FortiSandbox - Administration Guide

Version 2.5.1

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

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

FEEDBACK
Email: techdocs@fortinet.com

February 26, 2018
FortiSandbox 2.5.1 Administration Guide
34-251-467529-20180226

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-01-17	Initial release.
2018-01-18	Added a note to *Scan Profile* > *File Types*.
2018-01-22	Added Golden Image and Master Image statement to Appendix E.
2018-02-26	Added HA Cluster Topology diagram to *HA Cluster* > *Configure a cluster level fail-over IP set for Master unit* > *HA Cluster CLI Commands* > *What happens during a failover*.

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.

Fortinet's dynamic scanning is based on our custom Compact Pattern Recognition Language (CPRL) and ASIC hardware acceleration. The result is fast, powerful detection, unique to Fortinet, that uses a single signature to identify tens of thousands of variations of viral code. 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 pre-defined schedule, quarantine malicious files, and receive files from FortiGate, FortiWeb, FortiMail, and FortiClient. For example, FortiMail 5.2.0 and later allows you to forward email attachments to FortiSandbox for advanced inspection and analysis. Files can also be uploaded directly to it for sandboxing through the web GUI or JSON API. You can also submit a website URL to scan to help you identify web pages hosting malicious content before users attempt to open the pages on their host machines.

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

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

Infection Type	Description
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.
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.

Infection Type	Description
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 purposes.
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 incident response.
- Network Alert: Inspects network traffic for requests to visit malicious sites, establish communications with C&C servers and other activity indicative of a compromise. It provides a complete picture of the victim host's infection cycle.
- Manual analysis: Allows security administrators to manually upload malware samples via the FortiSandbox web GUI or JSON API to perform virtual sandboxing without the need for a separate appliance.
- Optional submission to FortiSandbox Community Cloud: Tracer reports, malicious files and other information may be submitted to FortiSandbox Community Cloud in order to receive remediation recommendations and updated in line protections.
- Schedule scan of network shares: Perform a schedule scan of network shares in Network File System (NFS) v2 to v4 and Common Internet File System (CIFS) formats to quarantine suspicious files.
- Scan job archive: You can archive scan jobs to a network share for backup and further analysis.
- Website URL scan: Scan websites to a certain depth for a predefined time period.
- Cluster supporting High Availability: Provide a non-interruption, high performance system for malware detection.

This section includes the following topics:

What's new in FortiSandbox 2.5.1

To view a detailed list of the new features and enhancements in FortiSandbox 2.5.1, please see the FortiSandbox 2.5.1 Release Notes available at the Fortinet Document Library.

About this document

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

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

To configure your FortiGate device to submit files to FortiSandbox, your FortiGate must be running FortiOS or FortiOS Carrier version 5.0.4 and later or 5.2.0 and later.
For more information, see *The FortiOS Handbook* in the Fortinet Document Library.

To configure your FortiMail email gateway to identify suspicious or high risk files in email and submit them to FortiSandbox, your FortiMail must be running FortiMail version 5.2.0 and later.
For more information, see the *FortiMail 5.2 Administration Guide* in the Fortinet Document Library.

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

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

Connecting to the Command Line Interface

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

To connect to the CLI through the console port:

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

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* available in the Fortinet Document Library.

Using the GUI

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

This section includes the following topics:

GUI overview

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

Connecting to the GUI

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

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

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

To connect to the FortiSandbox GUI:

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

   You can now proceed with configuring your FortiSandbox unit.

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

Default Port Information

FortiSandbox treats Port1 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	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 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. The Sandbox Community Cloud uses UDP port 53 or 8888 and TCP port 443. 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.
Port3	RJ-45	No service listens. Reserved for guest VM to communicate with the outside network.
Port5, Port6	SFP+	No service listens except OFTP.

FortiSandbox 3000D default ports

Port (Interface)	Type	Default Open Ports
Port1	RJ-45	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 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. The Sandbox Community Cloud uses UDP port 53 or 8888 and TCP port 443. 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	All ports are open.
Port3	RJ-45	All ports are open. Reserved for guest VM to communicate with the outside network.
Port5, Port6	SFP	All ports are open.
Port7, Port8	SFP+	All ports are open.

FortiSandbox 1000D default ports

Port (Interface)	Type	Default Open Ports
Port1	RJ-45	22 (SSH), 23 (Telnet), 80 and 443 (GUI), 514 (OFTP communication with FortiGate, FortiWeb, FortiClient & FortiMail). FortiGuard Distribution Servers (FDS) use 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. The Sandbox Community Cloud uses UDP port 53 or 8888 and TCP port 443. 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, Port5, Port6	RJ-45	All ports are open.
Port3	RJ-45	All ports are open. Reserved for guest VM to communicate with the outside network.
Port7, Port 8	SFP	All ports are open.

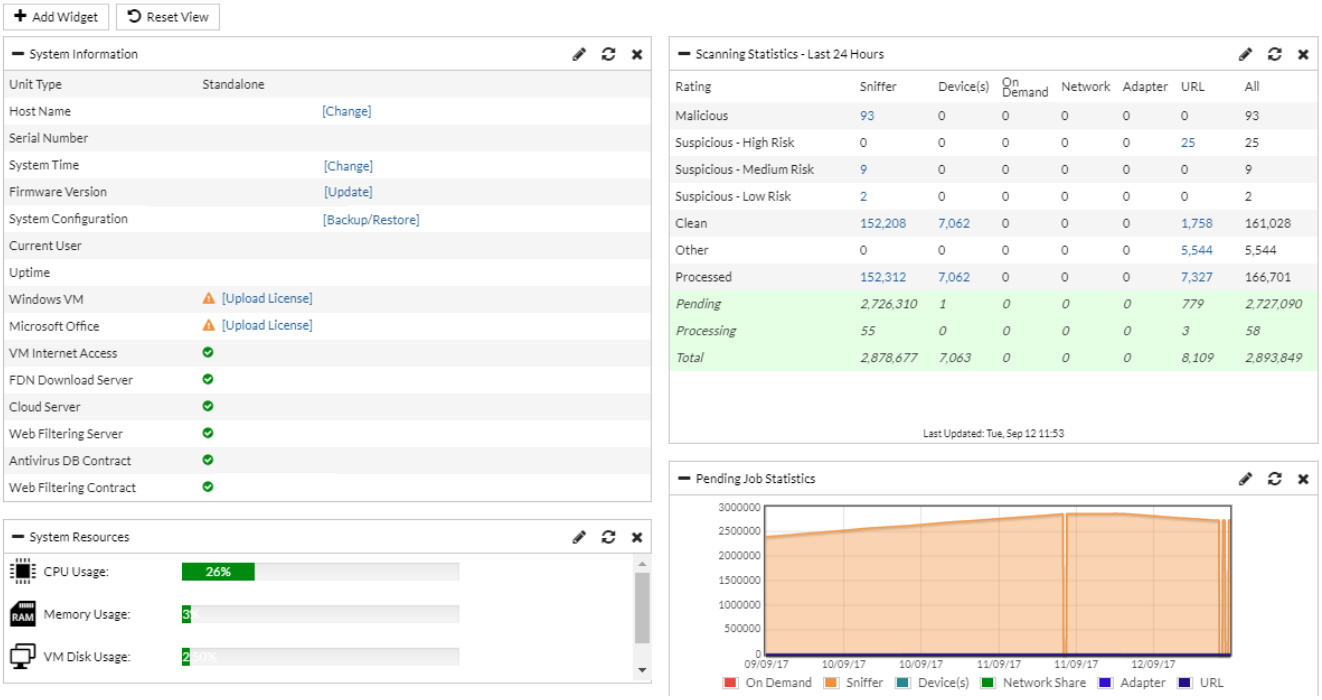
All ports mentioned above are the same for both IPv4 and IPv6 protocols..

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

For more information on FortiSandbox 1000D, FortiSandbox 3000D, FortiSandbox 3500D, FortiSandbox 2000E, and FortiSandbox 3000E interfaces, see Interfaces on page 73.

Dashboard

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



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

The following widgets are available:

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. Hover the cursor over the memory dial to view the total system 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.

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.

This section includes the following topics:

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 add a widget

In the 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 on page 23
- System Resources on page 25
- Scanning Statistics on page 26
- Scanning Activity on page 28
- Top Devices on page 29
- Top Critical Logs on page 30
- Pending Job Statistics on page 31
- Disk Monitor on page 32
- Sniffer Traffic Throughput on page 33

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

To edit a widget

Select the edit icon in the widget's title bar to open the edit widget window.

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 drop-down list. The options are: *Last 24 hours*, *Last 7 days*, *Last 2 weeks*. This option is only available on the following widgets: *Scanning Statistics*, *Top Devices*, *Disk Monitor*, and *Scanning Activity*.
Expand the right panel to full screen	Click the *Full Screen* button located in the upper right corner to toggle and only view the right side content.

System Information

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

This widget displays the following information and options:

Unit Type	The HA cluster status of the device: *Standalone*, *Master*, *Primary Slave*, or *Regular Slave*. Select *[Change]* to change the cluster status of the device.
Host Name	The name assigned to this FortiSandbox unit. Select *[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. To update the firmware, you must download the latest version from the Fortinet Customer Service & Support portal. Select *[Update]* and select the firmware image to load from the local hard disk or network volume.
System Configuration	The date and time of the last system configuration backup. Select *Backup/Restore* to browse to the *System Recovery* page.
System Utilities Version	The current sandbox engine version. Select *[Update]* to go to the FortiGuard Modules page, where you can upload package files. In this page, you can also override the FortiGuard server address.
Current Administrator	The administrator that is currently logged on to the system.
Uptime	The duration of time that the FortiSandbox unit has been running since it boot up.
Windows VM	Microsoft Windows VM license activation and initialization status. Displays an up icon if the Microsoft Windows VM is activated and initialized. Displays a *Caution* icon if the Microsoft Windows VM is initializing or having issues. Hover the mouse pointer on the status icon to view detailed information. 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 needs 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. Displays an up icon if the Microsoft Office is activated and initialized. Displays a *Caution* icon if the Microsoft Office is initializing or having issues. Hover the mouse pointer on the status icon to view detailed information. A warning is displayed when the license file is not available or has not been uploaded to FortiSandbox.
VM Internet Access	Displays the status of the FortiSandbox VM accessing the outside network. Displays an up icon if the VM can access the outside network. Displays a caution icon if the VM cannot access the outside network. Hover the mouse pointer on the status icon to view detailed information. If the VM cannot access the outside network, a simulated network (SIMNET) will start by default. SIMNET provides responses of popular network services, like `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 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*.
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 warning icon will appear.
Web Filtering Contract	The date that the web filtering contract expires. If the contract expires within 15 days, a warning icon will appear.
MacOS VM Contract	The date that the MacOS contract expires, and number of remote clones reserved in Fortinet MacOS cloud. In Cluster mode, the total reserved clone numbers will be displayed on the Master node. All cluster units share collected reserved clones from each unit. This means even a node that has no MacOS VM contract purchased, it can still upload MacOSX files to cloud to scan.

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 shutdown 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.

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 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 to job queue but have not been processed yet.
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 Master node of a cluster, the numbers in this widget are the total numbers of all cluster nodes.

Scanning Activity

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

If the time interval is set to *Last 24 hours*, a bar will be shown for each hour. If it is set to *Last 7 days* or *Last 2 weeks*, a bar will be shown for each day.

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 2 weeks.

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 total number of pending jobs for on-demand, sniffer, and network share for the past 72 hours.

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.

Select the edit icon to type a custom widget title and enter the refresh interval. The default refresh interval is 900 seconds.

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.

Dashboard Settings

Change the system host name

The *System Information* widget will display the full host name. However, if the host name is longer than 16 characters, the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed. 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 in to 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 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:

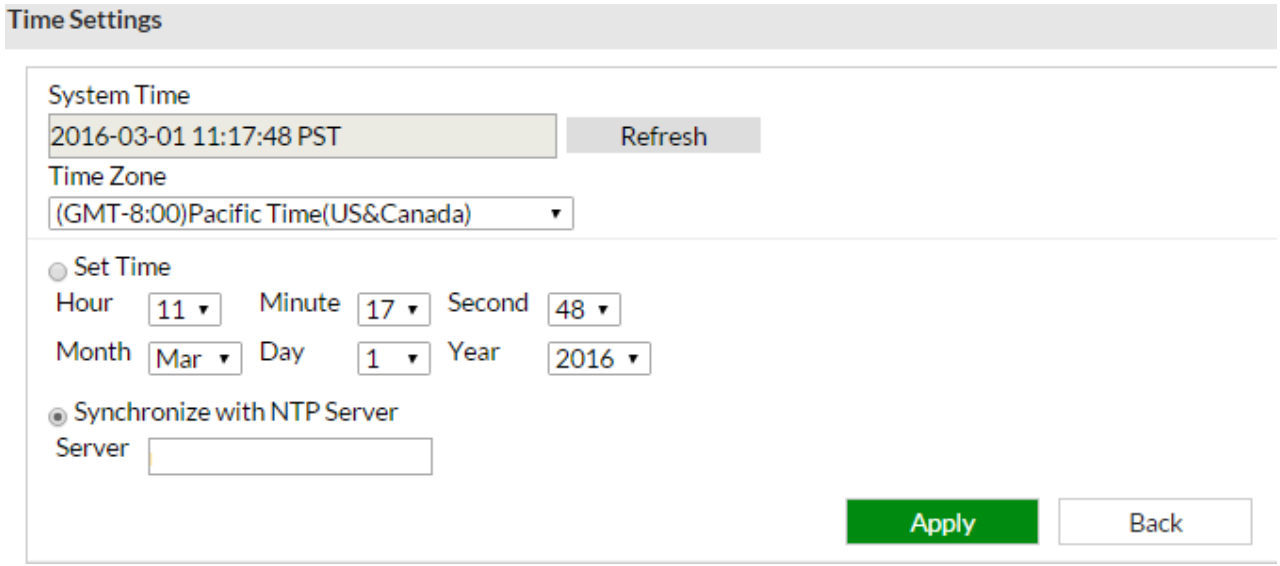
1. Go to *System* > *Admin* > *Settings*.
2. Change the idle timeout minutes (1 to 480 minutes) as required.
3. Select *OK* to save the setting.

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.

1. In the *System Information widget* > *System Time*
2. Click *[Update]*.



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 Microsoft Windows VM license used by the sandbox 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 to add Windows 8 or 10 support, 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. 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 drop down to log out of your administrative session.

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

Visit online help

Click the *Help* icon to visit Online Help.

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.
- 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 shutdown the unit

Always reboot and shutdown 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.

   Upon reboot, some databases may take up to ten minutes to be populated.
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 shutdown the FortiSandbox unit:

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

Backup or restore the system configuration

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

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

To backup the FortiSandbox configuration:

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 restore the FortiSandbox configuration:

1. Go to *Dashboard* >*System Information widget* > *System Configuration*.
2. Select *Backup/Restore*.
3. Click *Choose File*, locate the backup file on your management computer, then select *Restore* to load the backup file.
4. Select *OK* in the confirmation dialog box. The system configuration restore process has been started, you will be redirected to the login page once it has completed.

By performing a system restore, all of your current configurations will be replaced with the backup data. The system will reboot automatically to complete the restore operation. Only backup configuration from the previous or same release is supported.

To restore a backup configuration from to a unit in Cluster mode, you will need to change it to Standalone mode first.

FortiView

The FortiView menu provides access to the following menus:

The FortiView pages allow you to view and search threats detected by FortiSandbox.	
Operation Center	In this page you are able to view malware, which have been detected and what the status is 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 filename 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.
Event Calendar	A calendar view of major events, including user login/logout, scan condition changes and threat detection.
File/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 filename you can also do a pattern search.

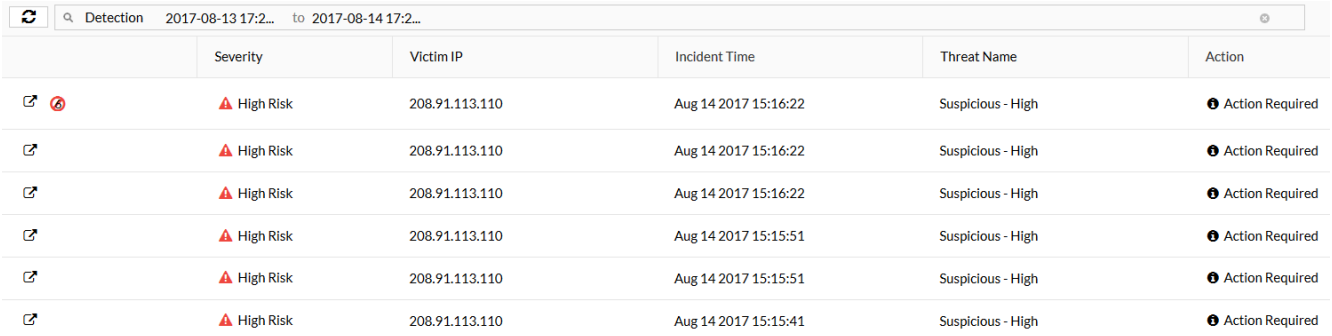
This section includes the following topics:

Operation Center

In this page you are able to view newly detected malware, which have been detected and what the status is from a security update perspective.

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

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



The following options are available:

Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.
Search	Show or hide the search filter field.
Time Period	Select the time period from the drop-down 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 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. Do not close the dialog box or navigate away from the page during report generation.
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, several fields, like victim host IP can be the search criteria. Search filters can be used to filter the information displayed in the GUI.
View Job	Click the *View Jobs* icon 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 occurrence of it. Hover your cursor on top of the icon, the number of blocks of this Malware is displayed.

In Cloud	An icon will appear if the malware is available in the FortiSandbox Community Cloud.
In Signature	An icon will appear if the malware is included in the current FortiSandbox generated Malware Package.
Perform Rescan	An icon will appear if the malware has a Malicious rating. Users can perform a Rescan to obtain its Sandboxing behavior details.
Archived File	An icon will appear if the file is an Archived File.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

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

To view file details:

1. Select a file.
2. Click the click the *View Details* icon. A new tab will open.
3. See Appendix A - View Details Page Reference on page 252 for descriptions of the *View Details* page.
4. Close the tab to exit the *View Details* page.

Threats by Topology

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

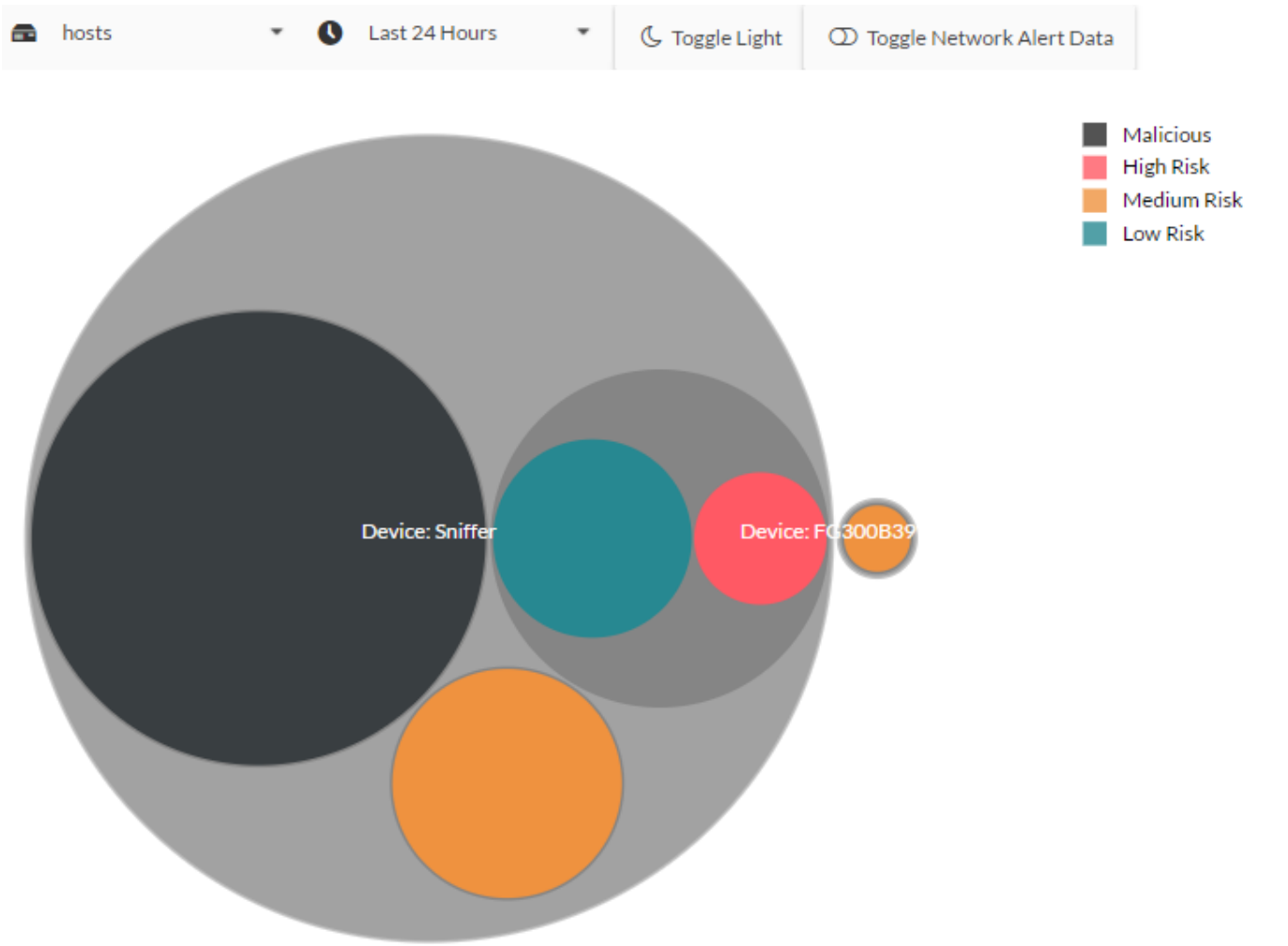
Devices (or input sources) are displayed in separated top level circles and the threats that occur on them are displayed inside them as second level circles. The radius of threat circle is proportional to threat event counts. Threat circles can be multiple levels and each level represents a subnet level.

Clicking on circles will drill down to the host level. At the host level, clicking on 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 drop-down list. Select one of the following: *24 Hours*, *7 Days*, *4 Weeks*, or *All*.
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.


hosts
Last 24 Hours
Toggle Light
Toggle Network Alert Data
Malicious
High Risk
Medium Risk
Low Risk
Device: Sniffer
Device: FG300B39

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 drop-down list. Select one of the following: 24 Hours, 7 Days, or 4 Weeks.
Export Data	Click the *Export Data* button to create a PDF or CSV snapshot report. Do not close the dialog box or navigate away from the page during report generation.
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. 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. For more information about user management, SSO, and VDOMs see *The FortiOS Handbook* located in the Fortinet Document Library.
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 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: 1. Click the *View Jobs* > *View Details* icons to drill down the entry. 2. 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* > *View Details* icons 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 select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click *OK* to continue. Click the close icon or select the *Close* button to close the dialog box. This feature is only available for files with a malicious rating.
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, destination IP address, and domain name, if available. 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, domain name, and number of detection times, if available.

Threats by Hosts - level 4

For more information on the information available in the *View Details* pages for malicious and suspicious files, see Appendix A - View Details Page Reference on page 252.

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* drop-down 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.
7. Click the *Cancel* button, to exit the report generator.

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

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 drop-down list. Select one of the following: *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 of Time Period drop-down. The time to generate the report is dependent on the number of events selected. Do not close the dialog box or navigate away from the page during report generation.
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. 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 by the 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 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	Select 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 select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click *OK* to continue. Click the close icon or select the *Close* button to close the dialog box. This feature is only available for files with a malicious rating.
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 information on about the information available in the View Details pages for malicious and suspicious files, See Summary Report on page 218

To create a snapshot report for all threats by files:

1. Select a time period from the first drop-down 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.
6. When the report generation is completed, select the *Download* button to save the file to your management computer.
7. Click the *Cancel* button, to exit the report generator.

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

Threats by Devices

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

Threats by Devices - level 1

The following options are available:

Time Period	Select the time period from the drop-down list. Select one of the following: *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 of Time Period drop-down. The time to generate the report is dependent on the number of events selected. Do not close the dialog box or navigate away from the page during report generation.
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. 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:

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 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 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	Select 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 select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click *OK* to continue. Click the close icon or select the *Close* button to close the dialog box. This feature is only available for files with a Malicious rating.
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 on the information available in the *View Details* pages for malicious and suspicious files, see Appendix A - View Details Page Reference on page 252.

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.

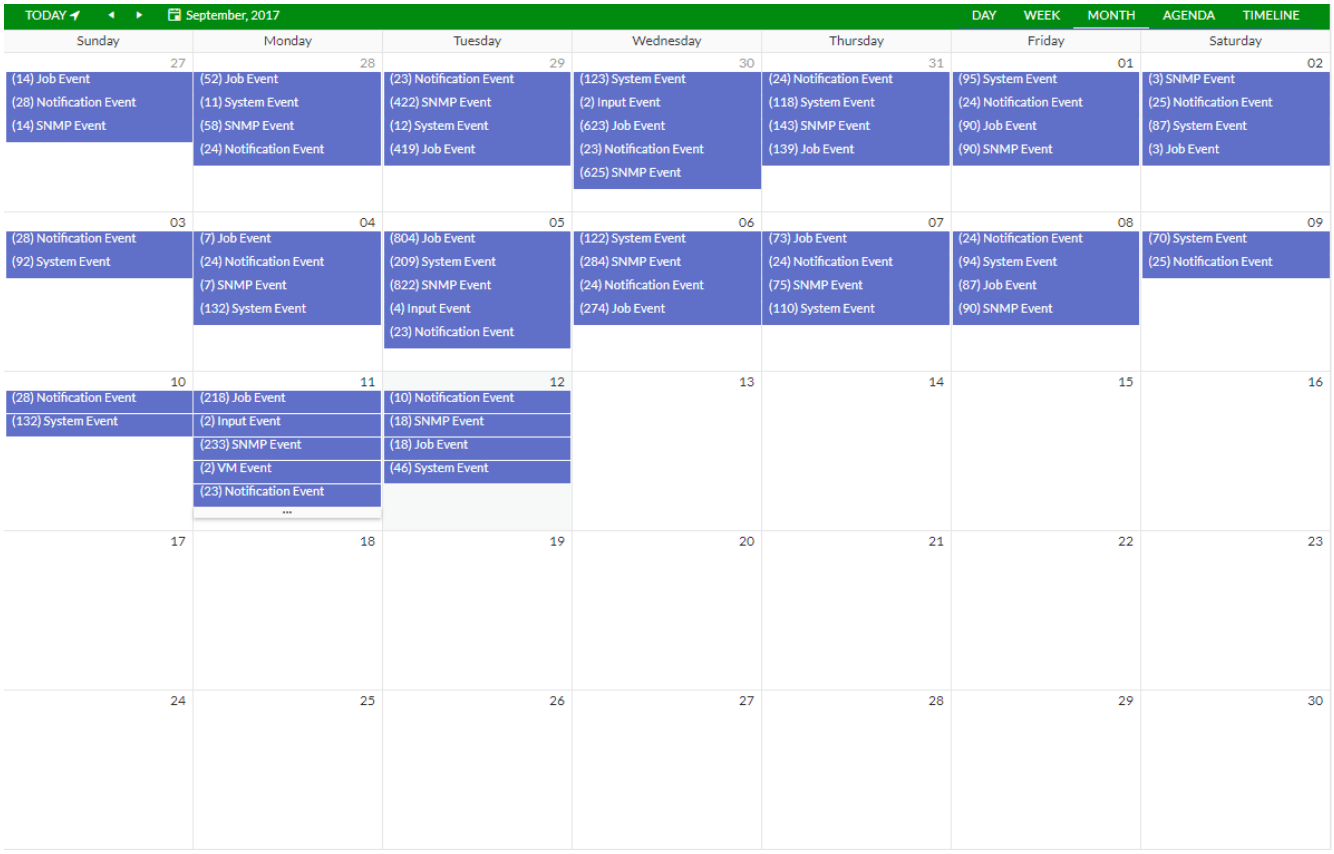
To create a snapshot report for all threats by devices:

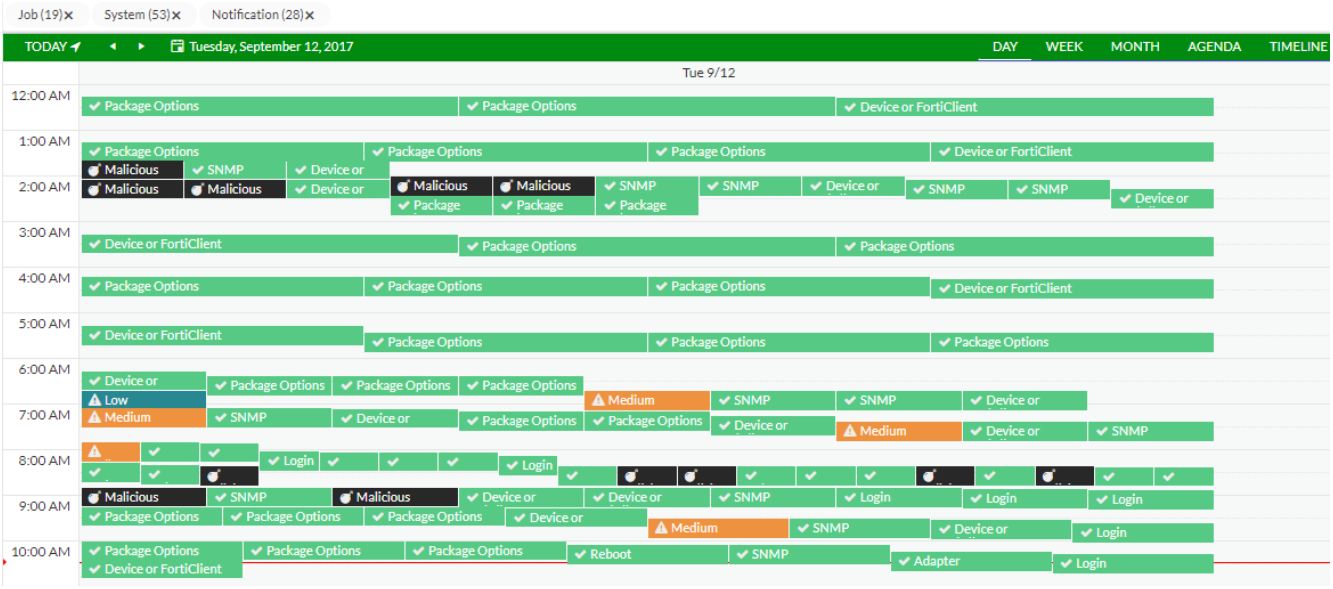
1. Select a time period from the first drop-down list.
2. Select to apply search filters to further drill down the information in the report.
3. Click the *Export Data* button in the toolbar. The *Report Generator* window opens.
4. Select either PDF or CSV for the report type. Optionally you can further define the report start/end date and time.
5. Click the *Generate Report* button to create the report.
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 PDF report is 5,000; the maximum number of events you can export to CSV report is 150,000.

Event Calendar

This page displays major events. You can show your events in a day, week, month, or timeline format. You can drill down to *day* level and click each event for its details. You can also show scheduled jobs like PDF reporting in the *Agenda* tab.





The following options are available:

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

The following events are displayed:

System Events	• System login/logout • Reboot/shutdown • Firmware upgrade • System critical errors • System configuration changes (includes user creation, scan profile change etc.)
Notification Events	• PDF report generation • Network share scan
Threat Events	• Malware/URL detection. Double clicking on the event will show its detailed information in a new browser tab.

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 and domains can also be searched based on name patterns, and a snapshot report can be created for all search results.

If the device is the Master node of a cluster, all jobs processed by the cluster are available to be searched. If the device is a Slave 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. During generation, do not close the dialog box or navigate away from the page.
Customize		Click the *Customize* icon to customize the Job View settings page. Go to Job View Settings on page 107 for more information.
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 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 customized rescan job of the Malicious file.
	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.

