Administration Guide

FortiSandbox 4.2.4

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

June 12, 2023
FortiSandbox 4.2.4 Administration Guide
34-424-881322-20230612

TABLE OF CONTENTS

Change Log **8**
Introduction **9**
FortiSandbox overview 9
What's new in FortiSandbox 4.2.4 9
Getting started **10**
Key Features 10
CLI 11
GUI 12
Connecting to the GUI 12
GUI interface 13
Configuration checklist 13
Update the firmware 14
Change the system host name 15
Backup or restore the system configuration 15
Configure the system time 17
Change the administrator password 18
Change the GUI idle timeout 19
Microsoft Windows VM license activation 19
Microsoft Office license upload and activation 20
Refresh current web page 21
Toggle left-side menu style 21
AI Mode 21
Reboot and shut down the unit 21
Log out of the unit 22
Perform a basic test 22
Port and access control information 22
Default Ports 22
Dashboard widgets **27**
Customize the Dashboard 28
Show unprocessed detection alert notifications on Dashboard > Status 29
System Information 30
Licenses 31
Connectivity and Services 32
Scan Performance (widget) 33
System Resources 34
Scan Statistics 34
File Scan 35
Top Devices 36
Pending Job Statistics 36
Top Critical Logs 36
Sniffer Traffic Throughput 36
Customized Threats Distribution 36
Quick Download 36
System Resources Usage 36

Fortinet Ex. 2003 - Page 3 of 245

Scan Performance (dashboard) 37
Operation Center 38
Threats by Topology 39
Threats by Hosts 40
Threats by Hosts - level 1 41
Threats by Hosts - level 2 42
Threats by Hosts - level 3 42
Threats by Hosts - level 4 43
Threats by Files 43
Threats by Files - level 1 44
Threats by Files - level 2 44
Threats by Files - level 3 45
Threats by Files - level 4 46
Threats by Devices 46
Threats by Devices - level 1 46
Threats by Devices - level 2 47
Threats by Devices - level 3 48
Threats by Devices - level 4 49
Security Fabric 50
Device 50
Supported Devices 52
Adapter 60
ICAP adapter 62
BCC Adapter 65
MTA adapter 68
Carbon Black Bit9 Server 72
Network Share 73
Scan Details 76
Quarantine 77
Sniffer 80
FortiNDR 82
Scan Job 84
Job Queue 84
VM Jobs 85
File Job Search 86
URL Job Search 87
Overridden Verdicts 88
File On-Demand 89
URL On-Demand 93
Cloud Storage 97
AWS S3 Settings 100
Azure File System 101
Azure Blob Storage 101
Scan Policy and Object 105
Scan Profile 105
File types 105

Scan Profile Pre-Filter Tab ... 106
Scan Profile VM Association Tab ... 108
Scan Profile Advanced Tab ... 112
File Scan Priority ... 115
File Scan Flow ... 115
URL Scan Flow ... 116
VM Settings ... 116
Virtual Machine ... 120
Clone Number for VM Image ... 121
VM Screenshot ... 122
Configure a custom VM ... 122
Simulator VMs ... 124
Set the default browser ... 126
Deploying for Static Scan ... 128
General Settings ... 129
Job Priority ... 132
Job Archive ... 133
Allowlist and blocklist ... 135
Web Category ... 137
Working Together With URL Pre-Filtering ... 138
Customized Rating ... 139
YARA Rules ... 140
Malware Package ... 144
URL Package ... 145
TCP RST package ... 146
Threat Intelligence ... 147
Malware and URL Package Options ... 147
IOC Package ... 149
Global Network ... 150
CLI ... 152
System ... 154
Administrators ... 154
Admin Profiles ... 158
Wildcard Admin Authentication ... 162
Device Groups ... 164
Interfaces ... 165
Edit an interface ... 166
Edit administrative access ... 167
Create an aggregate interface ... 167
Failover IP ... 169
Create an API Interface ... 170
DNS Configuration ... 171
Static Route ... 171
LDAP Servers ... 172
RADIUS Servers ... 174
Mail Servers ... 176

FortiGuard 178
Certificates 180
Login Disclaimer 182
SNMP 182
Configuring the SNMP agent 182
MIB files 187
Event Calendar 188
Event Calendar Settings 189
Job View Settings 189
Settings 191
HA-Cluster 193
Cluster setup 194
HA-Cluster pre-requisites 195
Example configuration 195
Cluster level failover IP 200
Health Check 200
Using an aggregate interface 201
Deploying primary and secondary nodes without VM Clones 202
Cluster Management 202
Synchronization 203
Access privilege 203
Job Summary 204
Managing worker nodes 204
HA Roles, Synchronization and Failover 205
Primary and worker roles 205
Heartbeat Synchronization 208
Failover scenarios 208
Performance tuning 209
Setting primary node processing capacity 209
Upgrading or rebooting a cluster 210
Main HA-Cluster CLI commands 210
Log & Report 212
Log Details 212
Logging Levels 212
Raw logs 213
Log Categories 213
Viewing logs in FortiAnalyzer 215
Customizing the log view 216
Columns 216
Summary Reports 217
Generate reports 217
Report Center 218
Customize Report 219
File Scan 220
File Statistics 222
Customizing the File Statistics report page 223

URL Scan ... 224
URL Statistics ... 226
Customizing the URL Statistics page ... 226
Network Alerts ... 227
Network Alerts Statistics ... 229
Customizing the Network Alerts Statistics page ... 230
Log Servers ... 231
Local Log ... 232
Diagnostic Logs ... 233
Appendix A - Advanced deployment scenarios ... 234
Deploying primary and secondary nodes without VM Clones ... 234
Deploying for Static Scan ... 234
Deploying for OT Industry ... 234
Appendix B - Job Details page reference ... 235
Appendix C - Malware types ... 240
Appendix D - Maximum Values ... 242
Configuration limits ... 242
File size limits ... 243
Client Device Connections ... 244

Fortinet Ex. 2003 - Page 7 of 245

Change Log

Date	Change Description
2023-04-14	Initial release.
2023-04-25	Added Maximum Values on page 242
2023-05-08	Updated Scan Details on page 76.

Introduction

This guide describes how to configure and manage your FortiSandbox system and the connected Fortinet Security Fabric devices. For documentation on Fortinet devices, such as FortiGate and FortiClient, see Fortinet Document Library.

FortiSandbox overview

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

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

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

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

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

What's new in FortiSandbox 4.2.4

- Added replacement message on Sniffer Mode when *TCP Reset* is enabled. See, Sniffer on page 80.
- Show disclaimer message on SSH session. See, Login Disclaimer on page 182
- Added csv file support on Microsoft Office scan profile group.
- Enhanced Network Share scan logic on handling 10K files (conserve mode).
- Increased VM memory size on VM00, 500F and 1000F models to improve scan performance.
- Introduced a new Optional VM 'WIN10O19V1' based on Windows 10 with Office 2019.

Getting started

The topics in this section are to help familiarize you with the FortiSandbox system and complete the required configurations to get you started.

This section includes the following topics:

- Key Features on page 10
- CLI on page 152
- GUI on page 12
- CLI on page 11
- Configuration checklist on page 13
- Port and access control information on page 22

Key Features

Key features of FortiSandbox include:

- Dynamic Anti-malware updates/Cloud query: Receives updates from FortiGuard Labs and send queries to the FortiSandbox Community Cloud in real time, helping to intelligently and immediately detect existing and emerging threats.
- Code emulation: Performs lightweight sandbox inspection in real time for best performance, including certain malware that uses sandbox evasion techniques and/or only executes with specific software versions.
- Full virtual environment: Provides a contained runtime environment to analyze high risk or suspicious code and explore the full threat life cycle.
- Advanced visibility: Delivers comprehensive views into a wide range of network, system and file activity, categorized by risk, to help speed up incident response.
- Network Alert: Inspects network traffic for requests to visit malicious sites, establish communications with C&C servers, and other activity indicative of a compromise. It provides a complete picture of the victim host's infection cycle.
- Manual analysis: Allows security administrators to manually upload malware samples via the FortiSandbox web GUI or JSON API to perform virtual sandboxing without the need for a separate appliance.
- Optional submission to FortiSandbox Community Cloud: Tracer reports, malicious files and other information may be submitted to FortiSandbox Community Cloud in order to receive remediation recommendations and updated in line protections.
- Schedule scan of network shares: Perform a schedule scan of network shares in Network File System (NFS) v2 to v4 and Common Internet File System (CIFS) formats to quarantine suspicious files.
- Scan job archive: You can archive scan jobs to a network share for backup and further analysis.
- Website URL scan: Scan websites to a certain depth for a predefined time period.
- Cluster supporting High Availability: Provide a non-interruption, high performance system for malware detection.

You can create custom VMs using pre-configured VMs, your own ISO image, or Red Hat VMs on VirtualBox. For more information, contact Fortinet Customer Service & Support.

For information on hard disk hot-swapping procedure, system recovery procedure using Rescue Mode, and password reset procedure, see the FortiSandbox Best Practices and Troubleshooting Guide in the Fortinet Document Library.

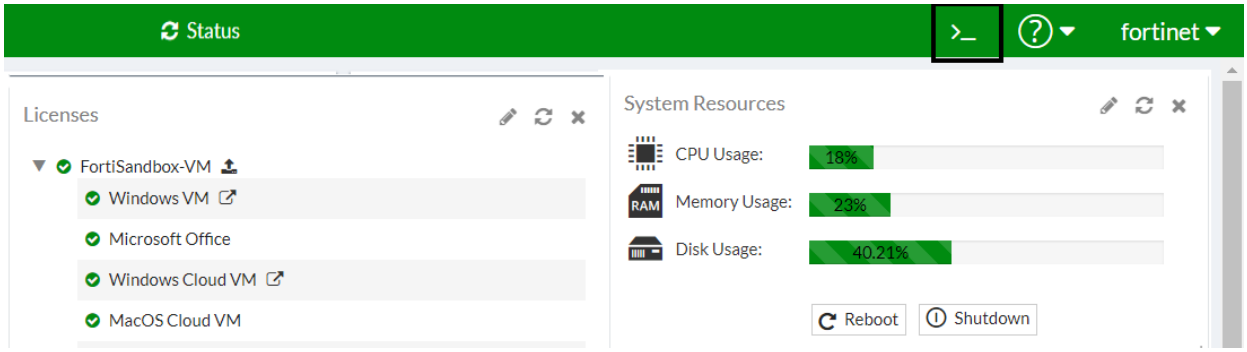
In addition to physical and virtual deployments, FortiSandbox is also available as a cloud-based advanced threat protection service. For more information, see https://docs.fortinet.com/product/fortisandbox-cloud/.

CLI

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

To connect to the CLI Console:

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



The CLI Console pane opens.

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

The CLI Console has the following buttons:

Connect / Disconnect	Toggles the connection to the console.

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

The CLI Console can only connect to a local FortiSandbox.

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

GUI

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

Connecting to the GUI

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

To connect to the FortiSandbox GUI:

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

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

GUI interface

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

The following options are available:

Refresh	Click the *Refresh* icon to refresh the page. For some pages such as *Scan Job* > *File Job Search*, if you click *Refresh*, you lose your current search criteria. Use the *Refresh* icon inside the content pane to continue searching without losing your criteria.
CLI Console	Click the *CLI Console* button >__ to open the CLI Console pane. See CLI on page 11.
Notifications	The bell icon displays messages and notifications that require your attention.
Online Help and Video Tutorials	The question mark icon lets you quickly access the *Online Help* and *Video Tutorials*. *Online Help* links to this Administration Guide in the Fortinet Document Library where you can find information about FortiSandbox and other Fortinet products. *Video Tutorials* links to the Fortinet Video Library for FortiSandbox at https://video.fortinet.com/product/fortisandbox where you can find video tutorials showing how to integrate other Fortinet products, including FortiGates, to FortiSandbox.
User	The user dropdown list lets you change the user password or logout.

Configuration checklist

Use the following checklist to verify you have completed all of the general configuraton tasks.

	Task	Description
☐	Update the firmware on page 14	Go to *Dashboard* > *Status* > *System Information widget* > *Firmware Version*.
☐	Change the system host name on page 15	Go to *Dashboard* > *Status* > *System Information widget* > *Hostname*.
☐	Backup or restore the system configuration on page 15	Go to *Dashboard* > *Status* > *System Information widget* > *System Configuration*.
☐	Configure the system time on page 17	Go to *Dashboard* > *Status* > *System Information widget* > *System Time*.
☐	Change the administrator password on page 18	Go to *System* > *Administrators*.
☐	Change the GUI idle timeout on page 19	Go to *System* > *Settings*.

	Task	Description
☐	Verify the Windows VM license is activated	Go to *Dashboard* > *Status* > *Licenses widget* > *Microsoft VM*.
☐	Upload and activate the Microsoft license	Go to *Dashboard* > *Status* > *Licenses widget* > *Microsoft Office*. After the license uploads, referesh the web page.
☐	Toggle left-side menu style on page 21	Go to *System* > *Settings*.
☐	Verify Services licenses are valid (Antivirus, Web Filtering, and Industrial Security Service).	Go to *Dashboard* > *Status* > *Licenses widget* > *Services*
☐	Verify connectivity and services are online	Go to *Dashboard* > *Status* > *Licenses widget* > *Connectivity and Services Widget*.
☐	(Optional) Disable AI Mode	Use the following CLI command to disable AI mode: `ai-mode`
☐	Reboot and shut down the unit on page 21	Go to *Dashboard* > *Status* > *System Resources widget*.
☐	Log out of the unit on page 22	Select your user name from the top right corner of the banner, and select *Logout* from the dropdown.
☐	Perfom a basic test	Go to *Scan Job* > *File On-Demand* > *Submit File*.

Update the firmware

Before any firmware update, complete the following:

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

Firmware best practice:

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

To update the FortiSandbox firmware:

1. Go to *Dashboard* > *Status* > *System Information widget* > *Firmware Version*.
2. Click the *View all firmware* link beside *Firmware Version*.

3. Click *Upload firmware* and then click *Upload File* to locate the firmware image on your management computer.
4. Click *Submit* to start the upgrade.

Change the system host name

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

To change the host name:

1. Go to *Dashboard* > *Status* > *System Information widget* > *Hostname*.
2. Click the *Change* link beside *Hostname*.
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*.

