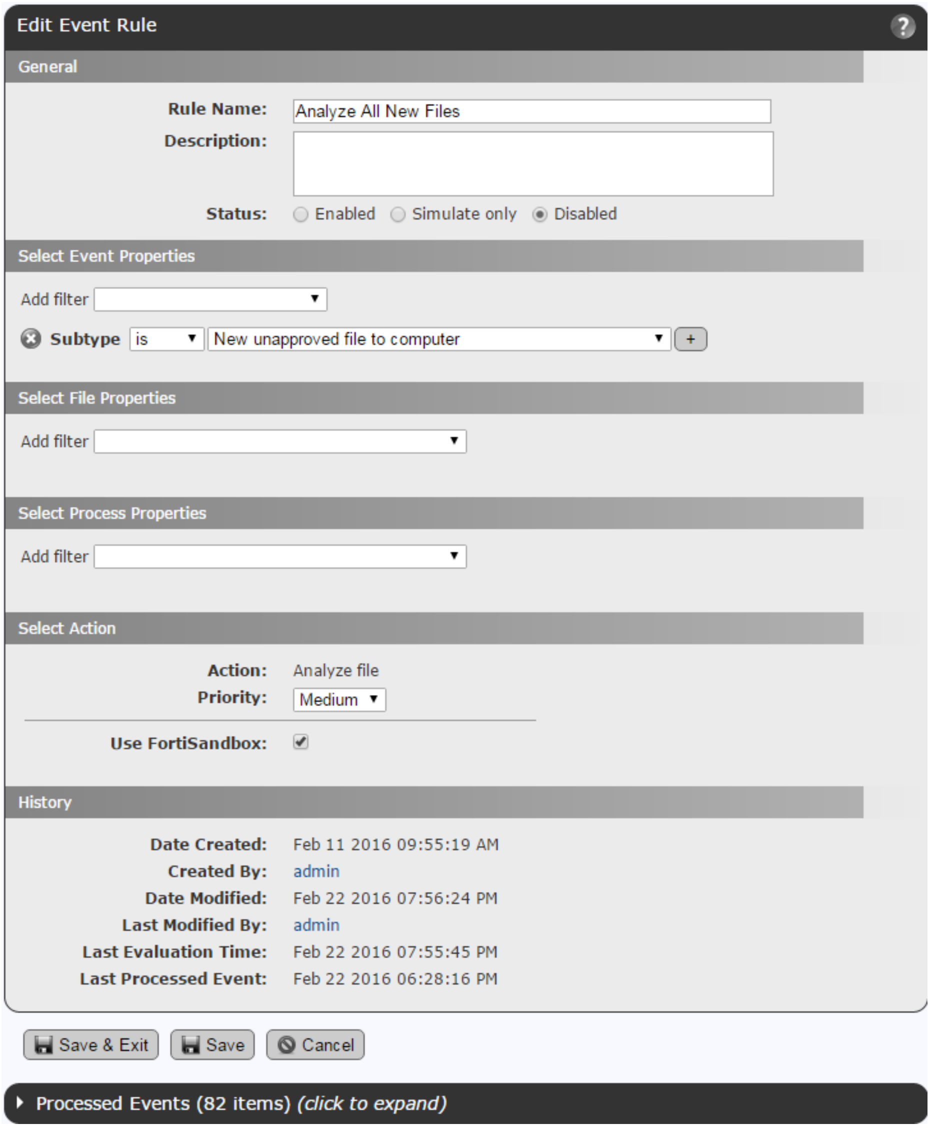
2 items Page 1/1

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



Edit Event Rule

General

Rule Name: Analyze All New Files

Description:

Status: ○ Enabled ○ Simulate only ● Disabled

Select Event Properties

Add filter

Subtype is New unapproved file to computer

Select File Properties

Add filter

Select Process Properties

Add filter

Select Action

Action: Analyze file

Priority: Medium

Use FortiSandbox: ☑

History

Date Created: Feb 11 2016 09:55:19 AM

Created By: admin

Date Modified: Feb 22 2016 07:56:24 PM

Last Modified By: admin

Last Evaluation Time: Feb 22 2016 07:55:45 PM

Last Processed Event: Feb 22 2016 06:28:16 PM

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.

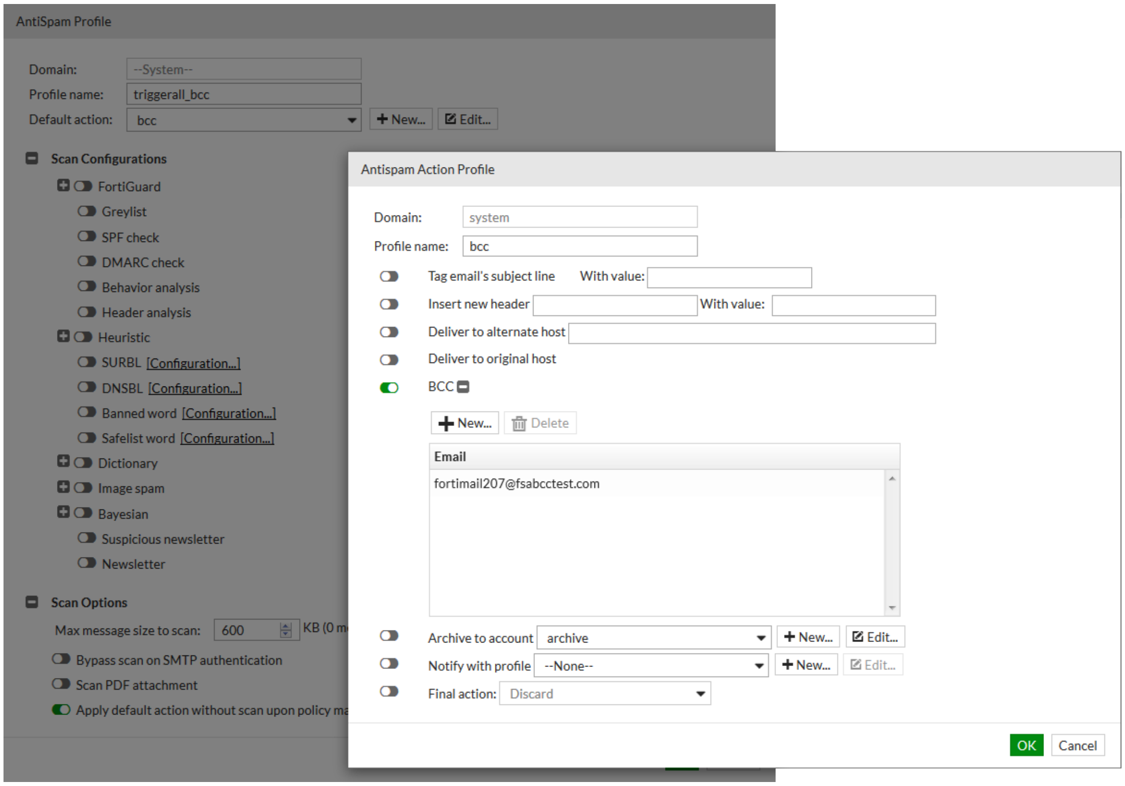
To configure the FortiSandbox:

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*.



AntiSpam Profile

Domain: --System--
Profile name: triggerall_bcc
Default action: bcc

Scan Configurations: FortiGuard, Greylist, SPF check, DMARC check, Behavior analysis, Header analysis, Heuristic, SURBL [Configuration...], DNSBL [Configuration...], Banned word [Configuration...], Safelist word [Configuration...], Dictionary, Image spam, Bayesian, Suspicious newsletter, Newsletter

Scan Options

Max message size to scan: 600 KB (0 m

Bypass scan on SMTP authentication
Scan PDF attachment
Apply default action without scan upon policy ma (enabled)

Antispam Action Profile

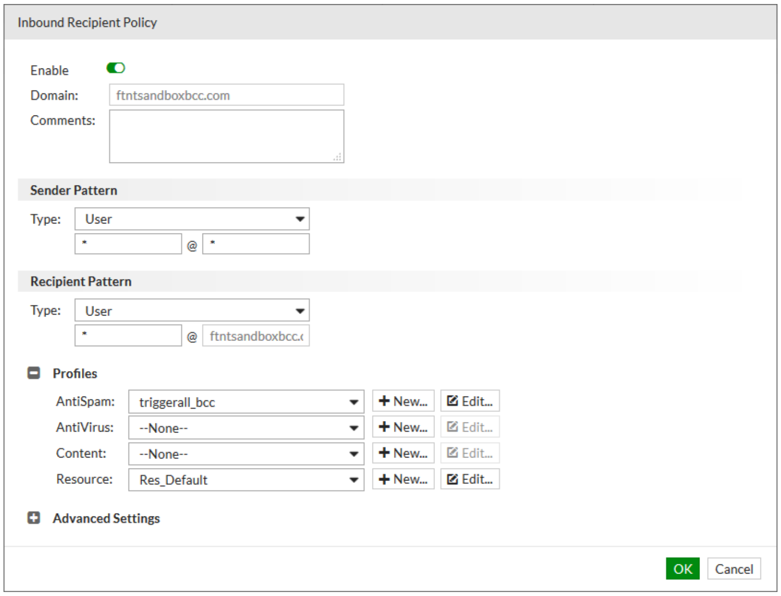
Domain: system
Profile name: bcc

Tag email's subject line With value:
Insert new header With value:
Deliver to alternate host
Deliver to original host
BCC (enabled)

Email
fortimail207@fsabcctest.com

Archive to account: archive
Notify with profile: --None--
Final action: Discard

2. Go to *Policy > Recipient Policy*:
   a. Select the domain for forwarding emails to the FortiSandbox, and apply the new AntiSpam profile.
   b. Add a new inbound policy, select the domain for forwarding emails to the FortiSandbox, and apply the new AntiSpam profile.