Perform Rescan	Click the icon to rescan the entry. In the *Rescan Configuration* dialog box you can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click *OK* to continue. Click the close icon or select the *Close* button to close the dialog box. This feature is only available for files with a Malicious rating.
Pagination	Use the pagination options to browse entries displayed.

The following information is displayed:

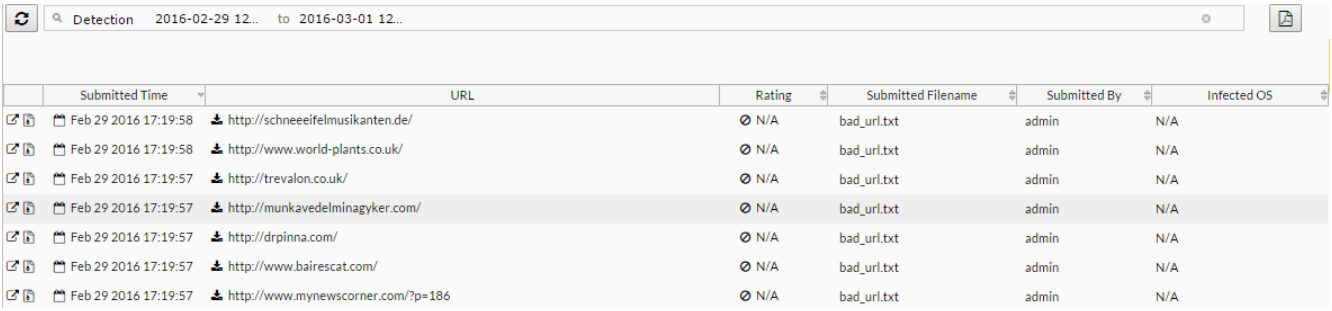
Total Jobs	The number of jobs displayed and the total number of jobs.

The displayed columns are determined by settings defined in *System* > *Job View Settings* > *File Detection Columns* page. Go to Job View Settings on page 107 for more information.

URL Scan Search

To view all URLs 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 Master node of a cluster, all jobs processed by the cluster are available to be searched. If the device is a Slave 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 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.
Customize		Click the *Customize* icon to customize the Job View settings page. Go to Job View Settings on page 107 for more information.
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 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 FortiMail, and its payload is also scanned as a file scan job.
	Perform Rescan	Click the icon to rescan the entry. In the Rescan Configuration dialog box you can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click *OK* to continue. Click the *Close* icon or the *Close* button to close the dialog box. This feature is only available for URLs with a Malicious rating.
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. Go to Job View Settings on page 107 for more information.

Network

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

This section includes the following topics:

Interfaces

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

This page displays the following information and options:

Interface	The interface name and description, where applicable. Failover IP will be listed under this field with the following descriptor: *(cluster external port)*.
port1 (administration port)	port1 is hard-coded as the administration interface. You can select to enable or disable HTTP, SSH, Telnet access rights on port1. HTTPS is enabled by default. port1 can be used for Device mode, although a different, dedicated port is recommended.
port2	port2 can be used for Sniffer mode, Device mode, and 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. It is recommended to put this interface on an isolated network behind a firewall. One special type of outgoing communication from a guest VM is used to connect to the Microsoft Windows activation server to activate the Windows Sandbox VM product keys. You must enable *Allow Virtual Machines to access external network through outgoing port* and setup the next hop gateway and DNS server to allow files running inside VMs to access the external network.
port4	port4 can be used for Sniffer mode, Device mode, and inter-node communication within a cluster.
port5/port6	port5 and port 6 can be used for Sniffer mode, Device mode, and inter-node communication within a cluster. On FortiSandbox 2000E, 3000E and 3500D devices, port5 and port6 are 10G fiber ports. It is recommended that they be used on a master node/primary slave as communications ports with the cluster slaves.

port7/port8	port7 and port8 can be used for Sniffer mode, Device mode, and inter-node communication within a cluster. On FortiSandbox 3000D devices, port7 and port8 are 10G fiber ports. It is therefore recommended that they be used on a master node/primary slave as communications ports with the cluster slaves.
IPv4	The IPv4 IP address and subnet mask of the interface.
IPv6	The IPv6 IP address and subnet mask of the interface.
Interface Status	The state of the interface, one of the following states: • Interface is up • Interface is down • Interface is being used by sniffer
Link Status	The link status. • Link up • Link down
Access Rights	The access rights associated with the interface. HTTPS is enabled by default on port1. You can select to enable HTTP, SSH, and Telnet access on port1.
Edit	Select the interface and select *Edit* from the toolbar to edit the interface.

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

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

For more information on FSA-1000D, FSA-3000D, FSA-2000E, FSA-3500D, FSA-3000E ports, see Default Port Information on page 16 .

Edit an interface

The IPv4/IPv6 address of an interface can be edited by selecting the interface name and clicking the *Edit* button from the toolbar.

Edit the IP address as required, then click *OK* to apply the changes. You can also change the interface status from *Up* to *Down* .

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

Edit administrative access

The port1 interface is used for administrative access to the FortiSandbox device. HTTPS is enabled by default, but you can edit this interface to enable HTTP, SSH, and Telnet support.

Edit the IP address and the access rights as required, then click *OK* to apply the changes.

Failover IP

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

The Master node and Primary Slave node local IP will be kept during failover.

Example:

Here is an example to set a fail-over 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* > *DNS* . FortiSandbox is configured to use the FortiGuard DNS servers by default.

Static Routing

The static routing page allows you to manage static routes on your FortiSandbox device. Go to *Network* > *Static 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 select *Edit* in the toolbar to edit the entry.
Delete	Select a static route in the list and select *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.

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.

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

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.

Delete a static route or routes:

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

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

System

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

The System menu provides access to the following menus:

Administrators	Configure administrator user accounts.
Admin Profile	Configure user profiles to define user's privileges
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 value for the Web UI and CLI interface and Web UI language. You can also reset all widgets to their default state.
Job View Settings	Define columns and orders of job result tables.

Some menus are not displayed on the Slave Nodes in a cluster.

This section includes the following topics:

Administrators

The Administrators menu allows you to configure administrator user accounts.

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

The following options are available:

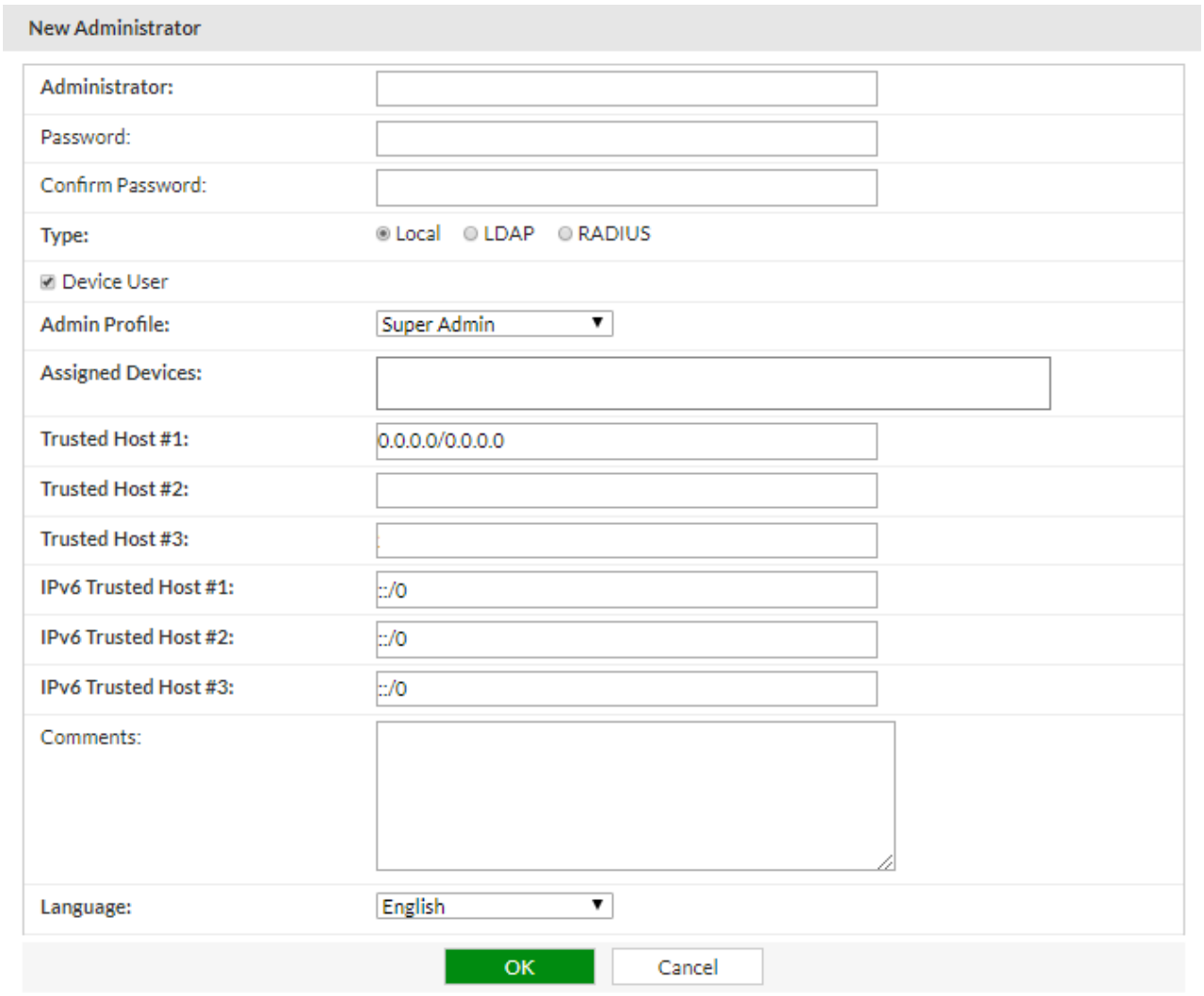
Create New	Select to create a new administrator account.
Edit	Select an administrator account from the list and select *Edit* in the toolbar to edit the entry.
Delete	Select an administrator account from the list and select *Delete* in the toolbar to delete the entry.
Test Login	Select a LDAP/RADIUS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

The following information is displayed:

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

Create a new user:

1. Login as a user whose Admin Profile has *Read/Write* privileges under *System* > *Admin access*, and go to *System* > *Administrators* .
2. Select + *Create New* from the toolbar .



3. Configure the following:

Administrator	Enter a name for the new administrator account. The administrator name must be 1 to 30 characters long and may only contain upper-case letters, lower-case letters, numbers, and the underscore character _.
Password	Enter a password for the account. The password must be 6 to 64 characters long and may contain upper-case letters, lower-case letters, numbers, and special characters. This field is available when *Type* is set to *Local* .
Confirm Password	Confirm the password for the account. This field is available when *Type* is set to *Local*.
Type	Select either Local, LDAP, or RADIUS.
LDAP Server	When *Type* is *LDAP*, select the LDAP server from the drop-down list. For information on creating an LDAP server, see LDAP Servers on page 92.

RADIUS Server	When *Type* is *RADIUS*, select the RADIUS server from the drop-down list. For information on creating a RADIUS server, see RADIUS Servers.
Device User	Tick the checkbox when user will be assigned devices. When the user logs in, only jobs belonging to the assigned devices or VDOMs/Protected Domains will be visible.
Admin Profile	Select the Admin Profile the user belongs to.
Assigned Devices	Assigned devices and/or VDOMs/Protected Domains to the user when the user is set to *Device User*. When the user clicks the panel, an Available Devices panel will slide out from the right side. This panel lists all available devices and VDOMs/Protected Domains. Users can assign devices and VDOMs/Protected Domains to the user by clicking the device serial number or VDOM/Protected Domains name. Users can also add or delete user defined devices which have not been seen by the FortiSandbox unit. After editing, click outside the device panel to accept the changes.
Trusted Host 1, Trusted Host 2, Trusted Host 3	Enter up to three IPv4 trusted hosts.
Trusted IPv6 Host 1, Trusted IPv6 Host 2, Trusted IPv6 Host 3	Enter up to three IPv6 trusted hosts.
Comments	Enter an option description comment for the administrator account.
Language	Set the GUI language for the user, either *English* or *Japanese*.

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

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

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 name of the user you would like to edit and select *Edit* from the toolbar.
3. Edit the account as required and then re-type the new password in the confirmation field.
4. Click *OK* to apply the changes.

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

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

Delete one or more user accounts:

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 account you want to delete.
3. Select *Delete* from the toolbar.
4. Select *Yes, I'm sure* in the confirmation page to delete the selected user or users.

LDAP/RADIUS user test login:

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

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

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.

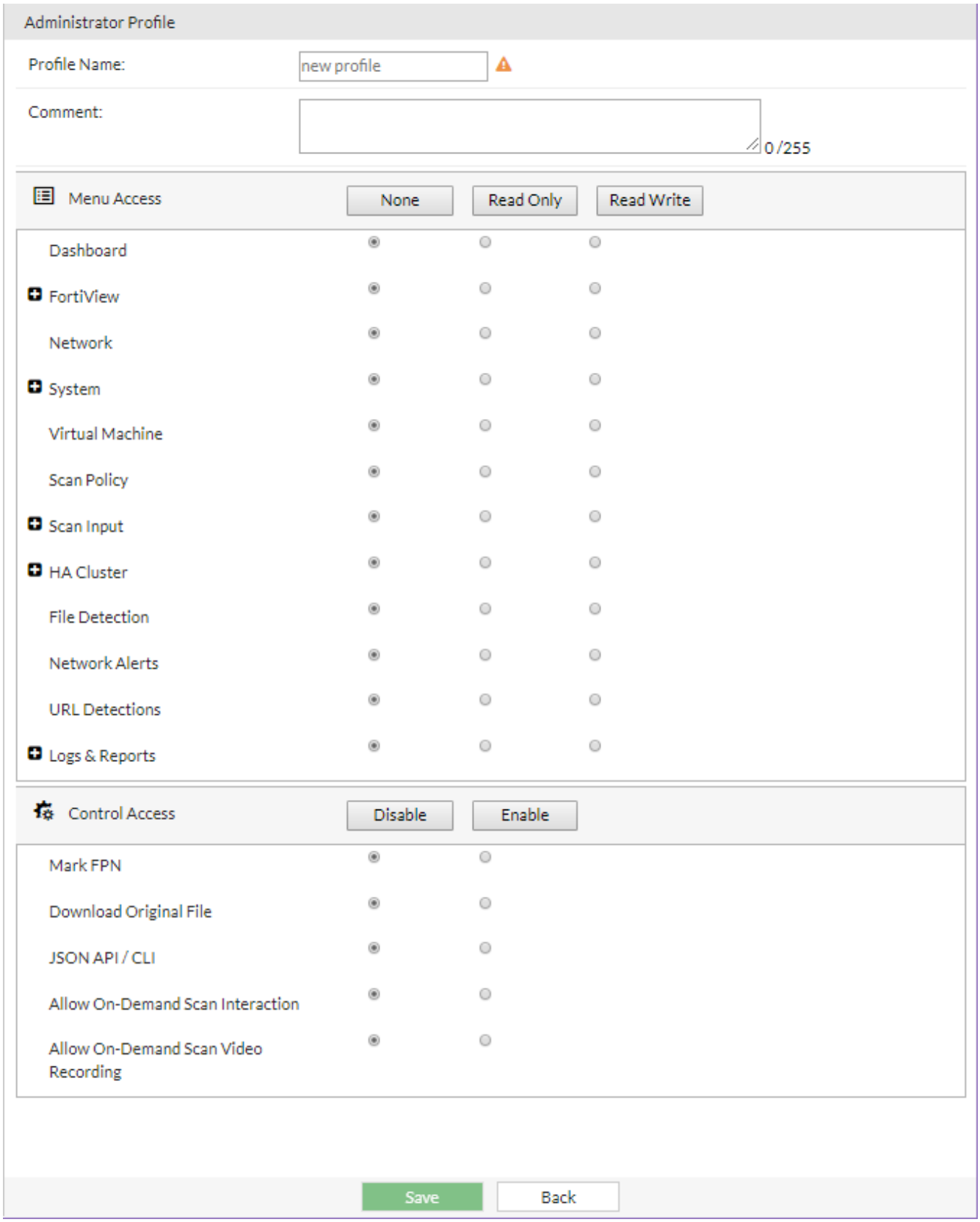
There are three predefined administrator profiles, which cannot be modified or deleted:

- 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
Save
Back

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

Certificates

In this page you can import, view, and delete certificates. Certificates are used for secure connection to an LDAP server, system HTTPS and SSH services. The FortiSandbox has one default certificate firmware.

FSA does not support generating certificates, but imports 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.

To import a certificate:

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

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

To view a certificate:

1. Go to *System* > *Certificates*.
2. Select the certificate from the list and select *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. Select *OK* to return to the Certificates page.

To delete a CA certificate:

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

Firmware certificate(s) cannot be deleted.

LDAP Servers

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

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

The following options are available:

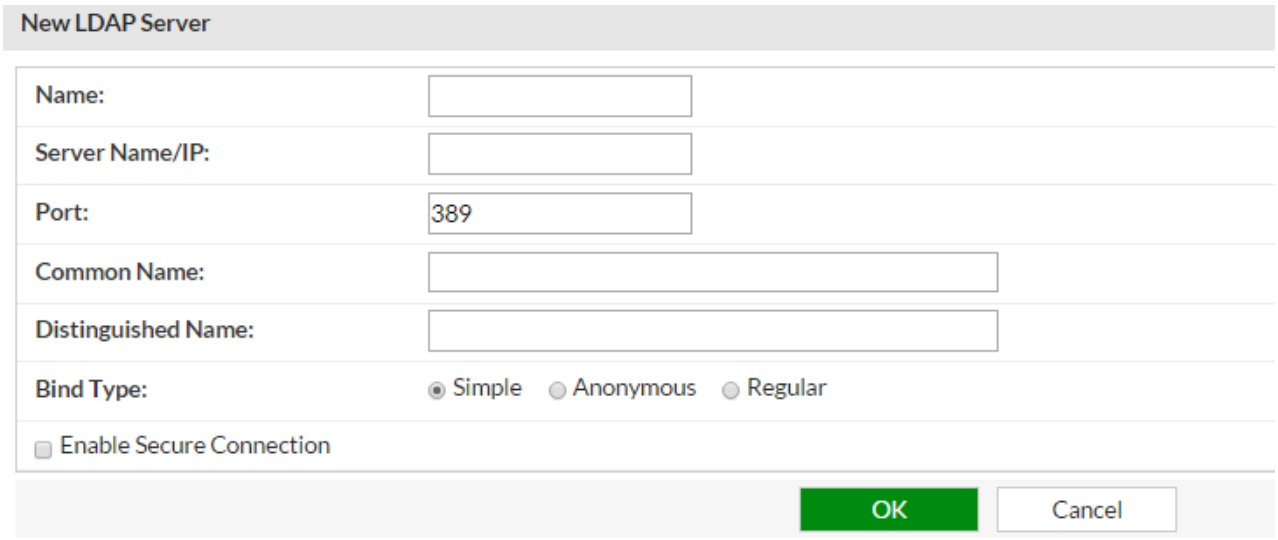
Create New	Select to add an LDAP server.
Edit	Select an LDAP server in the list and select *Edit* in the toolbar to edit the entry.
Delete	Select an LDAP server in the list and select *Delete* in the toolbar to delete the entry.

The following information is displayed:

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

To create a new LDAP server:

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



3. Configure the following settings:

Name	Enter a name to identify the LDAP server. The name should be unique to FortiSandbox.
Server Name/IP	Enter the IP address or fully qualified domain name of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.
Common Name	The common name identifier for the LDAP server. Most LDAP servers use `cn`. However, some servers use other common name identifiers such as `uid`.
Distinguished Name	The distinguished name used to look up entries on the LDAP servers use. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier.
Bind Type	Select the type of binding for LDAP authentication. The following options are available: • Simple • Anonymous • Regular
Username	When the *Bind Type* is set to *Regular*, type the user name.
Password	When the *Bind Type* is set to *Regular*, type the password.
Enable Secure Connection	Select to use a secure LDAP server connection for authentication.
Protocol	When *Enable Secure Connection* is selected, select either LDAPS or STARTTLS.
CA Certificate	When *Enable Secure Connection* is selected, select the CA certificate from the drop-down list.

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

RADIUS Servers

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

If you have configured RADIUS support and require a user to authenticate using an 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:

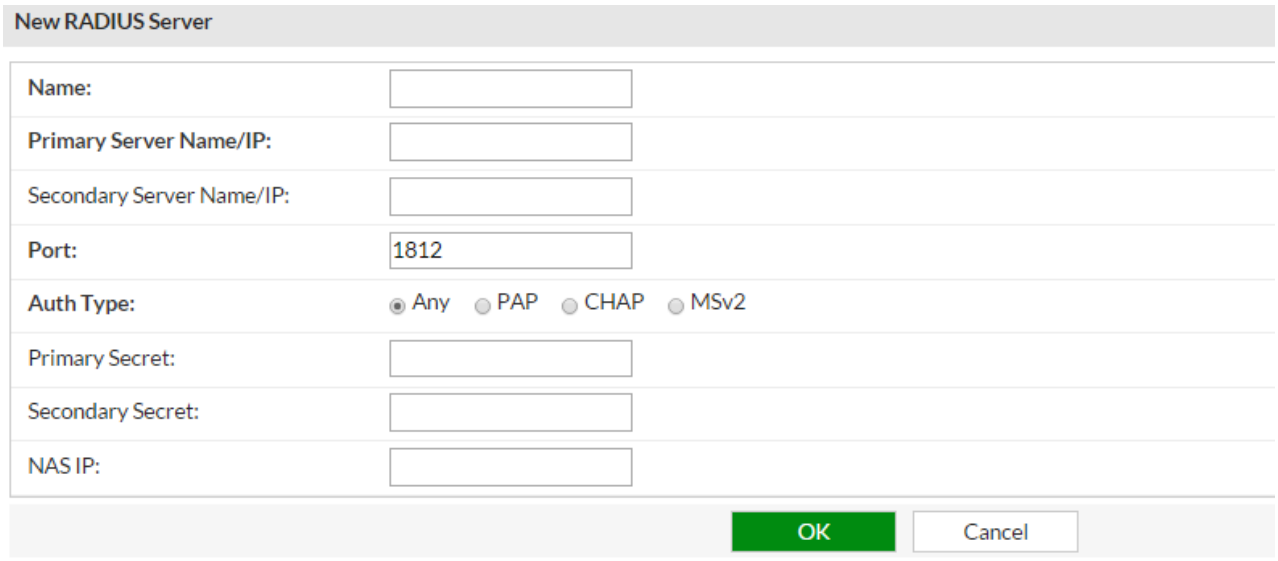
Create New	Select to add a RADIUS server.
Edit	Select a RADIUS server in the list and select *Edit* in the toolbar to edit the entry.
Delete	Select a RADIUS server in the list and select *Delete* in the toolbar to delete the entry.

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 one of: *ANY*, *PAP*, *CHAP*, or *MSv2*.

To add a RADIUS server:

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



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.

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 when a malicious file is detected and 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.
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 notification mail to global email list when malicious file is 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 below email list when malicious/suspicious verdict is returned to client device	Select to enable this feature. When enabled, a notification email is sent to a specific email list when a malicious/suspicious file is retrieved by a client device.
Global verdict notification email receivers list (separated by comma)	Enter the email addresses that comprise the global email list.
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 list	Select *Yes* to send a report email to the global email list.

	Send scheduled PDF report about an individual VDOM/Domain to its email address	Select to send PDF report to VDOM email address also. The report will only contain jobs sent from the VDOM. VDOM email address can be set in the VDOM edit page. It works the same way for protected FortiMail domains.
	Report Schedule Type:	Select the report schedule type. Options include: *Hourly*, *Daily*, and *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.
	Global email list to receive summary report (separated by comma)	Enter the email addresses that comprise the summary report global email list. The email addresses will receive reports including jobs from all input sources.
	Global email list to receive detail report (separated by comma)	Enter the email addresses that comprise the detail report global email list. The email addresses will receive reports including jobs from all input sources.
OK		Select *OK* to apply any changes made 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

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.

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

Configuring the SNMP agent

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

The SNMP manager can monitor the FortiSandbox system to determine if it is operating properly, or if 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.

Go to *System* > *SNMP* to configure the SNMP agent.

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.

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 • Log disk space is low • Interface IP is changed • Malware is detected

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

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 • Log disk space is low • Interface IP is changed • Malware is detected

4. Select *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.

FortiGuard

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

The following options and information are available:

Module Name	The FortiGuard module name, including: *AntiVirus Scanner*, *AntiVirus Extreme Signature*, *AntiVirus Active Signature*, *Network Alerts Signature*, *Sandbox Engine*, *Android Analytic Engine*, *Android Analytic Rating Engine* and *Traffic Sniffer*. All modules automatically install update packages when they are available on the FDN.
Current Version	The current version of the module.
Last Check Time	The time that module last checked for an update.
Last Update Time	The time that module was last updated.
Last Check Status	The status of the last update attempt.
Upload Package File:	Select *Browse* to locate a package file on the management computer, then select *Submit* to upload the package file to the FortiSandbox. When the unit has no access to the Fortinet FDN servers, the user can go to the Customer Service and Support site to download package files manually.
FortiGuard Server Location	Select FDN servers for package update and Web Filtering query. By default, the selection is *Nearest*, which means the closest FDN server according to the unit's time zone is used. When US Region is selected, only servers inside Unite States are used.
FortiGuard Server Settings	
Use override FDN server to download module updates	Select to enable an override FDN server, or FortiManager, to download module update, then enter the server IP address or FQDN in the text box. For more information, see Server overrides on page 1 on page 1. When an overridden FDN server is used, FortiGuard Server Location will be disabled. Click *Connect FDN Now* button to schedule an immediate update check.
Use Proxy	Select to enable a Proxy. Configure the Proxy Type (HTTP Connect, SOCKS v4, or SOCKS v5), Server Name, Port, Proxy Username, and Password.
Connect FDN Now	Click the *Connect FDN Now* button to connect the override FDN server/Proxy.
FortiGuard Web Filter Settings	

Use override server address for web filtering query	Select to enable an override server address for web filtering query, then enter the server IP address (IP address or IP address:port) or FQDN in the text box. For more information, see Server overrides on page 1. By default, the closest web filtering server according to the unit's time zone is used. If port is not provided, target UDP port 53 will be used.
Use Proxy	Select to enable a Proxy. Configure the SOCKS v5 server name or IP, Port, Proxy Username, and Password.
FortiSandbox Community Cloud Settings and Threat Intelligence	
Use override server port for community cloud server query (Ex.8888)	Select to enable an override server port for community cloud. Enter the port number in the text box. You can toggle between port 53 and port 8888.
Use Proxy	Select to enable a Proxy. Configure the SOCKS v5 server name or IP, Port, Proxy Username, and Password.

Select *Apply* to apply your changes.

Login Disclaimer

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

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

Settings

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

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

Configure the idle timeout:

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

Reset all widgets:

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

Job View Settings

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

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

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

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

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

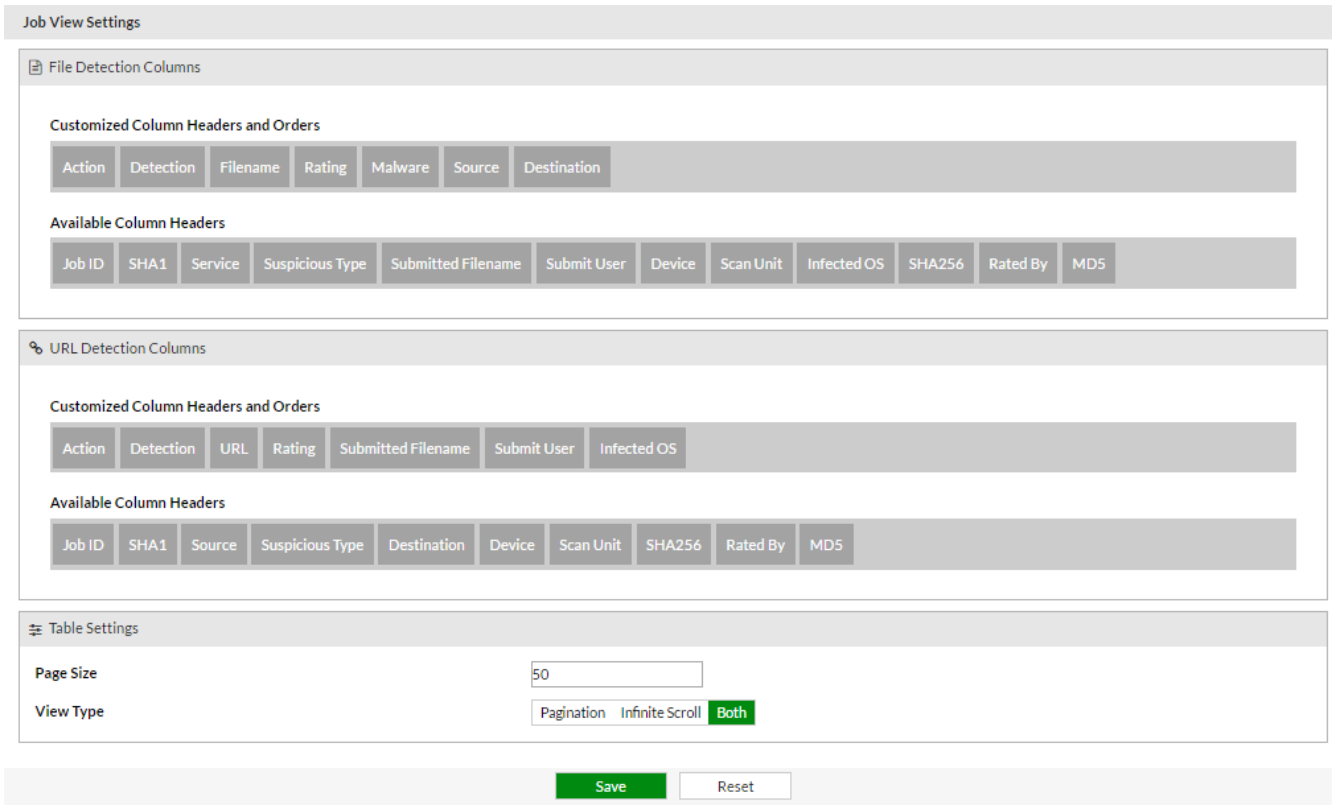
Selected columns, and their order, are displayed in the top row. Available columns are displayed in the bottom row. Drag and drop columns to adjust their order.

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

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

You can adjust column width, drag column headers to adjust their orders, 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 original page.

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



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 the file is detected through AV Rescan. Users can also view job details or perform a rescan of a 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 file name, or a file's parent archive file name, 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 a based on a modified hypervisor. The following table shows installed Windows OS license and installed Windows guest image OS types on each model.

Model, License and VM Information

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

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

VM Host Support

FSA-1000D	Supports 8 VM hosts.
FSA-3000D	Supports 28 VM hosts
FSA-3500D	Supports 8 VM hosts on each blade.
FSA-2000E	Supports 4 VM hosts by default, maximum up to 24 VM hosts.
FSA-3000E	Supports 8 VM hosts by default, maximum up to 56 VM hosts.
FSAVM00	No VM host by default, maximum up to 8 VM hosts.