Backup or restore the system configuration

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

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

To backup the FortiSandbox configuration to your local management computer:

1. Go to *Dashboard* > *Status* > *System Information widget* > *System Configuration*.
2. Click the *Backup/Restore* link beside *System Configuration*.
3. Under *Local Backup*, click *Backup* to save your backup file to your management computer.

To backup the FortiSandbox configuration to a remote server:

1. Go to *Dashboard* >*Status* > *System Information widget* > *System Configuration*.
2. Click the *Backup/Restore* link beside *System Configuration*.

3. Under *Remote Backup*, configure the following settings:

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

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

To backup the configuration to a local FortiSandbox:

1. Go to *Dashboard* >*Status* > *System Information widget* > *System Configuration*.
2. Under *Local Backup*, click *Local FSA*. The *Attention* dialog opens.
3. In the *Please enter your comment* field, type a description of the backup and click *OK*. The backup is added to the *Total backup count* table.

To restore the FortiSandbox configuration:

1. Go to *Dashboard* > *Status* > *System Information widget* > *System Configuration*.
2. Click the *Backup/Restore* link beside *System Configuration*.
3. Under *Restore*, click *Restore file*, locate the backup file on your management computer, then click *Restore* to load the backup file.
4. Select *OK* in the confirmation dialog box. Once the configuration restore process is completed, you will be redirected to the log in page.

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

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

To backup the FortiSandbox configuration using SCP or TFTP:

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

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

The options available are as follows:

-h Help Information

-s Remote SCP/TFTP server IP

-t Protocol type: SCP or TFTP

-u Scp/tftp user name

-f Remote server folder and the backup file name

Example 1:

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

Example 2:

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

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

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

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

The options available are as follows:

-h Help Information

-s Remote SCP/FTP/TFTP server IP

-t Protocol type: SCP, FTP or TFTP

-u Scp/ftp/tftp user name

-f Remote server folder and the backup configuration file name

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

Example 1:

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

Example 2:

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

Example 3:

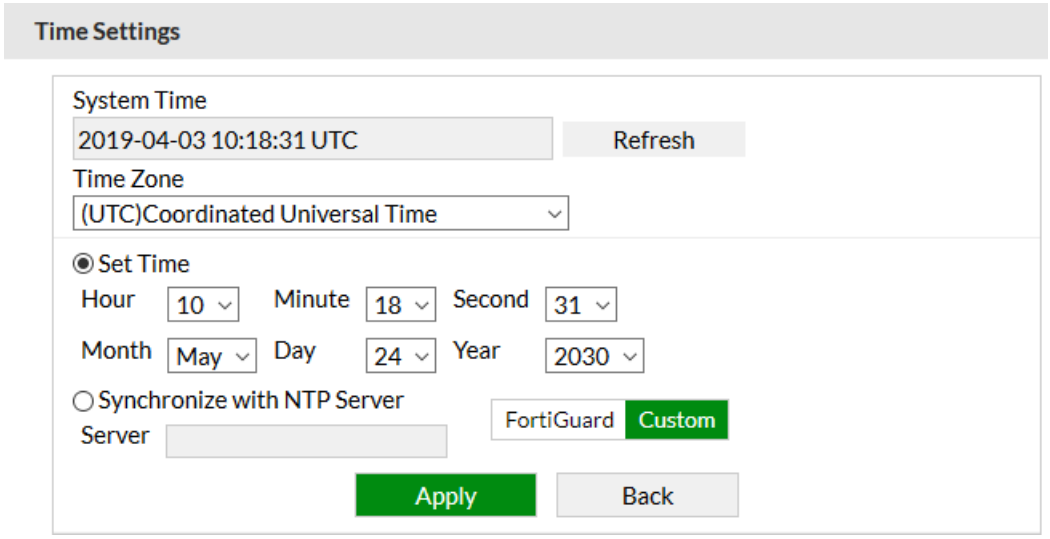
```
restore-sysconf –s1.2.3.4 –utest –tftp –f/fsa/backup.conf -o
```

Configure the system time

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

To configure the system time:

1. Go to *System Information widget* > *System Time*.
2. Click the *Change* link beside *System Time*.



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 use the FortiGuard NTP server or specify 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.

Change the administrator password

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

To change an administrator's password:

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

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

Change the GUI idle timeout

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

To change the idle timeout length:

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

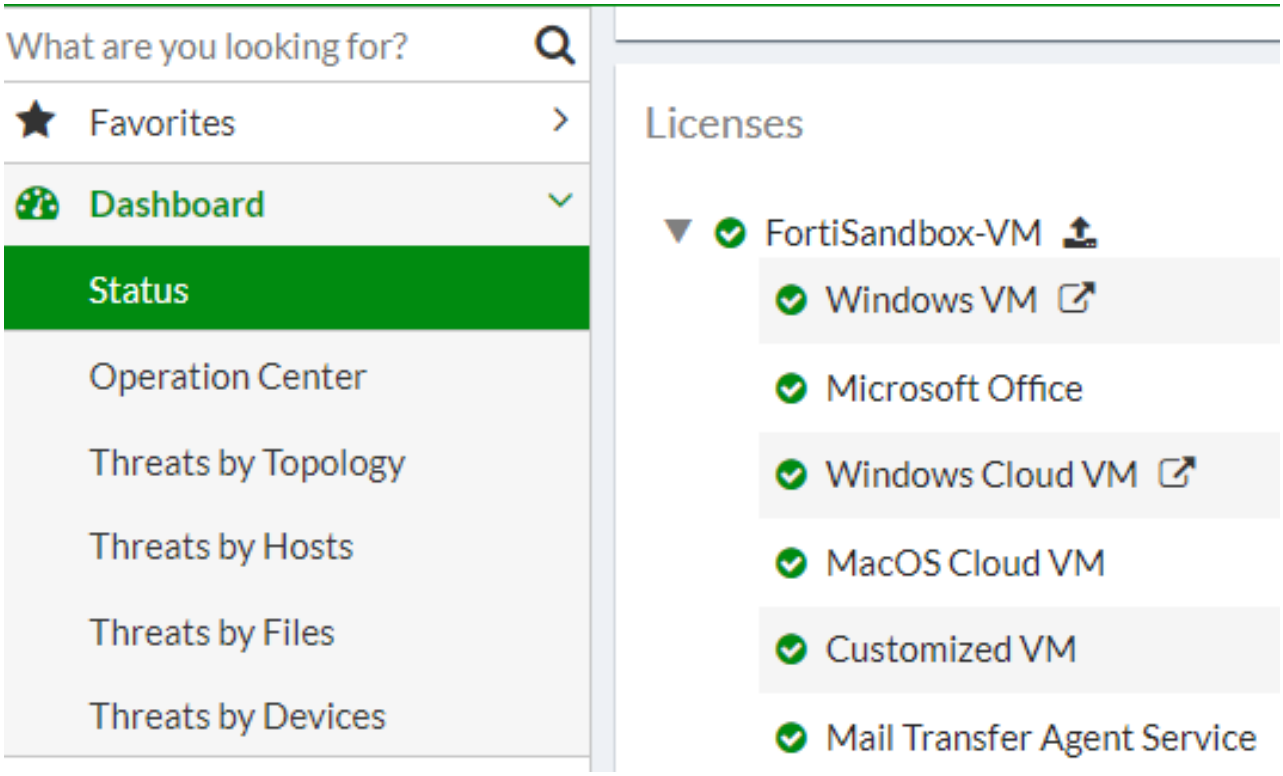
In this page you can also reset all widgets to their default settings.

Microsoft Windows VM license activation

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

To verify the Windows VM license is activated:

1. Go to *Dashboard* > *Status* > *Licenses* widget. A green checkmark appears next to *Microsoft VM*.



2. To activate the license, click the *Upload License* icon next to *Fortisandbox-VM*.
3. Browse to the location of the license file on your computer.
4. Click *Submit*. FortiSandbox will reboot after the license file is installed.

Microsoft Office license upload and activation

You can purchase add-on Office licenses from Fortinet and upload them from the *Dashboard* > *Status* > *Licenses* widget.

By default, physical FortiSandbox models are shipped with a number of Microsoft Office license keys. You can purchase more licenses from Fortinet to improve the scan capacity of Microsoft Office files, or to activate Microsoft Office software inside a newly installed optional Windows guest image.

To upload a Microsoft Office license:

1. Go to *Dashboard* > *Status* > *Licenses widget*.
2. Click the upload link beside *Windows VM* and navigate to the location of the license file on your computer.
3. Click *Submit*. The changes will be applied immediately.

After the license file is installed, you can scan Microsoft Office files including `.docx` and `.pptx` file.

Refresh current web page

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

Toggle left-side menu style

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

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

AI Mode

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

To enable or disable AI mode use the following CLI command:

```
ai-mode
```

Reboot and shut down the unit

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

To reboot the FortiSandbox unit:

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

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

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

Fortinet Ex. 2003 - Page 21 of 245

To shut down the FortiSandbox unit:

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

Log out of the unit

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

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

Perform a basic test

After FortiSandbox is configured, perform a simple Scan Job on a file to verify the service is working as expected.

To perform a basic test:

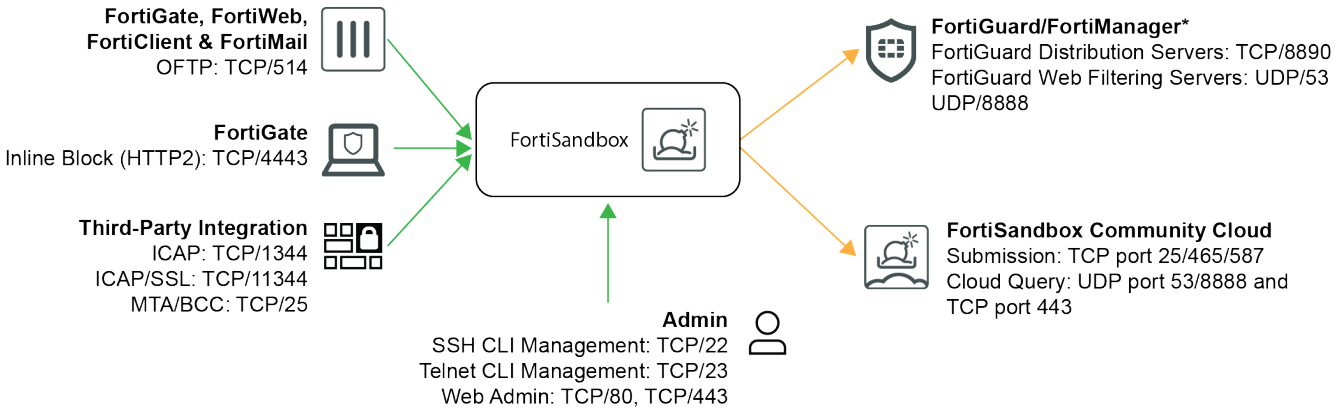
1. Go to *Scan Job* > *File On-Demand*.
2. Click *Submit* File. The *Submit New File dialog* opens.
3. Click Upload File and navigate to the file on your device.
4. Enable *Force to scan the file inside VM* > *Force to scan inside the following VMs* and select the VM to scan inside.
5. and then click Submit.
6. Close the dialog and wait a few mintues for FortiSandbox to process the file. After the file is processed, the *Status* will change to *Done* and the *Rating* is displayed.
7. To view the report:
   a. Click the *View Details* icon.
   b. Click the *View Job Detail* icon.
   c. Click the *Overview*, *Tree View* and *Details* tab to view the job details.
   d. Click *Export Job Detail page to PDF* to download the report.

Port and access control information

This topic contains information about the default ports by interface as well as the endpoints that need to be reachable by FortiSandbox.

Default Ports

The following section provides information about ports by interface, ports by FortiSandbox model, and ports by configuration.



*For more information, see Air Gapped Mode.

Ports by interface

The following table lists the services and ports for each FortiSandbox interface.

Interface	Services and Ports
Port1	Default for inbound traffic for Administration TCP ports 22 (SSH), 23 (Telnet), 80 and 443 (GUI).
Port3	Reserved for the outgoing traffic initiated by the guest VMs. For effective detection of 0-day, we strongly suggest to directly connect Port3 to the Internet via a perimeter firewall. Also, make sure that connectivity is isolated from your Intranet (internal network) to prevent lateral movement. If connected directly to a FortiGate device, make sure that the egress WAN interface does not have the Scan Outgoing Connections to Botnet Sites feature enabled, nor any active security profiles as this can affect the detection rate.
All ports except Port3	**Inbound**: The following services define the ports for inbound: • File, URL and Traffic submission via OFTP (TCP) port 514. • MTA and BCC Adapter uses TCP port 25 for inbound submission. • ICAP Adapter TCP port 1344. The port number is configurable. • Administration TCP ports 80 and 443 if manually configured via CLI command set admin-port. • SNMP local query port TCP or UDP 161. The port number is configurable. **Outbound**: The following services define the ports for outbound. The interface of the services is based on the static route configuration: • FortiGuard Distribution Servers (FDS) TCP port 8890 for downloading database and engine updates. • FortiGuard Web Filtering UDP port 53 or 8888 for URL category check. For secure connection which is configurable under *System* > *FortiGuard* > *FortiGuard Web Filter Settings*, it uses TCP/53 & TCP/8888. • FortiSandbox VM Download TCP port 443 for downloading VM images.

Interface	Services and Ports
	• FortiSandbox Community Cloud query both UDP port 53 or 8888 and TCP port 443 to query submissions by other FortiSandbox. • FortiSandbox Community Cloud submission TCP port 25, 465 or 587 to upload detected suspicious Zero-day detection information. It uses only one of the ports in sequence. All the ports are encrypted. FortiSandbox will attempt to connect to the ports in sequence with encryption. If the connection fails, FortiSandbox will re-attempt to connect in sequence without encryption. • FortiSandbox Windows Cloud VMs TCP port 514 to submit jobs to the Windows cloud VMs. License required. • FortiSandbox MAC Cloud VMs TCP port 443 to submit jobs to the MAC cloud VMs. License required. • Mail server port TCP 25, DNS server port UDP 53, remote Syslog server port TCP or UDP 514, LDAP server port TCP 389, SNMP managers port TCP or UDP 162, and NTP server port UDP 123. Make sure to check the Static Route configuration for the gateway and outgoing port to use. Also, the port number for the following are configurable: Mail, Remote Syslog, LDAP, SNMP.
Cluster ports (all other ports except Port1 and Port3)	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.