Inbound Recipient Policy

Enable

Domain: ftntsandboxbcc.com

Comments:

Sender Pattern

Type: User

* @ *

Recipient Pattern

Type: User

* @ ftntsandboxbcc.c

Profiles

AntiSpam: triggerall_bcc

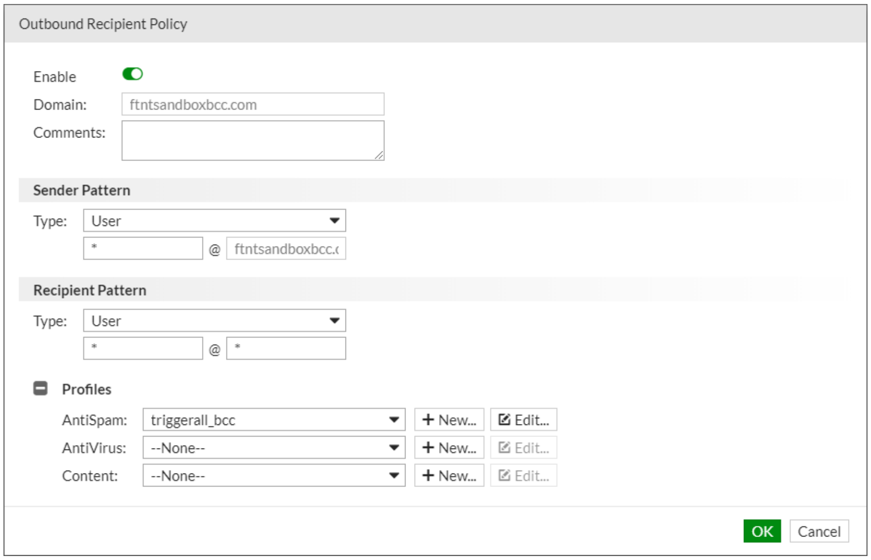
AntiVirus: --None--

Content: --None--

Resource: Res_Default

Advanced Settings

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: ftntsandboxbcc.com

Comments:

Sender Pattern

Type: User

* @ ftntsandboxbcc.c

Recipient Pattern

Type: User

* @ *

Profiles

AntiSpam: triggerall_bcc

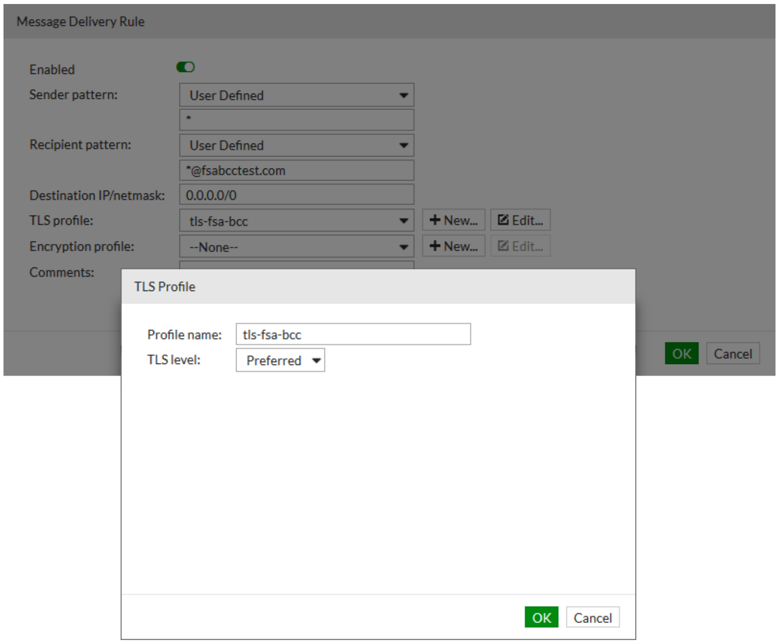
AntiVirus: --None--

Content: --None--

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: User Defined

*

Recipient pattern: User Defined

*@fsabcctest.com

Destination IP/netmask: 0.0.0.0/0

TLS profile: tls-fsa-bcc

Encryption profile: --None--

Comments:

TLS Profile

Profile name: tls-fsa-bcc

TLS level: Preferred

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:

Create New	Create a new network share.
Edit	Edit the selected entry.
Clone	Clone the selected entry. Only the *Network Share Name* is different. All other settings are the same as the original. In an HA-Cluster, you can only clone on the primary node. In a failover, all network shares move to the new primary.
Delete	Delete the selected entry.
Scan Now	Scan the selected entry.
Scan Details	View the selected entry's scheduled scan entries.
Test Connection	Test the selected entry's connection. The banner at the top displays the result.

The following information is displayed:

Name	Name of the network share.
Scan Scheduled	The scan scheduled status. Scheduled network scans are done in parallel.
Type	Mount type.
Share Path	File share path.
Quarantine	Displays if quarantine is enabled.
Enabled	Displays if the network share is enabled. A disabled network share does not run its scheduled scans.
Status	Displays if the network share status is accessible or down.

To create a new network share:

1. Go to *Scan Input* > *Network Share*.
2. Click *Create New*.
3. Configure the following options and click *OK*.

Enabled	Select to enable network share configuration. If network share is not enabled, its scheduled scan will not run.
Mount Type	Select the mount type. The following options are available: • CIFS (SMB v1.0, v2.0, v2.1, v3.0). For Microsoft DFS, only SMB v1.0 is supported. • NFSv2. • NFSv3. • NFSv4. • Azure File Share. See Cloud Storage on page 157. • AWS S3. See Cloud Storage on page 157. For domain-based DFS namespace, ensure the domain name can be resolved with the system Primary DNS server.
Network Share Name	Network share name.
Server Name/IP	Server FQDN or IP address.
Share Path	File share path in the format `/path1/path2`.
Scan Files Of Specified Pattern	Include or exclude files which match a file name pattern.
File Name Pattern	File name pattern.
Username, Password, Confirm Password	Username and password. For domain users, use the format `domain_name\user_name`.
Scan Job Priority	When multiple network share scans run at the same time, higher priority scans get more scan power.

Keep A Copy Of Original File On FortiSandbox	Keep a copy of the original file on FortiSandbox.
Skip Sandboxing for the same unchanged files	To improve scan speed, you can skip sandboxing scan on existing files (if applicable) and only do sandboxing scan on new files. Existing files are only scanned by AntiVirus engine and Community Cloud query.
Enable Quarantine of Malicious Files	Quarantine files with a Malicious rating in the selected location. Quarantined files are put in a folder with the name of the Job ID and each file is renamed with the Job ID for that file and a meta file with more information.
Enable Quarantine of Suspicious - High Risk files	Quarantine suspicious files with a High Risk rating in the selected location. Quarantined files are put in a folder with the name of the Job ID and each file is renamed with the Job ID for that file and a meta file with more information.
Enable Quarantine of Suspicious - Medium Risk files	Quarantine suspicious files with a Medium Risk rating in the selected location. Quarantined files are put in a folder with the name of the Job ID and each file is renamed with the Job ID for that file and a meta file with more information.
Enable Quarantine of Suspicious - Low Risk files	Quarantine suspicious files with a Low Risk rating in the selected location. Quarantined files are put in a folder with the name of the Job ID and each file is renamed with the Job ID for that file and a meta file with more information.
Enable Quarantine of Other rating files	Quarantine suspicious files with a Other rating in the selected location. Quarantined files are put in a folder with the name of the Job ID and each file is renamed with the Job ID for that file and a meta file with more information.
Enable copying or moving clean files to a sanitized location	Copy or move files with a Clean rating 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 into it with the original folder structure. To save space, uncheck *Keep a complete copy of clean files for every scheduled scan* so that files of the same path have only one copy in the sanitized location.
Enable Scheduled Scan	Enable scheduled scan and specify the schedule type.
Description	Optional description for the network share entry.
Send notification email after each scan	Email a summary report for each network share scan to the specified users.

When a file is moved, to leave a copy in its original location, go to the Quarantine edit page or sanitized share and select the *Keep Original File At Current Location*.

To run a network share scan immediately:

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

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:

Back	Go back to the network share page.
Refresh	Refresh the scans page.
Delete	Delete the selected scan.
Total	The total number of finished scanned jobs.
Start	The start time of the scan.
End	The end time of the scan.
Finished	Percentage of files that finished the scan. Click on the number to show details.
Malicious	The number of Malicious files discovered. Click on the number to show detected Malicious rating files. The number of quarantined files are also displayed.
Suspicious	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.
Clean	The number of Clean files detected. Click on the number to show detected Clean rating files.
Others	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.

Cloud Storage

FortiSandbox can scan files stored on cloud, and currently supports Azure FS and Amazon S3. Go to *Scan Input* > *Network Share* to view and configure cloud storage access information.

Cloud Storage scans can be scheduled or run on-demand, and connectivity to the cloud storage can be tested.

The following options are available:

Create New	Click to create a new cloud storage connection.
Edit	Select an entry from the list and then click *Edit* in the toolbar to edit the entry selected.
Delete	Select an entry from the list and then click *Delete* in the toolbar to remove the entry selected.
Scan Now	Select an entry from the list and then click *Scan Now* in the toolbar to scan the entries.
Scan Details	Select an entry from the list and then click *Scan Details* in the toolbar to view the scheduled scan entries.
Test Connection	Select an entry from the list and then click *Test Connection* in the toolbar to test the connection. The result message will be displayed in the top message bar.

The following information is displayed:

Name	The name of the cloud storage.
Scan Scheduled	The scan scheduled status. Scheduled network scans are done in parallel.
Type	The mount type.
Share Path	The cloud storage access URI.
Quarantine	Displays if quarantine is enabled.
Enabled	Displays if the cloud storage scan is enabled. If a cloud storage scan is disabled, its scheduled scan will not be executed.
Status	Displays the cloud storage connection status. The states are: • Network is Accessible • Network Down

To create a new cloud storage scan:

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.
Network Share Name	Enter the network share name.
Mount Type	Select the mount type from the dropdown list. Depending on the type selected, you will be asked for different information required to access your cloud storage. The following options are for cloud storage: • Azure File Share • AWS S3

SMB and NFS Settings	**Server Name/IP**	Enter the server fully qualified domain name (FQDN) or IP address.
	Share Path	Enter the file share path. In the format `/path1/path2`
	Username	Enter a user name. For a domain users, use format `domain_name\user_name`.
	Password	Enter the password.
	Confirm Password	Enter the password a second time for verification.
Scan Files Of Specified Pattern		Select to include or exclude files which match a file name pattern.
File Name Pattern		Enter the file name pattern.
Scan Job Priority		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 *High*, *Medium* (default), or *Low*.
Keep A Copy Of Original File On FortiSandbox		Select to keep a copy of the original file on FortiSandbox.
Skip Sandboxing for the same unchanged files		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.
Enable Quarantine of Malicious Files		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. 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.
Enable Quarantine of Suspicious - High Risk Files		Select to enable quarantine of *Suspicious High Risk* files, then select the quarantine location from the dropdown list. Files with a High Risk rating will be quarantined in the quarantine location. 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.
Enable Quarantine of Suspicious - Medium Risk Files		Select to enable quarantine of *Suspicious Medium Risk* files, then select the quarantine location from the dropdown list. Files with a Medium Risk rating will be quarantined in the quarantine location. 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.

Enable Quarantine of Suspicious - Low Risk Files	Select to enable quarantine of *Suspicious Low Risk* files, then select the quarantine location from the dropdown list. Files with a Low Risk rating will be quarantined in the quarantine location. 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.
Enable Quarantine of Other rating files	Select to enable quarantine of *Other Rating* 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. 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.
Enable moving clean files to a sanitized location	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 *Keep a complete copy of clean files for every scheduled scan*, then files of the same path will have only one copy saved in the sanitized location.
Enable Scheduled Scan	Select to enable scheduled scan. Select the schedule type from the dropdown list. Select the minute or hour from the second dropdown list.
Description	Enter an optional description for the network share entry.