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

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

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

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

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

For Android license, it's free

This section includes the following topics:

VM Status

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

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

VM Images

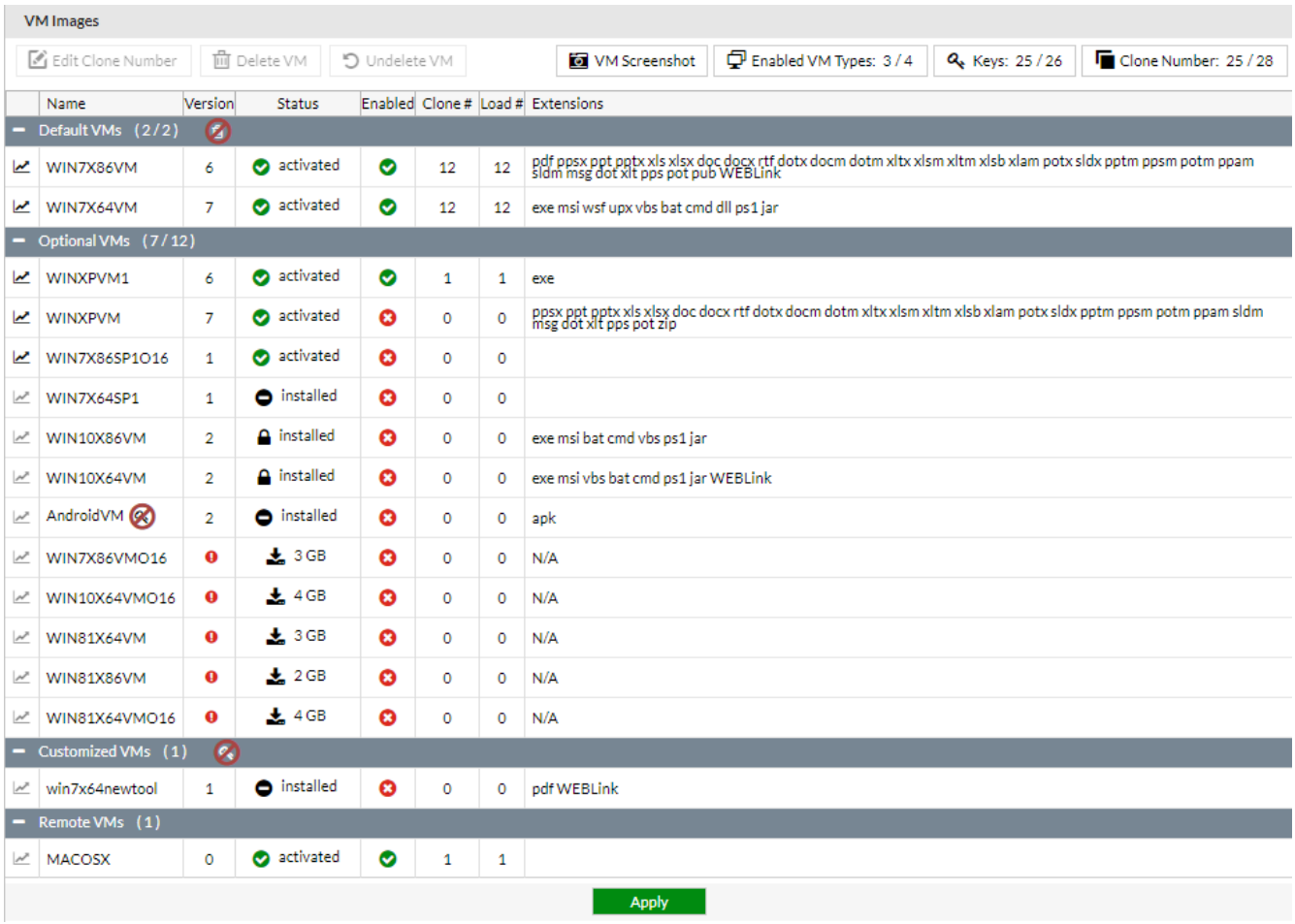
Go to *Virtual Machine* > *VM Images* to view all installed VM Images and configure the number of instances of each image.

VM Images are grouped to three categories:

Default VMs	Basic set of images installed on FortiSandbox by default. For FSA-AWS model, it's the installed Windows VMs on AWS.
Optional VMs	Fortinet published optional VM images.
Customized VMs	User created images and uploaded to FortiSandbox.
Remote VMs	In this 2.5.1 release, only MACOSX is supported as remote VMs. Users should purchase licenses from Fortinet which defines reserved clone numbers in the Fortinet MacOS Cloud. Without it, a TRIAL license is automatically provided. With the TRIAL license, it has the hard-coded clone number of `one`. Each unit can only upload one file to the MacOS Cloud to scan through *Scan Input* > *File On-Demand* page. In Cluster mode, all cluster units share collected reserved clones from each unit. This means even a node that has no MacOS VM contract purchased, it can still upload MacOSX files to the cloud for scanning. The TRIAL license is not available in cluster mode.

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

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



The following options are available:

Edit Clone Number	Select a VM Image and select *Edit Clone Number* from the toolbar to edit the entry. Click the green checkmark to save the new number. Then, click the *Apply* button to apply the changes.
Delete VM	Select a VM Image and select *Delete VM* from the toolbar to delete the entry. The default set of four Windows VMs cannot be deleted. Deleted VMs will only be deleted after the system reboots.
Undelete VM	After deleting a VM you have the option to *Undelete the VM* to recover it. After the system reboots and the delete action has been completed, the user cannot undelete a VM.
VM Screenshot	Select to take a screenshot of a running VM, and the file name the VM is scanning. The button is only available for *admin* user.

The following information is displayed:

Enabled VM Types	Max number of VM types that can concurrently run. It cannot exceed four on models other than FSA-3000E. On FSA-3000E, the number is six.
Keys	Max number of keys. This includes used key numbers and installed key numbers.

Clone Number	Max Clone number. It is the number of the installed Windows license. For example: • FSA-3000D, the maximum clone number is 28. • FSA-1000D, the maximum clone number is 8. • FSA-3500D, the maximum clone number is 8. • FSA-3000E, the maximum clone number is 56. • FSA-2000E, the maximum clone number is 24. • FSAVM00, the maximum clone number is 8.
Name	Name of the VM Image. The name is unique in the system. If the user uploads a new VM image of the same name, the current installation will be replaced. A *Chart* icon is located beside the *Name* column on the left side. When you click on the *Chart* icon, the VM's usage chart will appear.
Version	VM Image version. If a new version of an image is published on the Fortinet Image Server, a *New Version Available* icon will appear. Users can download, install and activate it.
Status	VM Image status. A VM image can be one of the following statuses: • Ready to Download • Ready to Upgrade • Downloading (shows a progress bar) • Ready to Install (Install or Remove downloaded image) • Installing • Installed (Disabled) • Installed (No Key Available) • Activated
Enabled	Number of enabled VMs. If an image's clone number is 0, it is disabled. Otherwise it is enabled.
Clone#	VM Clone number. The user can double click the number to edit it, then click the green check mark to save the new number. Click Apply to apply the change. The VM system will initialize again. The total clone number of all VM images cannot exceed the number of installed Windows license(s). For example, for FSA-3000D, the maximum clone number is 28.
Load#	The used VM Clone number in fact. For example, if a Cluster Master node is set to use 50% of sandboxing scan power, the Load # will be 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 non-suspicious ones will be scanned inside associated VM type. File type and VM association can be defined in the *Scan Policy* > *Scan Profile* page. Users can double click the value to access the *Scan Profile* page to edit the list.

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

Clone Number for VM Image

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

FSA-2000E

VM Image	Number of Clones
WIN7X86SP1O16	4

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

VM Image	Number of Clones
WIN7X64VM	4
WIN7X86VM	4

FSA-3000D

VM Image	Number of Clones
WIN7X64VM	14
WIN7X86VM	14

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

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

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

VM Screenshot

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

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

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

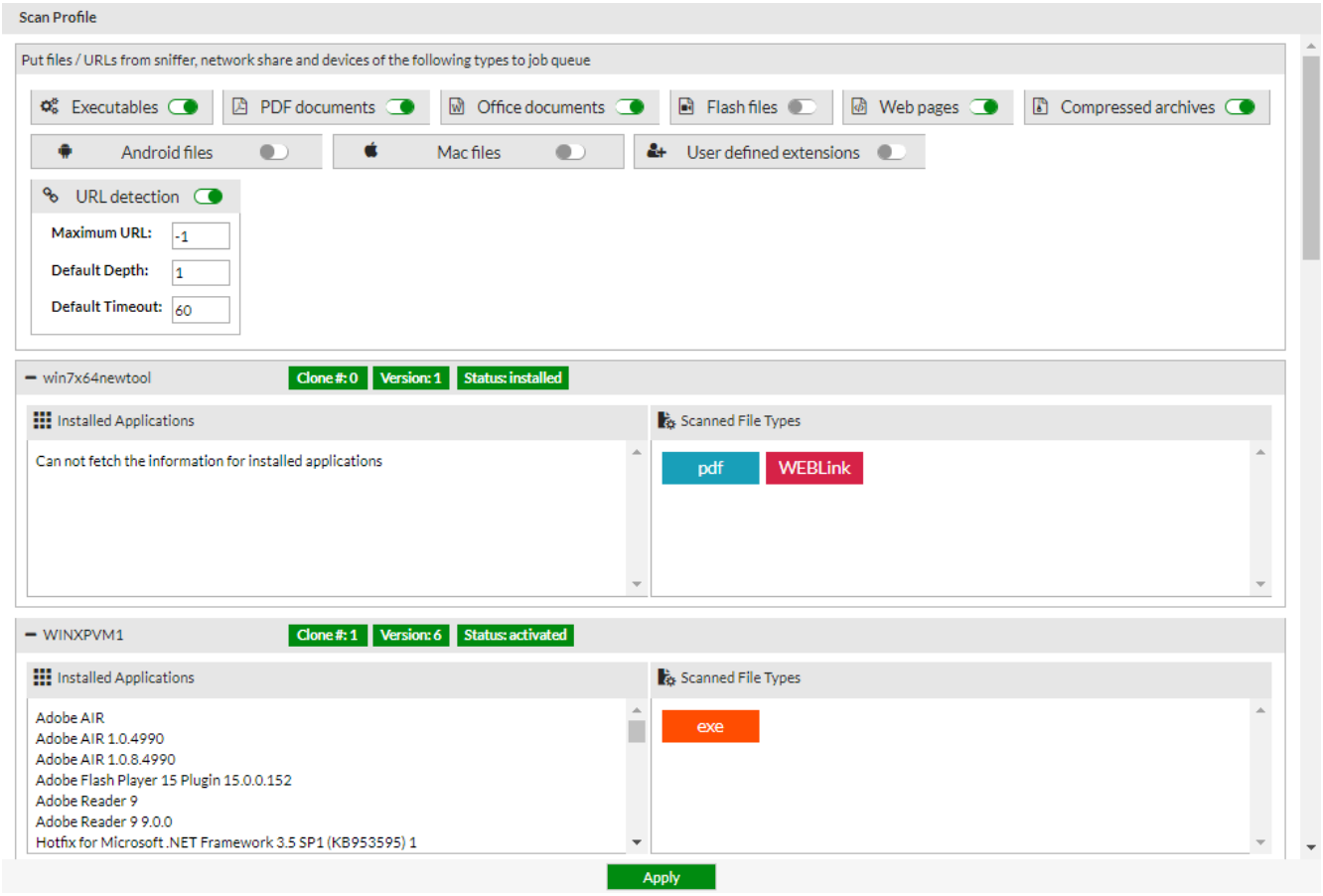
Scan Policy

This section includes the following topics:

Scan Profile

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.

By default, all Images sections are expanded.



File types

FortiSandbox, by default, supports the following file types:

Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS. Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command: sandboxing-prefilter -e -tdll Only the DLL files which can be executed inside a VM will be put into the Job Queue.
Archives	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more. Archive files will be extracted up to six levels and each file inside will be scanned according to Scan Profile settings. The max file number extracted: • On-Demand input: 10,000 • JSON API: 1,000 • 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, 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.

By default, FortiMail will hold a mail for a set period to wait for the verdict from FortiSandbox. When FSA scans an attachment or URL from FortiMail, it will check if the verdict is still needed as FortiMail might already have already released the email. If not, the scan will have an Unknown rating and skipped the status.

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

To scan MACOSX files, extra licenses should be purchased from Fortinet. MACOSX files will be uploaded to Fortinet MACOS cloud for scanning.

Scan Profile Part One

The first part of the Scan Profile page is to define file types and URLs that are allowed to enter the job queue if they are from a sniffer, device, adapter and/or network share.

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

To allow a file type to enter the job queue

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

URL Detection

When URL detection is enabled, it means FortiSandbox will scan URLs (WEBLinks). The user can also define default settings of depth FortiSandbox should visit the URL and the default timeout value that FortiSandbox should stop even when not all web page have been scanned.

If FortiSandbox unit has a long queue of pending jobs, user should consider turning off certain file types to job queue. For example, in most network environment, static web files (JavaScript, html, aspx files etc) and Adobe flash files consist of a big part of all files. When performance issue is met, user can consider turning them off.

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

To find out number of each file type and input source, user can use CLI command `pending-jobs` or *Scan Input* > *Job Queue* page.

Scan Profile Part Two

The second part is to define file type and VM image association. Association means files of a certain file type will be sandboxed by the associated VM image. This part shows all installed VM image(s), their clone numbers, version and status.

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

To configure association

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

Note: for an associated file to be sandboxed in the VM image

1. Its file type has to be configured to enter a job queue
2. The VM image has a non-zero clone number (i.e.: it is enabled)

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. For example, the user can associate web filters to VM types. If the sandboxing pre-filtering is *OFF*, by default, all of them will be scanned by associated VM types. This may up the system sandboxing scan capacity because web files are usually in large in size. It is recommended to turn on sandboxing pre-filtering for web files.

To improve the system scan capacity, users can turn on the sandbox pre-filtering of a file type through the `sandboxing-prefilter` CLI command. For more details, refer to the *FortiSandbox 2.5.1CLI Reference Guide*.

To edit associated file type

1. Click right side panel and a popup file type list will show up.
2. File types are grouped to different categories. Clicking the category title will toggle associations of all grouped file types. Clicking on individual file type will toggle its own association. When the file type is displayed in full length, it means the file type is associated.

Add a user defined extension

Make sure the user defined extension is enabled.

1. Click + sign and type 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* panel to finalize the list for double check.

2. Click *Apply* button to apply the changes. User can also click *Apply* button to apply changes directly. Files will then be scanned by associated VM images.

For files with a user defined extension, they will be scanned by a VM image no matter what file types they really are. During scan, the file will be opened with associated software pre-defined by VM image. For example, if FireFox is associated with HTML files, HTML files will be opened by FireFox.

FortiSandbox provides default scan profile settings. To be specific

- WIN7X86VM: Adobe PDF files and Office files
- WIN7X64VM: Executable files

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

If cluster nodes do not have the same list of enabled VM images, 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 Master node and the configurations will be synced to slave nodes. Master node will collected all installed VM image information. If a different VM image is only installed on a slave node, the user can still configure on the Master node and the result will be synchronized to that Slave node.

Link file types in Static Web files group is for shortcuts to a webpage or URL. While WEBLink types in URL detection group are for URL scans, which follows depth and timeout settings in Scan Profile Part 1

There might be malicious URLs inside Office files and PDF files. Users can choose to scan randomly selected URLs with the original file altogether inside a VM image. To turn this feature *ON*, use the `sandboxing-embeddedurl` CLI command. For more details, refer to the *FortiSandbox 2.5.1 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 before those in the low priority queue. 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, the low priority job queue will be processed. Therefore, it is recommended that different job queues are associated with different VM image(s). In this release, job queue priority can be adjusted in the *Scan Policy* > *Job Queue Priority* page. By default, the job queue priority is:

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

File Scan Flow

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

1. Filtering and Static Scan

   In this step, the file will be scanned by the Anti Virus engine and the YARA rule engine. Its file type will be compared with the *Scan Profile page, Part One* settings to decide if it should be put in the job queue. If yes, it will be compared with the Black/White list and overridden verdict list.

   For certain file types, such as Office and PDF files, they will be scanned statistically in virtual engines to detect suspicious contents. If they contain embedded URLs, the URLs will be 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 will be downloaded. This makes the malware information shareable amongst the FortiSandbox Community for fast detection.

3. Sandboxing Scan

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

URL Scan Flow

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

1. Static Scan

   In this step, the URL is checked against the *Overridden Verdict* list.
2. Sandboxing Scan

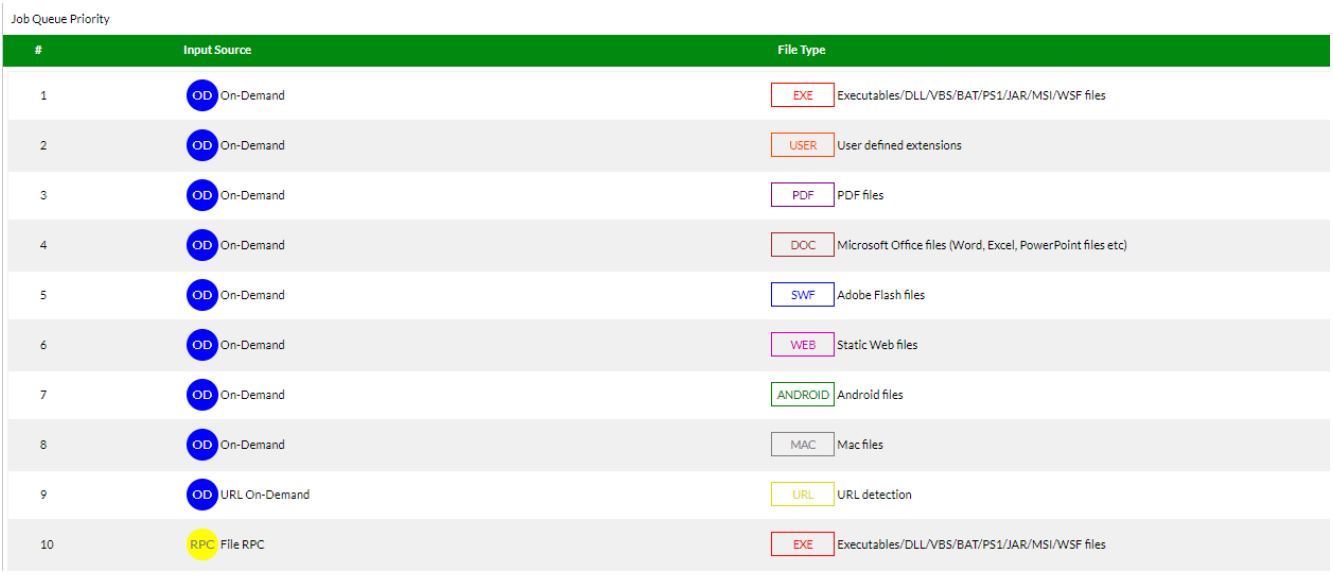
   If WEBLink is associated with a VM type as defined in *Scan Profile page, Part Two*, the URL will be scanned inside a clone of that VM type. If the URL type is enabled for `sandboxing pre-filtering` command, only URLs whose webfiltering category is *UNRATED* will be scanned inside a VM. For more information,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

The URL will be checked against the user uploaded white domain list and black domain list. If the domain of the URL falls into them, the URL will be rated as *Clean* or *Malicious* respectively.

Job Queue Priority

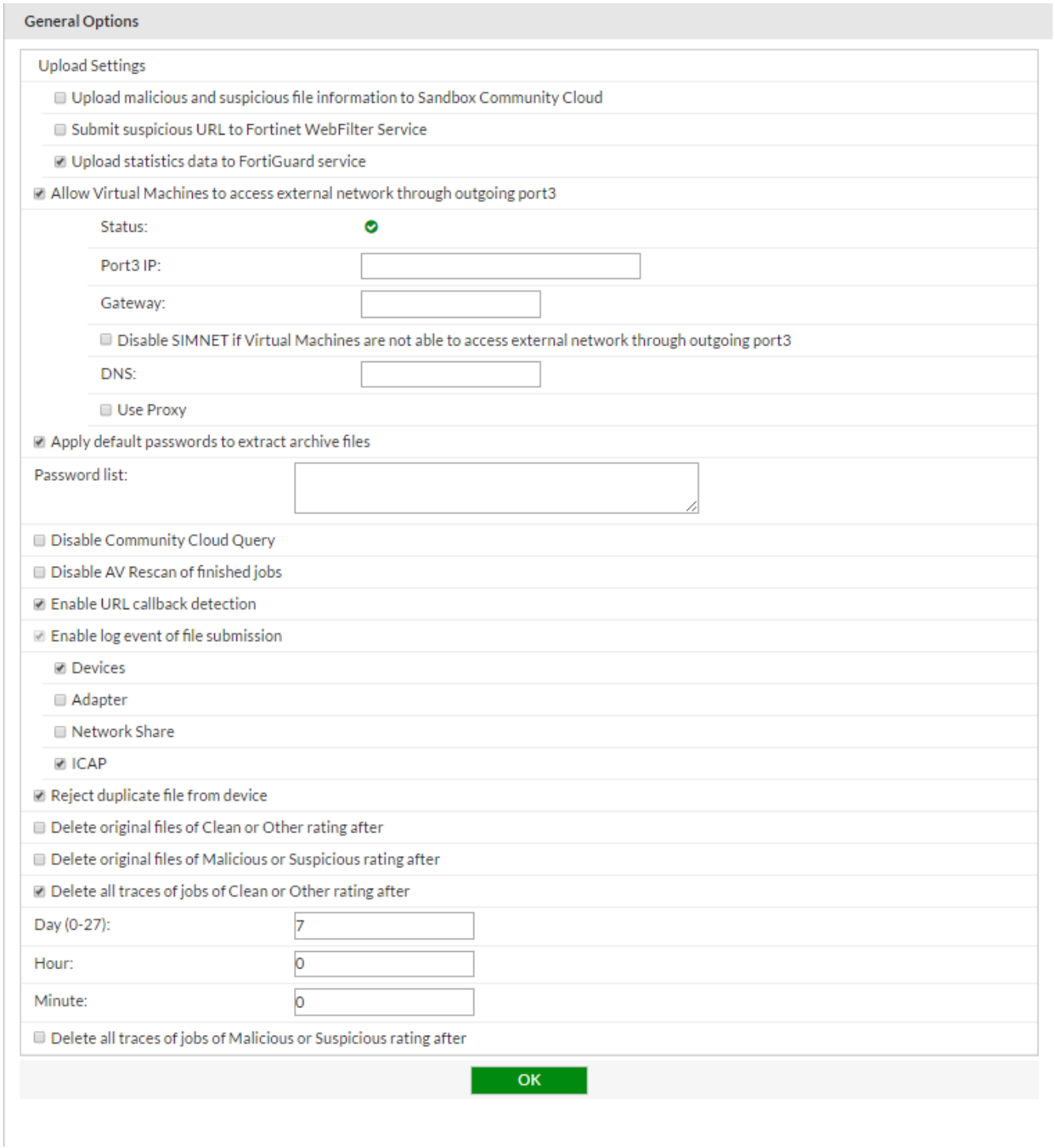
This page displays the job queue priority list. The priority list can be dynamically adjusted by dragging and dropping the file type entry in order of priority. The closer an entry is to the top, the higher the priority.

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



General

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



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 file checksum, tracer log, verdict, and original files are uploaded.
Submit suspicious URL to the Fortinet WebFilter Service		Enable to submit malware downloading URL to the FortiGuard Web Filter Service.
Allow Virtual Machines to access external network through outgoing port3		Enable to allow Virtual Machines to access external network through the outgoing port3. If the VM cannot access the outside network, a simulated network (SIMNET) will start 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 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*.
	Status	Port3 status.
	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 drop-down 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.
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 rated.
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.
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 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.

How to improve system scan performance

There is a limited number of files that a unit can process within a time period. There are certain ways to improve the unit's scan power

1. Only keep jobs with *Clean* rating for a short period. If the user is not concerned about processed files with a *Clean* rating, the user can configure the system to remove them after a short period. This will save the system resource and improve system performance. To do that, go to *Scan Policy* > *General*, and configure *Delete all traces of jobs of Clean or Other rating after*.
2. Turn on *Pre-Filtering* for certain file types. By default, if a file type is associated with a Windows VM image, all files of this file type will be scanned inside it. Sandboxing scans inside Windows VM is a slow and expensive process.

   For example, a FSA3000D unit can only scan 560 files/hr inside VM on average. Users can enable *Pre-Filtering* on certain file types. If it is enabled, files of that file type will be pre-filtered and have a *Clean* rating; only suspicious ones will be scanned inside a VM.

   The following file types support *Pre-Filtering*: DLL, PDF, SWF, JS, HTML, URL.

   For URL type, if *Pre-filtering* is enabled, only URLs whose web filtering category is *Unrated* will be scanned inside VM.
3. Associate every file type to only one VM type. Theoretically, one file should be scanned inside all enabled VM types to get best malware catch rate. However, to improve scan performance, every file type should be associated with only one VM type.
4. Allocate clone numbers of each VM type according to distribution of file types.

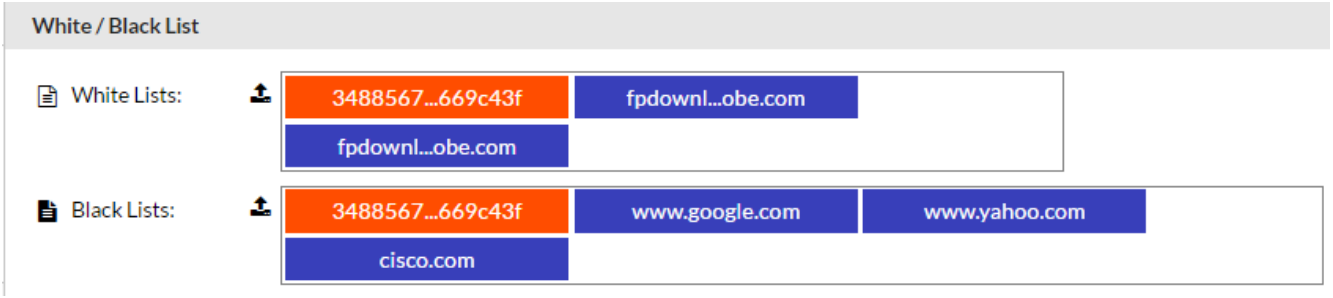
   Each unit can only prepare limited number of guest image clones. The number is determined by installed Windows license keys. Users should allocate clone numbers according to distribution of file types.

   For example, if there are a lot of Office files and WIN7X86VM is associated with Office files, user can decrease clone number of other VM types and increase the clone number of the WIN7X86VM image. If the user sees a large number of pending jobs, he can use `pending-jobs` CLI command, or go to *Scan Input* > *Job Queue* page, to find out files of which file type is the most waiting in the queue and increase clone numbers of its associated VM type. See Job Queue on page 167 for more information.

White/Black Lists

White and black lists help improve scan performance and malware catch rate and reduce the false positive and can be appended to, replaced, cleared, deleted, and downloaded. The lists contain the file's checksum values (MD5, SHA1, or SHA256 checksums, and the file's download domain). Users can put trusted domains in the White List to improve performance. *Wild Card* formats, like `*.domain`, is 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.

- If a white list entry is hit, the job rating will be *Clean* with a local overwrite flag.
- If a black list entry is hit, the job rating will be *Malicious* with a local overwrite flag. Malware names will be FSA/BL_DOMAIN, FSA/BL_MD5, FSA/BL_SHA1, or FSA/BL_SHA256.
- If the same entry exists on both lists and is hit, the black list will take priority and the file will be rated *Malicious*.



To manage the White/Black list manually:

1. Go to *Scan Policy* > *White/Black List*.
2. Click the *White* or *Black* list panel, the *Detail* panel will slide out from the right side.
3. Click the head of each type to expand or collapse the list.
4. Click the + button to add a new entry.
   Alternatively, click the *Trash* button to either remove the whole list or remove a single entry.
5. Click outside the *Detail* panel to accept the change.

To manage the White/Black list through files:

1. Go to *Scan Policy* > *White/Black List*.
2. Click the *File Upload* button for either the *White List* or *Black List*.
3. Select the list type from the drop down menu:
   - *Domain*
   - *MD5*
   - *SHA1*
   - *SHA256*
4. Select the *Action* to take from the drop down 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.

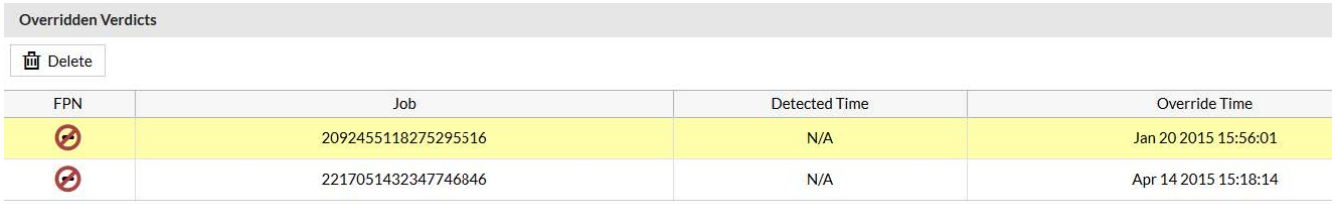
5. If the action is *Download*, click *OK* to download the list file to the management computer.
6. If the action is *Append* or *Replace*, click *Choose File*, locate the checksum file on the management computer, then click *OK*.
7. If the action is *Clear*, click *OK* to remove the list.

In a Cluster setting, White/Black lists should only be created on the Master node.

Overridden Verdicts

The *Overridden Verdicts* page displays jobs that the user has manually marked them as *False Positive* or *False Negative*. *Job IDs*, *Job Finish Time*, and the time that the user manually marks 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 without having to revert the FP/FN verdict in the Job Detail page.



YARA Rules

YARA is the third scan engine, which 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.
File Type	The file types the YARA rule is applied to.
Modify Time	The date and time the YARA rule was last modified.
Size	The size of the YARA rule.
Sha256	The Sha256 number.
Status	The current status (Active or Inactive) of the *Inactive* or *Active* YARA rule. Click the icon to toggle the status.

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.

If you want the same set of rules to match more than one file type, you should import the file more than once; for each import, set a different file type to match.