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

For redundancy and increase throughput, consider setting up Aggregate interface. See, Create an aggregate interface on page 167.

For any outgoing traffic, FortiSandbox uses a random port picked by the kernel.

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

The following table lists the available ports for each FortiSandbox model.

Interface Type	3000F/3000E/2000E	1000F	500F
RJ45	Port 1-4	Port 1-4	Port 1-4
SFP GbE		Port 5-8	
SFP+	Port 5-6		

Access Control List

The table below provides the default servers and options when configured. For further info on the services, refer to the notes column. We recommend periodically checking these entries for changes.

Services	Destination	Notes
FortiGuard Distribution Network (FDN)		
Database and Engine Download	fds1.fortinet.com:8890/TCP When configured to override region: • **Nearest**: fds1.fortinet.com:8890/TCP • **US Region**: usfds1.fortinet.com:8890/TCP • **Global**: globalupdate.fortinet.net:443/TCP	Default is *Nearest*. Configurable. For more information, see*FortiGuard* > *FortiGuard Server Location* in the *FortiSandbox Administration Guide*.
Web Filtering Service	securewf.fortiguard.net:53/TCP or 8888/TCP When configured to override region: • **Nearest**: securewf.fortiguard.net:53/TCP or 8888/TCP • **US Region**: ussecurewf.fortiguard.net:53/TCP or 8888/TCP • **Global**: securewf.fortiguard.net:53/TCP or 8888/TCP	Default is *Nearest*. When *Secure Connection* under FortiGuard Web Filter Settings is disabled, replace the TCP with UDP. For more information, see *FortiGuard* > *Secure Connection* in the *FortiSandbox Administration Guide*.
FortiSandbox		
Community Cloud Query	fqsvr.fortinet.net:53/UDP	For more information, see *General Settings* > *Community Cloud Query* in the *FortiSandbox Administration Guide*. Available only in Global (Canada).
Community Cloud Upload	fortinetvirussubmit.com:25/TCP *or* 465/TCP or 587/TCP	For more information, see *General Settings* > *Upload malicious and suspicious file* in the *FortiSandbox Administration Guide*. Available only in Global (Canada).
Rating Cloud Service (RSE)	fqdl.fortinet.net:443/TCP	For more information, see *Scan Profile Advanced Tab* > *Enable Rating Cloud Service* in the *FortiSandbox Administration Guide*. Available only in Global (Canada).
Windows Cloud VM Service	aptctrl1.fortinet.com:443/TCP *or* 514/TCP List of IP Addresses: • **Europe**: 83.231.212.128/25, 154.45.1.0/24, 154.52.11.0/24 • **US Region**: 208.184.237.0/24, 209.222.141.128/26 • **Japan**: 210.7.96.0/24, 154.52.7.0/24	Initially download a list of IP via the APTCTRL1 as configured on *WindowsCloudVM Settings*. For more information, see *FortiGuard* > *WindowsCloudVM Settings* in the *FortiSandbox Administration Guide*.

Services	Destination	Notes
	• **Global**: 173.243.139.0/24, 184.94.112.0/24, 154.52.26.0/24	
macOS Cloud VM Service	mac.fortisandbox.net:443/TCP or mac2.fortisandbox.net:443/TCP	Available only in Global (Canada).
VM Images Service	fsavm.fortinet.net:443/TCP	Uses GeoIP to select between two regions for faster download speed of the VM images. Available in Global (Canada) and Germany.

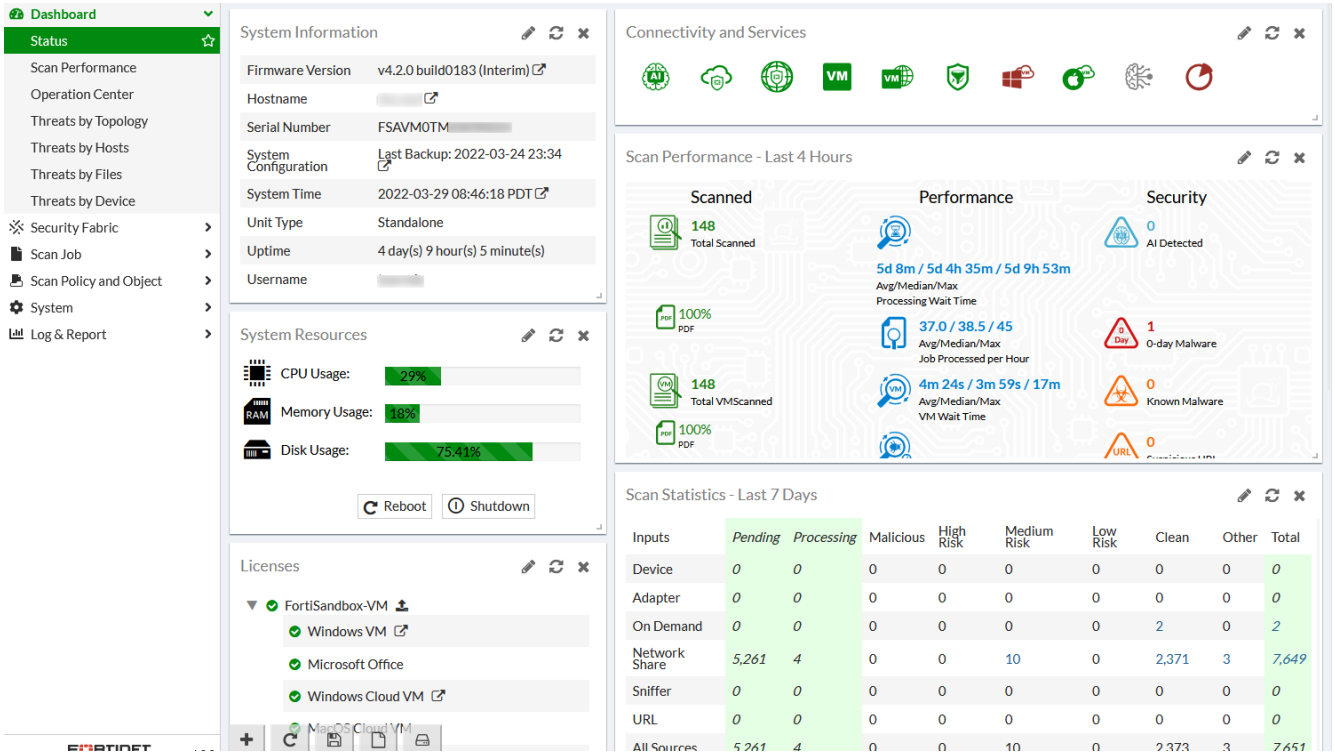
An alternative option is to use the Internet Service feature on the FortiGate to define a firewall policy that allows connection to that destination. For more information, see *Using Internet Service in a policy* in the *FortiGate/FortiOS Administration Guide*. Choose *Fortinet-FortiGuard* and *Fortinet-FortiCloud*.

Dashboard widgets

Dashboard > *Status* displays widgets that provide system information and enable you to configure basic system settings. All widgets appear in the *Dashboard* > *Status* page which you can customize.

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

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



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

The following widgets are available:

System Information	Displays basic information about the FortiSandbox system, such as the serial number and system up time.
Licenses	Displays license status information.
Connectivity and Services	Displays connectivity and services.
Scan Performance	Displays scan performance over a time period.
System Resources	Displays the real-time usage status of the CPU, memory, and disk usage.
Scan Statistics	Displays information about files scanned over a time period, This including Sniffer, Devices, On-Demand, Network, Adapter, and URL.

File Scan	Displays the number of clean, suspicious, and malicious events that occurred at specific times over a time period. Hover the pointer over a colored portion of a bar in the graph to view the number of events of the selected type that occurred.
Top Devices	Displays the total scanning jobs for the top five devices over a time period. Hover the pointer over a bar in the graph to view the number of scanning jobs for that device.
Pending Job Statistics	Displays pending scan job numbers over a time period. This widget allows you to monitor the workload trend on your FortiSandbox.
Top Critical Logs	Displays recent critical logs, including the time they occurred and a brief description.
Sniffer Traffic Throughput	Displays sniffed traffic throughput across time.
Customized Threats Distribution	Displays threat level distribution over two customized time intervals.
Quick Download	To quickly search a file according to its checksum. If found, the user can download the file, download the PDF report, and view job detail.
System Resources Usage	Displays system resources usage over a time period, including CPU, memory, and disk usage.

Customize the Dashboard

You can customize *Dashboard* > *Status*. 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 pointer 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 reset a widget back to default settings:

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

To add a widget:

1. In the *Status* dashboard, scroll down to the floating toolbar at the bottom of the page.

2. Click *Add Widget*, then select the widgets you want to add.
3. To hide a widget, click the close icon in its title bar.

The following is a list of widgets you can add to *Dashboard* > *Status*.

- System Information
- Licenses
- Connectivity and Services
- Scan Performance (widget)
- System Resources
- Scan Statistics
- File Scan
- Top Devices
- Pending Job Statistics
- Top Critical Logs
- Sniffer Traffic Throughput
- Customized Threats Distribution
- Quick Download
- System Resources Usage

To go to the top of *Dashboard* > *Status*:

After scrolling down the *Dashboard* > *Status* page, a *Back to Top* button appears in the floating widget tool bar. Click this button to go to the top of the page.

To edit a widget:

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

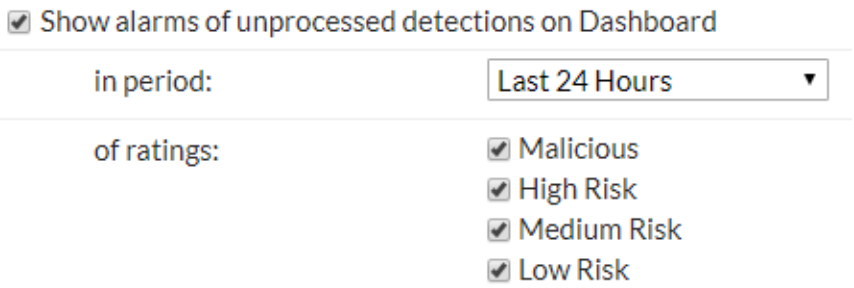
Custom widget title	Optionally, type a custom title for the widget. Leave this field blank to use the default widget title.
Refresh interval	Enter a refresh interval for the widget, in seconds.
Top Count	Select the number of entries to display in the widget. This option is only available on widgets where a top count is applicable.
Time Period	Select a time period to be displayed from the dropdown list. This option is only available on widgets where a time period is applicable.

Show unprocessed detection alert notifications on *Dashboard* > *Status*

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

To show alarms of unprocessed detections on *Dashboard* > *Status*:

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



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

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

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

System Information

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

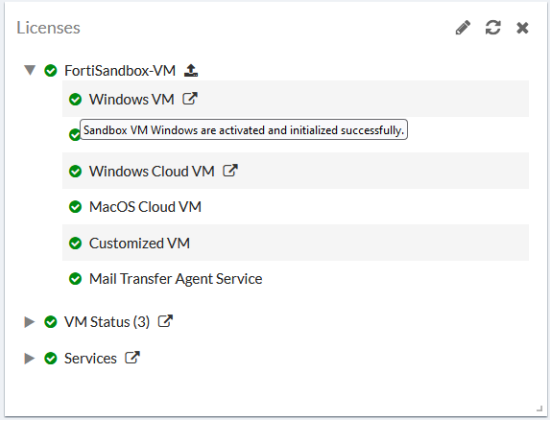
Firmware Version	The version and build number of the firmware installed on the FortiSandbox unit. When new firmware is available, a blinking *New firmware available* link appears. Clicking the link redirects you to a page where you can download and install available firmware, or manually upload firmware. You can also choose to create backup configurations.
Hostname	The name assigned to this FortiSandbox unit. Click *Change* to edit the FortiSandbox host name.
Serial Number	The serial number of this FortiSandbox unit. The serial number is unique to the FortiSandbox unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
System Configuration	The date and time of the last system configuration backup. Click *Backup/Restore* to go to the *System Recovery* page.
System Time	The current time on the FortiSandbox internal clock or NTP server. Select *Change* to configure the system time.
Unit Type	The HA cluster status of the device: *Standalone*, *Primary*, *Secondary*, or *Worker*. In an HA-Cluster, click *Change* to change the cluster status of the device.

	If the rating engine is not available or out-of-date, a red blinking *No Rating Engine* message appears.
Uptime	The duration of time that the FortiSandbox unit has been running since boot up.
Username	The administrator that is currently logged in.

Licenses

The *Licenses* widget displays information about the licenses on your FortiSandbox unit. Only the licenses available for your FortiSandbox appear.

Hover your mouse over the status icon to view the license status and details.



On VM models, use the *Upload License* link next to the *Fortisandbox-VM* field to install the license. The system reboots and activates the newly installed Windows guest VMs.

On hardware models, use the *Upload license* link next to the *Windows VM* field to install the license. The system does not require a reboot, and will activate the newly installed Windows guest VMs.

On FortiSandbox hardware units, the *Upload License* icon can accept the Microsoft Windows license file, Microsoft Office license file, and Microsoft Windows & Office license file as FSA-VM.

Windows VM	Microsoft Windows VM license activation and initialization status. For more information, see *Log & Report* > *Events* > *VM Events*. In addition to the pre-installed default set of Windows VM images, you 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 you try to use a Windows 10 image on a FortiSandbox unit, you might need to purchase Windows 10 license keys from Fortinet. After purchase, download your license file from the Fortinet Customer Service & Support portal. Then use the *Upload License* link next to the Windows VM field to install the license. The system reboots and activates the newly-installed Windows guest VMs.