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 *Keep Original File At Current Location* checkbox.

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.

Azure AWS S3 Settings

FortiSandbox can scan files stored on cloud using Azure AWS S3.

The following AWS S3 settings are available when creating a new Network Share:

AWS S3 Bucket Name	Enter the bucket name, found in the AWS management console in the *S3 Service* page.
S3 Bucket Folder Path	Enter the folder's path, starting with */*.
AWS IAM Access Key ID	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 *Security Credentials* link to generate the access key ID.
Secret Access Key	Enter the secret key matching the access key ID. The secret access key is displayed when you generate the access key ID.
Confirm Secret Access Key	Confirm the secret access key.

Azure Blob Settings

FortiSandbox can scan files stored on cloud using Azure Blob.

The following Azure file share settings are available when creating a new Network Share:

Domain of the Share URL	Enter the Azure file share URL's domain name, found in the Azure server's menu at *Storage Accounts* > *storage account name* > *Settings* > *Properties* > *URL*.
Path of the Share URL	Enter the path of the URL, found in the Azure server's menu at *Storage Accounts* > *storage account name* > *File Service* > *Files* > *Share path starting with /*.
Name of the Storage Account	Enter the name of the storage account, found in the Azure server's menu at *Storage Account* > *storage account name*.
Access Key of the Account	Enter the access key of the account, found in the Azure server's menu at *Storage Account* > *storage account name* > *Settings* > *Access Keys*.
Confirm Access Key	Confirm the access key.

Quarantine

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

The following options are available:

Create New	Select to create a new quarantine location.

Edit	Select an entry from the list and then select *Edit* 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.
Delete	Select an entry from the list and then select *Delete* 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:

Name	The name of the quarantine location.
Type	The mount type.
Share Path	The file share path.
Enabled	Displays if the quarantine location is enabled.
Status	Displays the quarantine access status. One of the following states: • Quarantine is Accessible • Quarantine Down

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:

Enabled	Select to enable quarantine location.
Quarantine Name	Enter the quarantine name.
Mount Type	Select the mount type from the dropdown list. The following options are available: • CIFS (SMB v1.0, v2.0, v2.1 and v3.0) • NFSv2 • NFSv3 • NFSv4
Server Name/IP	Enter the server fully qualified domain name (FQDN) or IP address.
Share Path	Enter the file share path. In the format `/path1/path2`.
Username	Enter a user name. For a domain user, use the format `domain_name\user_name`.
Password	Enter the password.
Confirm Password	Enter the password a second time for verification.
Keep Original File At Current Location	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.
Description	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:

Refresh	Refresh the Malware Package list.
View	Select a package version number and click the *View* button from the toolbar. The following information is shown: • 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. • Mark the detection as False Positive: If marked, the entry will be removed from future *Malware Packages*. If the unit is joining a global threat information sharing network, the change is also reported to the *Collector* and is shared by all units in the network. • Detected: The time and date that the item was detected. • Checksum: The file checksum (SHA256). • Rating: The risk rating. • Serial Number: From which unit the threat information is from. • Global/Local: If this threat information is from a local unit or from another unit.
Download SHA256 **Download SHA1** **Download MD5**	You have the option to download packages containing malware SHA256, SHA1, and MD5.

This page displays the following:

Version	The malware package release version.
Release Time	The malware package release time.
Total	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:

Refresh	Refresh the URL Package list.
View	Select a package version number and click the *View* button from the toolbar. The following information is shown: • Job Detail: 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. • Mark the URL as False Positive: 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 *Collector* and is shared by all units in the network. A new package will generate after removing the entry. • Detected: The time and date that the item was detected. • URL: The URL in the package. • Rating: The risk rating of the downloaded file. • Serial Number: From which unit the threat information is from. • Global/Local: If this threat information is from a local unit, or from another unit.
Download URL	Download a text file which contains URLs in the package.

This page displays the following:

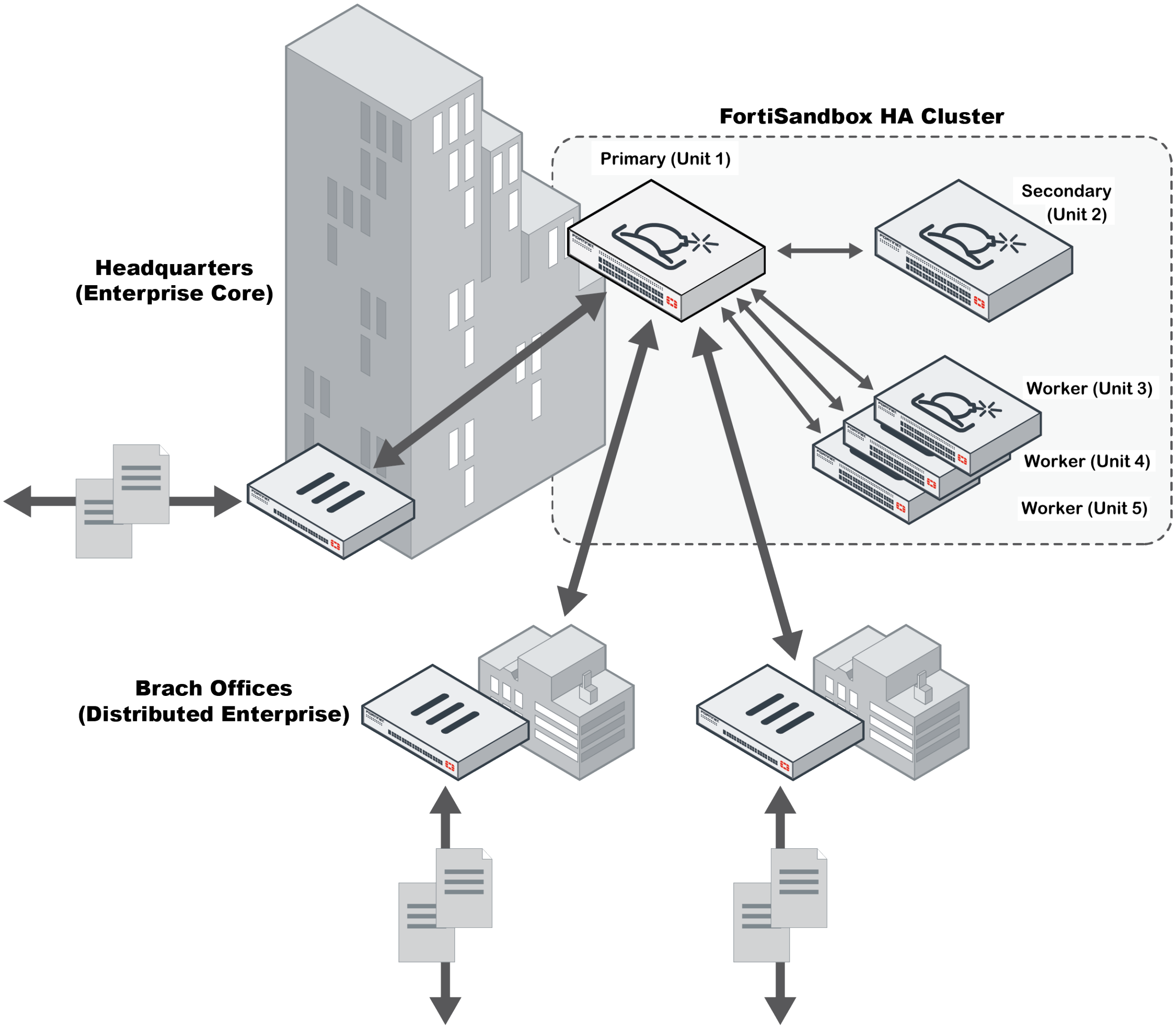
Version	The URL package release version.
Release Time	The URL package release time.
Total	The total number of malware antivirus signatures inside the package. The maximum number of signatures is 1000.

FortiSandbox only keeps URL packages generated in last 7 days.

HA-Cluster

A single FortiSandbox device can scan a limited number of files in a given time period. To handle heavier loads, you can use multiple FortiSandbox devices in a load-balancing high availability (HA) cluster.

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



Primary (formerly 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 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 node 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 node, we recommend using a FortiSandbox-3000D or higher.
Secondary (formerly primary slave)	The secondary node (Unit 2 in the diagram) is for HA support and normal file scans. It monitors the primary node's condition and, if the primary fails, the secondary will assume the role of primary. The former primary will then become a secondary when it is back up. The primary and secondary nodes must be the same model and have the same interface count.
Worker (formerly 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. Workers should have their own network settings and VM image settings. Workers can be any FortiSandbox model including FortiSandbox VM. Workers in a cluster do 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 nodes on the primary 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. You can perform the following tasks:
    - View the worker node's dashboard.
    - Change 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

We recommend that these ports be connected to the same switch and have IP addresses in the same subnet. If the job load is heavy, we recommend using the 10G fiber port 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.

Primary's role and worker's role

On the primary node, all functionality is 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 do not need to be configured on worker nodes:

- Job cleanup schedule
- Malware package generation settings
- Allowlist and blocklist (White / Black List)
- YARA rules
- Scan profile settings
- Job Queue Priority
- Overridden Verdicts
- URL category
- Customized Rating
- AI Mode
- Inter-cluster communication encryption
- TLS version

Although you can assign different VM types to each node in a cluster, we recommend all nodes share the same VM types. 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 for the entire cluster. If an association for a VM type is missing on the worker node, the sandbox scan cannot 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 are not scanned.

The following information is synchronized from the primary node to secondary node only, and is only applied when the secondary node becomes a primary node in 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
- Device group settings
- System Recovery settings
- Device (including FortiClient)
- Network Share settings
- Quarantine settings
- SNMP settings
- Widget settings
- Adapter settings
- Global network settings
- Login disclaimers
- Health Check settings
- Local Log settings
- Diagnostic Logs > CLI Logs settings
- Primary node scan power

Configure a cluster level failover IP set for primary unit

You can configure a cluster level failover IP for each port except port3 and any ports the sniffer is sniffing. This IP set works as an alias IP of the primary node network port. The primary node local IP set and secondary node Local IP set are kept locally during failover.

This failover IP set should be set on the current primary 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 node.

Main HA-Cluster CLI commands

In the primary and secondary 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.
`hc-status -l`	List the status of HA-Cluster units.
`hc-worker`	`-a` to add that worker or secondary unit to the cluster. `-r` to remove that worker or secondary unit from the cluster. `-u` to update that worker or secondary unit information.
`hc-primary -s<10-100>`	Turn on file scan on the primary node with 10% to 100% processing capacity.
`hc-primary -r<serial number>`	Remove the worker or secondary unit with the specified serial number from the primary node.