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:

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:

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

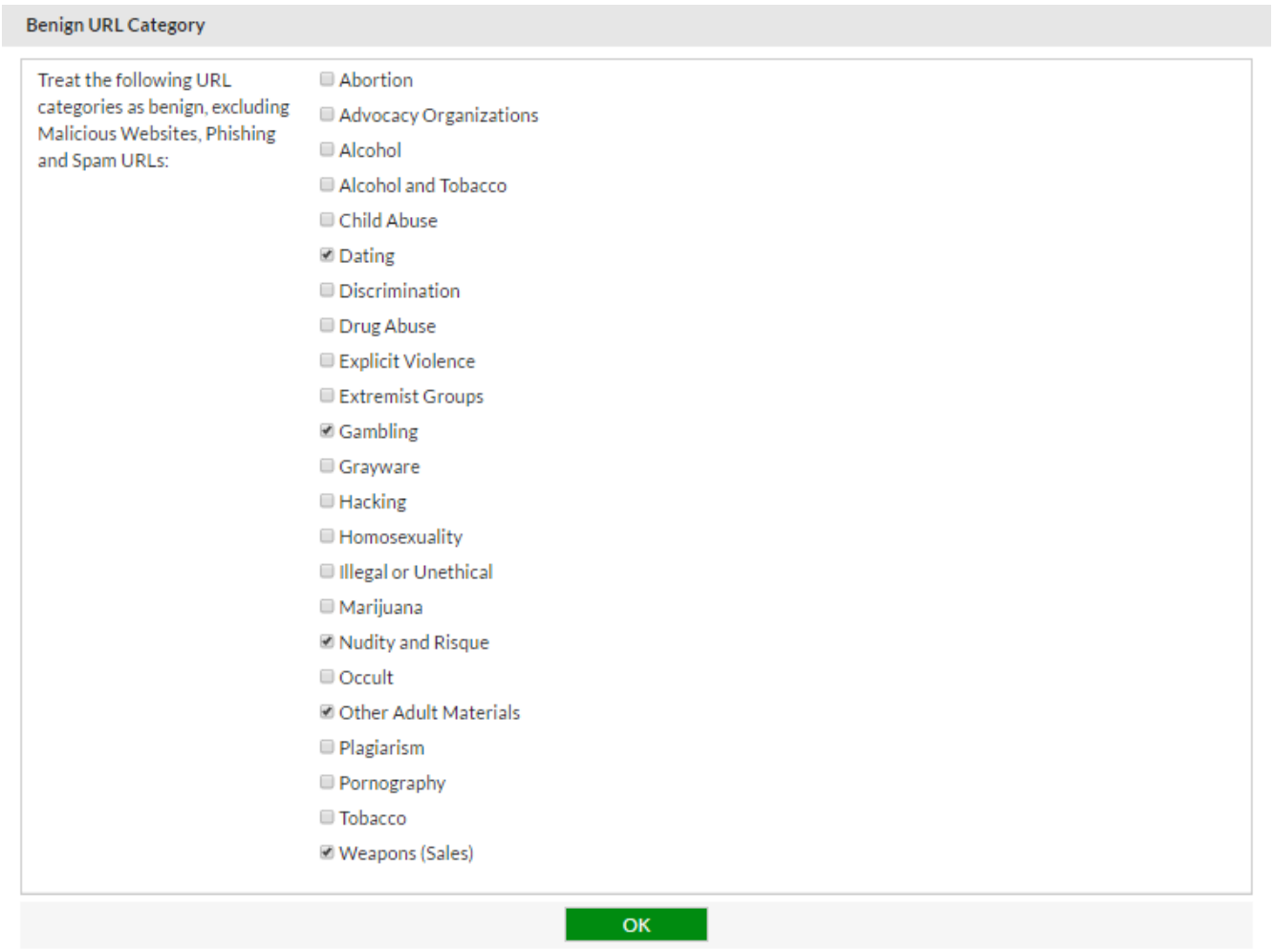
To change the status of a YARA rule:

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

URL Category

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

- Drug Abuse
- Explicit Violence
- Abortion
- Other Adult Materials
- Advocacy Organizations
- Gambling
- Extremist Groups
- Pornography
- Dating
- Weapons (sales)
- Homosexuality
- Marijuana
- Alcohol and Tobacco


Benign URL Category
Treat the following URL categories as benign, excluding Malicious Websites, Phishing and Spam URLs:
Abortion
Advocacy Organizations
Alcohol
Alcohol and Tobacco
Child Abuse
Dating
Discrimination
Drug Abuse
Explicit Violence
Extremist Groups
Gambling
Grayware
Hacking
Homosexuality
Illegal or Unethical
Marijuana
Nudity and Risque
Occult
Other Adult Materials
Plagiarism
Pornography
Tobacco
Weapons (Sales)
OK

Supporting URL Pre-Filtering

Devices like FortiMail can be configured to send all URLs inside an Email body to FortiSandbox. If sniffer is used, URLs inside email traffic can also be extracted and scanned. By default, all of them will be scanned inside the 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 URL's category is not defined as Benign in the *Scan Policy* > *URL Category* page, a job will be created and the URL will be rated as High Risk
3. If the URL's category is defined as Benign in the *Scan Policy* > *URL Category* page, 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. For more information, see the *FortiSandbox CLI Guide* for the `sandboxing-prefiltering` command.

Customized Rating

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

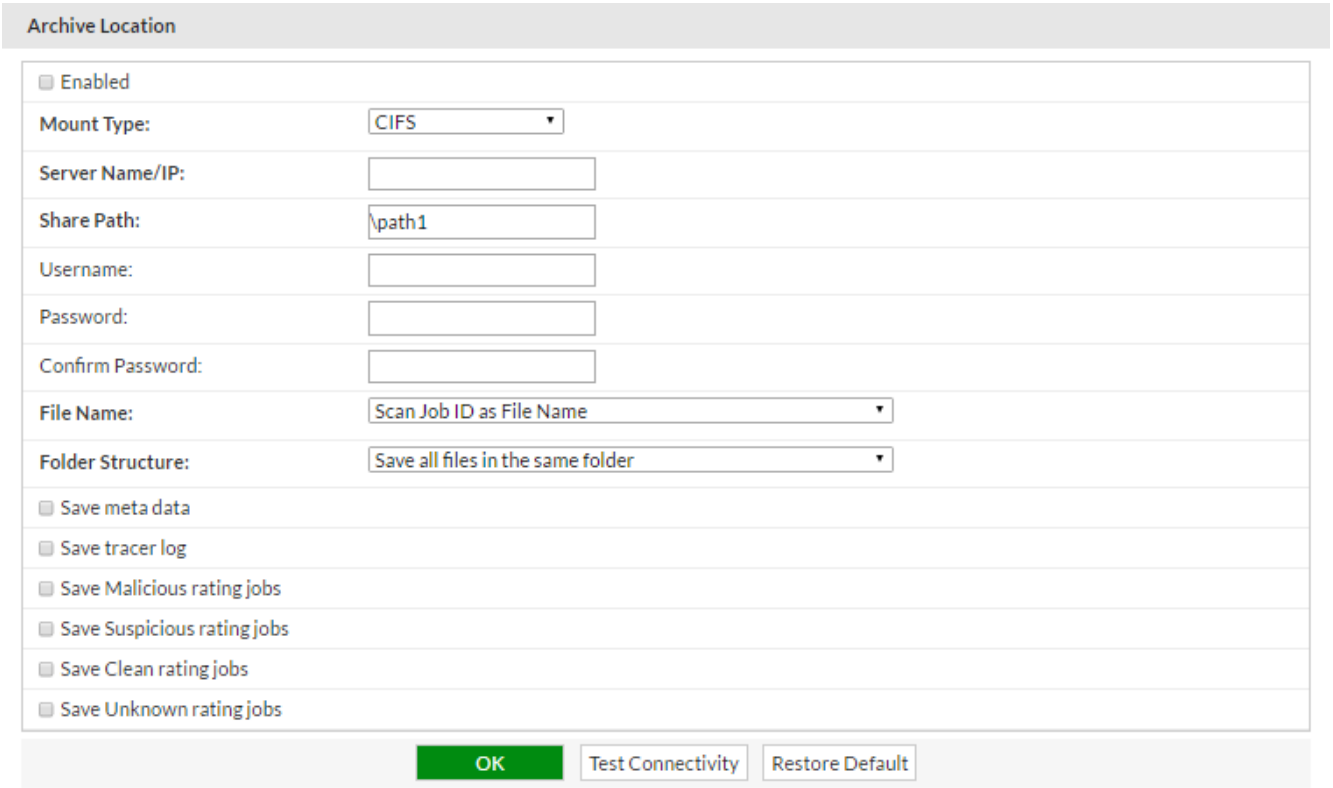
The following options can be configured:

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 predefine 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 Archive page allows you to adjust the archive location settings. 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.



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. The following options are available: • CIFS (SMB v2.0, v2.5) • 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 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 drop-down list. The following options are available: • Scan Job ID as File Name • Original File Name
Folder Structure	Select the folder structure from the drop-down 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
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 Unknown rating jobs	When selected, files of Unknown rating will be saved.

Package Options

The FortiSandbox can generate antivirus database packages (malware packages) and blacklist URL packages from scan results, and distribute them to FortiGate devices and FortiClient end points 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 end point is running version 5.4 or later and has successfully connected to the FortiSandbox, and
- FortiSandbox is running version 2.1 or later.

The FortiGate or FortiClient sends a malware package request to FortiSandbox every two minutes that includes its installed version (or 0.0, if none exists). The FortiSandbox receives the request then compares the version with the latest local version number. If the received version is different, FortiSandbox sends the latest package to the FortiGate or FortiClient. If the versions are the same, then FortiSandbox will display an already-up-to-date message.

A new package is generated when:

- The FortiSandbox has a new malware detection whose rating falls into an already configured rating. The new detection can be from local or from another unit if this unit joins a Global Threat Information Network.
- 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 locally by a black list, white list, or False Positive/False Negative (FPN) mark.

Malware and URL Package Options

The malware package options allow you to configure how many days worth of data that the malware packages save and the malware ratings that are included in the packages. It also defines where the malware information is from. It can be either from local detection, or from other units if the unit joins a Global Threat Information Network.

In a cluster environment, only the Master node generates Malware packages and URL packages.

The URL package contains downloaded URLs of detected malware.

Mode		Select either *Global* or *Local*. *Global* mode means the unit joins a threat information sharing network and generate packages with threat information from all units in the network. *Local* mode means the unit only uses local detections to generate packages.
Working As		This options is only available in *Global* mode. Select either *Collector* or *Contributor*, and configure its respective settings. In the *Global* mode, the unit can work either as threat information *Collector* or *Contributor*. In a Global network, only one *Collector* can exist. Collector should set authentication code to improve security. The *Collector* listens on TCP port 2443 and the traffic between Contributor and Collector is encrypted. *Contributors* upload detected malware information with Malicious and Suspicious ratings to Collector and download malware information which the Collector collects from other Contributors to local. Each Contributor can configure what to include in its own generated malware packages and STIX IOC package.
	Collector IP Address	Enter the collector IP address. Only available when *Contributor* is selected.
	Alias	The *Collector's* Alias.
	Authentication Code	Enter the authentication code of the *Collector*.
	Show Contributors	Enable to display the list of contributors. Only available when *Collector* is selected.

After the units receive threat information, packages can be generated locally with the following options: **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.
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.
	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 limitation, malware packages can only have 100K entries at the most.

Because of size limitations, URL package can only have 1000 entries at the most.

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. 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 the *Scan Input* > *Package Options* page.
2. 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 at *Scan Input* > *Package Options* page. 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">0696e7ec6646977967f2c6f4dcb641473e76b4d5c9beb6e4
                            33e0229c2accec5d</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 big.

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 local scans to detect sandbox evasion. FortiSandbox also has integrated web filtering to inspect and flag malicious URL requests. Based on the traced output of the OS sandbox, botnet and command & control (C&C/2C) channels are detected and classified.

There are five methods of importing files to your FortiSandbox ; sniffer mode, device mode (including FortiClient endpoints), adapter, network share, and on demand (including on demand through JSON API call and GUI submission). In sniffer mode, the FortiSandbox sniffs traffic on specified interfaces, reassembles files, and analyzes them. In device mode, your FortiGate, FortiWeb, FortiMail, or FortiClient end points are configured to send all 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.

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

File On Demand

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

On demand allows you to upload various file types directly to your FortiSandbox device. Upon upload, the file is inspected by FortiSandbox in the VM modules. You can then view the results and decide whether or not to install the file on your network.

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

You can select VM types to do the sandboxing by overwriting what is defined in the Scan Profile. When MACOSX is selected, the file will be uploaded to the MacOS cloud to be scanned. For password protected archive files, write down all possible passwords. If a password protected archive file contains a different password protected archive file, both passwords should be written down. The default password list set in the Scan Policy > General page will also be used t extract the archive files.

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

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

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 either generated from AV Rescan or manually launched Rescan of Malicious job 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 drop-down. Do not close the dialog box or navigate away from the page during report generation.
View Jobs	Click the icon to view the scan job(s) associated with the entry. In this page you can view detailed information for files scanned. If the file is an archive file, all files in the archive are displayed in this page. Click the back button to return to the on-demand page.
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 in this column to view the file rating. The rating can be one or more of the following: Clean, Low Risk, Medium Risk, High Risk, Malicious, or Unknown. For archive files, the possible ratings of all files in the archive will be 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 file 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 one slave node's job queue.

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

1. In the right-pane 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	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.
Scan Video	When the scan is submitted, if the *Record scan process in video* is selected, a video icon is displayed. Clicking it will allow user to select one VM type in which the scan is done and recorded. Select the VM type to play video or save it to a local hard disk. The reset of displayed columns are determined by settings defined in *System* > *Job View Settings* > *File Detection Columns* page. For more information, refer to Job View Settings on page 107.
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. See Appendix A - View Details Page Reference on page 252 for descriptions of the *View Details* page.
4. Click the parent job ID icon to view rescan file details.

   If the parent job is an archive file, all the childrens' file names are included in the Archive Files drop down list. Select 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 drop-down 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 and define the report start and end date and time.
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.
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 PDF report is 5,000; the maximum number of events you can export to CSV report is 150,000.

To submit a file to FortiSandbox :

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

Skip:	Select one or more of the following steps to skip: • Static Scan • AV Scan • Cloud Query • Sandboxing
Overwrite Scan Profile Settings to Scan in VM Type:	Overwrite *Scan Profile Settings* to Scan in VM Type by selecting one or more of the enabled VMs: **Note:** MACOS file scan is only available for On-Demand scans if no license is purchased. The file will be sent over to the MacOS Cloud and after the scan is finished, a detailed verdict will be downloaded. **License Consideration** of the MacOS file scan: • Each unit has one free trail license by default for the MacOS file scan. When you run `vm-license -l`, this record will show `KEY_MAC MACOS-TRAIL-TRAIL-TRAIL-TRAIL`. • With a TRIAL MacOS license, each unit can only upload one file to the MacOS Cloud. If there are other files, they will wait in the queue. • In the *Virtual Machine* > *VM Images* page, there is a Remote VMs section. With a TRIAL MacOS license, MACOS X has the hard-coded clone number of one. Enabled VM means its clone number is larger than `0`. If a VM type is not selected, settings from the *Scan Profile* page will be used. If VM images are not ready, the VM list will not be displayed. If no VM type is selected, settings from the Scan Profile page will be used. If any VM type is selected, settings from the Scan Profile will be overridden and the file will only be scanned in selected VM types. If VM images are not ready, the VM list will not be displayed.
Select a File	Click the *Browse* button and locate the sample file or archived sample file on your management computer.

Allow Interaction	Select the *Allow Interaction* checkbox to interact with the Windows VM. See To use the Allow Interaction Feature: on page 159 for more information.
Record scan process in video	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	Select to add the sample to malware package, if the result meets settings in Package Options.
Possible password(s) for archive file:	List all possible passwords contained inside a password protected archive 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.

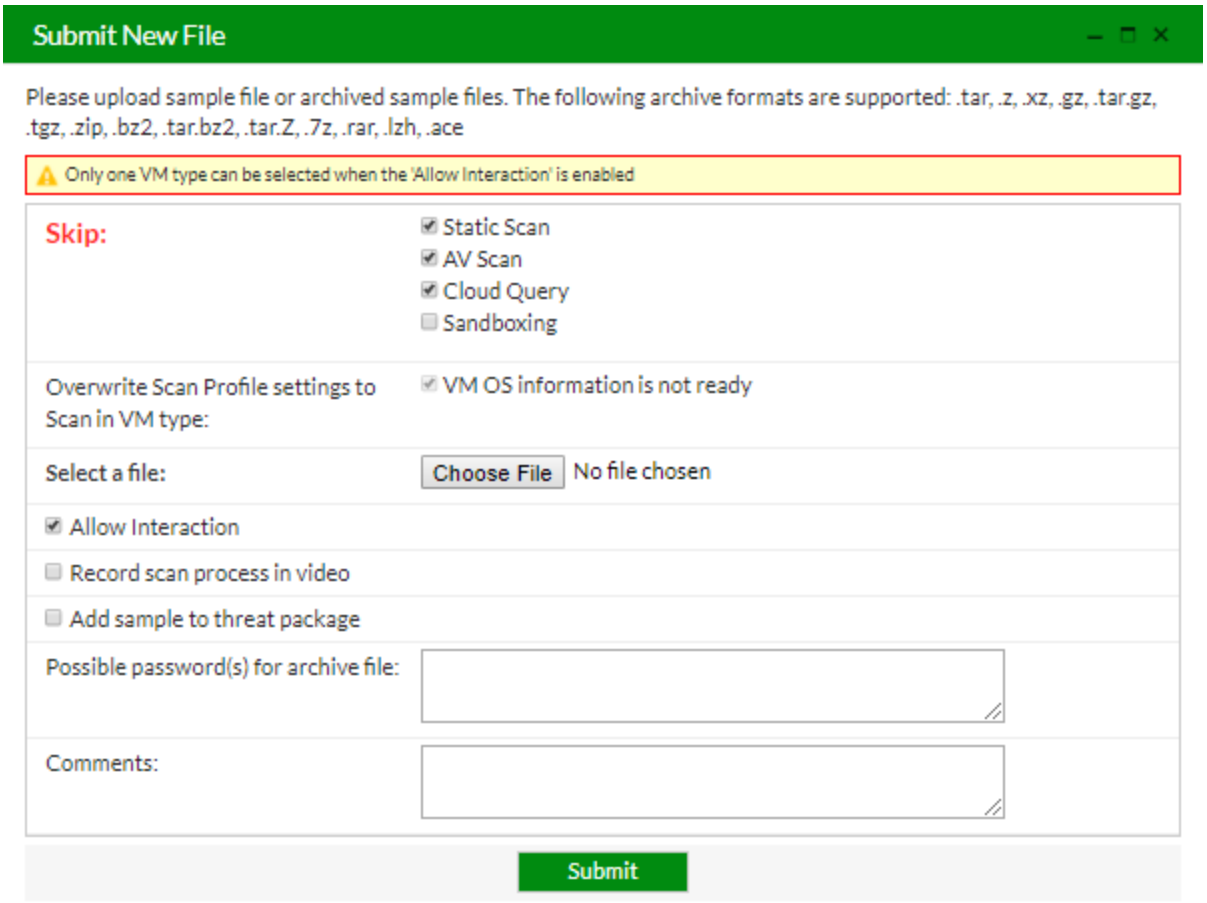
3. Click the *Submit* button. A confirmation dialog box will be displayed. Click *OK* to continue. The file will be uploaded to FortiSandbox for inspection.
4. Click the *Close* button to exit.

   The file will be listed in the *On-Demand* page. Once FortiSandbox has completed its analysis, you can select to view the file details.

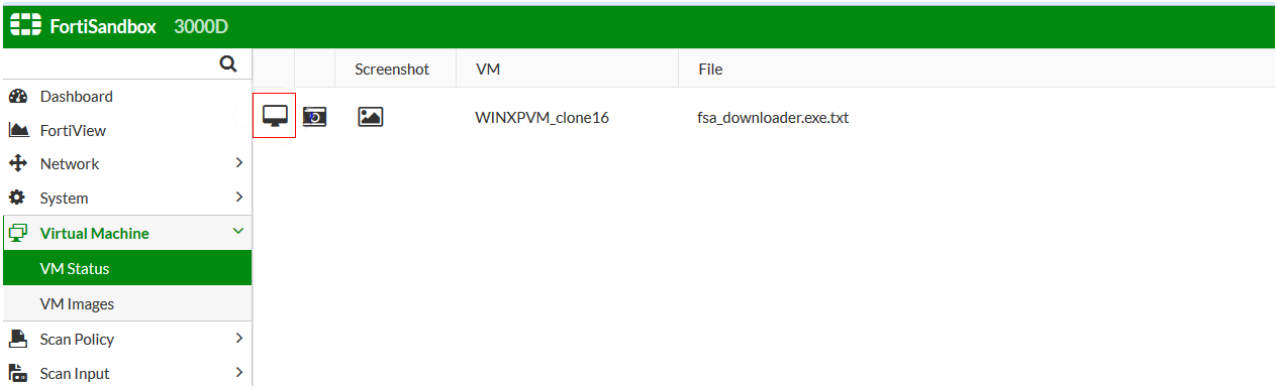
If the submitted file is an archive file with multiple files, the File Count, Rating and Status values might change until all files have finished scanning.

To use the Allow Interaction Feature:

1. Go to *Scan Input* > *File On-Demand* > *click Submit File from the toolbar*.
2. In the Submit New File window, check the *Allow Interaction* checkbox, and click *Submit*. One and only one VM type should be selected to do the scan.



3. Go to *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 VNC session will close after a few seconds. 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.

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 by FortiSandbox in the VM modules. 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 Malicious 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. Do not close the dialog box or navigate away from the page during report generation.
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, or Unknown. 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 will allow user to select one VM type in which the scan is done and recorded. Select the VM type to play 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, refer to Job View Settings on page 107.

3. Click the *View Details* icon to view file details. The *View Details* page will open a new tab. See Appendix A - View Details Page Reference on page 252 for descriptions of the *View Details* page.
4. Close the tab to exit the *View Details* page.

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

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

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 is value is defined in the *Scan Policy* > *Scan Profile* page.
Overwrite Scan Profile Settings to Scan in VM Type	Overwrite *Scan Profile Settings* to Scan in VM Type by selecting one or more of the enabled VMs: Enabled VM means its clone number is larger than `0`. If a VM type is not selected, settings from the *Scan Profile* page will be used. If VM images are not ready, the VM list will not be displayed. If no VM type is selected, settings from the Scan Profile page will be used. If any VM type is selected, settings from the Scan Profile will be overridden and the file will only be scanned in selected VM types. If VM images are not ready, the VM list will not be displayed.
Direct URL	To scan only a single URL, check the *Direct URL* checkbox. Enter the URL in the *Enter a URL* field.
Allow Interaction	Select the *Allow Interaction* checkbox to interact with the Windows VM. See To use the To use the Allow Interaction Feature: on page 165 for more information.
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

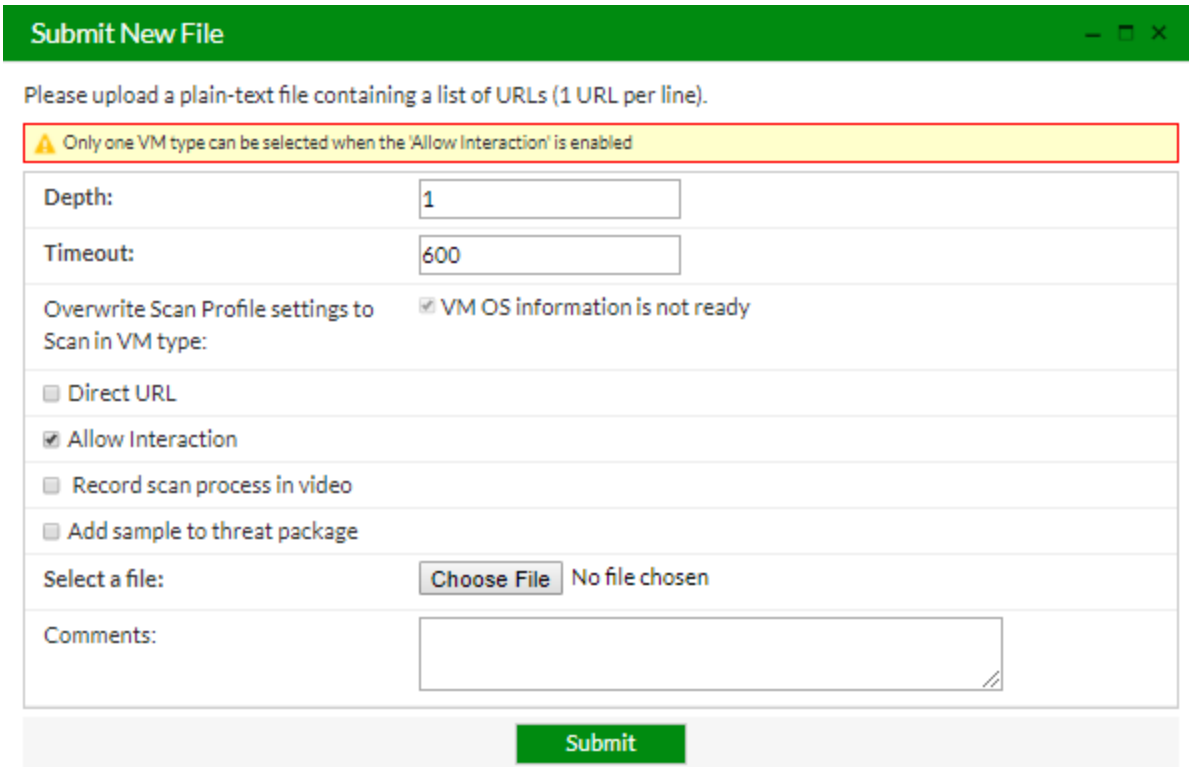
3.

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.

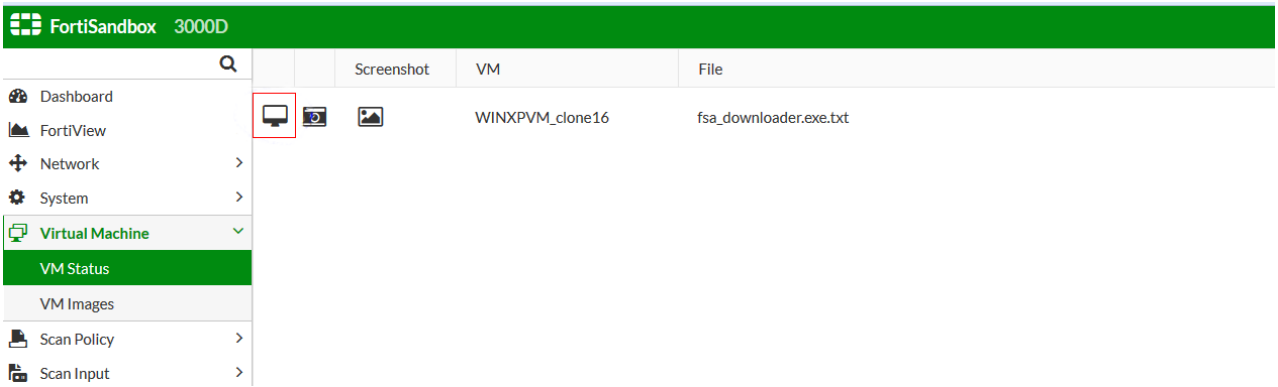
4. Click *Submit*.

To use the Allow Interaction Feature:

1. Go to *Scan Input* > *URL On-Demand* > *click Submit File / URL from the toolbar*.
2. In the Submit New File window, check the *Allow Interaction* checkbox, and click *Submit*.



3. Go to *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 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 *Scan Profile* page and change its settings.

Users can use this page's information to help make sure 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.

Input Source	File Type	Queued #	Ave Scan Time in Last 24 hrs (s)	Expected Finish Time	Arrival Rate (Last 1 hr)	VM Type (Clone #)	Prioritize
URL Sniffer	Job Queue Assignment Pending files	4910					
URL Sniffer	URL detection	283	48	00:22:47	794	WIN7X86VM(12)	
Sniffer	Job Queue Assignment Pending files	7					
Device	Executables/DLL/VBS/BAT/PS1/JAR/MSI/WSF files	0	19		2	WIN7X64VM(12) , WINXPVM1(1)	
Sniffer	Executables/DLL/VBS/BAT/PS1/JAR/MSI/WSF files	0	28		23	WIN7X64VM(12) , WINXPVM1(1)	
Device	Microsoft Office files (Word, Excel, PowerPoint files etc)	0	129			WIN7X86VM(12)	
Sniffer	Microsoft Office files (Word, Excel, PowerPoint files etc)	0	43		64	WIN7X86VM(12)	
Device	PDF files	0	36		8	WIN7X86VM(12)	
Sniffer	PDF files	0	78		10	WIN7X86VM(12)	
Device	Static Web files	0	3				
Sniffer	Static Web files	0	3		11		

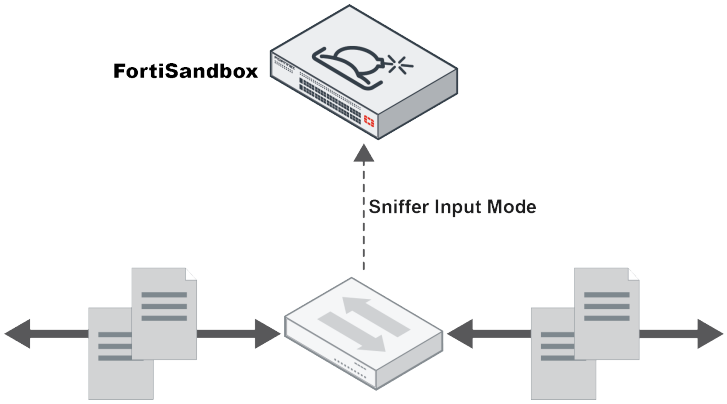
The following options are available:

Chart icon	When clicking on the *Chart* icon beside each VM type, the *VM's Usage Chart* will be displayed.
Trash icon	When clicking on the *Trash* icon, beside the Pending Job Number, the job queue will be purged.
Prioritize	When click on the *Prioritize* icon, it will take you to the *Job Queue Priority List* page where you will be able to 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.)
Pending #	Current pending job number. A *Trash Can* appears beside the pending job number. If you click on the *Trash Can* icon, the job queue will be purged.
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

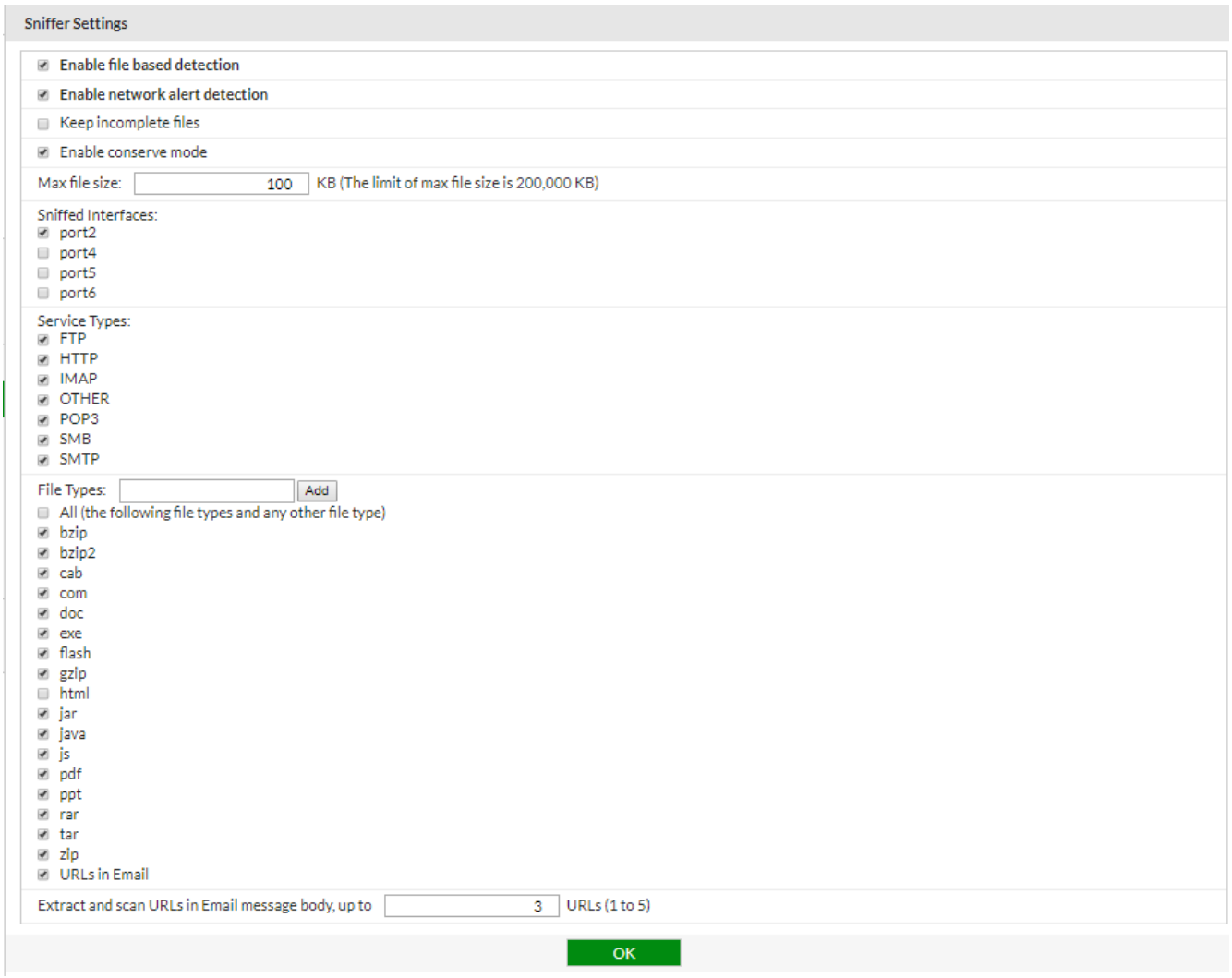


Sniffer mode relies on inputs from spanned switch ports. It is the most suitable infrastructure for adding protection capabilities to existing threat protection systems from various vendors.