Microsoft Office	Microsoft Office product activation status. The active icon and caution icon can both appear when Microsoft Office software is activated on some enabled VMs but not activated on other enabled VMs. For more information, see *Log & Report* > *Events* > *VM Events*.
Windows Cloud VM	Windows Cloud VMs are an extension of units' scan power by sending files to Fortinet Sandboxing cloud to scan. This line shows the date that Windows Cloud VM contract expires, and number of remote clones reserved in cloud. In a cluster environment, each VM00 unit in the cluster can purchase Windows cloud VM seat counts to expand the cluster's scan power. These cloud VM clones are local to that VM00 unit and are not shared.
MacOS Cloud VM	The date the MacOS contract expires and the number of remote clones reserved in Fortinet MacOS cloud. In cluster mode, the total reserved clone numbers displays on the primary node. All cluster units share a collected pool of reserved clones from each unit. This means that even nodes with no MacOS VM contract can still upload MacOSX files to the cloud for scanning.
Customized VM	Customized VM license activation and initialization status.
Mail Transfer Agent Service	Mail Transfer Agent Service license activation and initialization status.
VM Status	Status of the FortiSandbox guest VM accessing the outside network. This section only displays VMs that are enabled.
Antivirus	The date that the antivirus database contract expires. If the contract expires within 15 days, a caution icon appears.
Web Filtering	Status of the Web Filtering query server.
Industrial Security Service	Status of the Industrial Security Service.

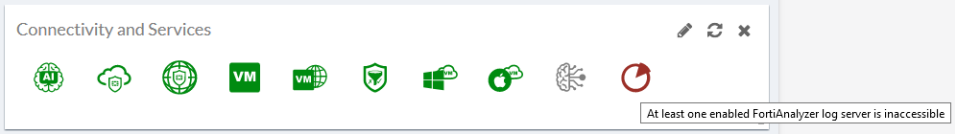
Connectivity and Services

This widget displays information about connectivity and services. The icon color indicates if the service is up, inaccessible, or not configured.

- **Green**: The service is accessible.
- **Red**: The service is inaccessible.
- **Gray**: The service is not configured.

Hover over an icon to see details about that service.

FortiAnalyzer server connectivity



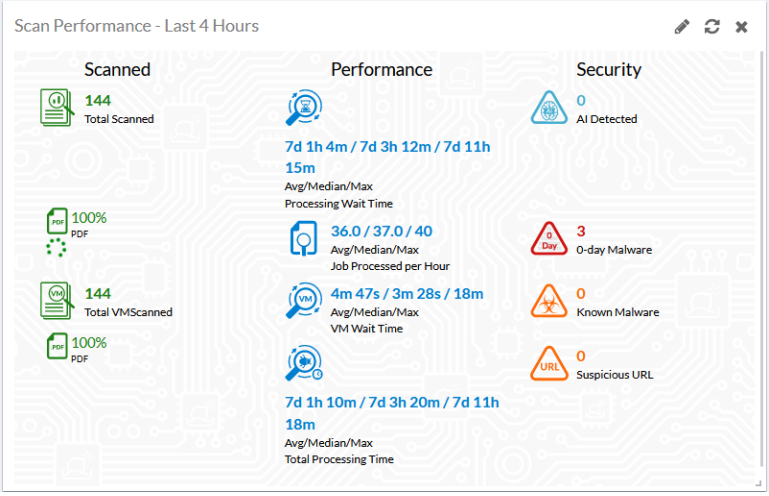
Green	FortiAnalyzer(s) are connected. Tooltip: • *All enabled FortiAnalyzer log servers are accessible.*
Red	The FortiAnalyzer server is not connected. Tooltip: • *At least one enabled FortiAnalyzer log server is inaccessible*: Multiple FortiAnalyzer Server are enabled but at least one is inaccessible. • *WARNING: FortiAnalyzer log servers(s) is enabled, but inaccessible*: One or all the FortiAnalyzer servers are inaccessible.
Gray	FortiAnalyzer is not configured or all FortiAnalyzer servers manually changed to disabled status. Tooltip: • *No FortiAnalyzer log server is enabled*.

In an HA Cluster, the Primary unit can check the non-primary node's dashboard status in the *HA Cluster* > *SN#* page.

By default, all nodes can set their own FortiAnalyzer server configuration. However, the Primary unit can sync its own log server configuration after selecting the sync log server and log settings options. To do this, go to *HA Cluster* > *Cluster Management*.

Scan Performance (widget)

The *Scan Performance* widget displays scan performance information including the number of files scanned, performance, and the security verdict. The data is accumulated every 10 minutes. To view granular information, see the Scan Performance page.



System Resources

This widget displays the following information and options:

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

Scan Statistics

This widget displays information about the files that have been scanned over a specific time period, including the following information.

Inputs	The input type from which the files were received.
Device, Adapter, On Demand, Network Share, Sniffer, URL, All Sources	The URL type is for scanned URLs received from FortiMail devices, URLs extracted from forwarded email body of BCC adapter, URLs from ICAP adapter, and sniffed URLs in email traffic.
Pending	The number of files pending. Pending files are files that are have just been received and have not been put into the job queue, and files that have been put into the job queue but have not yet been processed.
Processing	The number of files that are being processed.
Malicious	The number of files scanned for each input type that were found to be malicious in the selected time period. Click the number to view the associated jobs.

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 number to view the associated jobs.
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.
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 number 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 number 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, canceled by the user through a JSON API call, or terminated by the system. Click the number to view the associated jobs.
Total	The total number of files for each input type in the selected time period.

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

How admin permissions apply to scan statistics

An admin's permissions in the *Menu Access* section of the admin profile determines which jobs the admin can see in the *Scan Statistics* widget. See Admin Profiles on page 158.

Admin Profile	Permissions
Super Admin	The widget shows the number of jobs scanned including a hyperlink. When the admin clicks the hyperlink, they are redirected to a new page listing all the jobs.
Read Write	The widget shows the number of jobs scanned including a hyperlink. When the admin clicks the hyperlink, the new page will only show jobs which are submitted on-demand by the admin, and all other input jobs, such as *Sniffer*.
Read Only	The widget shows all job numbers. However, the hyperlink is disabled.

File Scan

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

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

Shift-select a period to zoom in. Shift-scroll to move left and right.

Hover the pointer over a colored portion of a bar in the graph to see the number of events of that type for that time period.

Top Devices

This widget displays the total number of scanning jobs for the top five devices over a selected time interval.

Hover the pointer over a bar in the graph to see the number of scanning jobs for that device.

Pending Job Statistics

This widget displays the pending job numbers of each input source.

Hover the pointer over the graph displays the number of pending jobs for the on-demand, sniffer, and Fortinet devices over a selected time period. Shift-select a period to zoom in. Shift-scroll to move left and right.

Top Critical Logs

This widget displays recent critical logs, including the time they occurred and a brief description of the event.

Sniffer Traffic Throughput

This widget displays the Sniffer Traffic Throughput in MB/s over a sselected time period.

Shift-select a period to zoom in. Shift-scroll to move left and right.

Customized Threats Distribution

This widget displays a chart of the detected malware rating distribution for two specified time periods. Hover the pointer over parts of the chart to see more details.

Quick Download

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

System Resources Usage

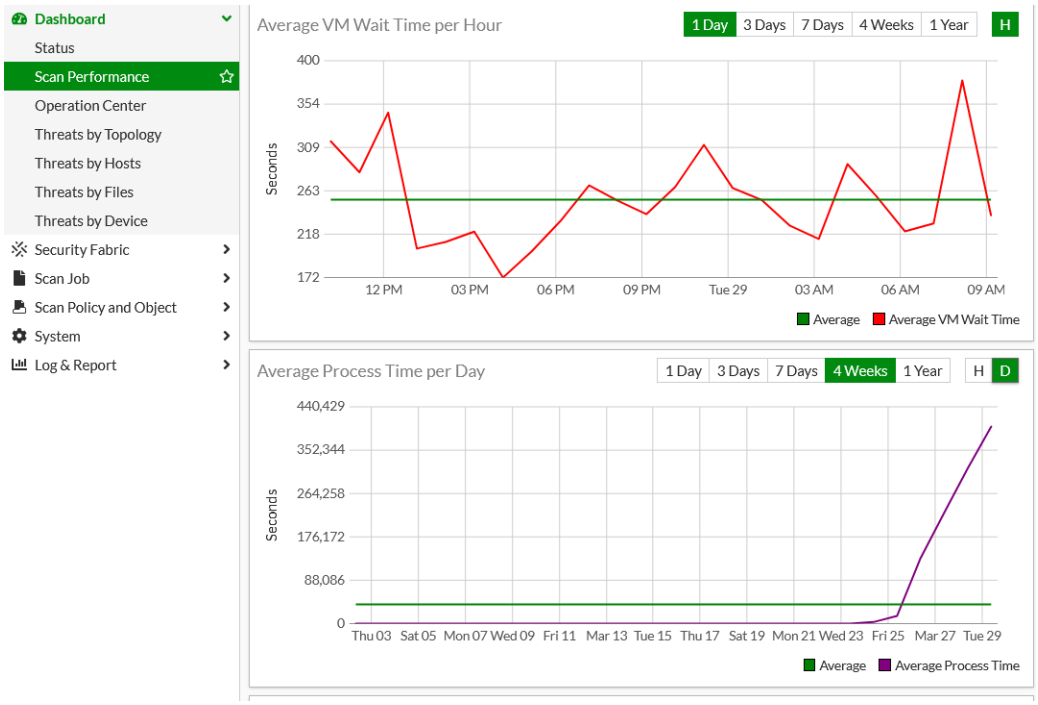
This widget displays a timeline of CPU, memory, and RAM disk usage over a specified time period.

Hover the pointer over the graph for more details. Shift-select a period to zoom in. Shift-scroll to move left and right.

Scan Performance (dashboard)

The *Scan Performance* dashboard tracks the FortiSandbox performance over time. The data is similar to the Scan Performance widget and is accumulated every 10 minutes. The page is automatically refreshed every 5 minutes. To view the Scan Performance dashboard, go to *Dashboard* > *Scan Performance*.

The options for the unit of time will vary based on the time range. For example, the hourly view H is displayed in shorter time ranges (*1 day*, *3 days* and *7 days*), whereas the day view D is displayed in longer ranges (*4 weeks* and *1 Year*).



The *Scan Performance* dashboard contains the following charts:

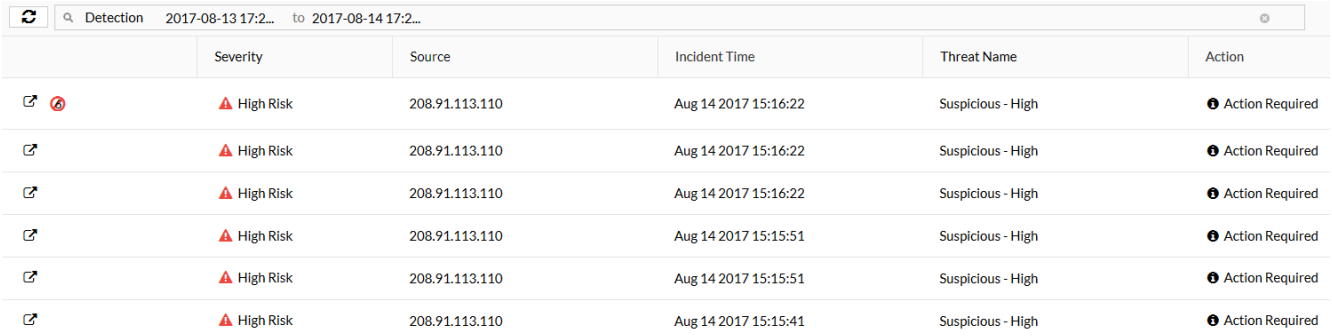
Scanned Count	The total number of scanned jobs per time unit.
VM Scan count	The total number of jobs that entered the VM for dynamic scan per time unit.
Average Processing Wait Time	The wait time in the initial processing queue.
Average VM Wait time	The wait time prior to entering the VM for dynamic scan based on the average calculated time divided by total jobs per time unit.
Average Process Time	The processing time from receiving to completing the scan based on the average calculated time divided by total jobs per time unit.
Average VM Scan Time	The processing time within the VM for dynamic scan based on the average calculated time divided by total jobs per time unit.

Operation Center

Use this page to view malware that has been detected and its status from a security update perspective. This page displays severity levels, victim IP addresses, incident time, threat, and current action status.

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

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



The following options are available:

Refresh	Refresh the entries after applying search filters.
Search	Show or hide the search filter field.
Time Period	Select the time period from the dropdown list. Select one of the following: 24 Hours, 7 Days, or 4 Weeks.
Clear all removable filters	Click the trash can icon to clear all removable filters.
Export to report	Click *Export to report* to create a PDF or CSV snapshot report. The time to generate the report depends on the number of events. You can wait to view the report or find the report later in *Log & Report* > *Report Center*.
Add Search Filter	Click the search filter field to add search filters. Use search filters to define what to display in the GUI. For example, you can use a field like source IP address as the search criterion.
View Job	Show the job detail page.
Number of Blocks	After a malware's signature is added to a Malware package and downloaded by FortiGate, FortiGate can block subsequent occurrences. Hover the pointer over the icon to see the number of blocks of this Malware.
In Cloud	An icon appears if the malware is available in the FortiSandbox Community Cloud.
In Signature	An icon appears if the malware is included in the current FortiSandbox generated Malware Package.

Perform Rescan	Rescan the suspicious or malicious entry. In the *Rescan Configuration* dialog box, you can force the file to do Sandboxing scan even if was detected in former steps of Static Scan, AV Scan, Cloud Query, or stopped from entering VM by Sandboxing-prefilter setting. The rescan job is in *Scan Job* > *File On-Demand*.
Archived File	An icon appears if the file is an Archived File.
Pagination	Use pagination options to browse entries.

This page displays the following information:

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

To view file details:

1. Select a file.
2. Click the *View Details* icon to open a new tab.
   For descriptions of the *View Details* page, see Job Details page reference on page 235.