After removing a worker or secondary node, use `hc-status -l` on the primary node to verify that the worker or secondary node 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:

Prepare the following hardware:

- Eleven cables for network connections.
- Four 1/10 Gbps switches.
- Three FortiSandbox 3000D units with proper power connections (units A, B, and C). In this example, unit A is the primary node, unit B is the secondary node, and unit C is the worker node.

Put the primary and secondary nodes on different power circuits.

Step 2 - Prepare the subnets:

Prepare four 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
- Switch D: 192.168.4.0/24: For the file submission port (port 4) on the primary and secondary unit.

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.
4. Connect port 4 of the primary and secondary FortiSandbox device to Switch D.

Step 4 - Configure the primary:

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
   set port4-ip 192.168.4.99/24
   set default-gw 192.168.1.1
   ```
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
   hc-settings -si -iport4 -a192.168.4.98/24
   ```
   For information about CLI commands, see the FortiSandbox CLI Reference Guide on the Fortinet Document Library.
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:

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
   set port4-ip 192.168.4.100/24
   set default-gw 192.168.1.1
   ```
3. Configure the device as the secondary node with the following commands:
   ```
   hc-settings -sc -tP -nPslaveB -cTestHCsystem -ppassw0rd -iport2
   hc-settings -l
   hc-worker -a -s192.168.2.99 -ppassw0rd
   ```
4. Review the cluster status with the following command:
   ```
   hc-status -l
   ```

Step 6 - Configure the worker:

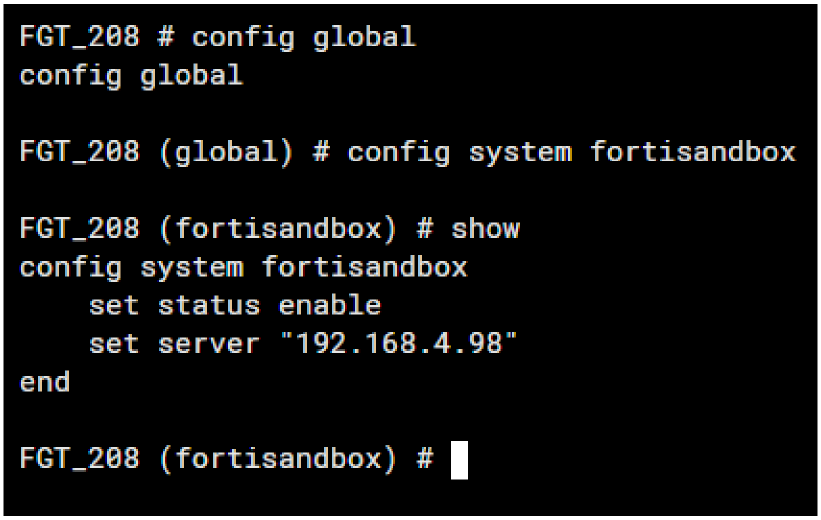
1. Power on the device (Unit C), and log into the CLI.
2. Configure the port IP addresses and gateway address with the following commands:
   ```
   set port1-ip 192.168.1.101/24
   set port2-ip 192.168.2.101/24
   set port3-ip 192.168.3.101/24
   set default-gw 192.168.1.1
   ```
3. Configure the device as a worker node with the following commands:
   ```
   hc-settings -sc -tR -cTestHCsystem -ppassw0rd -nSlaveC -iport2
   ```

```
hc-settings -l
hc-worker -a -s192.168.2.99 -ppassw0rd
```

4. Review the cluster status with the following command:
```
hc-status -l
```

Step 7 - Configure client devices to send files to FortiSandbox port4 failover IP:

1. Configure client devices to use unit A port4’s failover IP to submit files so that during failover, the new primary node (unit B) port4 will take over that IP.
   In FortiGate, enable FortiSandbox and connect it to the port4's failover IP.



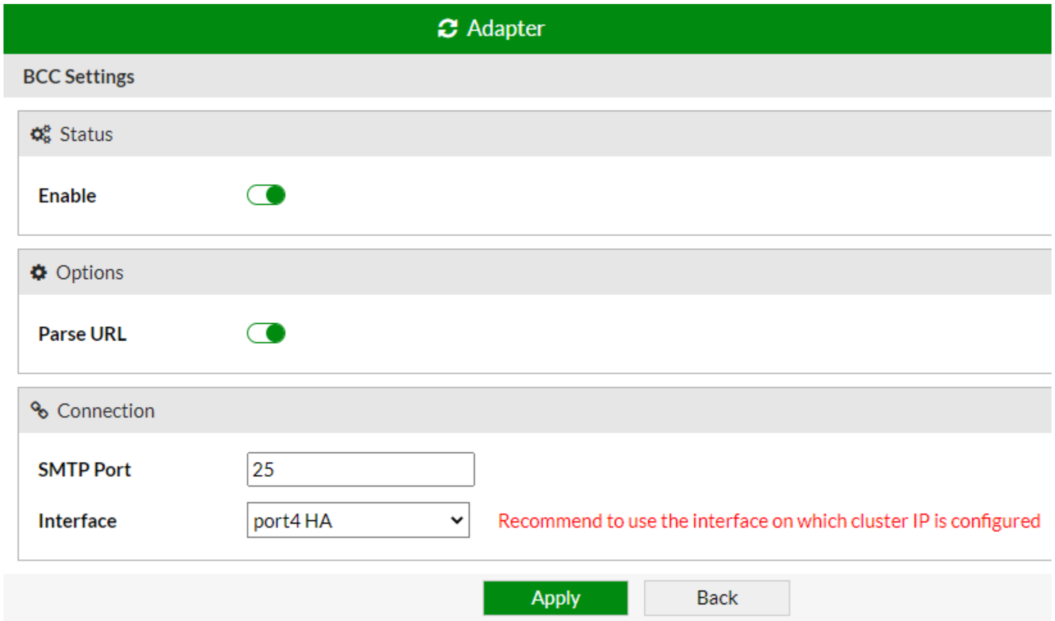
```
FGT_208 # config global
config global

FGT_208 (global) # config system fortisandbox

FGT_208 (fortisandbox) # show
config system fortisandbox
    set status enable
    set server "192.168.4.98"
end