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

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

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



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 are treated as not suspicious by default, such as dating. To check the list, go to 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, if there are already too many jobs in the pending queue (250K, or sniffed traffic throughput exceeds a certain value), sniffer will enter conserve mode, during which time only executable (.exe) and MS Office files are extracted. Optimal traffic throughput values for different models: • 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
Maximum 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 200,000kB. Note: Files that exceed the maximum file size will not be 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 your FortiSandbox. For FortiGate, you can select to send all files for inspection. For FortiMail, you can select to send email attachments or URLs in the email body to FortiSandbox for inspections or just the Suspicious ones. When files or URLs are received by FortiSandbox , they are executed and scanned within the VM modules. FortiSandbox also sends statistics back to the FortiGate, FortiWeb and FortiMail. When integrated with FortiGate, the following protocols are supported: HTTP, FTP, POP3, IMAP, SMTP, MAPI, IM, and their equivalent SSL encrypted versions. To view, edit, and authorize devices, go to *Scan Input* > *Device*.

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

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

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

config firewall profile-protocol-options

edit <name_str>

config http

set oversize-limit <size_int>

end

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

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

The following options are available:

Refresh	Click the *refresh* icon to refresh the entries displayed after applying search filters.
Device Filter	Users can filter devices by entering part of device name or serial number.
Clear all removable filters	Click the *trash can* icon to clear all removable filters.
Edit	Click to edit a device or a VDOM/Protected Domain. Users can edit device permission policy and device level email settings.
Delete	Click to delete the device or VDOM/Protect Domain. If a device is deleted, all its VDOMs/Protected Domain will be deleted also. If the device connects to FortiSandbox later, it will show up again as a new device.

This page displays the following:

Device Name	The name of the device and the VDOM or protected email domain that send files to FortiSandbox. For device, it has the format of: *Device Name*. For 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 or FortiMail serial number.
Malicious	The number of malicious files submitted by the FortiGate, FortiWeb or FortiMail 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 status.
High	The number of high risk files submitted by the FortiGate, FortiWeb or FortiMail to FortiSandbox in the last seven days.
Medium	The number of medium risk files submitted by the FortiGate, FortiWeb or FortiMail to FortiSandbox in the last seven days.
Low	The number of low risk files submitted by the FortiGate, FortiWeb or FortiMail to FortiSandbox in the last seven days.
Clean	The number of clean files submitted by the FortiGate, FortiWeb or FortiMail to FortiSandbox in the last seven days.
Others	The number of other files submitted by FortiGate, FortiWeb or FortiMail to FortiSandbox in the last seven days.
Malware Pkg	The malware package version currently on the device.
URL Pkg	The URL package versions currently on the device.
Authorized	If the device or VDOM/Protected Domain is authorized to submit files. Only authorized device or VDOM/Protected Domain is allowed to submit files to FortiSandbox.
Limit	If a submission limit is set for this device.
Status	The status of the FortiGate, FortiWeb or FortiMail. This field displays an up icon when the device is connected and a down icon for devices which are disconnected.

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

Supported Devices

In FortiOS, you can configure your FortiGate device to send suspicious files to FortiSandbox for inspection and analysis. FortiGate queries scan results and retrieves scan details. In FortiOS 5.4 and later, FortiGate can also download malware packages as a complimentary AV signature database to block future appearances of the same malware and download URL packages as complimentary web filtering black list.

FortiSandbox supports the following devices:

FortiGate	FortiSandbox is able to perform additional analysis on files that have been AV scanned by your FortiGate. You can configure your FortiGate to send all files or only suspicious files passing through the AV scan. 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 your FortiMail to send suspicious, high risk files and suspicious attachments. FortiSandbox is able to perform additional analysis on files that have been scanned by your FortiMail email gateway. 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. Recent release of FortiMail build can send suspicious URLs in the email body to FortiSandbox to do URL scans and block suspicious emails based on the scan result.
FortiClient	FortiSandbox can accept files from FortiClient to perform additional analysis, while FortiClient holds the files until the scan results are received. FortiClient will also receive additional antivirus signatures from FortiSandbox, generated from scan results, to supplement current signatures.
FortiWeb	You can now use a file upload restriction policy to submit uploaded files to FortiSandbox for evaluation. FortiSandbox evaluates whether the file poses a threat and returns the result to FortiWeb. If FortiSandbox determines that the file is malicious, FortiWeb performs the following tasks: • Generates an attack log message that contains the result (for example, messages with the Alert action in the illustration). • For 10 minutes after it receives the FortiSandbox results, takes the action specified by the file upload restriction policy. During this time, it does not re-submit the file to FortiSandbox (for example, messages with the Alert_Deny action in the illustration).

FortiGate devices

If port3 of the FortiSandbox is connected to an interface behind the FortiGate device, make sure the egress WAN interface does not have the *Scan Outgoing Connections to Botnet Sites* feature enabled, nor any active security profiles-- 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 how to configure FortiGate to send files to FortiSandbox, please refer to the *FortiOS Handbook* in the Fortinet Document Library.

To verify the FortiGate is connected to FortiSandbox:

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

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

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

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

To edit FortiGate settings in FortiSandbox:

1. On your FortiSandbox device, go to *Scan Input* > *Device*. All FortiGate devices and VDOMs will be listed on this page.
2. Select the FortiGate device that you want to edit. The *Edit FortiGate Settings* page opens.
3. Edit the following settings:

Device Status	
Serial Number	The device serial number is displayed.
Alias	The host name of the FortiGate unit. This is a read-only value.
IP	The IP address of the FortiGate is displayed.
Status	The status of the device, either connected or not connected. This field cannot be edited.
Last Modified	The date and time that the FortiGate settings were last changed is displayed.

Last Seen	The date and time that the FortiGate last connected to the FortiSandbox is displayed.
Permissions	
Authorized	Select the checkbox to authorize the FortiGate device. If this field is not checked, files sent from the FortiGate will be dropped. The date and time that the authorization status was changed is displayed.
New VDOMs/Domains inherit authorization	Select the checkbox to have new VDOMs inherit the authorization setting configured at the device level.
Email Settings	
Administrator Email	The email address entered in the *Notifier Email* field configured on the FortiGate device at *System* > *Config* > *FortiSandbox*. You cannot edit this field on the FortiSandbox.
Send Notifications	Select the checkbox to send notifications. When notifications are enabled, you will receive email notifications when a file from your environment has been detected as potential malware. The email will contain a link to the scan job details page. To receive notification emails, you must configure a mail server and enable *Send a notification email to the global email list when malicious files are detected* settings in *System* > *Mail Server*.
Send Reports	Select the checkbox to send job detail PDF reports. To receive reports and define report generation frequency, you must configure mail server and enable *Send scheduled PDF report about an individual VDOM/Domain to its email address* in *System* > *Mail Server*.

4. Click *OK* to save the settings.

To edit VDOM settings:

1. On your FortiSandbox device, go to *Scan Input* > *Device*. All FortiGate devices and VDOMs will be listed on this page.
2. Select the VDOM that you want to edit.
3. Edit the following settings:

Device Status	
Domain/VDOM	The device VDOM name. This field cannot be edited.
Alias	VDOM name is in the *Device Name: VDOM name* format.
IP	The IP address of the FortiGate. This field cannot be edited.
Status	The status of the device, either connected or not connected. This field cannot be edited. If the VDOM does not contact FortiSandbox after 15 minutes, the status will change to *Disconnected*.

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

4. Click *OK* to save the settings.

FortiMail devices

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

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

If protected domain information is not available, such as files from older versions of FortiMail or outgoing emails, jobs from them will be grouped in Unprotected domain name. For older versions of FortiMail devices, which does not send protected domain information to FortiSandbox, the user can not set a submission limitation.

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

To edit FortiMail Settings in FortiSandbox:

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

3. Edit the following settings:

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

4. Click *OK* to save the settings.

To edit Domain settings:

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

3. Edit the following settings:

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

4. Click *OK* to save the settings.

Upload suspicious attachments to FortiSandbox

For more information on how to configure FortiMail e to send files to FortiSandbox, please refer to the FortiMail Administration Guide available on the Fortinet Document Library.

Device and VDOM/Domain level notifications

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

Sample notification email

This email will contain a link to the *Scan Job Details* page. You can also view the *View Details* page in the Suspicious, Clean Files, and On-Demand dashboard pages.

You can enable or disable VDOM level notifications for each VDO sending files to FortiSandbox. To configure global notifications, go to *System* > *Mail Server*.

Device and VDOM/Domain level PDF reports

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

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

You can enable or disable device and VDOM/Domain level reports for each device or VDOM/Domain sending files to FortiSandbox in their edit page.

FortiWeb

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

FortiClient

FortiClient 5.4 and previous versions can silently connect to FortiSandbox without needing to be authorized. Users can de-authorize a FortiClient host manually.

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

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

The following options are available:

Refresh	Click the *refresh* icon to refresh the entries displayed after applying search filters.
Device Filter	Users can filter FortiClient by entering part of host name, host IP or serial number.
Edit	Click to edit the FortiClient. Users can enable or disable authorization of the FortiClient
Delete	Click to delete the FortiClient. If FortiClient connects to FortiSandbox later, it will show up again as a new one.

This page displays the following information:

FCT Serial	The FortiClient serial number.
Hostname	Hostname.
User	Current login user on the FortiClient host, if the information is available.
IP	Host IP Address.
Malicious	The number of malicious files forwarded by the FortiClient to FortiSandbox in the last seven days. Malicious files are not executed in the FortiSandbox VM module as the antivirus scanner has already determined the file rating.
High Risk	The number of high risk rating files submitted to FortiSandbox in the last seven days.
Medium Risk	The number of medium rating risk files submitted to FortiSandbox in the last seven days.
Low Risk	The number of low risk rating files submitted to FortiSandbox in the last seven days.
Clean	The number of clean rating files submitted to FortiSandbox in the last seven days.
Others	The number of other rating files submitted by FortiGate or FortiMail to FortiSandbox in the last seven days.
Malware Pkg	The malware package currently on the device.
URL Pkg	The URL package versions currently on the device.

Auth	If the FortiClient is authorized. The user can click on the FortiClient serial number and modify its authorization status manually.
Status	The status of the FortiClient host. This field displays an up icon when the device is connected and a down icon for devices which are disconnected.

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

Adapter

FortiSandbox uses adapters to connect to third party products. Carbon Black/Bit9 server and ICAP client are supported. FortiSandbox automatically create an ICAP adapter which allows FortiSandbox to work as an ICAP server.With an Adapter, FortiSandbox can analyze files downloaded from the Carbon Black server to send notifications of file verdict back to the server, or receive HTTP message from an ICAP client and return a response to it.

The following options are available:

Create New	Create a new adapter.
Edit	Edit an adapter.
Delete	Delete an adapter. ICAP adapter cannot be deleted.

This page displays the following information:

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

To create a new adapter:

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

3. Configure the following:

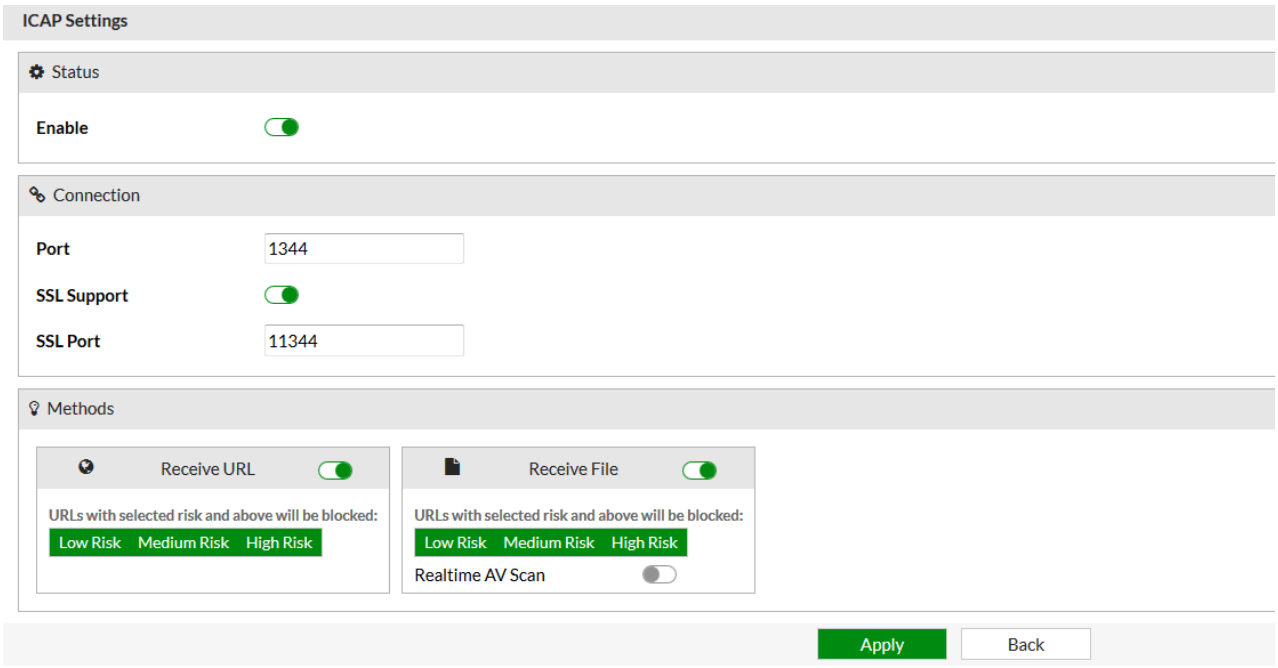
Vendor Name	Select *Carbon Blaclk/Bit9* as the vendor name.
Adapter Name	Enter the adapter name.
Server FQDN/IP	Enter the FQDN/IP address of the Carbon Black server.
Token	Enter the token string. Authentication token is assigned by the Carbon Black or ICAP server.
Timeout (seconds)	Enter the timeout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

4. Click OK to save the entry.

To edit an adapter:

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

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



5. Click *OK* to save the entry.

To delete an adapter

1. Go to *Scan Input* > *Adapter*.
2. Select an adapter.
   ICAP adapter cannot be selected.
3. Click the *Delete* button from the toolbar.
4. Click *Yes I'm sure* button from the *Are you sure* confirmation box.

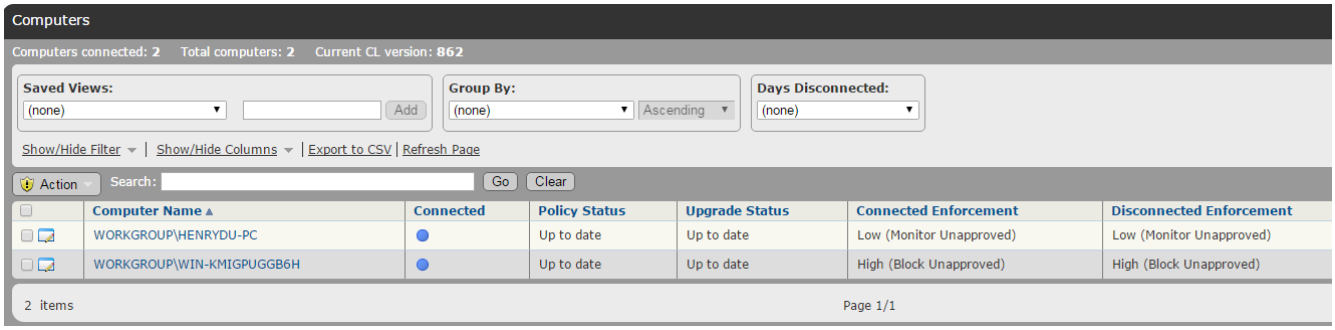
After a Carbon Black adapter is created, FortiSandbox will try to communicate with Carbon Black server. If the connection and authentication is successful, the status column will show a green icon, otherwise a red icon is displayed.

CLI command: `diagnose-debug adapter` can be used to troubleshoot communciations with the Carbon Black server.

Configure Carbon Black/Bit9 Server

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

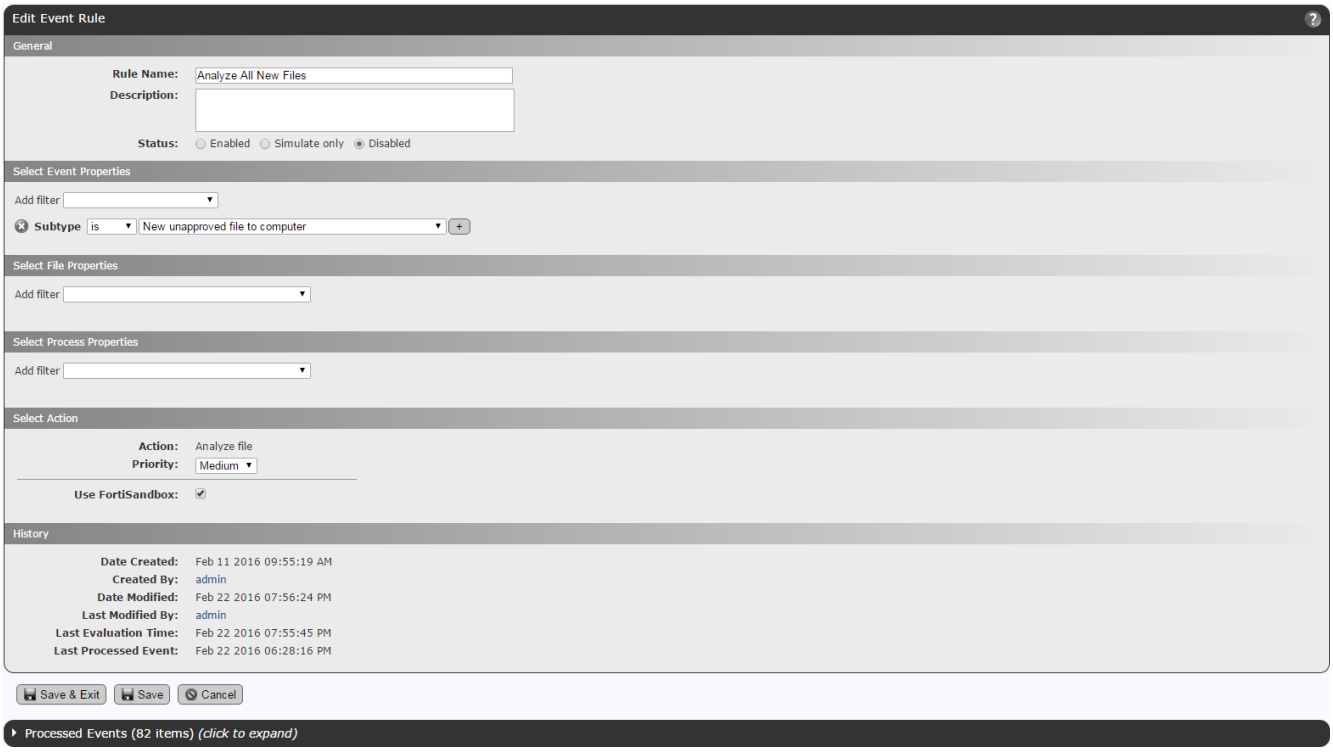
Submitting selected files to FortiSandbox



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

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

Creating an event rule to automatically submit files to FortiSandbox



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

How to view analysis results

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

Configure ICAP Client

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

When ICAP client sends a HTTP request to FortiSandbox, FortiSandbox extracts the URL and checks if a verdict is available. If the verdict is not a *user selected blocking rating* or 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. Scan Profile settings 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 or not available , 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. Scan Profile settings 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
```

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	Select to create a new network share.
Edit	Select an entry from the list and then select *Edit* in the toolbar to edit the entry selected.
Delete	Select an entry from the list and then select *Delete* in the toolbar to remove the entry selected.
Scan Now	Select an entry from the list and then select *Scan Now* in the toolbar to scan the entries.
Scan Details	Select an entry from the list and then select *Scan Details* in the toolbar to view the scheduled scan entries.
Test Connection	Select an entry from the list and then select *Test Connection* in the toolbar to test the connection. Result message will be displayed in the top message bar.

The following information is displayed:

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

To create a new network share:

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

Enabled	Select to enable network share configuration. If network share is not enabled, its scheduled scan will not run.
Network Share Name	Enter the network share name.
Mount Type	Select the mount type from the drop-down list. The following options are available: • CIFS (SMB v2.0 and v2.5) • 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`
Scan Files Of Specified Pattern	Select to include or exclude files which match a file pattern.
File Pattern Name	Enter the file pattern name.
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.
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 and only Sandboxing scan of 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 drop-down 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 drop-down 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 drop-down 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 drop-down 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 drop-down 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 drop-down list. Select the minute or hour from the second drop-down 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*.
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 *Scans* 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.

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 drop-down list. The following options are available: • CIFS (SMB v2.0 and v2.5) • 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 form 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 an 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	You have the option to download the malware's download URL. It is not related to URL scan.

This page displays the following:

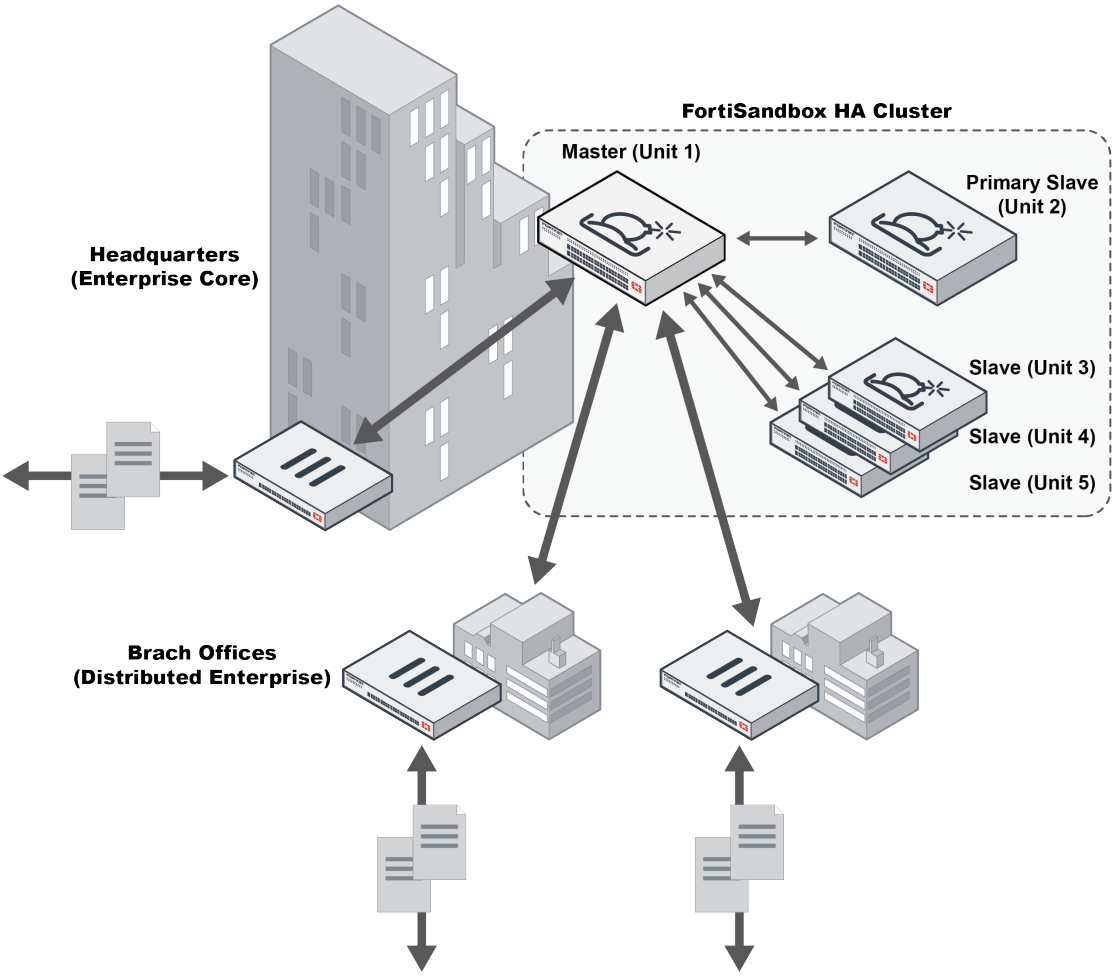
Version	The URL package release version.
Release Time	The URL package release time.
Total	The total number of malware antivirus signatures inside the package. The maximum number of signatures is 1000.

FortiSandbox only keeps URL packages generated in last 7 days.

HA-Cluster

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

There are three types of nodes in a cluster: Master, Primary Slave, and Slave.



Master	The Master node (Unit 1 in the diagram) manages the cluster, distributes jobs and gathers the results, and interacts with clients. It can also perform normal file scans. All of the scan related configuration should be done on the master node and they will be broadcasted from the Master node to the other nodes. Any scan related configuration that has been set on a slave will be overwritten. On the Master node, users can: • Change a slave node's role (Primary and Regular slave) • Configure a slave node's network settings • Upgrade slave nodes • View VM status page of slave nodes • Configure FortiGuard settings of slave nodes • Configure VM images of slave 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 Primary Slave node when necessary to trigger a failover Although all FSA models can work as a Master node, it is advised to use a FortiSandbox-3000D or above model.
Primary Slave	The Primary Slave node (Unit 2 in the diagram) is for HA support and normal file scans. It monitors the master's condition and, if the master node fails, the primary slave will assume the role of master. The former master will then become a primary slave when it is back up. The Primary Slave node must be the same model as the Master node.
Slave	The Slave nodes (Units 3 - 5 in the diagram) perform normal file scans and report results back to the master and primary slave. They can also store detailed job information. Slave nodes should have its own network settings and VM image settings. The Slave nodes can be any FortiSandbox model, including FortiSandbox VM. Slave nodes in a cluster does not need to be the same model.

The total number of slaves, include the primary slave, can not exceed 100.

It is advised to use FortiSandbox-3000D and above if the job load is heavy.

This section includes the following topics:

- Configure a cluster level fail-over IP set for Master unit
- Upgrading or rebooting a Cluster
- In-line mode
- Health Check
- Job Summary
- Status
- HA Cluster Information

Centrally manage Slave nodes on the Master node

Users can manage Slave nodes on the Master node.

1. Go to *HA Cluster*.
2. Select the Slave node's serial number.
3. Users can perform any of the following tasks:

1. View the Slave node's dashboard.
2. Switch the Slave node's role using the *Dashboard* > *System Information* widget.
3. Configure the Slave node's network settings (such as its IP address, routing table, DNS and Proxy settings). Configure Slave nodes' network settings for VM external traffic through port3.
4. Upgrade the Slave node (including firmware, AV database etc.).
5. View the Slave node's VM Status page.
6. View and configure Slave 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 includes:
   - job dispatch
   - job result reply
   - setting synchronization
   - cluster topology broadcasting

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

Master's Role and Slave's Role

On the Master node, all functionalities are 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 Master node and will be synchronized to other nodes. The following information is synchronized from the Master node to all other nodes so they should not be configured on Slave nodes:

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

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

The following information are synchronized from the Master node to Primary Slave nodes only, and are only applied when the Primary Slave node becomes a Master during a failover:

- Users
- Archive server settings
- Sniffer settings
- Mail server settings
- Network settings (including DNS, proxy, and routing tables)
- Scheduled task settings (network share scans, and scheduled report generation)
- Log server settings
- Uploaded certificates
- Devices
- SNMP settings
- Widget settings
- Adapter settings
- Others (login disclaimers)

Configure a cluster level fail-over IP set for Master unit

The user can configure a cluster level fail-over IP for each port except port3 and ports the sniffer is sniffing. This IP set works as an alias IP of the Master node network port. The Master node Local IP set and Primary Slave node Local IP set are kept during fail-over.

This fail-over IP set should be set on the current Master node through the CLI command `hc-settings`. Itshould be in the same subnet of each port's local IP. Client devices such as FortiGate should point to this fail-over IP. When a failover occurs, this fail-over IP set will be applied on the new Master node.

Main HA Cluster CLI Commands

hc-settings	Configure the unit as a HA Cluster mode unit. Configure cluster fail-over IP set.
hc-status	List the stats of HA Cluster units.
hc-slave	*Add*, *Update*, *Remove* a slave unit to or from the HA Cluster.
hc-master	Turn on/off the file scan on the Master node and adjust the Master's scan power.

Example configuration

This example shows the steps for setting up an HA cluster using three FortiSandbox 3000D units.

Step 1 - Prepare the hardware

The following hardware will be required:

- Nine cables for network connections
- Three 1/10 Gbps switches
- Three FortiSandbox 3000D units with proper power connections (units A, B, and C).

The master and primary slaves should be on different power circuits.

Step 2 - Prepare the subnets

Prepare three subnets for your cluster (customize as needed):

- Switch A: 192.168.1.0/24: For system management.
  - Gateway address: 192.168.1.1
  - External management IP address: 192.168.1.99
- Switch B: 192.168.2.0/24: For internal cluster communications.
- Switch C: 192.168.3.0/24: For the outgoing port (port 3) on each unit.
  - Gateway address: 192.168.3.1

Step 3 - Setup the physical connections

1. Connect port 1 of each FortiSandbox device to Switch A..
2. Connect port 2 of each FortiSandbox device to Switch B.
3. Connect port 3 of each FortiSandbox device to Switch C.

Step 4 - Configure the master

1. Power on the device (Unit A), and log into the CLI (See Connecting to the Command Line Interface on page 13)
2. Configure the port IP addresses and gateway address with the following commands:

```
set port1-ip 192.168.1.99/24
set port2-ip 192.168.2.99/24
set port3-ip 192.168.3.99/24
```

3. Configure the device as the master node and its cluster fail-over IP for Port1 with the following commands:

```
hc-settings -sc -tM -nMasterA -cTestHCsystem -ppassw0rd -iport2
hc-settings -si -iport1 -a192.168.1.98/24
```

   See the FortiSandbox CLI Reference Guide available on the Fortinet Document Library for more information about the CLI commands.

4. Review the cluster status with the following command:

```
hc-status -l
```

   Other ports on the device can be used for file inputs.

Step 5 - Configure the primary slave

1. Power on the device (Unit B), and log into the CLI.
2. Configure the port IP addresses and gateway address with the following commands:

```
set port1-ip 192.168.1.100/24
set port2-ip 192.168.2.100/24
set port3-ip 192.168.3.100/24
```

3. Configure the device as the primary slave node with the following commands:

```
hc-settings -s -tP -nPslaveB -iport2
hc-settings -l
hc-slave -a -s192.168.2.99 -ppassw0rd
```

4. Review the cluster status with the following command:

```
hc-status -l
```

Step 6 - Configure the normal slave

1. Power on the device (Unit C), and log into the CLI.
2. Configure the port IP addresses and gateway address with the following commands:

```
set port1-ip 192.168.1.101/24
set port2-ip 192.168.2.101/24
set port3-ip 192.168.3.101/24
```

3. Configure the device as a slave node with the following commands:

```
hc-settings -s -tR -nSlaveC -iport2
hc-settings -l
hc-slave -a -s192.168.2.99 -ppassw0rd
```

4. Review the cluster status with the following command:

```
hc-status -l
```

Step 7 - Configure other settings

VM Image settings and network settings, such as default gateway, static route, and DNS servers etc., should be configured on each unit individually. Scan related settings, such as the scan profile, should be set on Master unit only; they will be synchronized to the Slave node. For more details, refer to Master's Role and Slave's Role on page 205.

Step 8 - Finish

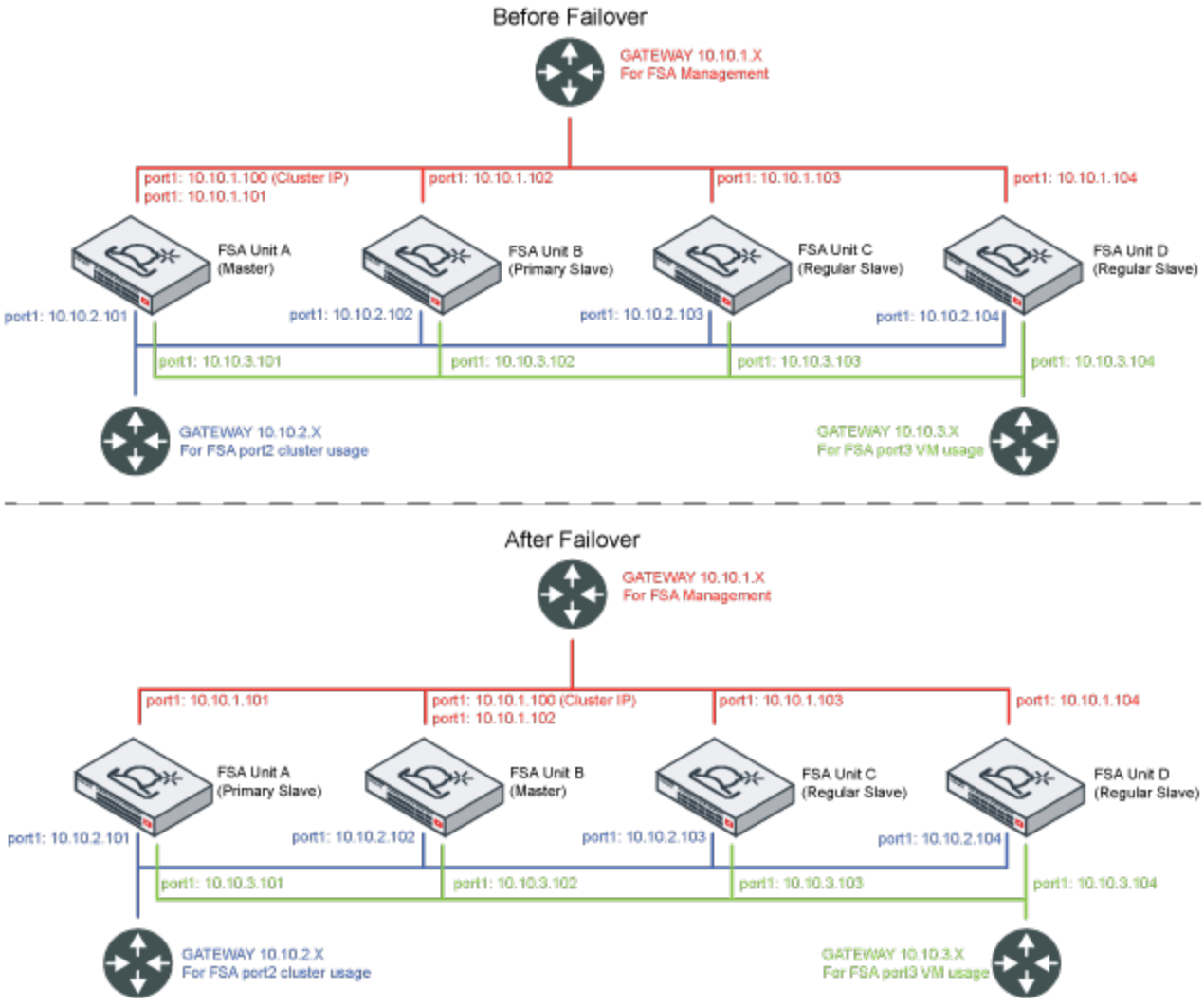
The HA cluster can now be treated like a single, extremely powerful standalone FortiSandbox unit.

In this example, files are submitted to, and reports and logs are available over IP address 192.168.1.99.

FortiSandbox 3500D unit has been configured as a cluster system, with blade 1 configured as the Master node, blade 2 as the Primary Slave node and the other blades as Regular Slave nodes.

What happens during a failover

The Master node and Primary Slave nodes sends heartbeats to each other to detect if it peers are alive. If the Master node is not accessible, such as rebooting, a fail-over will occur. Users can also configure a Ping server to frequently check the unit's network condition and downgrade itself to Primary Slave type when the condition is appropriate to trigger a failover. The failover logic handles two different scenarios:



Objective node available	The Object node is a slave (either Primary or Regular) that can justify the new Master. For example, if a cluster is consisted of one Master node, one Primary Slave node, and one Regular Slave node, the Regular Slave node is the objective node. After a Primary Slave node takes over the Master role, and the new role is accepted by the Object node, the original Master node will accept the decision when it is back online. After the original Master is back online, it will become a Primary Slave node.
No Objective node available	This occurs when the cluster's internal communication is down. For example, the cluster contains one Master node and one Primary Slave node and the Master node reboots; or the internal cluster communication is down due to a failed switch, all Primary Slave nodes become the Master (more than one Master unit). When the system is back online, the unit with the largest Serial Number will keep the Master role and the other will return back to a Primary Slave.

When the new Master is decided, it will:

1. Restart the main controller to rebuild the scan environment.
2. Apply all the setting synchronized from the original Master except port3 IP and the internal cluster IP of the original Master.

After a failover occurs, the original Master might become a Primary Slave node.

It keeps its original Port3 IP and internal cluster communication IP. All other interface ports will be shutdown as it becomes a slave node. Some functionalities will be turned off such as Email Alerts. If the user wants to re-configure its settings, such as the interface IP, the user must do that through the CLI command or the Master's Central Management page.

As the new Master takes over, the network settings of the management port (port1) and the port that client devices communicate with, will switch to it. As the new Master starts 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 Master unit's central management interface by going into each device's dashboard page. You must upgrade the cluster in the following order:

1. Slave devices
2. Primary Slave
3. Master

If you are upgrading from 2.1 to 2.2, you have to reconfigure the cluster on the master because 2.2 brings new features, such as redesigned scan profile, clone number for each VM, and isolated port3 configuration.

It is highly recommended to setup cluster level fail-over IP set so the fail-over between Master and Primary Slave can occur smoothly. If the user does not want the fail-over to happen, the user can change the Primary Slave unit role to Regular Slave. You can either do this through the UI dashboard or the CLI prior to the fail-over, then change the role back after the unit boots up.

Health Check

The Health Check page is only available on the Master node. Users can use the HA Health Check to set up a Ping server to ensure the network condition between client devices and FortiSandbox is always up. If not, the Master node will downgrade itself to a Primary Slave node if there is at least one Primary Slave node existing, a failover will occur after the configured period elapses. If no Primary Slave node exists, the Master node will keep its Master 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.
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 Master node will downgrade itself as a Primary Slave if there is an existing Primary Slave node.

To create a new HA Health Check

1. Go to *HA-Cluster* > *Health Check*.
2. Click + *Create New* from the tool bar.
3. Configure the settings.
4. Click *Ok*.

To edit a HA Health Check

1. Go to *HA-Cluster* > *Health Check*.
2. Select the Health Check you want to edit.
3. Click the *Edit* button from the toolbar.
4. Edit the settings.
5. Click *Ok*.

To delete a HA Health Check

1. Go to *HA-Cluster* > *Health Check*.
2. Select the Health Check you want to delete.
3. Click the *Delete* button from the toolbar.
4. Click the *Yes, I'm sure* button to delete the Health Check.

Job Summary

The Job Summary page shows job statistics data of each node in a cluster. It is only available on the Master node.

To view a HA Job Summary

1. Go to *HA-Cluster* > *Job Summary*.
2. Select either *File* or *URL* button to view file-based scan results and URL scan results..
   The following information is shown:

Time Period Drop down	Select the period of time over which the data was collected from the drop down. 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: *Master*, *Primary Slave*, or *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 master.

HA Cluster Information

On a Master, you can select a Slave to view and manage the following information pertaining to that Slave:

For more detailed information regarding each section, click on the respective link.

- System Status Dashboard: The following widgets are displayed: System Information, Scanning Statistics, System Resources, and Disk Monitor.
- Interfaces on page 73
- Static Routing on page 80
- DNS Configuration on page 79
- General on page 130 (VM Network)
- FortiGuard on page 103
- VM Status on page 112
- VM Images on page 113

File Detection

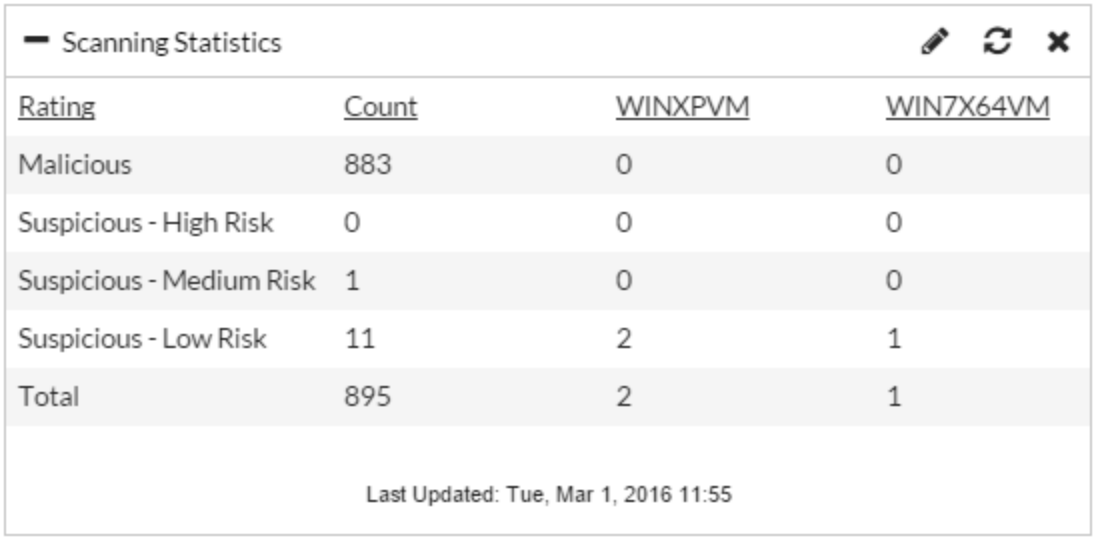
This section includes the following topics:

Summary Report

The *Summary Reports* page provides a page similar to the *System* dashboard. You can add and customize widgets in this page. By selecting a device and time period, you can customize what data is displayed. To view the summary reports page go to *File Detection* > *Summary Report*.

If the unit is the master node in a cluster, the data are a summary of all cluster nodes. Otherwise, only the individual unit's data are displayed.

On-Demand job data is not included.



The following options are available:

Add Widget	Click the button to add widgets to the summary report page.
Reset View	Click the 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 drop-down list. The options are: *Last 24 hours*, *Last 7 days*, *Last 2 weeks*.
Device	Select the device from the drop-down list.

The following widgets are available:

Scanning Statistics	Displays a table providing information about the files scanned for a selected device for a selected time period.

Scanning Statistics by Type	Displays a table proving information about file types, rating, and event count for a selected device over a selected time period.
Top Targeted Hosts	Displays a chart providing the number of infection events for specific hosts that have occurred 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 that have occurred for the host selected. Selecting the infected host allows you to drill down to the job details.
File Scanning Activity	Displays the number of clean, suspicious, and malicious events that have occurred 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 of the selected type that occurred at that time.
Top Infectious URLs	Displays a chart providing the top infectious URLs that have been detected 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 that have occurred for the malware selected.
Top Malware	Displays a chart providing the number of infection events for specific malware that have occurred 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 that have occurred for the malware selected. Selecting the malware name allows you to drill down to the job details related to them.
Top Callback Domains	Displays a chart providing the top callback domains that have been detected over a selected time period. Callback domains are hosts that files visit when executing in VM. Hover the cursor over a colored portion of a bar in the chart to view the exact number of infection events that have occurred for the malware selected.
Top File Types	Displays a chart providing the top file types that have been detected over a selected time period. When *Scanned by Sandboxing* is selected, only files that have finished sandboxing will be counted.

Customizing the summary report page

The FortiSandbox summary reports page can be customized. You can select the device and time period in the toolbar to display specific information. You can also select which widgets to display, where they are located in the page, and whether they are minimized or maximized.

To move a widget

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

To refresh a widget

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

To add a widget

In the 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.

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 Infectious URLs*: 3600 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

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. Do not close the dialog box or navigate away from the page during report generation.
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, users can also select the *Rescan* icon to perform a manual rescan of the file. By this way, you can find out the behavior of a known virus. You can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing in the rescan settings.
	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 customized 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 a Anti Virus rescan feature. When a new antivirus signature is available, FortiSandbox will perform a second antivirus scan of all the jobs from 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 107.

To view file details:

1. Select a file.
2. Click the *View Details* icon. A new tab will open. See Appendix A - View Details Page Reference on page 252 for descriptions of the *View Details* page.
3. Close the tab to exit the *View Details* page.

To rescan a file:

1. Select a file with Malicious Rating.
2. Click the *Perform Rescan* icon.
3. You can select to skip *Static Scan*, *AV Scan*, *Cloud Query*, and *Sandboxing*.
4. Click *OK* to start the rescan.
5. Click the close icon or select the *Close* button to close the dialog box.

Rescan results are found in the *Scan Input* > *File On-Demand*.

To create a snapshot report for all malicious files:

1. Click the *Export Data* button in the toolbar. The *Report Generator* window opens.
2. Select either PDF or CSV for the report type. Optionally you can further define the report start/end date and time.
3. 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.
4. Click the close icon or select the *Cancel* button, to quit the report generator.

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

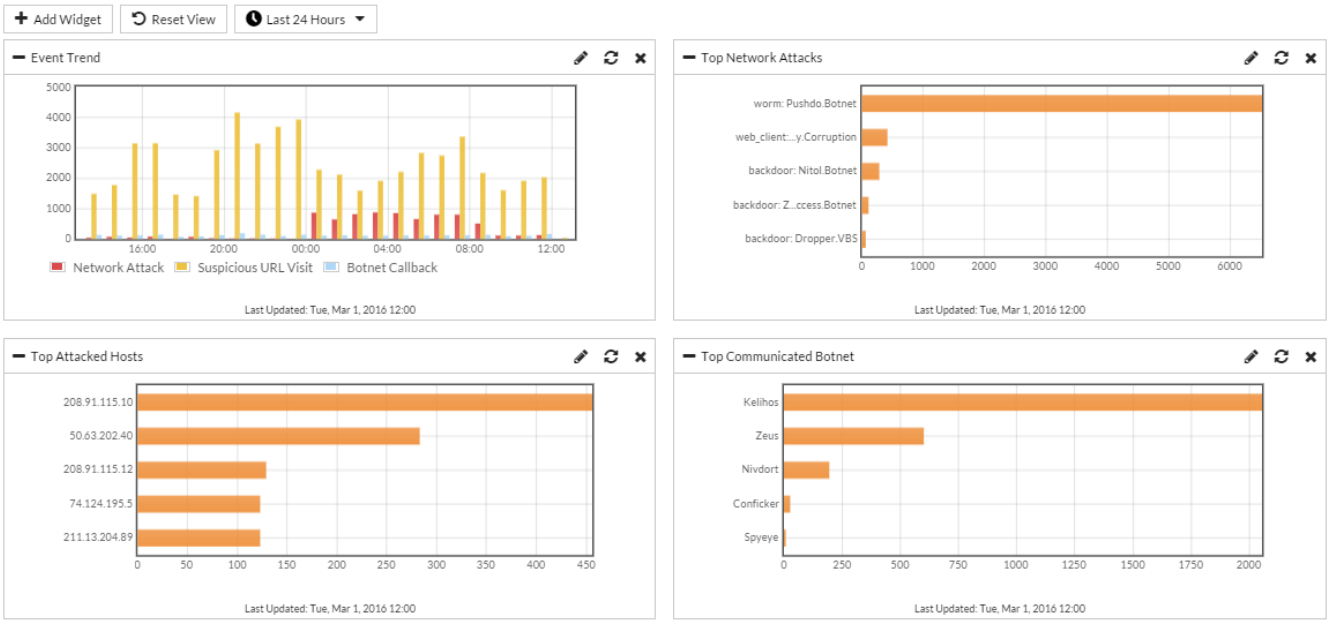
Network Alerts

Network Alerts allows you to view network based activity. 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

The *Summary Reports* page provides a page similar to the *System* dashboard. You can add and customize widgets in this page. By selecting the time period, you can customize what data is displayed. To view the summary reports page go to *Network Alerts* > *Summary Report*.



The following options are available:

Add Widget	Click the button to add widgets to the summary report page.
Reset View	Click the 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 drop-down list. The options are: *Last 24 hours*, *Last 7 days*, *Last 2 weeks*.

The following widgets are available:

Event Trend	Displays a table 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.
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 URL Hosts	Displays a table providing information about the top visited suspicious URL 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 visiting 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 add a widget

In the 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.

To edit a widget

Click the edit icon in the widget's title bar to open the edit widget settings window.

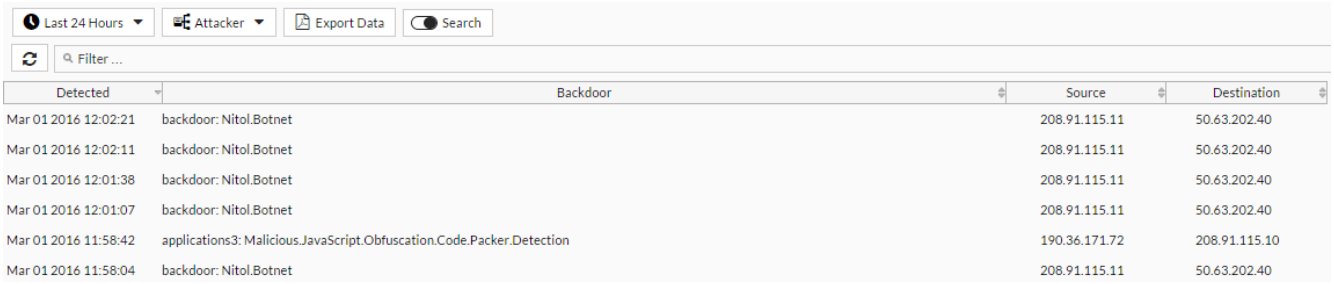
Configure the following information, and then select *OK* to apply your changes:

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 20 entries. This setting is available in all widgets except *Event Trend*.

Network Alerts

FortiSandbox scans sniffed traffic for connections to botnet servers using the botnet database and attack traffic using the IPS signature database. FortiSandbox then compares this traffic against the Web Filter database.

To view network alerts (Attacker, Botnet, and URL), go to *Network Alerts*. You can drill down the information displayed and apply search filters. You can select to create a PDF or CSV format snapshot report for specific types of network alert files. Search filters will be applied to the detailed report and will be displayed in the Report Profile section.



This page has the following options:

Time Period	Select the time period from the drop-down 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 drop-down 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	When selecting *Attacker* from the drop-down 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	When selecting *Botnet* from the drop-down 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. By default, FortiSandbox queries the public FDN service for the URL category. You can override the server address in the *System* > *Maintenance* > *FortiGuard* page.
URL	When selecting *URL* from the drop-down 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. Tip: 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. Do not close the dialog box or navigate away from the page during report generation.
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 drop-down list.
2. Select Attacker, Botnet, or URL from the second drop-down 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. Optionally you can further define the report start/end date and time.
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. 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 PDF report is 5,000; the maximum number of events you can export to CSV report is 150,000.

URL Detection

This section includes the following topics:

Summary Report

The *Summary Report* page provides a page similar to the *System* dashboard. You can add and customize widgets in this page. By selecting a time period, you can customize what data is displayed. To view the summary report page go to *URL Detection* > *Summary Report*.

Job data of URLs submitted through On-Demand or JSON API are also included in the Summary Report.

The following options are available:

Add Widget	Click the button to add widgets to the summary report page.
Reset View	Click the 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 drop-down list. The options are: *Last 24 hours*, *Last 7 days*, *Last 2 weeks*.
Device	Click the button to filter for a specific device.

The following widgets are available:

Scanning Statistics	Displays a table providing information about the URLs scanned per OS for a selected time period. Clicking on the number in the widget will drill down to the associated job list.
Scanning Statistics by Type	Displays a table proving information about URL types, rating, and event count for a selected time period. Clicking on the number in the widget will drill down to the associated job list.
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.
Top Infectious URLs	Displays a chart providing the top infectious URLs that have been detected 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 that have occurred for the malware selected. Clicking on the URL in the widget will drill down to the associated job list.

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.

To add a widget

In the 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.

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 • *Scanning Activity*: 300 seconds • *Top Infectious URLs*: 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 the *Top Infectious URLs* widget.

URL Scan

The URL Scan page shows jobs of URL based scans grouped by their ratings. URLs submitted through On-Demand are not included. Users can toggle to view Suspicious and Clean job ratings. By default, Suspicious jobs are displayed. URLs are submitted through the Fortinet device, like FortiMail and the JSON API.

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. Do not close the dialog box or navigate away from the page during report generation.
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	Click the icon to rescan the entry. In the Rescan Configuration dialog box you can select to skip Static Scan, AV Scan, Cloud Query, and Sandboxing. Click *OK* to continue. Click the *Close* icon or button to close the dialog box. This feature is only available for URLs with a Malicious rating.
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 107.

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

If the URL is submitted by FortiMail, Email sender/receiver and the subject will by shown as well.

Log & Report

The Log & Reports menu allows you to view and download all logs collected by the device, access reports, and generate reports. You can log locally to FortiSandbox, a remote syslog server, or FortiAnalyzer/FortiManager.

This section includes the following topics:

About Logs

Log Details

To view more details about a specific log in the log list, simply select that log. A log details pane 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.
Debug	Detailed information useful for debugging purposes.	Launching job for file. jobid=2726271637747836543 filename=log md5=ebe5ae2bec3b653c2970e8cec9f5f1d9 sha1=06ea6108d02513f0d278ecc8d443df86dac2885b sha256=d678da5fb9ea3ee20af779a4ae13c402585ebb070edcf20091cb20509000f74b

Raw logs

Raw logs can be downloaded and saved to the management computer using the *Download Raw Logs* button. The raw logs will be saved as a text file with the extension *.log.gz*. The user can search the system log for more information.

Sample raw logs file content

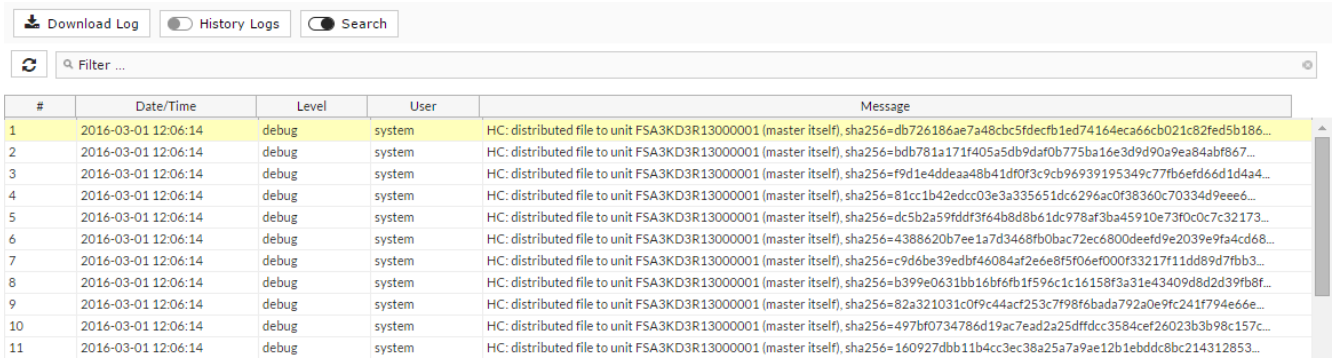
```
itime=1458669062 date=2016-03-22 time=17:51:02 logid=1220000020 type=event subtype=unknown
      pri=alert user=system ui=system action=rating status=success reason=none letype=6
      msg=fname=v32.cab jobid=2725911139058114340 sha1=f61045626e5f4f74108fb6b15dde284fe0249370
      sha256=f75fca6300e48ec4876661314475cdd7f38d4c73e87dfb5a423ef34a7ce0154f rating=Clean
      scantime=11 malwarename=N/A srcip=204.79.197.200 dstip=208.91.115.250 protocol=HTTP
      device=() url=http://officecdn.microsoft.com/pr/492350f6-3a01-4f97-b9c0-
      c7c6ddf67d60/Office/Data/v32.cab
itime=1458669062 date=2016-03-22 time=17:51:02 logid=0106000001 type=event subtype=system
      pri=debug user=system ui=system action=controller status=success reason=none letype=6
      pid=8605 msg="Sandboxing environment is not available for job 2725913445926977878, file
      type: htm, file extension: htm"
itime=1458669062 date=2016-03-22 time=17:51:02 logid=1220000020 type=event subtype=unknown
      pri=alert user=system ui=system action=rating status=success reason=none letype=6
      msg=fname=0_22_93_0_0_2_0_0_1.html jobid=2725913445926977878
      sha1=098a2ca8d81979f2bb281af236f9baa651d557d5
      sha256=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* 2.5.1 *Log Reference* available on the Fortinet Document Library.

Log Categories

In FortiSandbox, logs are group into different categories

All Events	Shows all logs.
System Events	Shows system level logs, like user creation and FDN downloads.
VM Events	Shows logs related to a VM system, such as VM initialization.
Job Events	Shows logs related to scans. Users can trace the scan flow of each file or URL.
HA-Cluster Events	Shows logs related to cluster configuration and fail overs.
Notification Events	Shows logs related to email alerts and SNMP traps.



The following options are available:

Download Raw Log	Select to download a file containing the raw logs to the management computer.
History Logs	Enable to include historical logs in Log Search.
Refresh	Select to refresh the log message list.
Add Search Filter	Click the search filter field to add search filters. Users can select different categories to search the logs. The Search feature is not case sensitive.
Pagination	Use these controls to jump or scroll to other pages. The total number of pagers and logs is also shown.

The following information is displayed:

#	Log number.
Date/Time	The time that the log message was created.

Level	The level of the log message. The available 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	Detailing log message.

Log Servers

FortiSandbox logs can be sent to a remote syslog server, common event type (CEF) server, or FortiAnalyzer. Go to *Log & Reports > Log Servers* to create new, edit, and delete remote log server settings. You can configure up to 30 remote log server entries.

The following options are available:

Create New	Select to create a new log server entry.
Edit	Select a log server entry in the list and select *Edit* in the toolbar to edit the entry.
Delete	Select a log server entry in the list and select *Delete* in the toolbar to delete the entry.

This page displays the following information:

Name	The name of the server entry.
Server Type	The server type. One of the following options: CEF, syslog , or FortiAnalyzer.
Server Address	The log server address.
Port	The log server port number.
Status	The status of the log server, *Enabled* or *Disabled*.

To create a new server entry:

1. Go to *Log & Reports > Log Servers*.
2. Select *+ Create New* from the toolbar.
3. Configure the following settings:

Name	Enter a name for the new server entry.
Type	Select *Log Server Type* from the drop-down list.
Log Server Address	Enter the log server IP address or FQDN.
Port	Enter the 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. Users can choose to send Clean Job Alert Logs by selecting *Include job with Clean Rating*. • Enable Critical Logs • Enable Error Logs • Enable Warning Logs • Enable Information Logs • Enable Debug Logs

4. Select *OK* to save the entry.

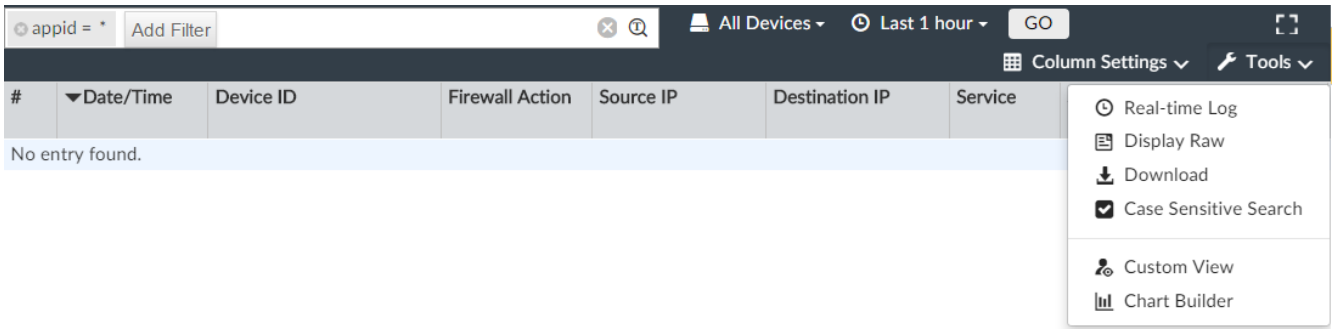
You can forward FortiSandbox logs to a FortiAnalyzer running 5.2.0 or later.

To edit or delete a syslog server, FortiAnalyzer, new common event entry

1. Go to *Log and Report* > *Log Servers*.
2. Select a syslog server, FortiAnalyzer, or new common event entry.
3. Click the *Edit* or *Delete* button from the toolbar.
1. Make the necessary edits.
2. Click the *Yes, I'm sure* button to delete the entry.

Viewing Logs in FortiAnalyzer

To view FortiSandbox logs in your FortiAnalyzer



1. Login to your FortiAnalyzer
2. Select FortiSandbox from the *Select an ADOM* prompt.
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 one of the columns and select to add a search filter. Select *GO* in the toolbar to apply the filter. Not all columns support the search feature.
Device		Select the device in the drop-down list.
Time Period		Select a time period from the drop-down 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		The tools button provides options for changing the manner in which the logs are displayed, and search and column options.
	Real-time Log	FortiSandbox does not support *Real-time Log*.
	Display Raw	Select to change view from formatted display to raw log display.
	Download	Select to download logs. A download dialog box is displayed. Select the log file format, compress with gzip, the pages to include and select *Apply* to save the log file to the management computer. This option is only available when viewing logs in formatted display.
	Case Sensitive Search	Select to enable case sensitive search.

Chart Builder	Select to create a custom chart.
Display Details button	Detailed information on 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 drop-down 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 on various columns to add search filters to refine the logs displayed. When a search filter is applied, the value is highlighted in the table and log details.
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 log message list can show raw or formatted. 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 drop-down menu from the toolbar.

To view formatted logs:

Go to *Tools* and select *Display Formatted* from the drop-down 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 drop-down 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
4. columns.
5. To reset to the default columns, click *Reset to Default*.
6. Click *OK* to apply your changes.

To change the order of the displayed columns:

Place the cursor in the column header area, and then move a column by dragging and dropping.

To filter column data:

1. You can filter log summaries by using the *Add Filter* box in the toolbar or by right-clicking an entry and selecting a context-sensitive filter.
2. Specify filters in the Add Filter box.

   Use Regular Search. In the selected summary view, click in the Add Filter box, select a filter from the dropdown list, and type a value. You can click on an operator to use it, such as greater than (>), less than (<), OR, and NOT. You can add multiple filters at a time, and connect them with "and" or "or".

   Use Advanced Search. Click the Switch to Advanced Search icon at the end of the Add Filter box. In Advanced Search mode, you provide the whole search criteria (log field names and values) by typing. Click Switch to Regular Search icon to go back to regular search.

From the Tools drop-down menu in the tool bar, you can use the Case Sensitive Search check box to specify whether you want Log View to treat the filter value that you type case-sensitive or not.

3. In the Device list, select a device.
4. In the Time list, select a time period.
5. Click *Go*.

To filter log summaries by using the right-click menu:

In a log message list view, right-click an entry, and select a filter criteria. The search criteria with a icon will return entries that match the filter values, while the search criteria with a icon will return entries that negate the filter values.

Depending on the column in which your mouse is located when you right-click, Log View will use the column value of the selected entry as the filter criteria. This context-sensitive filter is only available for certain columns.

For additional information, see the *FortiAnalyzer Administration Guide* in the Fortinet Document Library.

Report Access

Report Access lists all Executive Summary and Threat Activity reports including their statuses and the user that generated the report. You can download and delete the PDF reports in this page.

Report pages are not visible on the Slave node in a cluster.

Generate reports

To generate reports on demand, go to *Logs & Reports* > *Report Generate*.