Threats by Topology

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

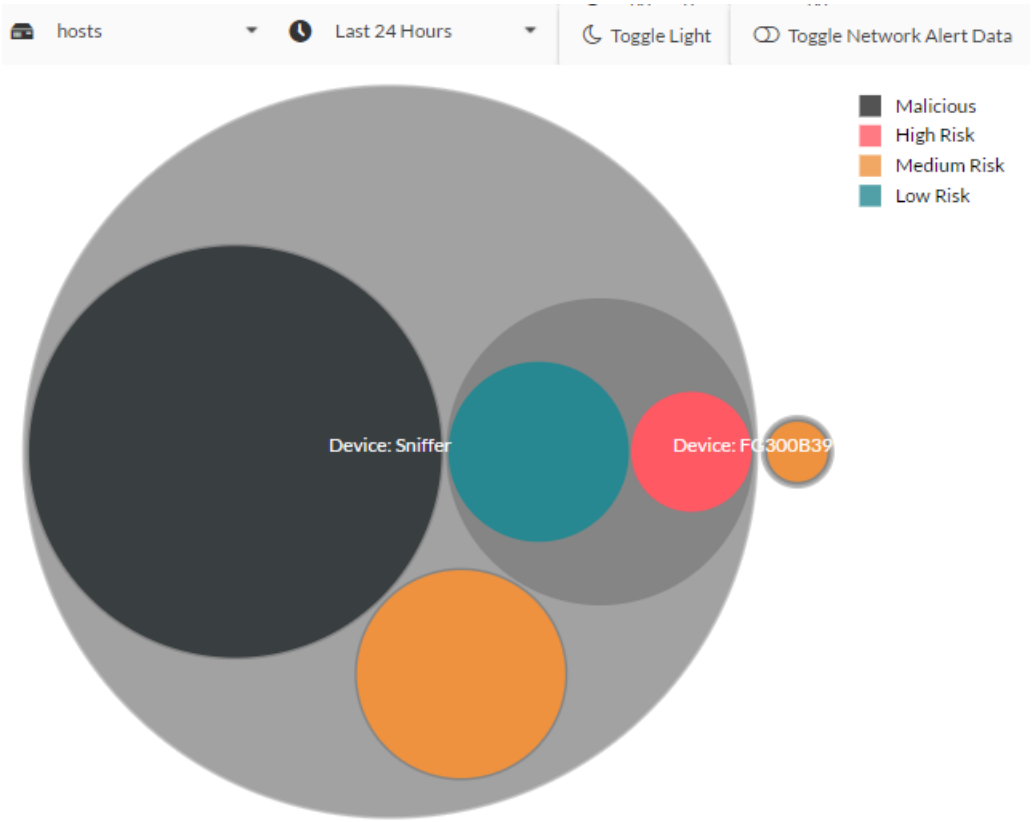
Devices (or input sources) are displayed in separated top level circles and the threats that occur on them are displayed inside them as second level circles. The radius of threat circle is proportional to threat event counts. Threat circles can be multiple levels and each level represents a subnet level.

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

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

The following options are available:

Hosts	Select the host.
Time Period	Select the time period from the dropdown list. Select *24 Hours*, *7 Days*, or *4 Weeks*.
Toggle Light	Select *Toggle Light* to change the topology background color.
Toggle Network Alert Data	Select to toggle and include Network Alert data from sniffed traffic.



Threats by Hosts

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

Threats by Hosts - level 1

The following options are available:

Time Period	Select the time period from the dropdown list. Select *24 Hours*, *7 Days*, or *4 Weeks*.
Export Data	Click the *Export Data* button to create a PDF or CSV snapshot report. You can wait till the report is ready to view, or navigate away and find the report later in *Log & Report* > *Report Center* page.
Search	Show or hide the search filter field.
Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.
Add Search Filter	Click the *Search Filter* field to add search filters. Click the *Cancel* icon to the left of the search filter to remove the specific filter. Click the *Clear All Filters* icon in the search filter field to clear all filters. In this page, the threat target host or user name can be the search criteria. You can input a partial value to search all records that contain it. Search filters can be used to filter the information displayed in the GUI.
View Job	Click the *View Jobs* icon to drill down the entry.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

Host/Username	The device and username that is the target of threats. A duplicate user name or host from a different VDOM is considered a different user.
Device Name	The device name.
# 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 Hosts	The number of hosts displayed and total number of hosts.

Threats by Hosts - level 2

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

The following information is displayed:

Back		Click *Back* button to return to the main landing page.
Threat Timeline Chart		This chart displays the number of threats and types of threats which occurred to the threat target during the period of time. Hover the mouse pointer over the dots in the chart and more detailed threat information will be displayed.
Summary of		The following fields are displayed: Device, Threat Target, Time Period, Total Files, number of: Malicious Files, Suspicious Files, and Network Events.
Details		
	Malicious Files	Malicious file information including malware name, Threat Source, and number of detection times. The options are: • Click the *View Jobs* icon to drill down the entry. • Click the malware name to view the related FortiGuard Encyclopedia page.
	Suspicious Files	Suspicious file information including file name, file type, rating, the malware hosting address and number of detection times. Click the *View Jobs* icon to drill down the entry.
	Attacker Events	Attacker event information including backdoor name, attack origin address and port, attack destination address and port, and number of detection times.
	Botnet Events	Botnet event information including botnet name, user IP address, user port, destination IP address, destination IP port and number of detection times.
	URL Events	Suspicious URL event information including site category, host or IP address, URL, type, user IP address, user port and number of detection times.

Threats by Hosts - level 3

The following options are available:

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

The following information is displayed:

Malicious Files	Displays the date and time that the file was detected, malware name, source IP address, and destination IP address. Click the malware name to view the related FortiGuard Encyclopedia page.
Suspicious Files	Displays the date and time that the file was detected, file type, rating, source IP address, destination IP address and number of detection times, if available.
Total Jobs	The number of jobs displayed and the total number of jobs.

Threats by Hosts - level 4

For more about the information available in the *View Details* pages for malicious and suspicious files, see Job Details page reference on page 235.

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

To create a snapshot report for all threats by users:

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

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

Threats by Files

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

Threats by Files - level 1

The following options are available:

Time Period	Select the time period from the dropdown list. Select *24 Hours*, *7 Days*, or *4 Weeks*.
Export Data	Click the *Export Data* button to create a PDF or CSV snapshot report. The time period of jobs included in the report depends on the selection made in the Time Period dropdown. The time to generate the report is dependent on the number of events selected. You can wait until the report is ready to view, or navigate away and find the report later in the *Log & Report* > *Report Center* page.
Search	Show or hide the search filter field.
Refresh	Click the *Refresh* icon to refresh the entries displayed after applying search filters.
Add Search Filter	Click the *Search Filter* field to add search filters. Click the *Cancel* icon to the left of the search filter to remove the specific filter. Click the *Clear All Filters* icon in the search filter field to clear all filters. When the filter *Filename* is used, click the = sign to toggle between the exact and pattern search. Search filters can be used to filter the information displayed in the GUI.
View Jobs	Click the *View Jobs* icon to drill down the entry.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

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

Threats by Files - level 2

The following options are available:

Back	Click the *Back* icon to return to the main landing page.
Threat Timeline Chart	Displays the number of threats and types of threats which occurred to the threat target during the peroid of time. Hover over the dots in the chart to view more detailed threat information.
Search	Show or hide the search filter field.
Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.

Add Search Filter	Click the search filter field to add search filters. Click the cancel icon to the left of the search filter to remove the specific filter. Search filters can be used to filter the information displayed in the GUI.
View Jobs	Click the *View Jobs* icon to drill down the entry.
Pagination	Use the pagination options to browse entries displayed.

The following information is displayed:

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

Threats by Files - level 3

The following options are available:

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

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

The following information is displayed:

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

Destination	Displays the destination IP address. Click the column header to sort the table by this column.
Rating	Displays the file rating. Click the column header to sort the table by this column.
Total Jobs	The number of jobs displayed and the total number of jobs.

Threats by Files - level 4

For more about information in the *View Details* pages for malicious and suspicious files, see File Statistics on page 222

To create a snapshot report for all threats by files:

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

The maximum number of events you can export to a PDF report is 5000. The maximum number of events you can export to a CSV report is 150000. Jobs over that limit are not included in the report.

Threats by Devices

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

Threats by Devices - level 1

The following options are available:

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

Search	Show or hide the search filter field.
Refresh	Click the *Refresh* icon to refresh the entries displayed after applying search filters.
Add Search Filter	Click the *Search Filter* field to add search filters. Click the *Cancel* icon beside the search filter to remove the specific filter. Click the *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. You can input a partial value to search all records that contain it.
View Jobs	Click the *View Jobs* icon to drill down the entry.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

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

Threats by Devices - level 2

The following information is displayed:

Search	Show or hide the search filter field.
Export Data	Click the *Export Data* button to create a PDF snapshot report. You can wait until the report is ready to view, or view the report in later in *Log & Report > Report Center* page.
Add Search Filter	Click the search filter field to add search filters. Click the cancel icon to the left of the search filter to remove the specific filter. Search filters can be used to filter the information displayed in the GUI.

Threat Timeline Chart	Displays the number of threats and types of threats which occurred to the threat target during the peroid of time. Hover over the dots in the chart to view more detailed threat information.
Back	Click the *Back* button to return to the main landing page.
Summary of	Displays a summary of the device type selected.
Details	Detailed information includes device name, selected time period, and total number of malicious and suspicious files.
Malicious Files	Malicious file information including malware name, destination IP address, and number of detection times. Click the *View Details* icon or double-click the row to drill down the entry. Click the malware name to view the related FortiGuard Encyclopedia page.
Suspicious Files	Suspicious file information including file name, file type, risk level, destination IP address, and number of detection times. Click the *View Details* icon or double-click the row to drill down the entry.

Threats by Devices - level 3

The following options are available:

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

The following information is displayed:

Malicious Files	Displays the date and time that the file was detected, malware name, source IP address, and destination IP address. Click the malware name to view the related FortiGuard Encyclopedia page.
Suspicious Files	Displays the date and time that the file was detected, file type, rating, source IP address, destination IP address, and number of detection times, if available.
Total Jobs	The number of jobs displayed and the total number of jobs.

Threats by Devices - level 4

For more information about the malicious and suspicious files in the *View Details* pages, see Job Details page reference on page 235.

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

To create a snapshot report for all threats by devices:

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

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

Security Fabric

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

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

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

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

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

Device

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

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

Use the *Security Fabric* > *Device* page to view, edit, and authorize devices.

Fortinet Ex. 2003 - Page 50 of 245

Devices such as FortiGate can query a file's verdict and retrieve detailed information from FortiSandbox. FortiGate can also download malware and URL packages from FortiSandbox as complementary AV signatures and web filtering blocklists. These packages contain detected malware signatures and their downloading URLs.

The default file size scanned and forwarded by FortiGate is 10MB and the maximum size depends on the FortiGate memory size. To change the file size on the FortiGate side, use the following CLI commands:

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

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

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

In *Security Fabric* > *Device*, the following options are available:

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

This page displays the following:

Device Name	Name of the device and the VDOM or protected email domain that send files to FortiSandbox. For a device, it has the format of: *Device Name*. For a VDOM, it has the format of: *Device Name: VDOM Name*. For a FortiMail protected domain, it has the format: *Device Name : Domain Name*.
Serial	The FortiGate, FortiWeb, FortiClient, FortiClient EMS, or FortiMail serial number.
Malicious, High, Medium, Low	The number of malicious, high risk, medium risk, or low risk files submitted by the device to FortiSandbox in the last seven days. FortiClient EMS displays the number of files submitted to FortiSandbox by FortiClient endpoints that are managed by EMS.
Clean	Number of clean files submitted by the device to FortiSandbox in the last seven days. FortiClient EMS displays the number of clean files submitted to FortiSandbox by FortiClient endpoints that are managed by EMS.
Others	Number of other files submitted by the device to FortiSandbox in the last seven days. FortiClient EMS displays the number of other rating files submitted to FortiSandbox by FortiClient endpoints that are managed by EMS.
Mal Pkg	Malware package version currently on the device.
URL Pkg	URL package versions currently on the device.
Auth	Shows if the device or VDOM/Protected Domain is authorized to submit files. Only authorized device or VDOM/Protected Domain can submit files to FortiSandbox.

Limit	Shows if this device has a submission limit.
Status	Status of the device. An icon shows that the device is up or connected, down, or disconnected. If a device, its VDOM, or protected domain does not contact FortiSandbox for more than 15 minutes, the status changes to disconnected.
Delete	Click to delete the device, VDOM, or protect domain. When you delete a device, all its VDOMs and protected domains are also deleted. If the device is FortiClient EMS, its managed FortiClient endpoints are kept. If the device connects to FortiSandbox again, it appears as a new device.

FortiSandbox uses a Fortinet proprietary traffic protocol (based on OFTP) to communicate with connected Security Fabric devices via TCP port 514. The traffic data is encrypted over TLS.

Supported Devices

FortiSandbox supports the following devices:

FortiGate	FortiSandbox can perform additional analysis on files that have been AV scanned by FortiGate. You can configure FortiGate to send all files or only suspicious files passing through the AV scan. FortiGate can retrieve scan results and details from FortiSandbox, and also receive antivirus and web filtering signatures to supplement the current signature database. When FortiGate learns from FortiSandbox that a terminal is infected, the administrator can push instruction for self-quarantine on a registered FortiClient host.
FortiMail	You can configure FortiMail to send suspicious, high risk files and suspicious attachments to FortiSandbox. FortiSandbox can perform additional analysis on files that have been scanned by your FortiMail email gateway. Suspicious email attachments include: • Suspicious files detected by heuristic scan of the AV engine. • Executable files and executable files embedded in archive files. • Type 6 hashes (binary hashes) of spam email detected by FortiGuard AntiSpam service. FortiMail can send suspicious URLs in the email body to FortiSandbox for URL scans and then block suspicious emails based on the scan result.
FortiWeb	You can use a file upload restriction policy to submit uploaded files to FortiSandbox for evaluation. If FortiSandbox determines that the file is malicious, FortiWeb performs the following tasks: • Generate an attack log message that contains the result, for example, messages with the Alert action. • For 10 minutes after it receives the FortiSandbox results, take the action specified by the file upload restriction policy. During this time, it does not re-submit the file to FortiSandbox, for example, messages with the Alert_Deny action.

FortiClient EMS	You can configure a FortiSandbox IP address in an endpoint profile. FortiClient EMS attempts to submit an authorization request to FortiSandbox. FortiSandbox administrators can authorize it and set limitations about submission speed. Subsequently, all FortiClient endpoints managed by FortiClient EMS are considered authorized by the same FortiSandbox and follow the submission speed limit.
FortiClient	FortiSandbox can accept files from FortiClient to perform additional analysis while FortiClient holds the files until the scan results are received. FortiClient can also receive additional antivirus signatures from FortiSandbox, generated from scan results, to supplement current signatures.