FGT_208 (fortisandbox) #
```

2. If you enable adapters such as ICAP, BCC, or MTA on the primary port4’s failover IP, in adapter’s client configuration, you must specify primary port4’s failover IP to make adapter clients send traffic to FortiSandbox HA cluster. The following examples are for BCC and ICAP settings.



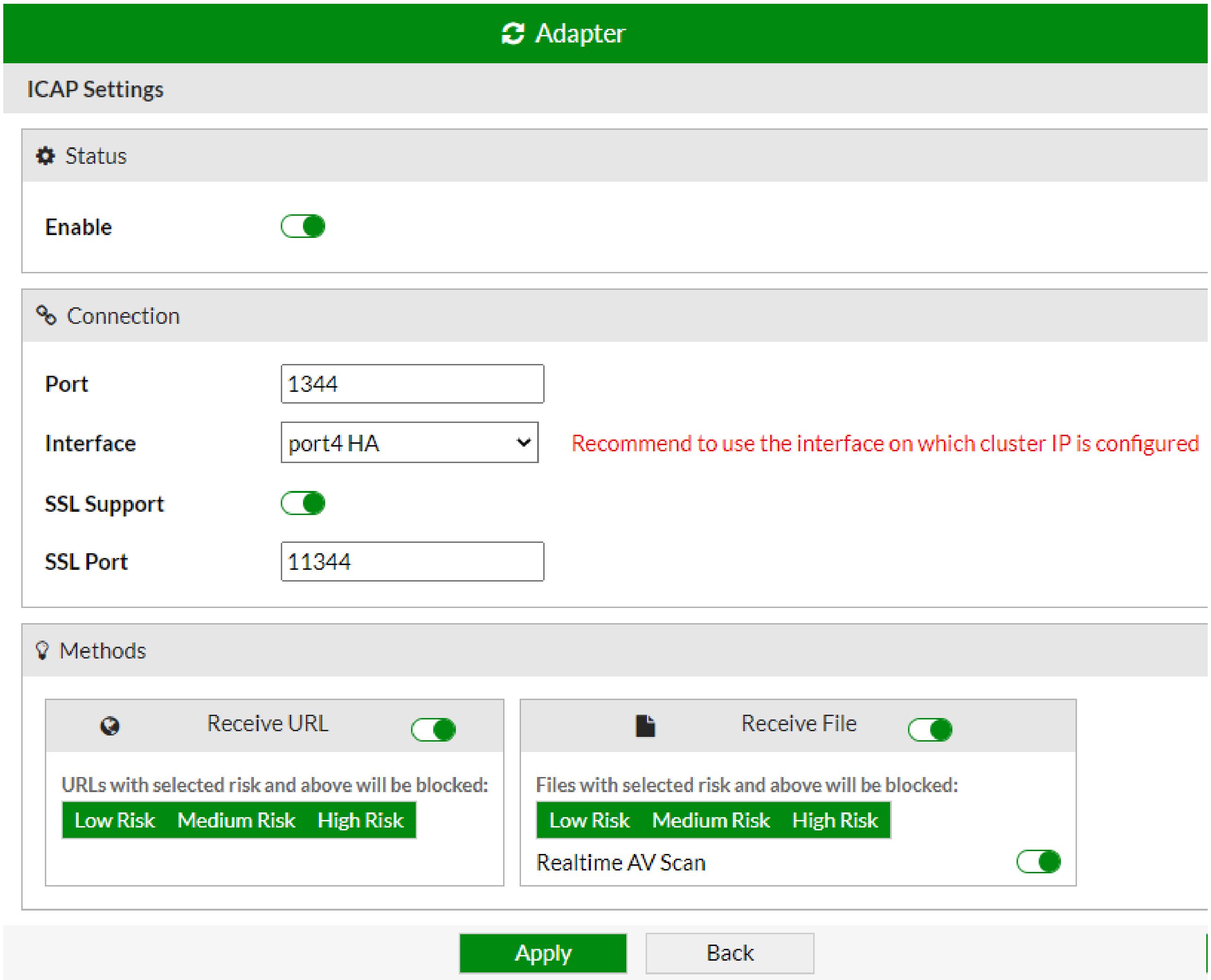
Enable: ●

Parse URL: ●

SMTP Port: 25

Interface: port4 HA

Recommend to use the interface on which cluster IP is configured



Adapter

ICAP Settings

Status

Enable: ON

Connection

Port: 1344

Interface: port4 HA

Recommend to use the interface on which cluster IP is configured

SSL Support: ON

SSL Port: 11344

Methods

Receive URL: ON

URLs with selected risk and above will be blocked: Low Risk | Medium Risk | High Risk

Receive File: ON

Files with selected risk and above will be blocked: Low Risk | Medium Risk | High Risk

Realtime AV Scan: ON

Step 8 - Configure the following settings on each unit:

- In *Virtual Machine* > *VM Images*, set each unit's clone number.
- Configure *Network* settings such as default gateway, static route, and system DNS.
- In *Scan Policy* > *General* set port3 gateway and DNS server.

Scan related settings, such as the scan profile, should be set on primary unit only; they will be synchronized to the worker node. For details, see Primary's role and worker's role on page 168.

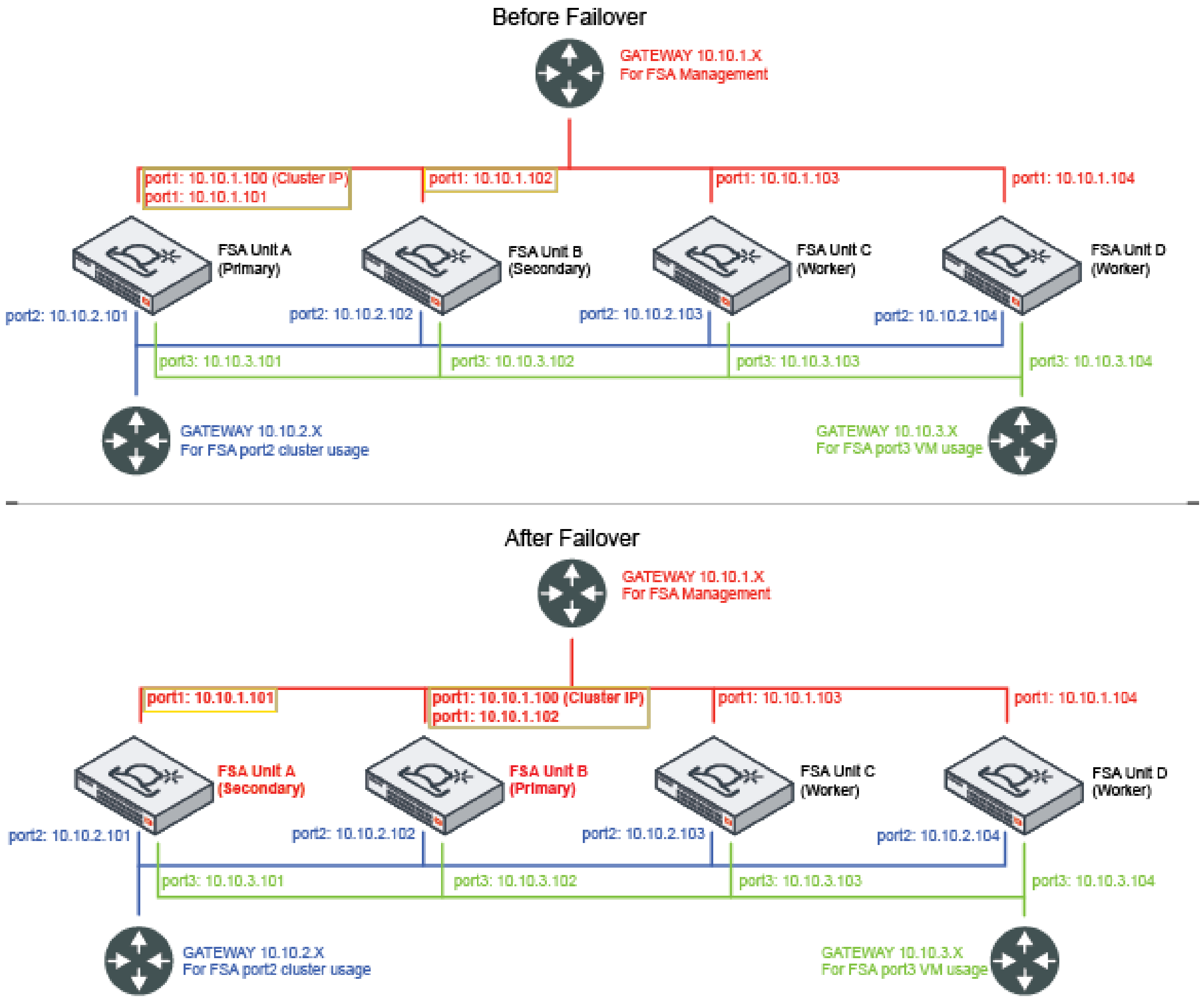
Scan input related settings should be set on primary node only as only primary node receives input files.

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-primary -r<serial number>`; then use `hc-status -l` to verify that the worker unit has been removed.

What happens during a failover

The primary node and secondary node send 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 occurs. You can also configure a ping server to regularly check the unit's network condition and downgrade itself to secondary type to trigger a failover. In a failover, the secondary and primary switch roles and the cluster IP addresses change, as indicated by the boxes in the lower image.



The failover logic handles two different scenarios:

Objective node available	The objective node is a worker (either secondary or worker) that can decide the new primary. For example, if a cluster consists 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, 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	When there is no objective node in the cluster, the cluster topography is not stable and the failover process may take several rounds of role changes. This occurs when there is no communication between nodes because the cluster's internal communication is down . During the failover process, the final roles of primary and secondary are decided by three principal factors: the internal connections, the health check, and the serial number. **Internal Connections** The internal connections in a cluster involve two ports: port1 and the cluster internal port, typically port2 depending on your configuration. Port1 is used when a node prompts itself to be the primary and needs confirmation from other nodes. The cluster internal port is used for cluster nodes to detect whether its connection to other nodes in the cluster is available or not, and is used to ask the secondary to failover when its health check fails. **Health Check** The health check is used to check the connection with the ping server. If this connection fails in the primary node, it triggers a failover. **Serial Number** Once the port1 connection is recovered, the unit with the newer serial number will keep the primary role and the unit with the older serial number will become the secondary.

When the new primary is decided, it will:

1. Build up the scan environment.
2. Apply all the settings synchronized from the original primary except the 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 are shut down as it becomes a worker node. Some functionality is turned off such as email alerts. If you want to reconfigure settings, such as the interface IP, you must do that through the CLI command or the primary's Central Management page.

Do not change the new primary node's configuration before the old primary node has returned online, because there is a risk the configuration could be lost. If it is absolutely necessary to reconfigure the new primary, it is recommended to first remove the old primary from the cluster using the CLI command `hc-primary -r`.

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. Workers
2. Secondary
3. Primary

It is highly recommended to setup cluster level failover IP set so the failover between primary and secondary can occur smoothly. If you do not want the failover to happen, you 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 node. You 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 node if there is at least one secondary node existing, a failover will occur after the configured period elapses. If no secondary node exists, the primary node will keep its primary role.

The following options are available:

Create New	Create a new health check ping server.
Edit	Edit a health check ping server.
Delete	Delete a health check ping server.

This page displays the following information:

Interface	The interface port to connect to the ping server. Port3 cannot be used.
Remote Server	IP address or fully-qualified domain name of the remote ping server.
Ping	Enable or disable sending the ping packet to the remote server to ensure the network connection is up.
TCP Echo	Enable or disable sending TCP Echo packet to ensure the network connection to the remote sever is up.
Interval	Time interval in seconds (30-180 seconds) to send a ping or TCP Echo packets.
Failover Threshold	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 if there is an existing secondary 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 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:

Time Period Drop down	Select the period of time over which the data was collected from the dropdown. You have the following options: *Last 24 Hours*, *Last 7 Days*, and *Last 4 Weeks*.
Serial Number	The serial number of the device in the cluster.
Pending	The number of files in the job queue waiting to be scanned.
Malicious	The number of malicious files detected.
Suspicious	The number of suspicious files detected.
Clean	The number of clean files detected.
Other	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:

Serial Number	The serial number of the device in the cluster.
Type	The type of the device: *Primary* (formerly *Master*), *Secondary* (formerly *Primary Slave*), or *Worker* (formerly *Regular Slave*).
Alias	The device's alias.
IP Address	The device's internal communication IP address.
Status	The status of the device: *Active* or *Inactive*.

The total number of cluster members are shown at the bottom of the list. This number cannot exceed 101, including the primary.

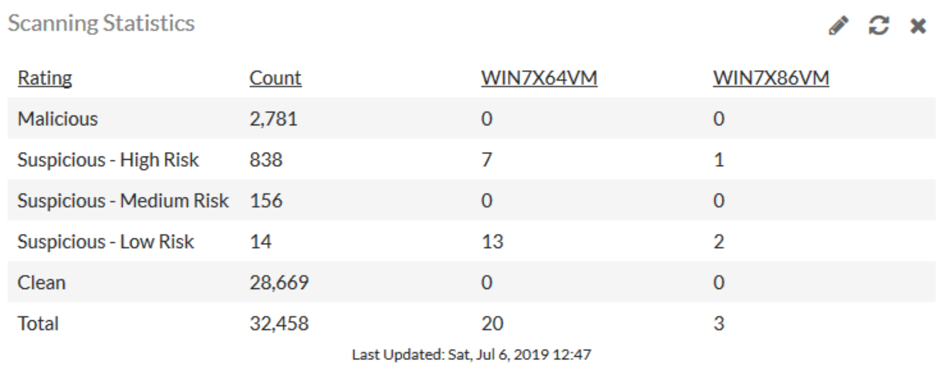
File Detection

Summary Report

The *Summary Report* is similar to the *System* dashboard. You can add and customize widgets in this page. Select a device and time period to customize the data to display.

If the unit is the primary 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:

Add Widget	Click the + button to add widgets to the summary report page.
Reset View	Click *Reset* to restore widgets to the default setting.
Time Period	Select a time period from the dropdown list. The options are: *Last 24 hours*, *Last 7 days*, or *Last 4 weeks*.
Device	Select the device from the dropdown list.

The following widgets are available:

Scanning Statistics	Information about the files scanned for a selected device for a selected time period.
Scanning Statistics by Type	Information about file types, rating, and event count for a selected device over a selected time period. To view all the file types, click *Edit* and increase the top count. Default is five.
Top Targeted Hosts	Number of infection events for specific hosts for a selected device over a selected time period.

	Hover the cursor over a colored portion of a bar in the chart to view the exact number of infection events for that host. Selecting the infected host allows you to drill down to the job details.
File Scanning Activity	Number of clean, suspicious, and malicious events at specific times over a selected time period for the selected device. Hover the cursor over a colored portion of a bar in the graph to view the exact number of events for the selected type for that time period.
Top Malware	Number of infection events for specific malware for a selected device over a selected time period. Hover the cursor over a colored portion of a bar in the chart to view the exact number of infection events for that malware. Selecting the malware name allows you to drill down to the job details.
Top Callback Domains	The top callback domains detected over a time period. Callback domains are hosts that files visit when executing in the VM. Hover the cursor over a colored portion of a bar in the chart to view the exact number of infection events for that malware.
Top File Types	The top file types detected over a time period. When *Scanned by Sandboxing* is selected, only files that have finished sandboxing are counted.

Customizing the summary report page

You can customize the FortiSandbox summary reports page. You can select the device and time period in the toolbar. You can also select which widgets to display, where they are located on the page, and whether you want to minimized or maximized them.

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:

Custom widget title	Optionally, enter a custom title for the widget. Leave this field blank to use the default widget title.

Refresh interval	Enter a refresh interval for the widget, in seconds. The widgets have default refresh values: • *Scanning Statistics*: 3600 seconds • *Scanning Statistics by Type*: 3600 seconds • *Top Malware*: 3600 seconds • *Scanning Activity*: 300 seconds • *Top Targeted Hosts*: 10 seconds • *Top Callback Domains*: 3600 seconds
Top Count	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 *Scanning Statistics*, *Scanning Statistics by Type*, and *Scanning Activity*.

File Scan

The *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		
	Suspicious	Click the *Suspicious* icon to view the suspicious jobs.
	Clean	Click the *Clean* icon to view the clean or unknown jobs.
	Malicious	Click the *Malicious* icon to view the malicious jobs.
Show Rescan Job Only		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 *File Detection* > *File Scan* > *Malicious* and enable *Show Rescan Job Only*.
Refresh		Click the button to refresh the entries displayed.
Search		Show or hide the search filter field.
Add Search Filter		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.

Export Data		Click the *Export Data* 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 *Log & Report* > *Report Center* page.
Customize		Click the *Customize* button to customize the Job View Settings. The change will be applied to all file based scan result pages.
Action		
	View Details	Click the *View Details* icon to view the file description and analysis details. The information displayed is dependent on the file selected.
	Perform Rescan	For malicious jobs, you can also select *Rescan* to manually rescan the file. This way, you can find out the behavior of a known virus. You can select to force the file to do a Sandboxing scan even if it was detected in previous steps of a Static Scan, AV Scan, Cloud Query, or if it was stopped from entering the VM by a Sandboxing-prefilter setting. You can find the job in *Scan Input* > *File On-Demand*.
	Archived File	An icon will appear if the file is an Archived File.
	FortiGuard Static Scan	The icon displays that the file is rated by the user's overridden verdict or FortiGuard advanced static scan.
	File Inside Archive	The icon displays that the file is a file extracted from an archive file.
	Rescan Job	The icon displays that the job is Malicious from an AV Rescan or a rescan job of a Malicious file.
	AV Scan	An icon will appear if this job is from an AV Rescan.
Pagination		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 78.

To view file details:

1. Select a file.
2. Click *View Details*. A new tab opens.
   For information on the *View Details* page, see Appendix A - View Details page reference on page 202.

To rescan a file:

1. Select a file with a Suspicious Rating that is not rated by VM or any malicious rating file.
2. Click *Perform Rescan*.
3. You can force the file to do Sandboxing scan even if was detected in former steps of Static Scan, AV Scan, Cloud Query, or stopped from entering VM by Sandboxing-prefilter setting.
4. Click *OK* to start the rescan.

Rescan results are in *FortiView > File Scan Search* and *Scan Input > File On-Demand*.

In this version, the maximum number of events you can export to a PDF report is 1000. The maximum number of events you can export to a CSV report is 15000. Jobs over the maximum are not included in the report.

Network Alerts

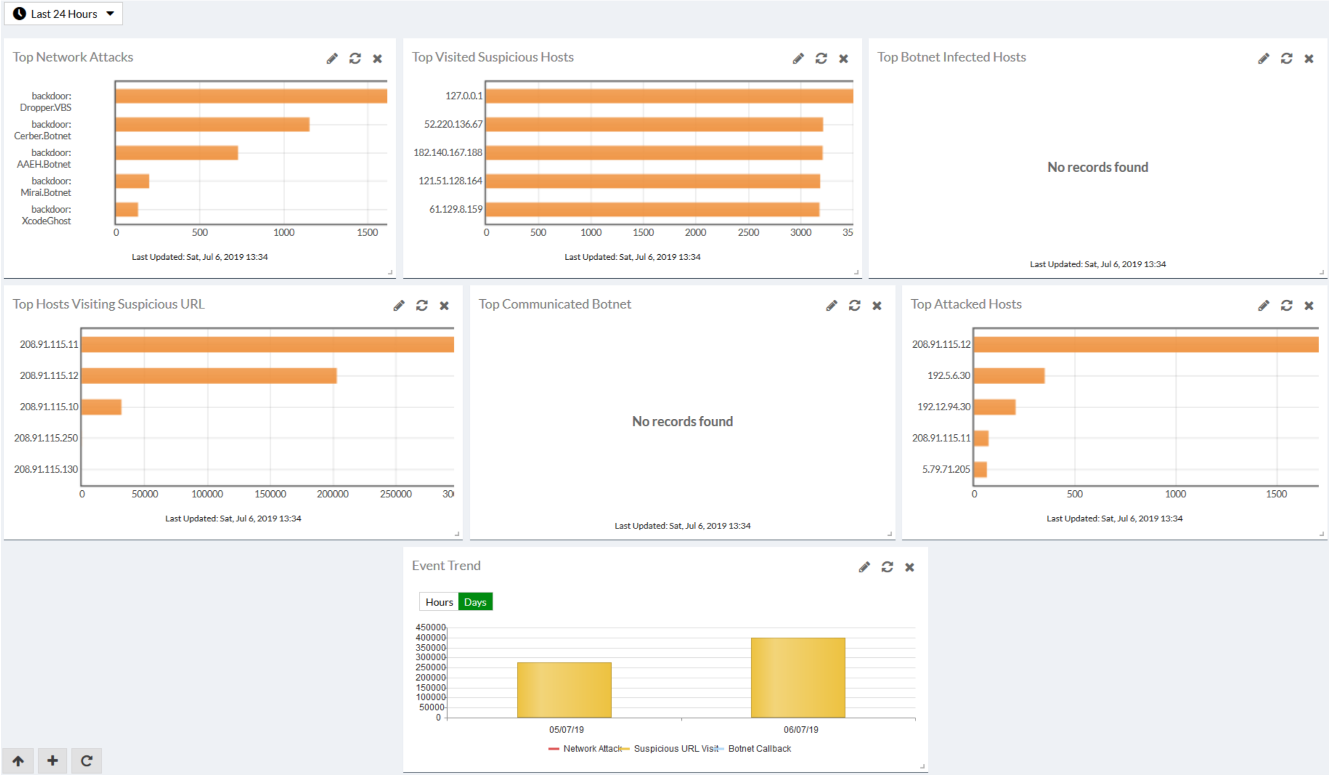
Network alerts show detected connection attempts to known botnets, attacks on hosts on your network, and harmful websites visited from your network. You must enable network alerts detection in *Scan Input > Sniffer*. Sniffed data is scanned by the IPS engine to populate data on this page. You can select 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 Report* 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.

Reset View	Click the *Reset* button to restore widgets to the default setting. A confirmation dialog box will be displayed, select *OK* to continue.
Time period	Select a time period to be displayed from the dropdown list. The options are: *Last 24 hours*, *Last 7 days*, *Last 4 weeks*.

The following widgets are available:

Event Trend	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.
Top Network Attacks	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.
Top Attacked Hosts	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.
Top Communicated Botnet	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.
Top Botnet Infected Hosts	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.
Top Visited Suspicious Hosts	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.
Top Hosts Visiting Suspicious URL	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.

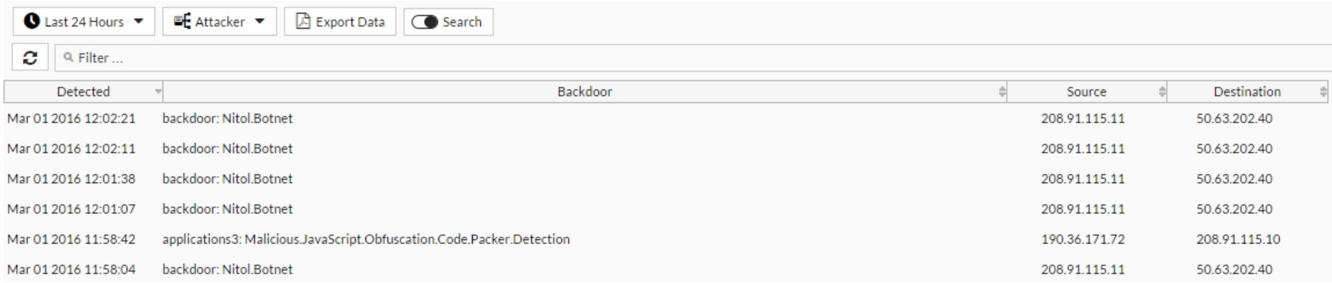
Configure the following information, and then select *OK* to apply your changes:

Custom widget title	Optionally, enter a custom title for the widget. Leave this field blank to use the default widget title.
Refresh interval	Enter a refresh interval for the widget, in seconds. Set the field to 0 to disable. The widgets have default refresh values: • *Event Trend*: 3600 seconds • *Top Network Attacks*: 3600 seconds • *Top Attacked Hosts*: 3600 seconds • *Top Communicated Botnet*: 3600 seconds • *Top Botnet Infected Hosts*: 3600 seconds • *Top Visited Suspicious URL Hosts*: 3600 seconds • *Top Hosts Visiting Suspicious URLs*: 3600 seconds
Top Count	Select the number of entries to display in the widget. The top count can be between 5 to 15 entries. This setting is available in all widgets except *Event Trend*.

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 Filtering Criteria section.



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:

Time Period		Select the time period from the dropdown list. Select one of the following: *24 Hours*, *7 Days*, or *4 Weeks*. 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.
Alert Type		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.
	Attacker	Shows attacks against hosts on your network. When selecting *Attacker* from the dropdown list, the following information is displayed: • Detected: The date and time that the attack was detected by FortiSandbox. • Backdoor: The name of the attack. • Source: The attacker's IP address. • Destination: The attacked host IP address. All columns include a filter to allow you to sort the entries in ascending or descending order.
	Botnet	Shows detected connections to knows botnets. When selecting *Botnet* from the dropdown list, the following information is displayed: • Detected: The date and time that the botnet contact was detected by FortiSandbox. • Name: The botnet name. • Source: The IP address of the infected host. • Destination: The botnet command and control IP address. The *Detected*, *Name*, and *Source* columns include a filter to allow you to sort the entries in ascending or descending order.
	URL	Shows visited suspicious websites from your network. When selecting *URL* from the dropdown list, the following information is displayed: • Detected: The date and time that the malicious URL was visited. • Rating: The severity of the visiting activity. • Category: The URL's web filtering category. • Host: The host IP address. The first level domain name of the URL. • URL: The visited URL address. • Type: The URL type, http or https • Source: The IP address of the host who visited the malicious URL. The *Detected*, *Category*, *Hostname*, *URL*, *Type*, and *Source* columns include a filter to allow you to sort the entries in ascending or descending order. **Tooltip**: Certain URL categories are set as *Benign* by default. To view and change, go to *Scan Policy > URL Category*.
Export Data		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 *Log & Report > Report Center* page.
Refresh		Click the icon to refresh the log message list.
Search		Show or hide the search filter field.

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

URL Detection > Summary Report is similar to the *System* dashboard. You can add and customize widgets. Select a time period to customize the data to display. This report does not include URLs submitted through On-Demand, RPC, and rescan.

The following options are available:

Add Widget	Click the + button to add widgets to the *Summary Report* page.
Reset View	Click *Reset* to restore widgets to the default setting.
Time Period	Select a time period from the dropdown list: *Last 24 hours*, *Last 7 days*, or *Last 4 weeks*.
Device	Filter for a specific device.

The following widgets are available:

Scanning Statistics	Information about the URLs scanned per OS. Click the number in the widget to drill down to the job list.
Scanning Statistics by Type	Information about URL types, rating, and event count.
Scanning Activity	Number of clean, suspicious, and malicious jobs. Hover the cursor over a colored portion of the graph to view the number of events. 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:

Custom widget title	Enter an optional, custom title for the widget. Leave this field blank to use the default title.
Refresh interval	Enter a refresh interval for the widget, in seconds. The default refresh values are: • *Scanning Statistics*: 3600 seconds • *Scanning Statistics by Type*: 3600 seconds • *Scanning Activity*: 300 seconds
Top Count	Number of entries to display in the widget from 5 to 20 entries. This setting is available in the *Top Infectious URLs* widget.

URL Scan

The *URL Scan* page shows jobs of URL-based scans grouped by their ratings. You can toggle to view jobs of different ratings. The default displays Suspicious jobs.

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	
Suspicious	Click the *Suspicious* icon to view the suspicious jobs.
Clean	Click the *Clean* icon to view the clean jobs.
Malicious	Click the *Malicious* icon to view the malicious jobs.
Refresh	Click the button to refresh the entries displayed.
Search	Show or hide the search filter field.
Add Search Filter	Click the search filter field to add search filters. When the search criteria is the *Submitted Filename*, 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.

Export Data		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 *Log & Report > Report Center* page.
Customize		Click the *Customize* button to customize the Job View Settings.
Action		
	View Details	Click the *View Details* icon to view the file description and analysis details. The information displayed is dependent on the file selected.
	FortiGuard Static Scan	The icon displays that the URL is rated by the user's overridden verdict or FortiGuard advanced static scan.
	Archive File	The icon displays that the URL is from a file through On-Demand scan.
	File Downloading URL	The icon displays that the URL is from FortiMail and its payload is also scanned as a file scan job.
	Perform Rescan	All suspicious items which are not rated by the VM can be rescanned. All malicious files can be rescanned. In the *Rescan Configuration* dialog box, you can customize the new scan's depth and timeout value. You can also force the URL to do Sandboxing scan even if was detected in former steps of the allowlist and blocklist check or stopped from entering VM by a Sandboxing-prefilter setting. Results are in *Scan Input > URL On-Demand* and *FortiView > URL Scan Search*.
Pagination		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 78.

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 version, the maximum number of events you can export to a PDF report is 1000. The maximum number of events you can export to a CSV report is 15000. Jobs over the maximum are not included in the report.

Log & Report

Use the Log & Report page to view and download all logs collected by the device, access scheduled reports, and generate reports. You can see logs local to FortiSandbox, or set up a remote log server, such as one linking to FortiAnalyzer.

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
Alert	Immediate action is required.	Suspicious URL visit domain.com from 192.12.1.12 to 42.156.162.21:80.
Critical	Functionality is affected.	System database is not ready. A program should have started to rebuild it and it shall be ready after a while.
Error	An erroneous condition exists and functionality is probably effected.	Errors that occur when deleting certificates.
Warning	Functionality might be affected.	Submitted file AVSInstallPack.exe is too large: 292046088.
Information	General information about system operations.	LDAP server information that was successfully updated.

Log Level	Description	Example Log Entry
Debug	Detailed information useful for debugging purposes.	Launching job for file. jobid=2726271637747836543 filename=log md5=ebe5ae2bec3b653c2970e8cec9f5f1d9 sha1=06ea6108d02513f0d278ecc8d443df86dac2885b sha256=d678da5fb9ea3ee20af779a4ae13c402585ebb070edcf20091cb20509000f74b

Raw logs

You can download and save raw logs to the management computer using the *Download Log* button. Raw logs are saved as a text file with the extension *.log.gz*. You 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=424c62eaaa4736740e43f5c7376ec6f209b0d3df0e0cadcc94324280eafa101f 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
```