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.

Appendix A - View Details Page Reference

When you click on the *View Details* icon, a new tab will open in your browser.

The following information are descriptions of the *View Details* page for:

- *Last drill-down level of the FortiView pages*
- *Scan Input > File and URL On Demand*
- *File Detection > Malicious Files*
- *File Detection > Suspicious Files*
- *File Detection > Clean Files*

Item	Description
File type	The file type, *High Risk Downloader* for example.
Virus Name	The name of the virus.
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.
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.
Received	The date and time the file was received by FortiSandbox.
Started	The date and time the scan started and the timezone.
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.

Item	Description
Scan Bypass Configuration	When available, the scan bypass configuration will be displayed.
Virus Total	By clicking the Virus Total link, a new page will open to query 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.
More Details	View additional file information including the following: Packers, File Type, Downloaded From, Filename, File Size (bytes), Sent Over (protocol), MD5, SHA1, SHA256, ID, Submitted By, Start Time, Finish Time, Scan Time, Scan Unit, Device that submitted this file, VDOM/Domain that submitted this file, Detection OS (VM images that scanned this file), and Infected OS (VM image name that detected this malware).
	If the file is from FortiMail, Email related information, such as the Email Sender, Receiver, and Subject will also be shown.
Suspicious Indicators	A summary of the Malware's suspicious indicators if there are any.
Behavior Summary	View the file behavior summary.
Analysis Details are located in the right pane if the web browser width is enough. Otherwise, it will follow the Behavior Summary section.	
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. If the Malware is detected by non-Sandboxing scan, such as FortiGuard static scan, the tab title is displayed as *N/A*.

Item		Description
	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.
	Screenshot	Download a screenshot image when the file was running in the sandbox. This image is not always available.
	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*. **Caution:** The original file should only be unzipped on a management computer in an analysis environment.
	Tracer Log	A text file containing detailed information collected inside the Sandbox VM.

Item		Description
	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*. **Caution:** The tracer log should only be unzipped on a management computer in an analysis environment.
	YARA Hits	If the file hits FortiSandbox internal YARA rules, detailed information is displayed.
	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.
	Suspicious Indicators	A summary of suspicious indicators, if available. Clicking a certain indicator will display its detail.
	Botnet Info	The botnet name and target IP address.
	Files Created	The executable has been observed to drop some files. Click the *Files Created* drop-down 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* drop-down 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* drop-down 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* drop-down 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* drop-down 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.

Item		Description
	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.
	Print	Click the print icon to print the malware details page information.
	Open in New Window	Click the icon to open the page in a new web browser window.

Appendix B - Reset a Lost Password

Periodically a situation arises where the FortiSandbox needs to be accessed or the admin account's password needs to be changed but no one with the existing password is available. If you have physical access to the device and a few other tools the password can be reset.

This procedure will require the reboot of the FortiSandbox unit.

You will need:

- Console cable
- Terminal software such as Putty.exe (Microsoft Windows) or Terminal (Mac OS X)
- Serial number of the FortiSandbox device

To reset the FortiSandbox password:

1. Connect the computer to the FortiSandbox via the Console port on the back of the unit.
2. Start a terminal emulation program on the management computer.
3. Select the COM port and use the following settings:

Speed (baud)	9600
Data bits	8
Stop bits	1
Parity	None
Flow Control	None

4. Press `Open` to connect to the FortiSandbox CLI.
5. The FortiSandbox should then respond with its name or hostname. (If it does not try pressing Enter)
6. Reboot the FortiSandbox using the power button.
7. Wait for the FortiSandbox name and login prompt to appear.
8. Type in the username: maintainer.
9. The password is bcpb + the serial number of the firewall. (The letters of the serial number are in UPPERCASE format, Example: bcpbFSA3KD3R13000024)

On the FortiSandbox 3000D, after the device boots, you have ten minutes to type in the username and password. You may opt to have the credentials ready in a text editor, and then copy and paste them into the login screen. There is no indicator of when your time runs out so it is possible that it might take more than one attempt to succeed.

10. Now you should be connected to the FortiSandbox. To change the admin password, enter the following CLI commands:
    ```
    admin-pwd-reset <password_string>
    ```
11. You can now proceed to log in to the FortiSandbox using admin and the password you set in the previous step.

The maintainer user can be disabled through CLI command `set-maintainer`. Refer to *FortiSandbox CLI Reference Guide* available in the Fortinet Document Library for more details.

Appendix C - Hot Swapping Hard Disks

If a hard disk on a FortiSandbox unit fails, it must be replaced. FortiSandbox devices support hardware RAID and the hard disk can be replaced while the FortiSandbox unit is running, also known as hot swapping. The default RAID level is RAID-10 (FSA-3000D) or RAID-1 (FSA-1000D).

To identify which hard disk failed the following diagnostic commands are available:

`hardware-info`	Display general hardware status information. Use this command to view CPU, memory, disk, and RAID information, and system time settings.
`disk-attributes`	Display system disk attributes.
`disk-errors`	Display any system disk errors.
`disk-health`	Display disk health information.
`disk-info`	Display disk hardware status information.
`raid-hwinfo`	Display RAID hardware status information.

To hot-swap a hard disk on a device that supports hardware RAID, simply remove the faulty hard disk and replace it with a new one.

Electrostatic discharge (ESD) can damage FortiSandbox equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiSandbox chassis.

When replacing a hard disk, you need to first verify that the new disk has the same size as those supplied by Fortinet and has at least the same capacity as the old one in the FortiSandbox unit. Installing a smaller hard disk will affect the RAID setup and may cause data loss. Due to possible differences in sector layout between disks, the only way to guarantee that two disks have the same size is to use the same brand and model.

The size provided by the hard drive manufacturer for a given disk model is only an approximation. The exact size is determined by the number of sectors present on the disk.

The FortiSandbox unit will automatically add the new disk to the current RAID array. The status appears on the console. The RAID Management page will display a green check mark icon for all disks and the *RAID Status* area will display the progress of the RAID re-synchronization/rebuild.

Once a RAID array is built, adding another disk with the same capacity will not affect the array size until you rebuild the array by restarting the FortiSandbox unit.

Appendix D - Create a Customized Virtual Machine Image using Pre-Configured VMs

In FSA-1000D, FSA-3000D, FSA-3500D and VM, the maximum number of clones allowed for all VM types for the whole system is limited by the Windows license shipped with the unit.

For FSA-2000E and FSA-3000E, the maximum number of clones for default VMs and optional VMs is limited by the Windows license and the number of stacked licenses provided by Fortinet.

For customized VMs, on FSA-2000E, the clone number is up to 20 and on FSA-3000E, the clone number is up to 48.

All customized VMs should be activated before uploading to the unit. Customers should purchase licenses from Microsoft distributors to do activation.

It is recommended that the size of customized VM image is less than 10GB.

The guest VM images published by Fortinet might not reflect the user's working environment. For example, on current Windows 8 and Windows 10 images, no Microsoft Office software is installed. FortiSandbox allows user to create their own guest image, install software running in their environment and upload the image to the unit to scan files. This document provides step-by-step instructions on how to create and utilize them.

You can choose to use the VMs provided by Fortinet or by creating your own. If you would like to create your own VMs see Appendix E - Create a Customized Virtual Machine Image using your own ISO on page 264.

Fortinet prepared a base set of supported VM images for customers to create their own customized images more easily. These images have complete VirtualBox configurations and necessary software. What customer needs to do:

1. Download and install Oracle VM Virtual Box 5.0.XX and open the base image and create a clone image of it.
2. Activate the base Windows image with valid license key.
3. Install software and components that meet their environment on the base image.

For detailed instructions, please refer to steps below. These base images can be downloaded from:

VM Download	Size	32 or 64 bit image
https://fsavm.fortinet.net/vmtools/V5Win10Entx64.zip	4.8G	64
https://fsavm.fortinet.net/vmtools/V5Win10Entx86.zip	3.7G	32
https://fsavm.fortinet.net/vmtools/V5Win7EntSP1x64.zip	3.4G	64
https://fsavm.fortinet.net/vmtools/V5Win7ProSP1x86.zip	2.7G	32
https://fsavm.fortinet.net/vmtools/V5Win81Entx64.zip	3.8G	64

VM Download	Size	32 or 64 bit image
https://fsavm.fortinet.net/vmtools/V5Win81Entx86.zip	2.7G	32
https://fsavm.fortinet.net/vmtools/V5WinXpSp3.zip	704Mb	32
Their checksum value can be found at: https://fsavm.fortinet.net/vmtools/md5.txt		

1. Download, install Oracle VM Virtual Box 5.0, open the base image and create a clone

VirtualBox 5.0 can be downloaded from https://fsavm.fortinet.net/vmtools/VirtualBox-5.0.26-108824-Win.exe. The checksum value can be found at https://fsavm.fortinet.net/vmtools/md5.txt

For help with VirtualBox installation and troubleshooting, please refer to The Virtual Box Manual.

VirtualBox is an open source software and licensed under GNU General Public License V2 license. The detailed information of its license can be found at https://www.virtualbox.org/wiki/Licensing_FAQ

Mac OS is not supported.

2. Install Software and Components on the Customized VM Image

After a clone of the base image is created, the user can install applications and components required in their environment on the clone image. They can be but not limited to the following list:

- .Net Framework
- Microsoft Office suite
- Adobe Acrobat Reader
- Oracle Java Run Time

There are two ways to install them:

1. Put their installers on a computer in management network that VM image can download through http, ftp protocols or network share. This requires network settings of VM image to be configured to access hosting computer.
2. Package their installation package as an ISO file in the VirtualBox Manager, select the VM image, click Settings button or right click on the VM image name to open Settings page.
   Go to the Storage page > *Empty optical drive node* > *disk icon* > Chose a *virtual CD/DVD disk file*, select the *ISO file*. Then inside the VM image, go to *drive D* to install the software.

After installation of a software or component, go to *Control Panel* > *Add or Remove Programs on Windows XPControl Panel* > *Programs and Features* in Windows 7, 8, and 10 to verify that the installation is successful.

Automatic update of software should be disabled. For details, please refer to software's manual. For example, to disable automatic update on Acrobat Adobe Reader, refer to https://helpx.adobe.com/acrobat/kb/automatic-updates---acrobat-reader.html

Use a text editor and create a meta file, enter in the installed applications for this VM image. The meta file will be used later and its content is displayed in the *Scan Profile* > *Installed Applications* of FortiSandbox.

It is recommended that installed software should be launched at least once to make sure they can open smoothly. Certain software needs to be configured to associate with the file types as the default application. For example, Adobe Reader needs to be launched after installation to be the default PDF application.

For Windows 10, the default web browser is *Windows Edge* which FortiSandbox does not currently support. It is recommended to change the default web browser to be *Internet Explorer*. To do that:

1. Go to *Start* > *Settings* > *System* > *Default apps*.
2. Click Web Browser in the right pane and select Internet Explorer.

Windows OS and other installed software should be activated.

Fortinet is not responsible for software's support and their license rights.

3. Setup FortiSandbox Tracer Engine Launcher

1. Open an editor, such as Notepad and type in the following scripts:

```
@echo off
:checker
   if not exist d:\launcher.bat (
   echo Wait for d:\launcher.bat
   rem sleep 5
   ping -n 5 127.0.0.1 >nul
   goto checker
)
start /min d:\launcher.bat
```

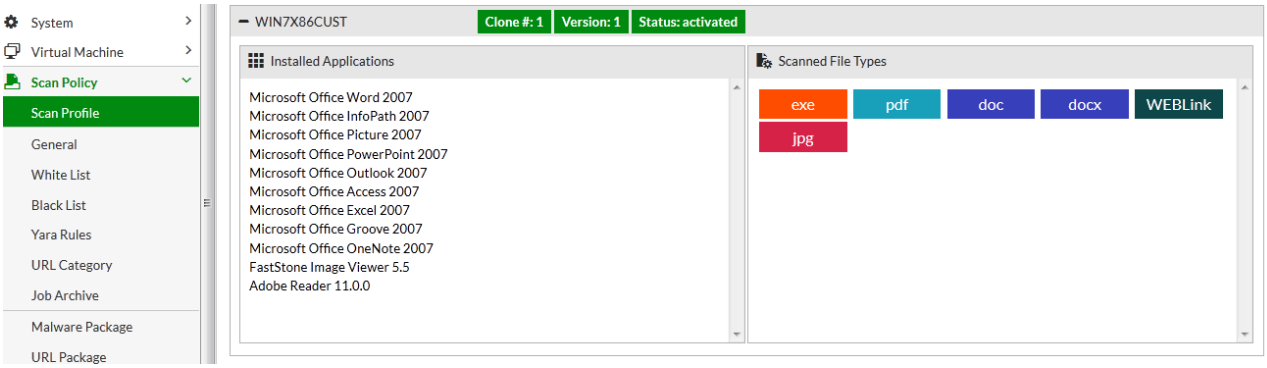
2. Save the file as `autorun.bat` on your *Desktop*.
3. Find the `autorun.bat` file on your *Desktop*, and *Right-click* > *Cut*.
4. On Windows XP and Windows 7, go to *Start* > *All Programs* > *Startup* > *Right-click* > *Open All Users*. Windows Explorer will open. Paste the `autorun.bat` file.

   On Windows 8 and Windows 10, go to *Start* > *Run...*, enter shell:startup to open the startup folder. paste the `autorun.bat` file.

The `D:\` directory for the `autorun.bat` file is created after the VM image is uploaded.

4. Install the Customized VM Image to FortiSandbox and Apply It

1. Put the VM image's `.vdi` file and its meta file from **Step 4** to a server that supports `ftp` or `scp` protocol.
2. In the FortiSandbox CLI interface:
   a. execute CLI command `vm-customized` as follows:
   ```
   vm-customized -cn -t<ftp|scp> -s<server_ip> -u<username> -p<password> -f</vdi_file_path/vid_file_name> -vo<Windows_type> -vn<custom_vm_name> -d<Machine uuid> -k<MD5_of_vdi_file_in_lowercase>
   ```
   Tip: `Machine uuid` can be found in `<Machine>` section of `.vbox` file of the image build directory, such as `C:\Users\user_name\VirtualBox VMs\WIN7X86SP1\`
   b. If a customized VM image of the same name exists on the unit, the installation will fail. Go to the *VM Image* page and set its clone number to `0`. Click *Apply* to disable existing images. Use `-r` to replace the existing one with new one. The *Scan Profile* settings for the image will be inherited.
   c. The installation process can take up to one hour, depending on unit model and network speed. If installation fails or stops unexpectedly, execute the command again.
   d. It is optional to upload the meta file. The information in the meta file will be displayed in the *Installed Applications* area in *Scan Profile* page of the FortiSandbox. To install it, execute CLI command `vm-customized` as follows:
   ```
   vm-customized -cf -mproduct.list -t<ftp|scp> -s<server_ip> -u<username> -p<password> -f</meta_file_path/meta_file_name> -vn<custom_vm_name> -mproduct.list
   ```
   The `custom_vm_name` should be the same as step a.
   e. The unit will reboot after installation.
3. After unit reboots, user can enable it by setting up its clone number to be more than `0` in the *VM Image* page and associate file types in the *Scan Profile* page to scan files.



For example, the above is a Windows 7 customized image. It has an image file editor called *FastStone Image Viewer* and it is associated to open JPG files. The user can create a *User defined extension* for JPG files and associate it to this customized image. Subsequently, all JPG files will be scanned by this customized image and opened by the FastStone Image Viewer.

Appendix E - Create a Customized Virtual Machine Image using your own ISO

In FSA-1000D, FSA-3000D, FSA-3500D and VM, the maximum number of clones allowed for all VM types for the whole system is limited by the Windows license shipped with the unit.

For FSA-2000E and FSA-3000E, the maximum number of clones for default VMs and optional VMs is limited by the Windows license and the number of stacked licenses provided by Fortinet.

For customized VMs, on FSA-2000E, the clone number is up to 20 and on FSA-3000E, the clone number is up to 48.

All customized VMs should be activated before uploading to the unit. Customer should purchase licenses from Microsoft distributors to do activation.

The guest VM images published by Fortinet might not reflect the user's working environment. For example, on current Windows 8 and Windows 10 images, no Microsoft Office 2010 software is installed. FortiSandbox allows user to create their own guest image, install software running in their environment and upload the image to the unit to scan files. Specifically, users can create the guest image on top of their Golden Image or Master Image to best simulate their OS installations. This document provides step-by-step instructions on how to create and utilize them.

You can choose to use the VMs provided by Fortinet or by creating your own. If you would like to create a customized image using pre-configured VMs see Appendix D - Create a Customized Virtual Machine Image using Pre-Configured VMs on page 260.

1. Download and Install Oracle VM Virtual Box 5.0

VirtualBox 5.0 can be downloaded from https://fsavm.fortinet.net/vmtools/VirtualBox-5.0.26-108824-Win.exe. The checksum value can be found at https://fsavm.fortinet.net/vmtools/md5.txt

For help with VirtualBox installation and troubleshooting, please refer to The Virtual Box Manual.

VirtualBox is an open source software and licensed under GNU General Public License V2 license. The detailed information of its license can be found at https://www.virtualbox.org/wiki/Licensing_FAQ

Mac OS is not supported.

2. Prepare the Operating System Installation Package

In FortiSandbox 2.5.1, the following operating systems can be used to build a customized VM image.

- Microsoft Windows XP 32 bit
- Microsoft Windows Server 2003 32 bit
- Microsoft Windows 7 32/64 bit
- Microsoft Windows 8.1 32/64 bit
- Microsoft Windows 10 32/64 bit
- Microsoft Windows Server 2008 32/64 bit
- Microsoft Windows Server 2012 64 bit

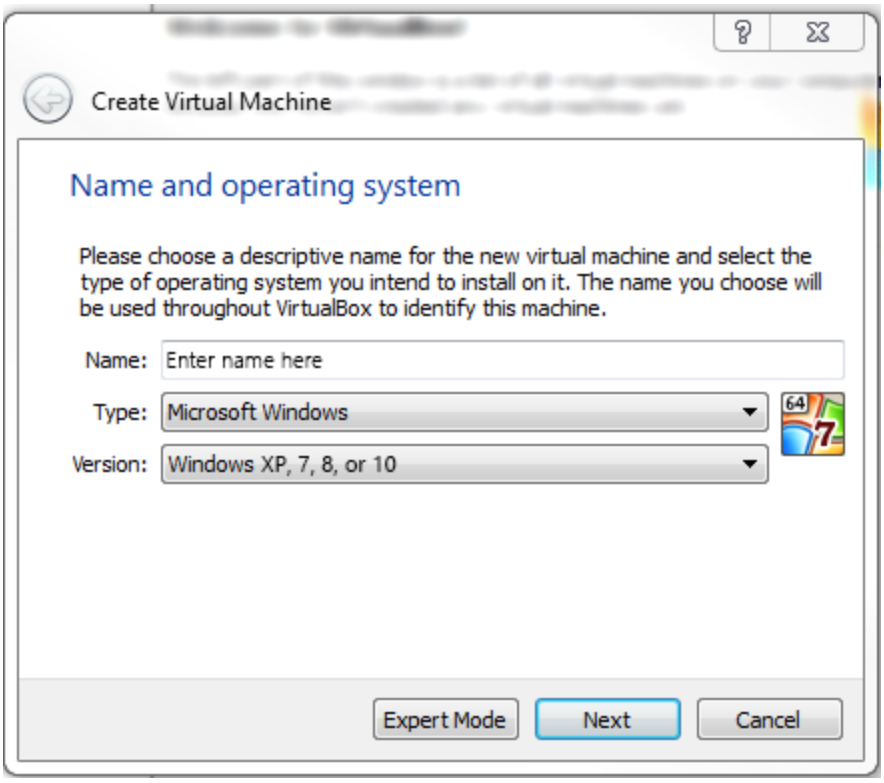
The installation package of above operating systems should be packaged as an ISO file. The ISO file should be copied to the host installed with VirtualBox.

The Windows Operating System is available from Microsoft and Microsoft Channel Partners. Fortinet does not provide their installation package, their support or their license rights.

To support 64-bit operating systems, hardware virtualization must be enabled on motherboard BIOS on the host installed with VirtualBox.

3. Create a Customized Image in Virtual Box

1. Launch Virtual Box and click *New*.



2. Enter a meaningful name for the new image. The name cannot be more than 15 characters.
In the *Type* field > *Microsoft Windows* > select the *OS version*.

The following VM image names are reserved by Fortinet and should not be used by customized images.

- WINXPVM
- WINXPVM1
- WIN7X86VM
- WIN7X64VM
- WIN7X64SP1
- WIN7X86SP1O16
- WIN7X86VMO16
- WIN8X64VMO16
- WIN81X86VM
- WIN81X64VM
- WIN81X64VMO16
- WIN10X86VM
- WIN10X64VM
- WIN10X64VMO16

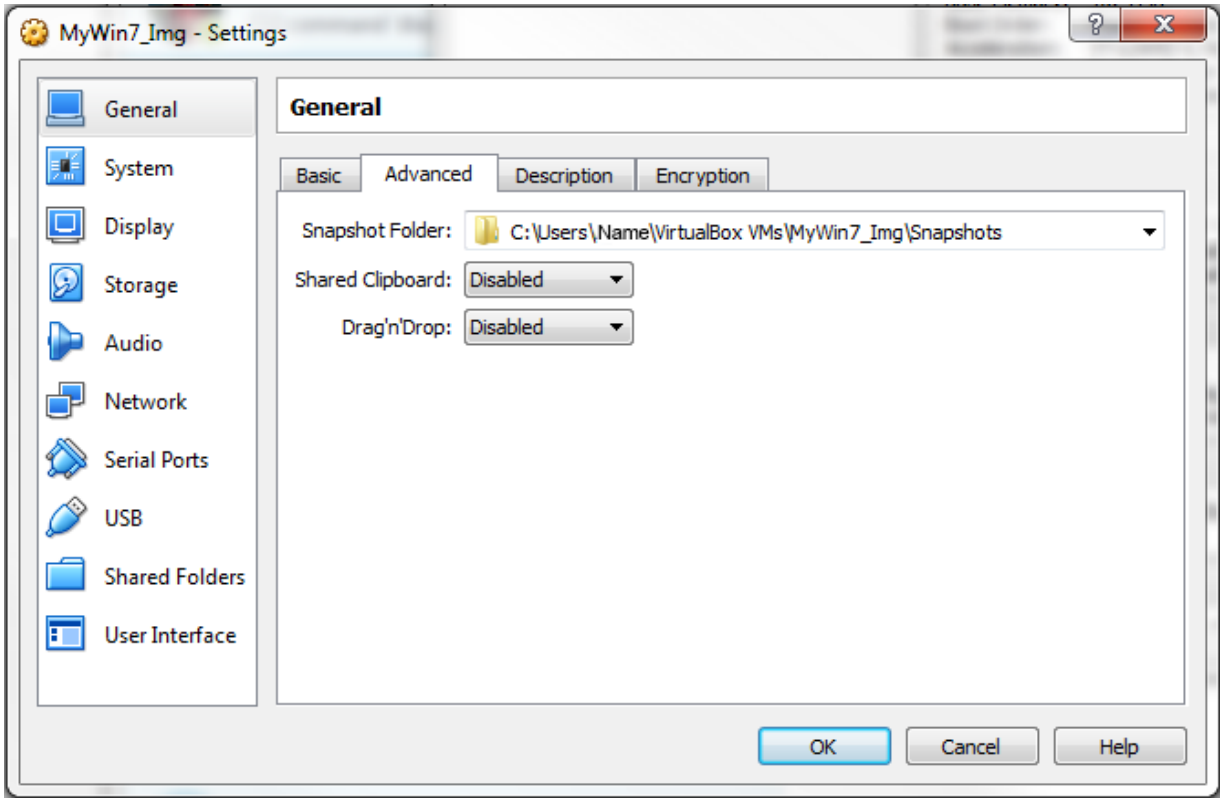
3. Click *Next*.
4. In the *Memory Size* page, allocate the base memory size.

Windows XP, Windows Server 2003 32 bit	512MB
Windows 7, 8, 10, Windows Server 2008 R2, Windows Server 2012	1024MB

Click *Next*.

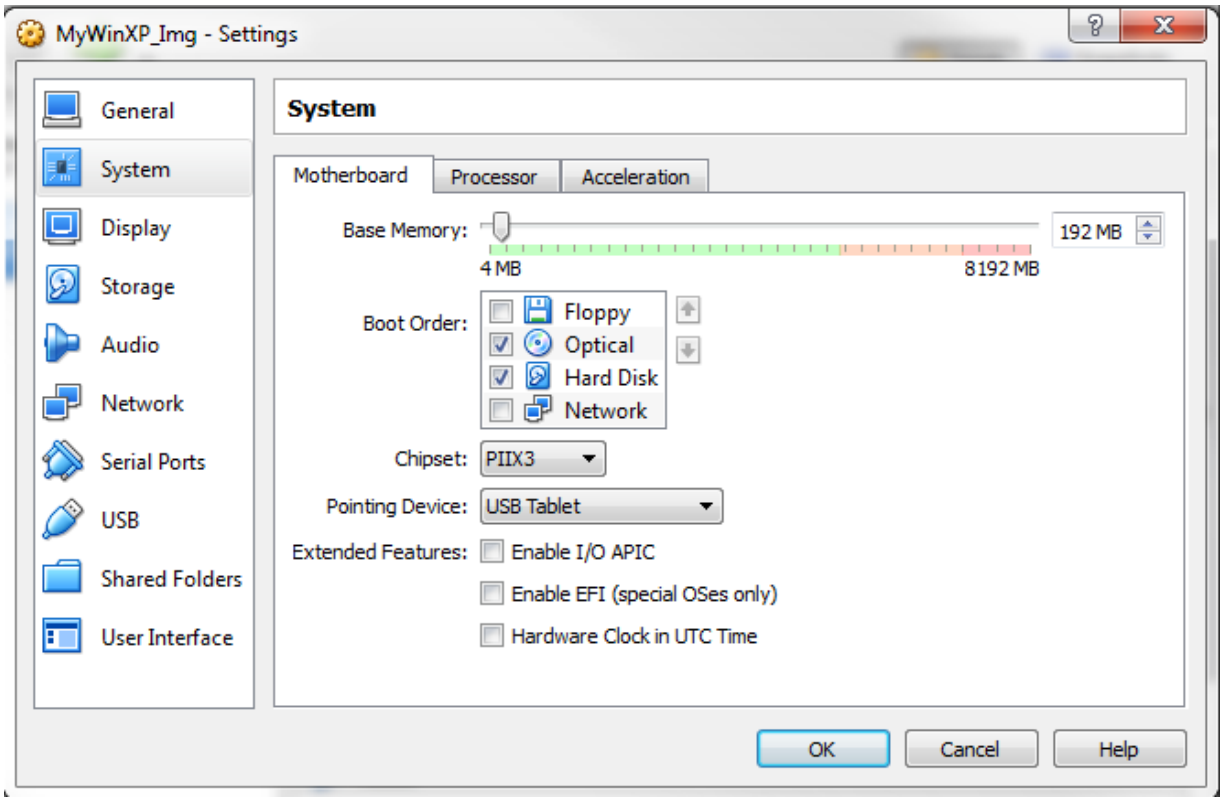
5. In the *Hard Drive* page, select *Create a virtual hard drive now* and click *Create*.
6. In the *Hard drive file type* page, select *VirtualBox Disk Image (.vdi) format*. Click *Next*.
7. In the *Storage on physical hard drive* page, select *Dynamically allocated*. Click *Next*.
8. In the *File location and size* page, set the path of the virtual disk file (optionally) and allocation 20GB virtual disk size for the VM. Click *Create*. The VM will be created and will appear in the left pane.
9. Click the *Settings* button or right click on the VM image name to configure the VM image settings defined below:

a. Go to *General* > *Advanced*, and apply the following settings:

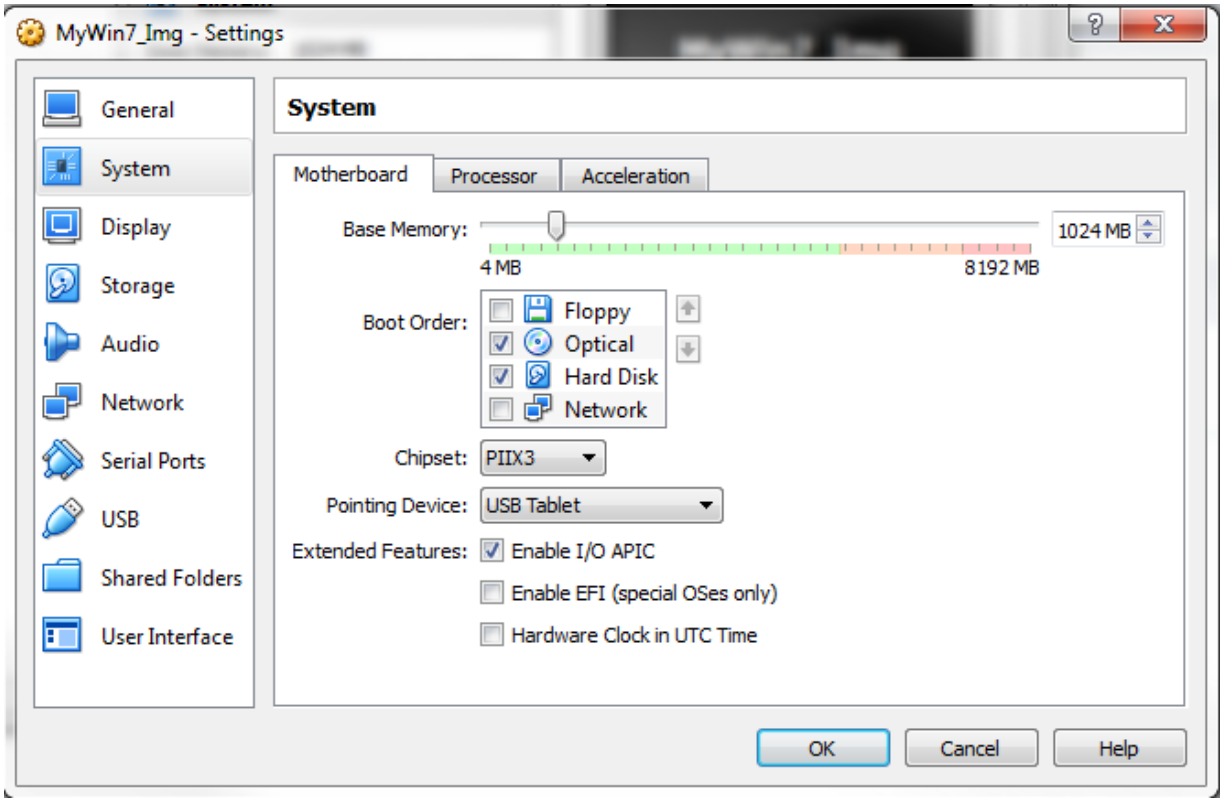


b. Go to *System* > *Motherboard*, and apply the following settings:

For Windows XP and Windows Server 2003 32 bit:



For Windows 7, Server 2008, 8, 10, Server 2012:



Processor Tab		
	Processor(s)	1
	Execution Cap	100
	Enable PAE/NX	Check the box
Acceleration Tab		
	Enable VT-x/AMD-C	Check the box
	Enable Nested Paging	Check the box

c. Go to *Display*, keep the default settings.

d. Go to *Storage*, and apply the following settings:

If the operating system is Windows XP or Windows Server 2003 32 bit:

i. Click *Controller: IDE*, set *Type* to *PIIX 4* and *enable Use host I/O cache*.

ii. Click on the *Empty Optical Drive* node, make sure the *CD/DVD Drive* is set as the *IDE Secondary Master*.