FortiGate devices

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

On FortiSandbox, go to *Security Fabric* > *Device* to see the FortiGate devices and VDOMs.

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

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

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

To edit FortiGate settings in FortiSandbox:

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

Device Status	
Serial Number	Device serial number.
Hostname	FortiGate host name.
IP	IP address of the FortiGate.
Status	Status of the device.
Last Modified	Date and time the FortiGate settings were last changed.
Last Seen	Date and time the FortiGate last connected to FortiSandbox.
Permissions & Policy	

Authorized	Enable to authorize the FortiGate device. If disabled, files sent from FortiGate are dropped.
New VDOMs/Domains Inherit Authorization	Enable to have new VDOMs inherit the authorization setting configured at the device level.
Email Settings	
Administrator Email	Email address in *Notifier email* in FortiGate at *Security Fabric* > *Settings* > *Sandbox Inspection*.
Send Notifications	Enable to send notifications. When enabled, you receive email notifications when a file from your environment is detected as potential malware. The email contains a link to the scan job details page. To receive notification emails, configure a mail server in *System* > *Mail Server* and enable *Send a notification email to the Device/Domain/VDOM email list when Files/URLs with selected rating are detected*. Otherwise, a warning icon displays.
Send PDF Reports	Enable to send PDF reports of job details. To receive reports and define report generation frequency, configure a mail server in *System* > *Mail Server* and enable *Send scheduled PDF report to Device/Domain/VDOM email address*. Otherwise, a warning icon displays.
Inline Block Policy	Enable to check for a trusted verdict in FortiGate. • If Yes, the verdict is returned and the file is dropped and a log is created. • If No, the file is added to the job queue. Select the risk level to be blocked: *Malicious*, *High Risk*, *Medium Risk* or *Low Risk*.

To edit VDOM settings:

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

Device Status	
Domain/VDOM	Device VDOM name.
Serial Number	Device serial number.
Hostname	VDOM name in the format of `Device-Name:VDOM-name`.
IP	IP address of the FortiGate.
Status	Status of the device.
Files Transmitted	Number of files and URLs transmitted to FortiSandbox in the last seven days.
Last Modified	Date and time the authorization status was changed.
Last Seen	Date and time the FortiGate VDOM last connected to FortiSandbox.
Permissions & Policy	

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

Inline Block Policy

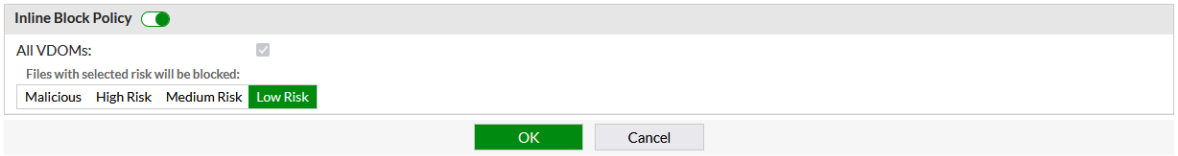
The *Inline Block Policy* improves the scan performance by checking for a trusted verdict in FortiGates running FOS v7.2 and higher.

- If a trusted verdict is found, the verdict is returned, the file is released, and a log is created.
- If a trusted verdict is not found, the file is added to the job queue and action is taken based on the policy configuration.

For information about Inline Block, see Understanding the Inline Block feature in the *Best Practices and Troubleshooting Guide*.

To enable Inline Block Policy:

1. Go to *Security Fabric > Device* and select a FortiGate device.
2. Enable *Inline Block Policy*.



3. Under *Files with selected risk will be blocked*, select the risk level (*Malicious*, *High Risk*, *Medium Risk* or *Low Risk*.). You can select multiple risk levels.
4. Click *OK*.

FortiSandbox must be reachable via port 4443.

To automatically enable Inline Block policy on all FortiGates:

```
device-authorization -I
```

The FortiGate needs to be authorized manually in the *Security Fabric > Device* page before FortiSandbox can accept files from it. FortiGate can only connect to FortiSandbox by an Admin or API port for Inline Blocking.

FortiMail Devices

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

If FortiMail sends protected domain information, the domain names and jobs counts from them are listed. For each protected domain, you can set a submission limitation. If protected domain information is not available, such as files from older versions of FortiMail or outgoing emails, jobs from them are grouped in the Unprotected domain name.

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

To edit FortiMail Settings in FortiSandbox:

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

Device Status	
Serial Number	Device serial number.
Hostname	FortiMail host name.
IP	IP address of the FortiMail.
Status	Status of the device.
Last Modified	Date and time the FortiMail settings were last changed.
Last Seen	Date and time the FortiMail last connected to FortiSandbox.
Permissions & Policy	
Authorized	Enable to authorize the FortiMail device. If disabled, files sent from FortiMail are dropped.
New VDOMs/Domains Inherit Authorization	Enable to have new protected domains inherit the authorization setting configured at the device level.
Email Settings	
Administrator Email	Email address in *Notifier email* in FortiMail.

Send Notifications	Enable to send notifications. When enabled, you receive email notifications when a file inside an email is detected as potential malware. The email contains a link to the scan job details page. To receive notification emails, configure a mail server in *System* > *Mail Server* and enable *Send a notification email to the Device/Domain/Vdom email list when Files/URLs with selected rating are detected*. Otherwise, a warning icon is displays.
Send PDF Reports	Enable to send PDF reports of job detail. To receive reports and define report generation frequency, configure a mail server in *System* > *Mail Server* and enable *Send scheduled PDF report about an individual VDOM/Domain to its email address*. Otherwise, a warning icon is displays.

To edit Domain settings:

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

Device Status	
Domain/VDOM FQDN	Protected domain name.
Hostname	Domain/VDOM name in the format of `FortiMail Device Name: Domain name`.
IP	IP address of the FortiMail.
Status	Status of the device.
Files/URLs Transmitted	Number of files and URLs sent to the domain in the last seven days.
Last Modified	Date and time the authorization status was changed.
Last Seen	Date and time last file/URL was sent to this domain.
Permissions & Policy	
Authorized	Enable to authorize the FortiMail domain.
Submission Limitation	Limit the protected domain submission speed. Select *Unlimited* or specify the number of submissions per *Hour* or *Day*. When the limit is reached, FortiSandbox rejects files and URLs sent to this domain.
Email Settings	
Email	Enter the administrator email addresses for the domain, separated by commas.
Send Notifications	Enable to send notifications when viruses or malware to this domain is detected. To receive notification emails, configure a mail server in *System* > *Mail Server* and enable *Send a notification email to the Device/Domain/VDOM email list when Files/URLs with selected rating are detected*. Otherwise, a warning icon is displays.
Send PDF Reports	Enable to send PDF reports of jobs.

	To receive reports and define report generation frequency, configure a mail server in *System* > *Mail Server* and enable *Send scheduled PDF report about an individual VDOM/Domain to its email address*. Otherwise, a warning icon is displays.
Send Reach Limit Alert Email	Enable to send an alert email to the domain email address when *Submission Limitation* is reached.

Upload suspicious attachments to FortiSandbox

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

Device and VDOM/Domain level notifications

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

Device and VDOM/Domain level PDF reports

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

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

FortiWeb Devices

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

FortiClient EMS Devices

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

To edit EMS settings in FortiSandbox:

1. On your FortiSandbox device, go to *Security Fabric* > *Device*.
2. Click the device name to open the *Edit Device Settings* page.

3. Edit the following and then click *OK*.

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

FortiClient

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

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

To view connected FortiClient endpoints in FortiSandbox, go to *Security Fabric* > *FortiClient*.

The following options are available:

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

This page displays the following:

FCT Serial	The FortiClient serial number.
Hostname	FortiClient host name.
User	Current user logged into the FortiClient host, if available.
IP	Host IP Address.

Malicious, High, Medium, Low	The number of malicious, high risk, medium risk, or low risk files submitted by FortiClient to FortiSandbox in the last seven days. Malicious files are not executed in the FortiSandbox VM module as the antivirus scanner has already determined the file rating.
Clean	Number of clean files submitted by the device to FortiSandbox in the last seven days.
Others	Number of other files submitted by the device to FortiSandbox in the last seven days.
Mal Pkg	Malware package version currently on the device.
Auth	If the FortiClient is authorized, you can click the FortiClient serial number and modify its authorization status.
Limit	Shows if this device has a submission limit.
Status	Status of the FortiClient host. An icon shows that the device is connected (up) or down.
Delete	Click to delete the FortiClient. If the device connects to FortiSandbox again, it appears as a new device.

To edit FortiClient settings in FortiSandbox:

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

FortiClient Status	
Serial Number	Device serial number.
Hostname	FortiClient host name.
IP	IP address of the FortiClient.
Status	Status of the device.
Files Transmitted	Number of files transmitted to FortiSandbox in the last seven days.
Last Seen	Date and time that FortiClient last connected to FortiSandbox.
Permissions & Policy	
Authorized	Enable to authorize the device.
Submission Limitation	Limit the submission speed. Select *Unlimited* or specify the number of submissions per *Hour* or *Day*. When the limit is reached, FortiSandbox sends a signal to FortiClient to stop file submission to save resources on both devices.

Adapter

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

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

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

You can use the MTA adapter to inspect and quarantine suspicious emails. For more information, see MTA adapter on page 68 and the FortiSandbox user guide in the AWS marketplace.

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

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

The following options are available:

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

This page displays the following information:

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

To create an adapter:

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

Vendor Name	Select *Carbon Blaclk/Bit9*.
Adapter Name	Enter the adapter name.

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

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

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

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

ICAP adapter

FortiSandbox can work as an ICAP server with proxy secure gateway devices (ProxySG) that supports ICAP. The ProxySG will serve as an ICAP client to FortiSandbox. The ICAP client waits (i.e. holds the URL) for the verdict from the FortiSandbox.

To configure an ICAP adapter, first you will use the CLI to configure the client, and then you will use FortiSandbox GUI to configure the server.

Request and response

The ICAP client only supports POST, GET and PUT methods.

If no verdict is available, the URL or files will be put into the *Job Queue* for a scan. URL scan flow will apply.

When an ICAP client sends a HTTP request to FortiSandbox, FortiSandbox extracts the URL and checks if a verdict is available.

Status Code	Meaning
200	• Verdict is not a *user selected blocking rating* or is not available.
403	• Verdict is *user selected blocking rating*. • If *Realtime Web Filtering* is enabled, the URL will be scanned in real time by *Web Filter*.

When an ICAP client sends a HTTP response to FortiSandbox, FortiSandbox extracts the file from it and checks if verdicts are available.

Status Code	Meaning
200	• Verdict is not a *user selected blocking rating* or is not available.
403	• Verdict is *user selected blocking rating*. • If *Realtime Scan* is enabled, the file will be scanned by the defined scan type(s) (*AV Scan*, *Static Scan*, or *Cloud Query*).

When ICAP client sends a preview request:

Status Code	Meaning
204	• Not supported.

To configure ICAP client:

The following configuration is for a SQUID 4.x to reach the FortiSandbox. You should add this configuration to the end of the `squid.conf` file.

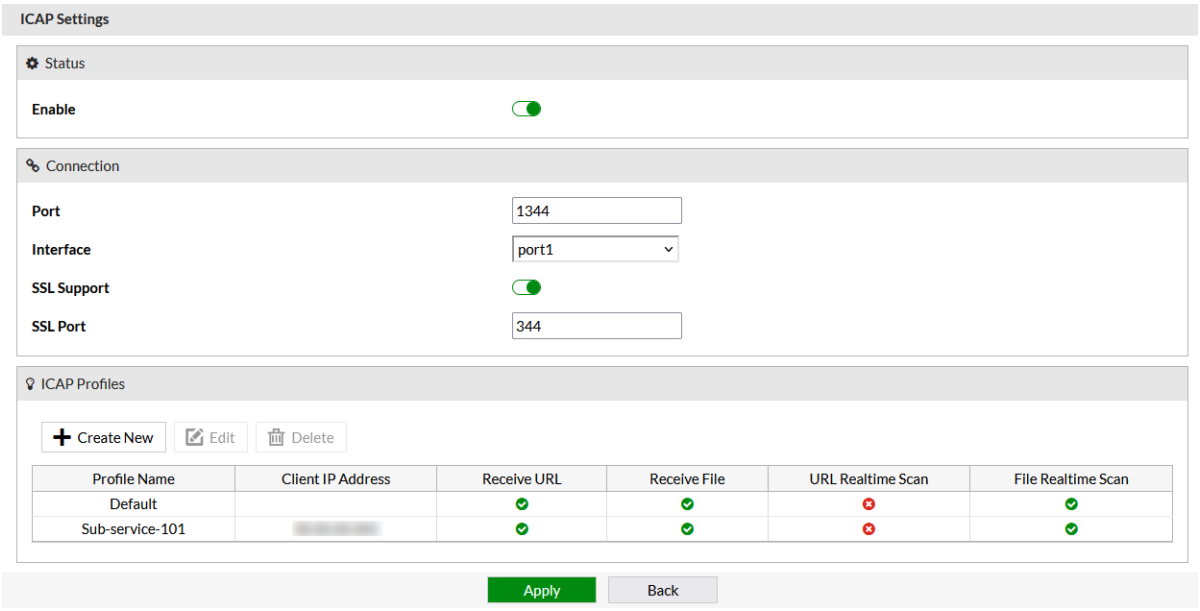
```
cache deny all
icap_enable on
icap_send_client_ip on
icap_send_client_username on
icap_client_username_header X-Authenticated-User
icap_preview_enable off
icap_persistent_connections off
icap_service svcBlocker1 reqmod_precache icap://fortisandbox_ip:port_number/reqmod bypass=0
     ipv6=off
adaptation_access 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
```

To configure FortiSandbox as an ICAP server:

1. Go to *Security Fabric* > *Adapter*.
2. Select the *ICAP* adapter and click *Edit*.
3. *Enable* the ICAP adapter.

4. Under *Connection*, configure the following settings, and then click *Apply*.

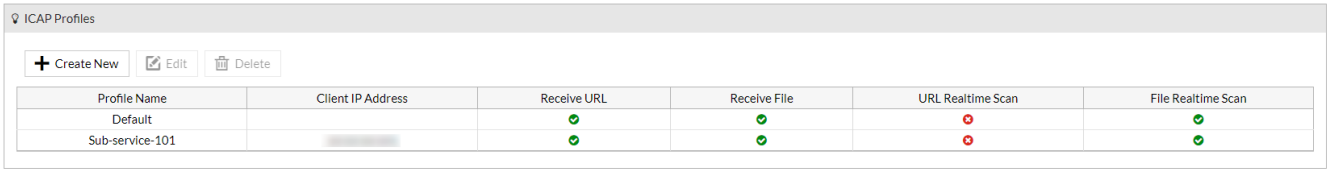
Port	The port the ICAP server listens on. Default is 1344.
Interface	The interface the ICAP server listens on. For a cluster, we recommend specifying the interface corresponding to the cluster IP interface (for example, *port1 HA*).
SSL support	*Enable* to allow SSL traffic.
SSL port	The port the ICAP server listens on for SSL traffic. Default is 11344.