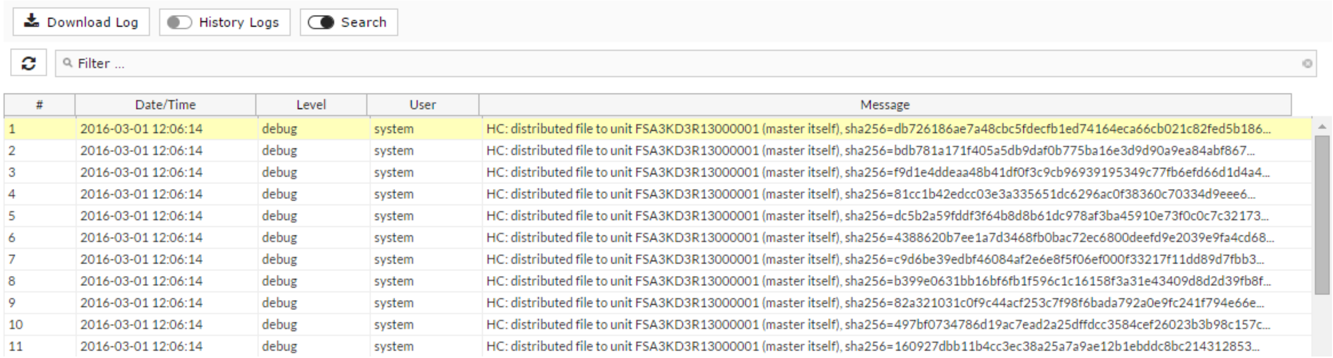
Fort detailed log format information, please refer to the *FortiSandbox 3.2.1 Log Reference* available on the Fortinet Document Library.