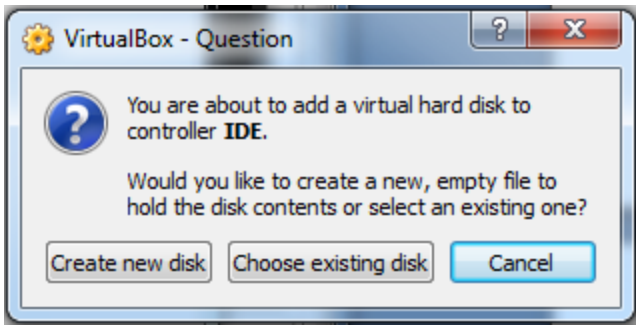
iii. Click the *icon* > *Choose a virtual CD/DVD disk file*, select the *ISO file* containing the operating system installation package.

If the operating system is Windows 7, Server 2008, 8, 10, Server 2012:

i. Click *Controller: SATA node*, right click > Remove Controller to remove it.

ii. Right click in the *Storage Tree* panel, and choose *Add IDE Controller*.

iii. Click the *Add Hard Disk* icon. The following prompt will appear:



iv. Click *Choose Existing Disk* and select the *virtual disk file (*.vdi)* that was created in the previous steps.

v. Click *Controller: IDE*, set *Type* to *PIIX4*, and *enable Use host I/O cache*.

vi. Click on the *Empty Optical Drive* node, make sure the *CD/DVD Drive* is set as the *IDE Secondary Master*.

vii. Click the *icon* > *Choose a virtual CD/DVD disk file*, select the *ISO file* containing the operating system installation package.

e. Go to *Audio*, and uncheck the *Enable Audio* checkbox.

f. Go to *Network*, and apply the following settings:

If the operating system is Windows XP or Windows Server 2003 32 bit:

Adapter 1 Tab		
	Network Adapter	Check the box
	Attached to	NAT
	Adapter Type	Intel PRO/1000T Server (82543GC)
	Cable Connected	Check the box

Adapter 2 Tab		
	Network Adapter	Check the box
	Attached to	NAT
	Adapter Type	Intel PRO/1000T Server (82543GC)
	Cable Connected	Check the box

If the Operating System is Windows 7, Server 2008, 8, 10, or Server 2012:

Adapter 1 Tab		
	Network Adapter	Check the box
	Attached to	NAT
	Adapter Type	Intel PRO/1000MT Server (82545EM)
	Cable Connected	Check the box

Adapter 2 Tab		
	Network Adapter	Check the box
	Attached to	NAT
	Adapter Type	Intel PRO/1000MT Server (82545EM)
	Cable Connected	Check the box

g. Go to *Serial Ports*, keep the default settings.

h. Go to *USB*, *uncheck the Enable USB Controller* checkbox.

i. Go to *Shared Folders*, make sure no shared folders exist.

10. Click *OK* to apply the settings.

11. In the *VirtualBox Manager* page, click the 

icon to turn on the image. The operating system will start installing. Follow the on-screen instructions to complete the installation.

4. Install Software and Components on the Customized VM Image

After a customized VM image is installed, the user can install applications and components required in their environment. They can be but not limited to the following list:

- .Net Framework
- Microsoft Office suite
- Adobe Acrobat Reader
- Oracle Java Run Time

There are two ways to install them:

1. Put their installers on a computer in management network that VM image can download through http, ftp protocols or network share. This requires network settings of VM image to be configured to access hosting computer.
2. Package their installation package as an ISO file in the VirtualBox Manager, select the VM image, click Settings button or right click on the VM image name to open Settings page.
   Go to the Storage page > *Empty optical drive node* > *disk icon* > Chose a *virtual CD/DVD disk file*, select the *ISO file*. Then inside the VM image, go to *drive D* to install the software.

After installation of a software or component, go to *Control Panel* > *Add or Remove Programs on Windows XP or Windows Server 2003 32 bitControl Panel* > *Programs and Features* in Windows 7, Server 2008, 8, Server 2012 and 10 to verify that the installation is successful.

Automatic update of software should be disabled. For details, please refer to software's manual. For example, to disable automatic update on Acrobat Adobe Reader, refer to https://helpx.adobe.com/acrobat/kb/automatic-updates---acrobat-reader.html

Use a text editor and create a meta file, enter in the installed applications for this VM image. The meta file will be used later and its content is displayed in the *Scan Profile* > *Installed Applications* of FortiSandbox.

Certain software needs to be configured to associate with the file types as the default application. For example, Adobe Reader needs to be launched after installation to be the default PDF application.

All applications that are used during a job scan should be launched after installation to finish their initialization. This is especially important for software like web browsers such as Internet Explorer, Adobe Reader and Microsoft Office software.

For Windows 10, the default web browser is *Windows Edge* which FortiSandbox does not currently support. It is recommended to change the default web browser to be *Internet Explorer*. To do that:

1. Go to *Start* > *Settings* > *System* > *Default apps*.
2. Click Web Browser in the right pane and select Internet Explorer.

Windows OS and other installed software should be activated.

Fortinet is not responsible for software's support and their license rights.

5. Modify the VM Image Environment

If the operating system is Windows XP or Windows Server 2003 32 bit:

1. Go to *Control Panel* >*Security Center* and disable Windows Automatic Updates.
2. Disable any installed antivirus software.
3. Navigate to the *Start Menu* > *right click on My computer* > *click Properties*

   In *Hardware* tab, click *Driver Signing button* and select *Ignore – Install the software anyway and don't ask for my approval*.

   In *Advanced* tab, click the *Error Reporting* button and check *Disable the Error Reporting function*. Also, uncheck *But notify me when critical errors occur*.

   In *System Restore* tab, make sure the *System Restore* function is *off*.
4. Make sure the built-in Administrator account is enabled. Open a command prompt and execute `net user Administrator /active: yes`.
5. Setup Administrator auto-login:
   a. Open a command prompt and enter `control userpasswords2`. This will open the User Accounts page.
   b. Uncheck *Users must enter a user name and password to use this computer* to ensure the Administrator has automatic login privileges
   c. Click *Apply*.
   d. Use *Administrator* as the login account, password is optional.
   e. Go to the *User Accounts* > *Advanced* tab.
   f. Under *Advanced User Manager* > *click the Advanced* button to open the `lusrmgr` page.
   g. Click the *Users* folder to select the *Administrator* and edit its properties.
   h. Make sure its password never expires.
6. Open a command prompt and enter `powercfg –h off` to disable host hibernation if it is supported.
7. Go to *Control Panel* > *Display Properties*, navigate to *Screen Saver* tab and select *None* from the Screen Saver dropdown menu.
8. Go to *Control Panel* > *Network Connection*, and rename the following:

Local Area Connection 1	**renamed to:**	`eth0`
Local Area Connection 2	**renamed to:**	`eth1`

If there are network devices already named as `eth0` and `eth1`, change them to different names first.

The exact names showing in *Network Connection* page might not be *Local Area Connection 1* or *Local Area Connection 2*. You may might need to swap `eth0` and `eth1` names to make the customized image to work on FortiSandbox.

If system doesn't allow rename to `eth0` or `eth1` with messages like connection `eth0` or `eth1` already exists, but they are not showing up in *Network Connections* page,

a. Click *Start* > *Run*, type `cmd.exe`, and then press *ENTER*.

b. Type `set devmgr_show_nonpresent_devices=1`, and then press *ENTER*.

c. Type `Start DEVMGMT.MSC`, and then press *ENTER*.

d. Click *View* > *Show Hidden Devices*. Expand the *Network Adapters* tree. Right-click the greyed out network adapters, and click *Uninstall*.

9. Go to the *Start* menu, execute *Run…* and enter `%TEMP%` . This will open the `%TEMP%` folder. Delete everything in the folder.

To maximize catch rate, it is recommended the Windows Firewall is disabled. To do that, go to *Control Panel* > *Security Center* > *Windows Firewall* and turn it off.

If the operating system is Windows 7 or Server 2008:

1. Turn off Windows automatic update. Go to *Control Panel* > *System and Security* > *Windows Update* > *Change*. From the dropdown menu, select *Never check for updates*.
2. Disable Windows Defender or any installed antivirus software. Go to *Start* menu and type *Windows Defender* to locate and launch it. Click *Tools* > *Options* > *Administrator*, uncheck *Use this program* check box, click *Save*.
3. Go to *Control Panel* > *System and Security* > *Action Center* > *Change Action Center* settings, uncheck every item. Click *Problem Reporting* settings, check *Never check for solution*.
4. Run a command prompt as the *Administrator* and enter `powercfg -h off` to disable host hibernation.
5. Go to *Control Panel* > *Appearance and Personalization* > *Change* screen saver, select *(None)* from the *Screen Saver* dropdown list.
6. Make sure Administrator account is enabled. Go to the *Start* menu, search command prompt. Right click on it and launch it as the *Administrator*. Execute `net user Administrator /active: yes`.
7. Setup auto-login for the *Administrator* account.
   a. Open a command prompt and type in `control userpasswords2`. This will open the *User Accounts* page.
   b. Make sure the Administrator account has the automatically login privilege by un-checking option *Users must enter a user name and password to use this computer*.
   c. Click *Apply*.

d. Use *Administrator* as the login account, and setup the password.

e. Go to *User Accounts* > *Advanced* tab.

f. Under the *User Accounts* > *Advanced tab* > *Advanced User Management* > *click the Advanced button* button to open the `lusrmgr` page.

g. Click on the *Users Folder* to select *Administrator* and edit its properties.

h. Make sure its password never expires.

8. Go to *Control Panel* > *Network and Internet* > *Network and Sharing Center* > *Change Adapter* settings, rename the following:

Ethernet 1	**renamed to:**	`eth0`
Ethernet 2	**renamed to:**	`eth1`

If there are network devices already named as `eth0` and `eth1`, change them to different names first.

The exact names showing in *Network Connection* page might not be *Local Area Connection 1* or *Local Area Connection 2*. You may might need to swap `eth0` and `eth1` names to make the customized image to work on FortiSandbox.

If system doesn't allow rename to `eth0` or `eth1` with messages like connection `eth0` or `eth1` already exists, but they are not showing up in *Network Connections* page,

a. Click *Start* > *Run*, type `cmd.exe`, and then press *ENTER*.

b. Type `set devmgr_show_nonpresent_devices=1`, and then press *ENTER*.

c. Type `Start DEVMGMT.MSC`, and then press *ENTER*.

d. Click *View* > *Show Hidden Devices*. Expand the *Network Adapters* tree. Right-click the greyed out network adapters, and click *Uninstall*.

9. Go to the *Start* menu, execute *Run…* and enter `%TEMP%` . This will open the `%TEMP%` folder. Delete everything in the folder to save disk space.

10. If the Windows Firewall is on, go to *Control Panel* > *System and Security* > *Windows Firewall* > *Advanced Settings*. If the Windows Firewall is off, the following steps are not necessary:

a. Click on *Inbound Rules* > *Add New Rule* > *click Program*.

b. Check *This Program Path* and type: `c:\Windows\System32\ftp.exe`. Then, click *Next*.

c. Check *Allow the Connection*, then click *Next*.

d. Provide a name for the rule such as *Allow FTP*.

e. Click *Finish*.

Follow these steps to create Outbound Rules for the same executable.

To maximize the catch rate, it is recommended to configure the following settings:

Turn off Windows Firewall
Go to *Control Panel* > *System and Security* > *Windows Firewall* > *Customize Settings* page and turn it off for both private and public networks.

Turn off UAC (User Account Control Settings)
Search for *UAC* in *Start* menu, open the *Change the User Account Control Setting*, move the slider to *Never*, click *OK*.

Use public profile for all unidentified networks
Go to *Control Panel* > *System and Security* > *Administrative Tools* > *Local Security Policy* > *Network List Manager Policies* > *right click on Unidentified Networks* > *Properties*, change *Location Type* to *Public*, click *OK*.

Turn off system protection for hard drive
Go to the *Start* menu, right click on *Computer* > *Properties* > *System protection* > *System Protection tab* > *Protection Settings* > *Local Disk (C:)* > *Configure*, check *Turn off system protection*, click *OK*.

11. If the Windows Firewall is off, execute the following commands in the command prompt:

```
sc config mpssvc start= demand
sc config wscsvc start= demand
net start wscsvc
net start mpssvc
netsh firewall set opmode disable
netsh advfirewall set allprofiles state off
```

The warning message about netsh firewall can be ignored

If the operating system is Windows 8 or Server 2012:

1. Turn off Windows automatic update. Go to *Control Panel* > *System and Security* > *Windows Update* > *Change Settings*. Change the dropdown menu to *Never Check for Updates*.
2. If the operating system is Windows 8, disable Windows Defender or any installed antivirus software. Go to the *Start* menu and type *Windows Defender* to locate and launch the program. Go to *Settings* > *Real Time Protection* and uncheck the *Turn on Real-Time Protection*.
3. In the *Control Panel* > *System Security* > *Action Center* page, expand the *Maintenance* section. Click on the settings under the *Check for solutions to problem reports*, select *Never check for solution* to disable the *Action Center* notifications. In the *Action Center* > *Change Action Center Settings* page, uncheck every item and click *OK*.
4. Command prompt as Administrator and enter `powercfg-h off` to disable the host hibernation.
5. Right click on the *Desktop* and select *Personalize*. Navigate to the *Screen Saver* settings. Change the Screen Saver dropdown list to *None* to disable the Screen Saver.
6. Make sure the Administrator account is enabled. Go to the *Start* Menu and search for the *Command Prompt*. Right click on it and launch it as the Administrator. Execute `net user Administrator /active: yes`.
7. Set up auto-login for the Administrator account.

a. Open a command prompt and enter `control userpasswords2`. The *User Accounts* page will open.
b. Make sure the *Administrator* has automatically login privilege enabled by unchecking the *Users must enter a user name and password to use this computer* option.
c. Click *Apply*.
d. User the *Administrator* as the login account and setup the password.
e. Go to *User Accounts* > *Advanced tab*.
f. Go to *Advanced User Management* > *click the Advanced button* to open the `lusrmgr` page.
g. Click on the *Users* folder, and select *Administrator* to edit its properties
h. Make sure its password never expires.

8. Go to *Control Panel* > *Network and Internet* > *Network Sharing* > *Change Adapter settings*, rename the following:

Ethernet 1	**renamed to:**	`eth0`
Ethernet 2	**renamed to:**	`eth1`

If there are network devices already named as `eth0` and `eth1`, change them to different names first.

The exact names showing in *Network Connection* page might not be *Local Area Connection 1* or *Local Area Connection 2*. You may might need to swap `eth0` and `eth1` names to make the customized image to work on FortiSandbox.

If system doesn't allow rename to `eth0` or `eth1` with messages like connection `eth0` or `eth1` already exists, but they are not showing up in *Network Connections* page,

a. Click *Start* > *Run*, type `cmd.exe`, and then press *ENTER*.

b. Type `set devmgr_show_nonpresent_devices=1`, and then press *ENTER*.

c. Type `Start DEVMGMT.MSC`, and then press *ENTER*.

d. Click *View* > *Show Hidden Devices*. Expand the *Network Adapters* tree. Right-click the greyed out network adapters, and click *Uninstall*.

9. Go to *Start menu* > *enter Run...*> *enter* `%TEMP%` and press enter. The `%TEMP%` folder will appear. Delete everything in the folder.
10. Go to *Control Panel* > *Appearance and Personalization* > *Taskbar and Navigation*.
11. In the *Navigation* tab, check *When I sign in or close all apps on a screen, go to the desktop instead of start in the Start screen area* checkbox. click *OK* to save the change.

To maximize the catch rate, it is recommended to configure the following settings:

Turn off Windows Firewall
Go to *Control Panel* > *Windows Firewall*. Select Turn off Windows Firewall for both public and private networks.

Turn off UAC (User Account Control Settings)
Search for *UAC* in *Start* menu, open the *Change the User Account Control Setting*, move the slider to *Never*, click *OK*.

If the operating system is Windows 8, use public profile for all unidentified networks
Go to *Control Panel* > *System and Security* > *Administrative Tools* > *Local Security Policy* > *Network List Manager Policies* > *right click on Unidentified Networks* > *Properties*, change *Location Type* to *Public*, click *OK*.

If the operating system is Windows 8, turn off system protection for hard drive
Go to *Control Panel* > *System and Security* > *System*, click *Change Settings* next to the Computer name, domain and workgroup settings section. Navigate to *System Protection* tab, select *Configure...*, and select *Disable system protection*.

12. If the Windows Firewall is turned off, execute the following commands in the command prompt:

```
sc config mpssvc start= demand
sc config wscsvc start= demand (remove this line for Server 2012 OS)
net start wscsvc (remove this line for Server 2012 OS)
net start mpssvc
netsh firewall set opmode disable
netsh advfirewall set allprofiles state off
```

The warning message about netsh firewall can be ignored.

If the operating system is Windows 10:

1. Disable *Windows Defender* or any installed antivirus software. Go to the *Start* > *type Windows Defender* to locate and launch the program. Go to *Settings* > *Real-Time Protection* and uncheck *Turn on Real-Time Protection*.
2. Go to *Start* >*execute Run...* and enter `gpedit.msc` and click *OK*. The *Local Group Policy Editor* will open.
3. In the left pane, go to *Computer Configuration* > *Administrative Templates* > *Windows Components* > *Windows Defender*. In the right pane, double click on the *Turn off Windows Defender* policy to edit it. Click *OK* to save the change.
4. Go to *Start* > *Settings* > *System* > *Notifications & Actions*. Turn off all notifications.
5. Open a command rompt as the *Administrator*, enter `powercfg-h off` to disable hibernation.
6. Right click on the *Desktop* and select *Personalize*. Navigate to the *Screen Saver* setting and change the Screen Saver dropdown list to *None* to disable the Screen Saver.
7. Make sure the Administrator account is enabled. Go to *Start* > *search Command Prompt* > *right click on the application* to launch it as the Administrator. Execute `net user Administrator /active: yes`.
8. Setup auto-login for the Administrator account.

a. Open the command prompt and type in `control userpasswords2`. The *User Accounts* page will appear.
b. Make sure the Administrator account automatically login privilege enabled by unchecking the *Users must enter a user name and password to use this computer* option.
c. Click *Apply*.
d. Use *Administrator* as the login account; the password is optional.
e. Go to *Users Accounts* > *Advanced tab*.
f. Go to *Advanced User Management* > *click the Advanced button* to launch the `lusrmgr` page.
g. Click on the *Users* folder to select the *Administrator* to edit its properties.
h. Make sure its password never expires.

9. Go to *Control Panel* > *Network and Internet* > *Network and Sharing Center* > *Change Adapter settings*. Rename the following:

Ethernet 1	**renamed to:**	`eth0`
Ethernet 2	**renamed to:**	`eth1`

10.

If there are network devices already named as `eth0` and `eth1`, change them to different names first.

The exact names showing in *Network Connection* page might not be *Local Area Connection 1* or *Local Area Connection 2*. You may might need to swap `eth0` and `eth1` names to make the customized image to work on FortiSandbox.

If system doesn't allow rename to `eth0` or `eth1` with messages like connection `eth0` or `eth1` already exists, but they are not showing up in *Network Connections* page,

a. Click *Start* > *Run*, type `cmd.exe`, and then press *ENTER*.

b. Type `set devmgr_show_nonpresent_devices=1`, and then press *ENTER*.

c. Type `Start DEVMGMT.MSC`, and then press *ENTER*.

d. Click *View* > *Show Hidden Devices*. Expand the *Network Adapters* tree. Right-click the greyed out network adapters, and click *Uninstall*.

11. Go to *Start* > *execute Run...* > *enter* `%TEMP%`. The `%TEMP%` folder will appear. Delete everything in the folder.

To maximize the catch rate, it is recommended to configure the following settings:

Turn off Windows Firewall
Go to *Control Panel* > *System and Security* > *Windows Firewall*. Select *Turn off Windows Firewall* for both public and private networks.

Turn off UAC (User Account Control Settings)
Search for *UAC* in *Start* menu, open the *Change the User Account Control Setting*, move the slider to *Never*, click *OK*.

Use public profile for all unidentified networks
Go to *Control Panel* > *System and Security* > *Administrative Tools* > *Local Security Policy* > *Network List Manager Policies* > *right click on Unidentified Networks* > *Properties*, change *Location Type* to *Public*, click *OK*.

Turn off system protection for hard drive
Go to *Control Panel* > *System and Security* > *System*, click *Change Settings* next to the Computer name, domain and workgroup settings section. Navigate to *System Protection* tab, select *Configure...*, and select *Disable system protection*.

12. If Windows Firewall was turned off, execute the following commands in a command prompt:

```
sc config mpssvc start= demand
sc config wscsvc start= demand
net start wscsvc
net start mpssvc
netsh firewall set opmode disable
netsh advfirewall set allprofiles state off
```

The warning message about `netsh firewall` can be ignored

6. Setup FortiSandbox Tracer Engine Launcher

1. Open an editor, such as Notepad and type in the following scripts:

```
@echo off
:checker
   if not exist d:\launcher.bat (
   echo Wait for d:\launcher.bat
   rem sleep 5
   ping -n 5 127.0.0.1 >nul
   goto checker
)
start /min d:\launcher.bat
```

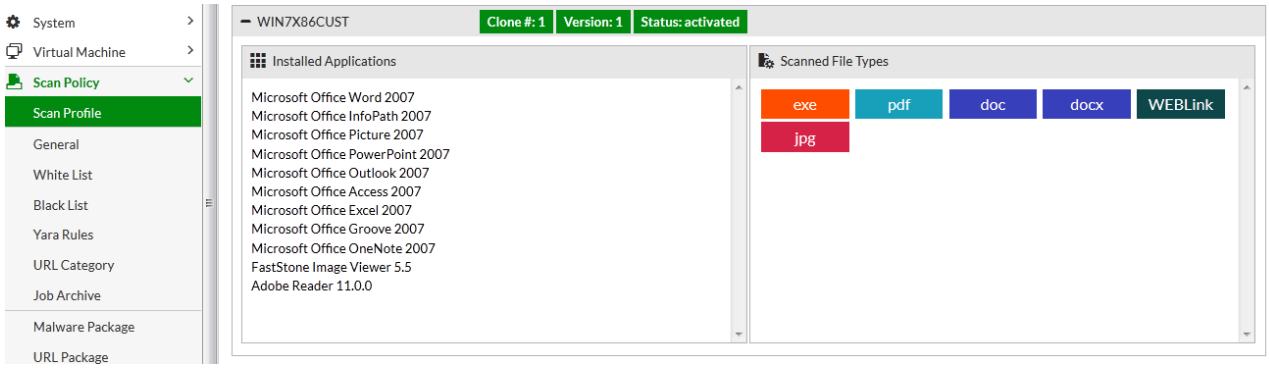
2. Save the file as `autorun.bat` on your *Desktop*.
3. Find the `autorun.bat` file on your *Desktop*, and *Right-click* > *Cut*.
4. On Windows XP and Windows 7 or Windows Server 2003 or 2008, go to *Start* > *All Programs* > *Startup* > *Right-click* > *Open All Users*. Windows Explorer will open. Paste the `autorun.bat` file.

   On Windows 8 and Windows 10, go to *Start* > *Run...*, enter `shell:startup` to open the startup folder. paste the `autorun.bat` file.

The `D:\` directory for the `autorun.bat` file is created after the VM image is uploaded.

7. Install the Customized VM Image to FortiSandbox and Apply It

1. Put the VM image's `.vdi` file and its meta file from **Step 4** to a server that supports `ftp` or `scp` protocol.
2. In the FortiSandbox CLI interface:
   a. execute CLI command `vm-customized` as follows:
   ```
   vm-customized -cn -t<ftp|scp> -s<server_ip> -u<username> -p<password> -f</vdi_file_
       path/vdi_file_name> -vo<Windows_type> -vn<custom_vm_name> -d<Machine uuid> -
       k<MD5_of_vdi_file_in_lowercase>
   ```
   Tip:`Machine uuid` can be found in `<Machine>` section of `.vbox file` of the image build directory, such as `C:\Users\user_name\VirtualBox VMs\vm_name\`
   b. If a customized VM image of the same name exists on the unit, the installation will fail. Go to the *VM Image* page and set its clone number to `0`. Click *Apply* to disable existing images. Use `-r` to replace the existing one with new one. The *Scan Profile* settings for the image will be inherited.
   c. The installation process can take up to one hour, depending on unit model and network speed. If installation fails or stops unexpectedly, execute the command again.
   d. It is optional to upload the meta file. The information in the meta file will be displayed in the *Installed Applications* area in *Scan Profile* page of the FortiSandbox. To install it, execute CLI command `vm-customized` as follows:
   ```
   vm-customized -cf -mproduct.list -t<ftp|scp> -s<server_ip> -u<username> -p<password> -
       f</meta_file_path/meta_file_name> -vn<custom_vm_name> -mproduct.list
   ```
   The `custom_vm_name` should be the same as step a.
   e. The unit will reboot after installation.
3. After unit reboots, user can enable it by setting up its clone number to be more than `0` in the *VM Image* page and associate file types in the *Scan Profile* page to scan files.



For example, the above is a Windows 7 customized image. It has an image file editor called *FastStone Image Viewer* and it is associated to open JPG files. The user can create a *User defined extension* for JPG files and associate it to this customized image. Subsequently, all JPG files will be scanned by this customized image and opened by the FastStone Image Viewer.

Glossary

A

AAA
Authentication, Authorization, and Accounting

AD
Active Directory

ADOM
Administrative Domain

AES
Advanced Encryption Standard

AMI
Amazon Machine Image

AP
Access Point

API
Application Programming Interface

APN
Access Point Name

APT
Advanced Persistent Threat

ATP
Advanced Threat Protection

AV
Antivirus

AVP
Attribute Value Pairs

AWS
Amazon Web Service

B

BGP
Border Gateway Protocol

C

C&C
Command and Control

CA
Certificate Authority

CASI
Cloud Access Security Inspection

CBC
Cipher Block Chaining

CHAP
Challenge-Handshake Authentication Protocol

CIDR
Classless Inter-Domain Routing

CLI
Command Line Interface

CN
Common Name

CoA
Change of Authorization

CPU
Central Processing Unit

CRL
Certificate Revocation List

CSR
Certificate Signing Request

CSV
Comma Separated Value

CVE
Common Vulnerabilities and Exposures

D

DC
Domain Controller, Direct Current

DES
Data Encryption Standard

DH
Diffie-Hellman

DHCP
Dynamic Host Configuration Protocol

DLL
Dynamic-Link Library

DLP
Data Loss Prevention

DN
Distinguished Name

DNAT
Destination Network Address Translation

DNS
Domain Name System

DSCP
Differentiated Services Code Point

DSRI
Disable Server Response Inspection

DTLS
Datagram Transport Layer Security

E

EA
E-mail Address

EAPOL
Extensible Authentication Protocol over LAN (Local Area Network)

EC
Endpoint Control

EC2
Elastic Compute Cloud

EGP
Exterior Gateway Protocol

EMS
Enterprise Management Server

ESD
Electrostatic Discharge

ESP
Encapsulated Security Payload

F

FAZ
FortiAnalyzer

FCT
FortiClient

FDN
FortiGuard Distribution Network

FDS
FortiGuard Distribution Servers

FG
FortiGate

FGFM
FortiGate-FortiManager

FMG
FortiManager

FQDN
Fully Qualified Domain Name

FSA
FortiSandbox

FSSO
Fortinet Single Sign-On

FTP
File Transfer Protocol

G

GCF
Gatekeeper Confirm

GPRS
General Packet Radio Service

GRE
Generic Routing Encapsulation

GTP
GPRS Tunneling Protocol

GUI
Graphical User Interface

GUID
Globally Unique Identifier

H

HA
High Availability

hcache
Hard Cache

HDD
Hard Disk Drive

HTML
HyperText Markup Language

HTTP
HyperText Transfer Protocol

I

I/O
Input / Output

IBP
Identity-based Policy

ICAP
Internet Content Adaptation Protocol

ICMP
Internet Control Message Protocol

IGP
Interior Gateway Protocol

IKE
Internet Key Exchange

IMAP
Internet Message Access Protocol

IOC
Indicators of Compromise

IP
Internet Protocol

IPS
Intrusion Prevention System

IPsec
Internet Protocol Security

ISDB
Internet Service Database

ISP
Internet Service Provider

IV
Initialization Vector

J

JSON
JavaScript Object Notation

L

L2TP
Layer 2 Tunneling Protocol

LACP
Link Aggregation Control Protocol

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

M

MAC
Media Access Control

MD5
Message Digest 5

MGCP
Media Gateway Controller Protocol

MIB
Management Information Base

MMC
Microsoft Management Console

MSCHAP
Microsoft Challenge-Handshake Authentication Protocol

MSS
Maximum Segment Size

N

NAC
Network Access Control or Compliance

NAS
Network Access Server

NAT
Network Address Translation

NAT-PT
Network Address Translation (NAT) Port Translation

NDcPP
Network Device Collaborative Protection Profile

NGFW
Next-Generation Firewall

NNTP
Network News Transfer Protocol

NOC
Network Operations Center

NPU
Network Processing Unit

NTLM
NT LAN Manager

NTP
Network Time Protocol

O

OCSP
Online Certificate Status Protocol

OFTP
Odette File Transfer Protocol

ONC-RPC
Open Network Computing Remote Procedure Call

OSPF
Open Shortest Path First

OTP
One-time Password

OU
Organization Unit

OUI
Organizationally Unique Identifier

OVF
Open Virtualization Format

P

PAP
Password Authentication Protocol

PAT
Port Address Translation

PEM
Power Entry Module

PFS
Perfect Forward Secrecy

PKCS
Public Key Cryptography Standards

PKI
Public Key Infrastructure

PoE
Power over Ethernet

POP3
Post Office Protocol 3

PPP
Point-to-Point Protocol

PPPoE
Point-to-Point Protocol over Ethernet

PPTP
Point-to-Point Tunneling Protocol

PSK
Pre-Shared Key

R

RADIUS
Remote Authentication Dial-In User

RAID
Redundant Array of Independent Disks

RAM
Random Access Memory

RAS
Registration, Admission, and Status

RBAC
Role Based Access Control

RCF
Registration Confirm

RDP
Remote Desktop Protocol

REST
Representational State Transfer

RFC
Remote Function Call

RSH
Remote Shell

RSSO
RADIUS Single Sign-On

RTM
Real-Time Monitor

RTP
Real-Time Protection

RTSP
Real-Time Streaming Protocol

S

SAN
Storage Area Network

SAP
Shelf Alarm Panel

SCEP
Simple Certificate Enrollment Protocol

SCP
Secure Copy

SCVP
Server-based Certificate Validation Protocol

SDK
Software Development Kit

SDN
Software-Defined Networking

SFTP
Secure (or SSH) File Transfer Protocol

SHA1
Secure Hash Algorithm 1

SIP
Session Initiation Protocol

SMTP
Simple Mail Transfer Protocol

SNAT
Secure Network Address Translation

SNI
Server Name Indication

SNMP
Simple Network Management Protocol

SOC
Security Operations Center

SQL
Structured Query Language

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSO
Single Sign-On

T

TACACS+
Terminal Access Controller Access-Control System

Tcl
Tool Command Language

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security

TNS
Transparent Network Substrate

TTL
Time-to-live

U

UDP
User Datagram Protocol

UID
Unique Identifier

URI
Uniform Resource Identifier

URL
Uniform Resource Locator

UTM
Unified Threat Management

UUID
Universally Unique Identifier

V

VDOM
Virtual Domain

VHD
Virtual Hard Disk

VIP
Virtual Internet Protocol

VLAN
Virtual Local Area Network

VM
Virtual Machine

VMDK
Virtual Machine Disk

VoIP
Voice over Internet Protocol

VPC
Virtual Private Cloud

VPN
Virtual Private Network

VSA
Vendor Specific Attribute

W

WAF
Web Application Firewall

WAN
Wide Area Network

WCCP
Web Cache Communication Protocol

WIDS
Wireless Intrusion Detection System

WPA
Wi-Fi Protected Access

WPA2
Wi-Fi Protected Access II

WSDL
Web Services Description Language

WTP
Wireless Transaction Protocol

X

XAuth
Extended Authentication

XML
eXtensible Markup Language

XSS
Cross-site Scripting

XVA
XenServer Virtual Appliance

Index