ICAP profiles

FortiSandbox supports multiple ICAP profiles for multiple proxy servers (ICAP clients) with different configuration requirements.

- You can edit but not delete the *Default* profile that is built-in to FortiSandbox.
- Configuring a new profile will override the settings defined in the *Default* profile for matched proxy server by IP.
- If a client does not match a user-defined profile the *Default* profile is applied.

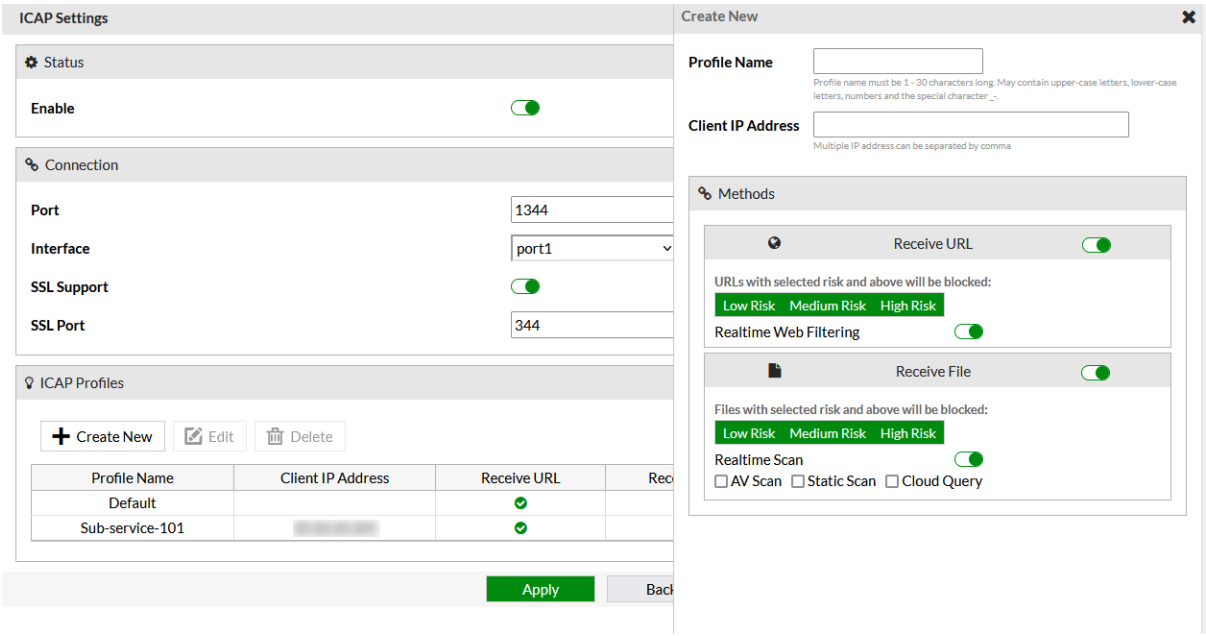


To create an ICAP profile:

1. Go to *Security Fabric* > *Adapter*.
2. Select the *ICAP* adapter and click *Edit*.
3. Under *ICAP Profiles*, click *Create New*. The *Create New* pane opens.

4. Configure the profile and click *Apply*.

Profile Name	Enter a name for the profile.
Client IP Address	Enter the client IP address. Separate multiple IPs with a comma.
Methods	
Receive URL	*Enable* to allow the ICAP server to receive URLs, and then select the risk level to be blocked. Options are *Low Risk*, *Medium Risk*, and *High Risk*.
Realtime Web Filtering	Enable to allow real-time URL web filtering.
Receive File	*Enable* to allow the ICAP server to receive files, and then select the risk level to be blocked. Options are *Low Risk*, *Medium Risk*, and *High Risk*.
Realtime Scan	Enable to allow real-time file scanning, including *AV Scan*, *Static Scan* and *Cloud Query*. You can enable multiple options.



5. Click *Apply* on the *ICAP Settings* page.

BCC Adapter

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

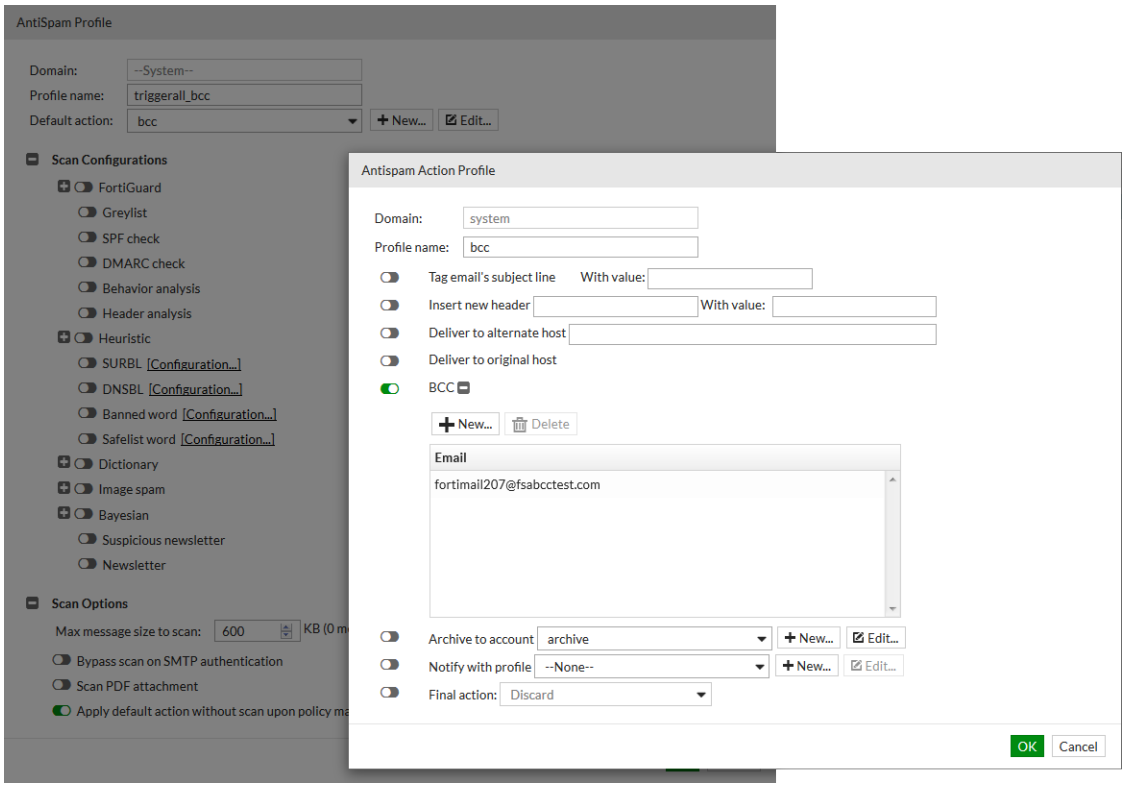
This feature is for information only, like sniffer mode. It will not block any email.

To configure the FortiSandbox:

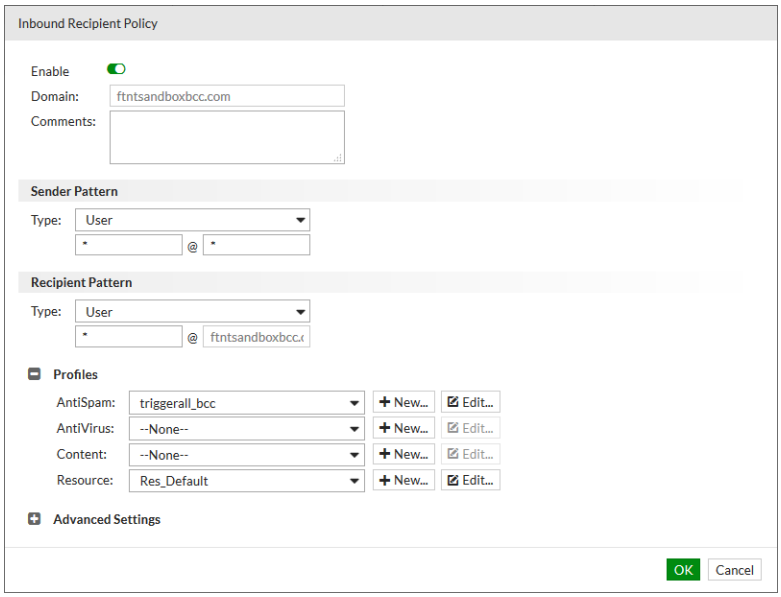
1. Enable the BCC adapter:
   a. Go to *Security Fabric* > *Adapter* in the navigation tree.
   b. Select *BCC* and click *Edit* in the toolbar. The BCC adapter is disabled by default.
   c. Enable the BCC adapter.
   d. Enable *Parse URL* to allow the FortiSandbox to extract the first three URLs in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

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

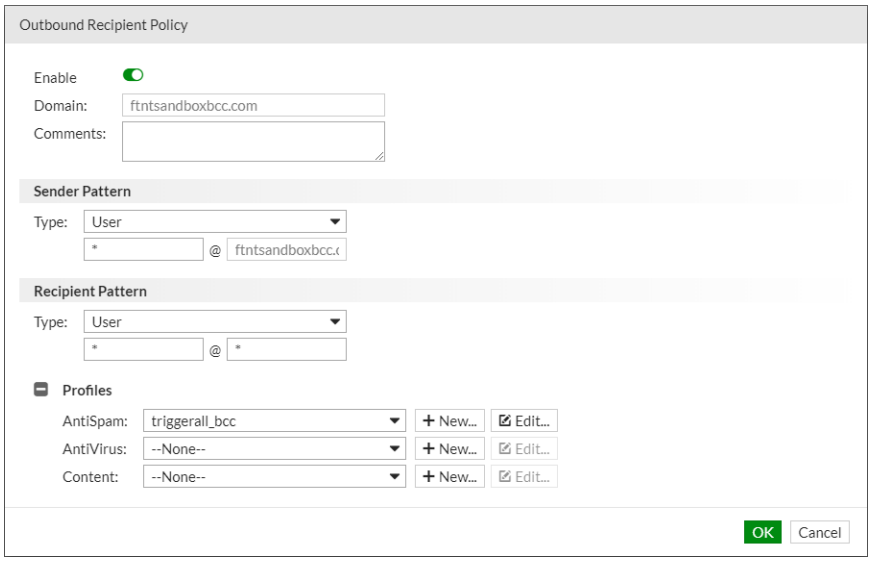
1. Go to *Profile* > *AntiSpam* and create a new AntiSpam profile:
   a. Enable *Apply default action without scan upon policy match*.
   b. Configure *BCC* as the default action.
   c. Edit the default action: enable *BCC*, and add a BCC address, such as *fortimail207@fsabcctest.com*.



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

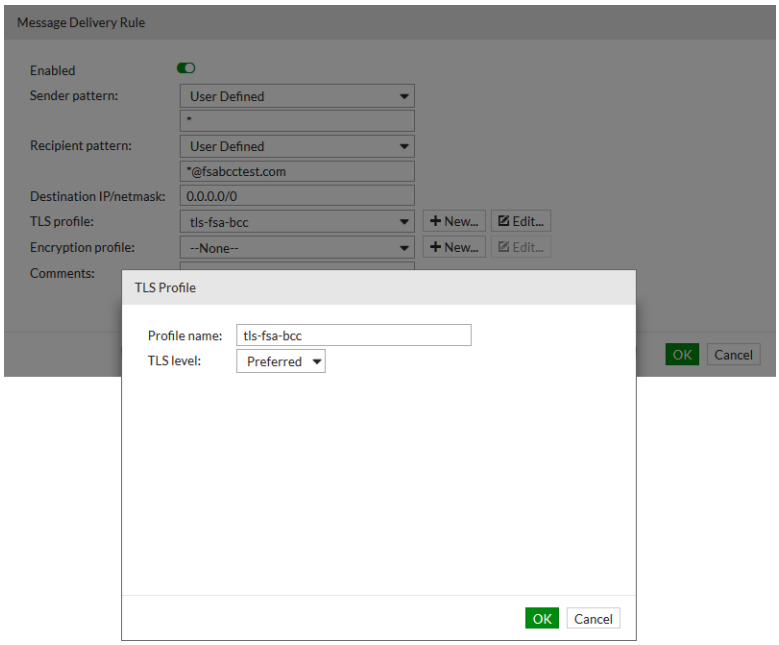


   c. Add a new outbound policy, select the domain for forwarding emails to the FortiSandbox, and apply the new AntiSpam profile.



3. Go to *Policy* > *Access Control*:
   a. On the *Delivery* tab, add a TLS policy with a recipient pattern matching the previously added BCC address (in this example: **@fsabcctest.com*).

b. Set *TLS Profile* as *none* or *Preferred*.



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

MTA adapter

The *Mail-Transfer-Agent* (MTA) adapter feature allows email servers like Sendmail to relay emails to FortiSandbox via SMTP protocol. The adapter requires a subscription license. The license is automatically downloaded through FortiGuard and limits the per-mailbox seat count.

The FortiSandbox extracts files and URLs on the email being relayed. All email addresses in the To, CC, and BCC fields are counted and tracked for those matching the configured email domains. If the seat count limit is exceeded by 10%, the system will log a warning system event. An email is relayed and not scanned if it meets the following criteria:

- There is no valid MTA subscription license.
- The FortiSandbox disk usage exceeds the defined percentage.