Log Categories

Logs are group into different categories:

All Events	All logs.
System Events	Logs related to system operation, such as user creation and FDN downloads.

VM Events	Logs related to guest VM systems, such as VM initialization.
Job Events	Logs related to scans. You can trace the scan flow of each file or URL.
HA-Cluster Events	Logs related to cluster configuration and failovers.
Notification Events	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=bdb781a171f405a5db9daf0b775ba16e3d9d90a9ea84abf867...
3	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=f9d1e4ddeaa48b41df0f3c9cb96939195349c77fb6efd66d1d4a4...
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=dc5b2a59fddf3f64b8d8b61dc978af3ba45910e73f0c0c7c32173...
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=c9d6be39edbf46084af2e6e8f5f06ef000f33217f11dd89d7fbb3...
8	2016-03-01 12:06:14	debug	system	HC: distributed file to unit FSA3KD3R13000001 (master itself), sha256=b399e0631bb16bf6fb1f596c1c16158f3a31e43409d8d2d39fb8f...
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:

Download Log	Download a file containing the raw logs to the management computer.
History Logs	Enable to include historical logs in Log Search.
Refresh	Refresh the log message list.
Add Search Filter	Add search filters. You can select different categories to search the logs. Search is not case sensitive.
Pagination	Jump or scroll to other pages. You can see the total number of pages and logs.

The following information is displayed:

#	Log number.
Date/Time	Time the log message was created.
Level	Level of the log message. Logging levels are: • Alert: Immediate action is required. • Critical: Functionality is affected. • Error: Functionality is probably affected. • Warning: Functionality might be affected. • Information: Information about normal events. • Debug: Information used for diagnosis or debugging.
User	The user to which the log message relates. User can be a specific user or system.
Message	Detailed log message.
Action	Action that was taken on the operation, such as *Update*, *Controller*, *Rescan*, and so on.
Status	Status of the log, such as *None*, *Success*, or *Failure*.
User Interface	User interface that was used, such as *GUI* or *System*.

Log Servers

FortiSandbox logs can be sent to a remote syslog server, common event type (CEF) server, or FortiAnalyzer. Go to *Log & Report* > *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:

Create New	Create a new log server entry.
Edit	Edit the selected log server entry.
Delete	Delete the selected log server entry.

This page displays the following information:

Name	Name of the server entry.
Server Type	Server type. The following options are available: CEF, syslog (TCP/UDP), or FortiAnalyzer.
Server Address	Log server address.
Port	Log server port number.
Status	Status of the log server, *Enabled* or *Disabled*.

To create a new server entry:

1. Go to *Log & Report* > *Log Servers*.
2. Click *Create New*.
3. Configure the following settings:

Name	Name of the new server entry.
Type	Select log server type from the dropdown list.
Log Server Address	Log server IP address or FQDN.
Port	Port number. The default port is 514.
Status	Select to enable or disable sending logs to the server.
Log Level	Select to enable the logging levels to be forwarded to the log server. The following options are available: • Enable Alert Logs. By default, only logs of non-Clean rated jobs are sent. To send Clean Job Alert Logs, select *Include job with Clean Rating*. • Enable Critical Logs • Enable Error Logs • Enable Warning Logs • Enable Information Logs • Enable Debug Logs

4. Click *OK*.

You can forward FortiSandbox logs to a FortiAnalyzer running version 5.2.0 or later.

To edit or delete a log server:

1. Go to *Log and Report* > *Log Servers*.
2. Select an event entry.
3. Click *Edit* or *Delete*.

Local Log

As there is a size limit of total logs that FortiSandbox can save locally, you can choose to turn off logs for specified severity levels.

To turn off logs from specific severity levels:

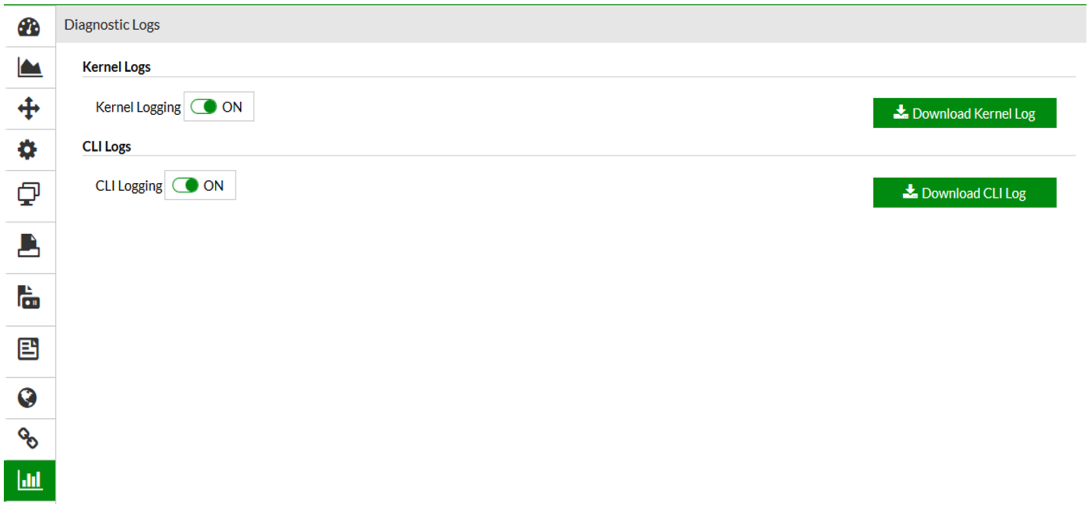
1. Go to *Log & Report* > *Local Log*.
2. Uncheck a level to turn off logs from that severity level.

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 button next to *Kernal Logging* or *CLI Logging* to enable or disable that logging.



Diagnostic Logs

Kernel Logs

Kernel Logging ON

CLI Logs

CLI Logging ON

Viewing logs in FortiAnalyzer

To view FortiSandbox logs in your FortiAnalyzer:

1. Log into FortiAnalyzer.
2. In the *Select an ADOM* prompt. select FortiSandbox.
3. Click the *Log View* tile.

The following options are available:

Add Filter	Enter a search term to search the log messages. You can also right-click an entry in a column and select to add a search filter. Click *GO* to apply the filter. Not all columns support the search feature.
Device	Select the device in the dropdown list.
Time Period	Select a time period from the dropdown list. Options include: *Last 30 mins*, *Last 1 hour*, *Last 4 hours*, *Last 12 hours*, *Last 1 day*, *Last 7 days*, *Last N hours*, *Last N days*, or *Custom*.
GO	Select to apply the time period and limit to the displayed log entries. A progress bar is displayed in the lower toolbar.
Column Settings	Select specific columns to be displayed. You can also reset the columns to its default.
Tools	*Tools* has options for changing how to display logs, options for search, and to add or delete column.
Real-time Log	FortiSandbox does not support *Real-time Log*.

	Display Raw	Select to change view from formatted display to raw log display.
	Download	This option is only available when viewing logs in formatted display. Click to download logs. Select the log file format, then compress with gzip the pages to include and select *Apply* to save the log file on the management computer.
	Case Sensitive Search	Select to enable case sensitive search.
	Chart Builder	Select to create a custom chart.
Display Details button		Detailed information about the log message selected in the log message list. The item is not available when viewing raw logs. *Log Details* are only displayed when enabled in the *Tools* menu.
Search Scope		Select the maximum number of log entries to be displayed from the dropdown list. Options include: *1000*, *5000*, *10000*, *50000*, or *All*.

This page displays the following information:

Logs	The columns and information shown in the log message list will vary depending on the selected log type and the view settings. Right-click 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.
Status Bar	Displays the log view status as a percentage.
Pagination	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.

   Case-sensitive search. Use the *Tools* dropdown list to specify case-sensitive search.
3. In the Device list, select a device.
4. In the Time list, select a time period.
5. Click *Go*.

To filter log summaries using the right-click menu:

In the log message list, right-click an entry, and select a filter criteria. The search criteria with a + (plus) icon returns entries that match the filter values, while the search criteria with a - (minus) icon returns entries that negate the filter values.

Right-click a column for Log View to use that column value as the filter criteria. This context-sensitive filter is not available for all columns.

For more 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 status, and the user who generated the report. You can download and delete the PDF reports.

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:

Generate Report	Generate a report.
Download Report	Download a report.
Refresh	Click the button to refresh the entries displayed.
Delete	Delete a report.

This page displays the following information:

Time Period	Time period of data the report includes.
Report Type	Type of report.
Size	Report size.
Status	Status of the report.
User	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:

Status	The status of report generation process: Done, Stopped, or In Progress.

Start Time	The time report generation starts.
Finish Time	The time report is ready.
Report Type	The type of report: PDF or CSV.
Report Size	The size of the report, in kilobytes.
Download Count	The number of times that the report has been downloaded.
Progress	Percentage that the report has finished
Source	The location that the report is scheduled to generate.
Detection Period	The time range of the jobs that this report contains.
Actions	You can view, delete, and download a report.
Pagination	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 the *View Details* icon, a new tab opens 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. The information is in three tabs: *Overview*, *Tree view*, and *Details*.

The *Overview* tab shows overview information of a job, including input source, scan conditions, file type, and so on. A global map shows the source and destination of the file or URL.

Item	Description
File type	File type, for example, *High Risk Downloader*.
Virus Name	Name of the virus.
FortiGuard Encyclopedia Analysis	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.
Mark as clean (false positive) / Mark as suspicious (false negative)	Select to mark the file as clean (false positive) or suspicious (false negative). This field is dependent on the file risk type. In the *Apply Override Verdict* dialog box type a comment and select *Submit* or *Submit feedback to Cloud* to send the file to the FortiGuard team for analysis. After a file has an overridden verdict, its future rating will be the overridden one until you reset the verdict. After a file's verdict is overridden, the job will be listed in the *Scan Profile > Overridden Verdicts* page for easy tracking.
Export Job Details to Page	Export the job details to a PDF report.
Download Original File	Download the password protected original file (`.zip` format) to your management computer for further analysis. The default password for this file is *fortisandbox*. ⚠ Unzip the original file only on a management computer in an analysis environment.
Received	The date and time the file was received by FortiSandbox.
Started	The date and time the scan started and the timezone.

Item	Description
Status	The status of the scan. Status: *Done*, *Canceled*, *Skipped*, and *Timed Out*.
Rated by	Which scan module made the rating decision, such as the AV Scanner, FortiSandbox Community Cloud, Static File Scan, or VM Engine.
Submit Type	The input source of the file such as FortiMail.
Source IP	The malware host IP address.
Destination IP	The IP address of the client that downloaded the virus.
Digital Signature	The digital signature availability status of the scanned file.
AI Mode	Whether AI mode is on or off.
Scan Bypass Configuration	When available, the scan bypass configuration will be displayed.
SIMNET	The SIMNET status when the scan is running.
Virus Total	By clicking the Virus Total link, a new page will open to query https://www.virustotal.com. Only a limited number of queries per minute is allowed without manual interaction with the Virus Total website.
The Original Job of this Rescan Job	Click the link to view the original job if this one is an AV rescan or On-Demand rescan job.
Details Information	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, No VM Reason (reason why sample was not scanned inside VM), Launched OS, Infected OS, and Anti Evasion Enabled. If the file is from FortiMail, Email related information, such as the Email Sender, Receiver, and Subject will also be shown.
Indicators	A summary of the Malware's behavior indicators if there are any.
Behavior Summary	View the file behavior summary.

The *Tree View* tab 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* tab 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
Analysis Details	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.

Item	Description
	If the Malware is detected by non-Sandboxing scan, such as FortiGuard static scan, the tab title is displayed as *N/A*.
Behavior Chronology Chart	View the file's behavior over time and its density during its execution. Clean behaviors: green bubble. Suspicious behaviors: red, blue, or orange bubble. The higher the bubble, the more serious the event is. To view the event details, hover the mouse on top of the bubble. If a file scan is scanned with more than one VM type, the VM tab will dynamically switch to the chart for that type. If the file hits any imported YARA rule, a YARA tab will appear with detailed information. including: • The hit rule • Rule's risk level • Rule set name • Link to original YARA rule file
Captured Packets	Select the *Captured Packets* 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. The *Captured Packets* button is not available for all file types.
Tracer Package	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 *fortisandbox*. ⚠ Unzip the tracer log only on a management computer in an analysis environment. To see all dropped files by the file being scanned, use the **-g** argument. This generates a file named filemap.txt in the backup directory of the tracer package.
Tracer Log	A text file containing detailed information collected inside the Sandbox VM.
STIX IOC	Download the IOC in STIX2 format.
Traffic Signature	Displays the signatures of industrial application network traffic that are detected. Click the name to go to its FortiGuard page.
IPS Signature	Displays IPS signatures that are detected, the signatures are displayed. Click the name to go to its FortiGuard page.
Screenshot	Download screenshot images when the file was running in the sandbox. This image is not always available.
YARA Hits	If the file hits FortiSandbox internal YARA rules, detailed information is displayed.

Item	Description
Office Behaviors	Suspicious indicators detected by FortiGuard advanced Office file static scan engine.
Virtual Simulator	Suspicious indicators detected by FortiGuard advanced Web file static scan engine.
Indicators	A summary of behavior indicators, if available. 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.
MITRE ATT&CK Matrix	Displays malware's attack techniques and tactics. By default, a light version is displayed. Click the toggle button to swap between the Lite Matrix and Full Matrix.
Botnet Info	The botnet name and target IP address.
Files Created	The executable has been observed to drop some files. Click the *Files Created* dropdown icon to view the files created by the file. This field may not be available for all file types.
Files Deleted	This executable has been observed to delete some files. Click the *Files Deleted* dropdown icon to view the files deleted by the file. This field may not be available for all file types.
File Modified	The executable file has been observed to modify some files.
Launched Processes	The executable spawns some processes. Click the *Launched Processes* dropdown icon to view the processes launched by the file. This field may not be available for all file types.
Registry Changes	The executable applies autostart registry modifications to be able to start itself automatically. Click the *Registry Changes* dropdown icon to view the registry changed made by the file. This field may not be available for all file types.
Network Behaviors	Users that are infected by this executable will notice HTTP connections with certain URL/IP addresses. Click the *Network Behaviors* 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.
Behaviors In Sequence	The executable file's behavior during execution, in time sequence.
Tracer/Rating Engine Version	The tracer/rating package version is displayed at the bottom of the job detail page and in the PDF Report.

Change Log

Date	Change Description
2020-08-20	Initial release.
2020-08-27	Removed unused Event Calendar section.
2020-09-22	Updated General on page 100.
2020-09-28	Updated Administrators on page 57 that two-factor authentication is not available for FortiSandbox VM.
2020-10-16	Updated screenshot in LDAP Servers on page 66.
2020-11-30	Updated Primary's role and worker's role on page 168.
2021-01-12	Updated *Server Type* in Log Servers on page 195.
2021-02-11	Deleted appendices regarding creating custom VMs using pre-configured VMs, your own ISO image, and Red Hat VMs on VirtualBox. For information about these functions, contact Fortinet Customer Service & Support. Deleted appendices regarding hard disk hot-swapping procedure, system recovery procedure using Rescue Mode, and password reset procedure. For information about these functions, see the FortiSandbox Best Practices and Troubleshooting Guide in the Fortinet Document Library.
2021-05-11	Updated Configuring the SNMP agent on page 72.
2021-06-04	Added note to Global Network on page 113.