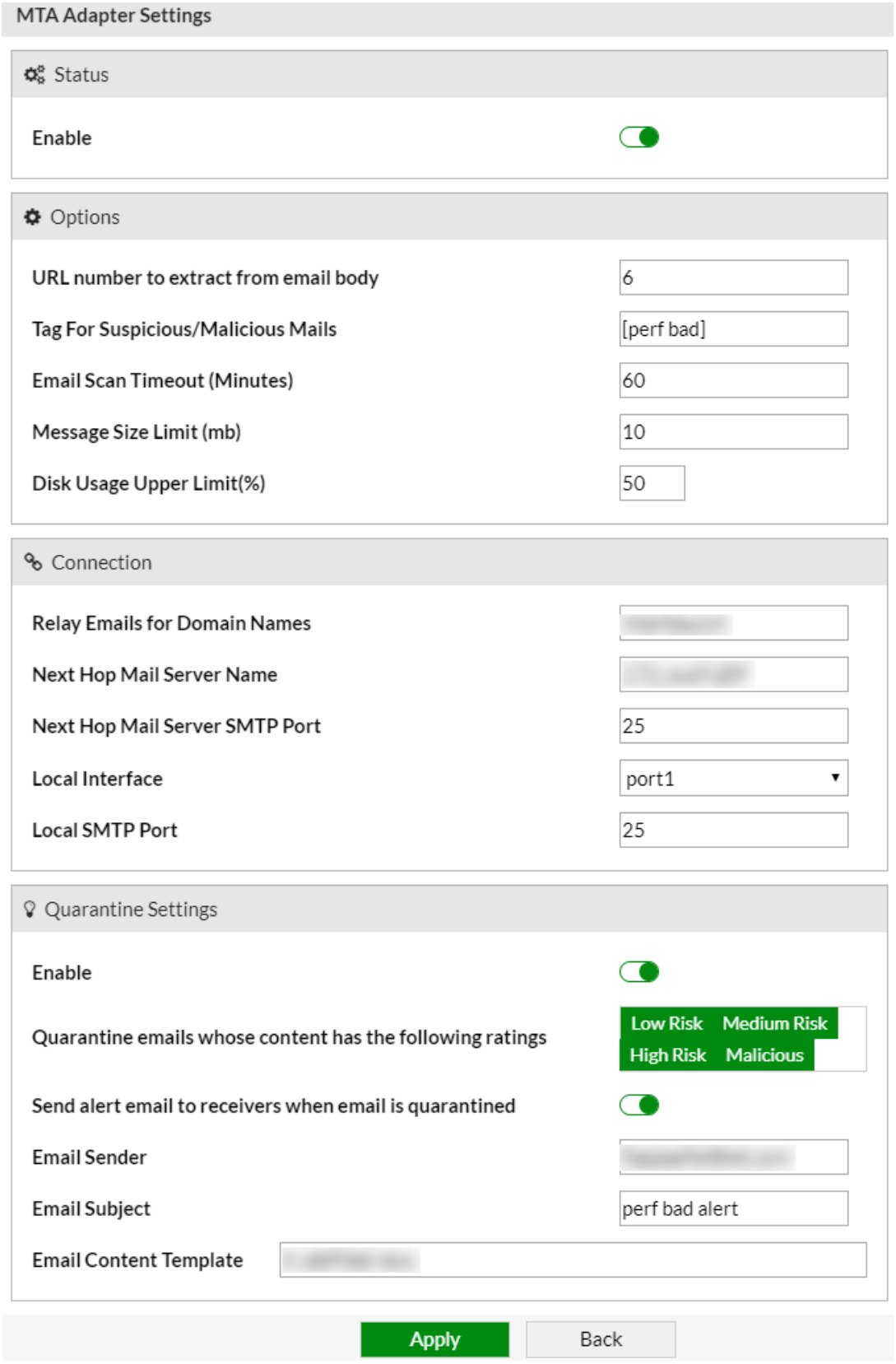
If quarantine is disabled and an email scan result is suspicious or malicious, a tag will be prepended to the original email subject line and is relayed to the recipient email address. The tag is configurable on the MTA configuration page. Otherwise, the email is relayed without change. You cannot delete the email address.

If quarantine is enabled and an email scan result is suspicious or malicious and matches the defined quarantine rating level, the email is quarantined and the recipient will not receive the email. If you have enabled *Send alert email to receivers when email is quarantined*, the recipient will receive an alert email stating that an email is quarantined. The quarantined emails will be saved in FortiSandbox until you release or delete them (see, Processing quarantined emails).

To configure the MTA adapter:

1. Go to *Security Fabric* > *Adapter*.
2. Select the *MTA* adapter and click *Edit*.

3. Enable the adapter.



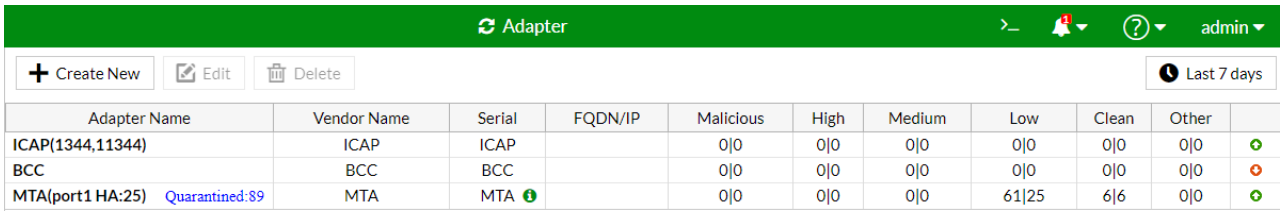
4. Configure the following settings and then click *Apply*.

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

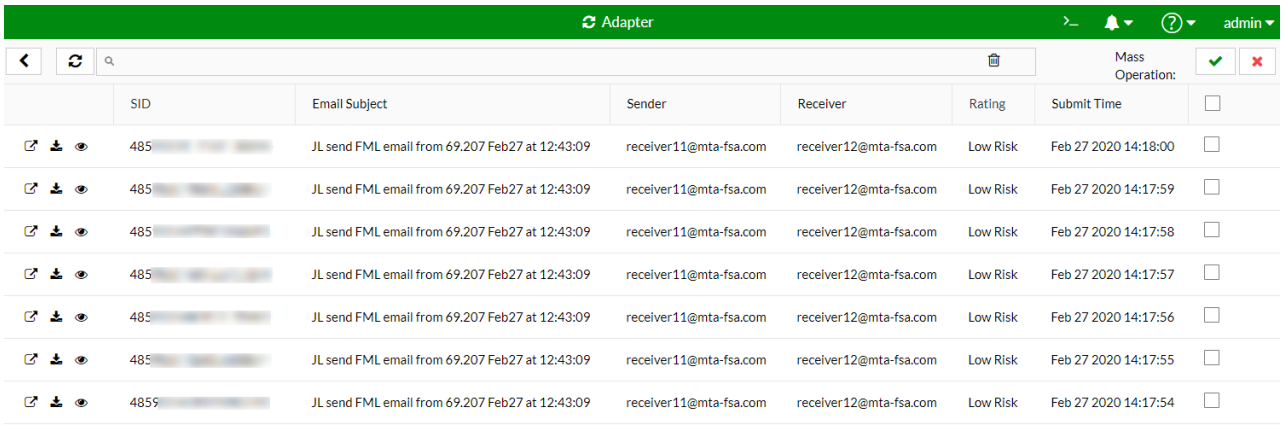
Processing quarantined emails

To release or delete quarantined emails:

1. Go to *Security Fabric* > *Adapter*.
   If there are quarantined emails, the number of quarantined emails is displayed beside the MTA adapter name.



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



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

Using MTA in HA-Cluster

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

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

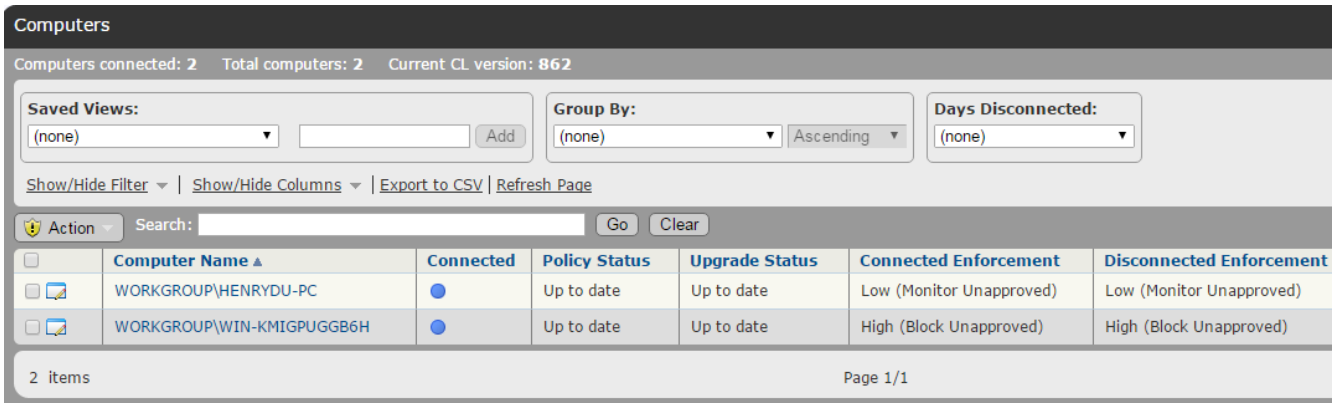
In a cluster, configure the *Local Interface* to the interface of the cluster IP address so that the secondary can take over the configuration in a failover.

- To view jobs in a cluster, go to *HA-Cluster* > *Job Summary*.
- To view logs in the primary node, go to *Log & Report* > *Events* > *Job Events*.
- To view logs in a worker node, go to *Log & Report* > *Events* > *All Events*.

Carbon Black Bit9 Server

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

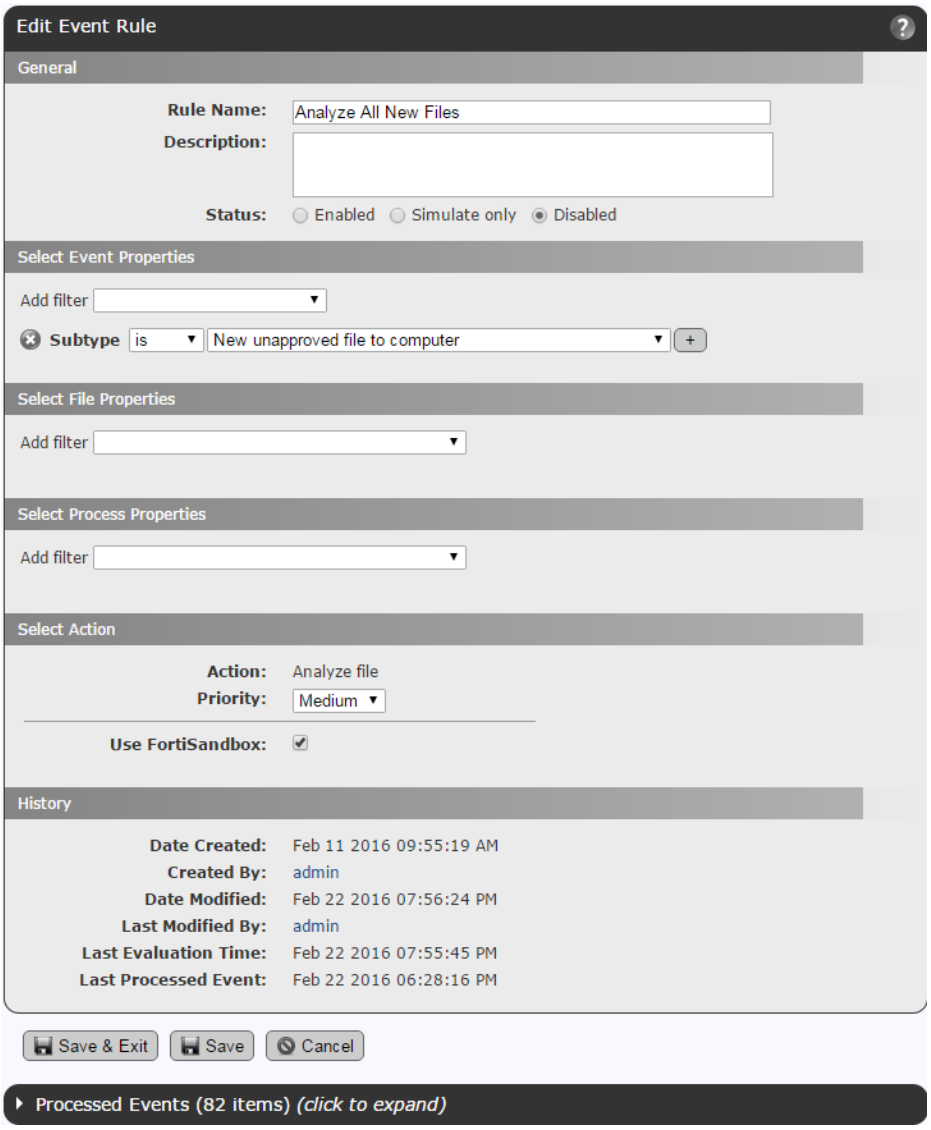
Submitting selected files to FortiSandbox



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.

Network Share

FortiSandbox can scan files stored on a network share and optionally quarantine any malicious files. Go to *Security Fabric* > *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.

Network Share is only available in the Primary node of an HA cluster.

To improve the scan performance, delete any empty sub-folders in the Network Share.

The following options are available:

Create New	Create a new network share.
Edit	Edit the selected entry.
Clone	Clone the selected entry. Only the *Network Share Name* is different. All other settings are the same as the original.
Delete	Delete the selected entry.
Scan Now	Scan the selected entry.
Scan Details	View the selected entry's scheduled scan entries.
Test Connection	Test the selected entry's connection. The result is displayed in the banner at the bottom right corner.

The following information is displayed:

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

To create a new network share:

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

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

Mount Type	Select the mount type. The following options are available: • CIFS (SMB v1.0, v2.0, v2.1, v3.0). • NFSv2, NFSv3, NFSv4. • AWS S3, AWS S3 BJ, AWS S3 NX. SeeAWS S3 Settings on page 100. • Azure File Share. See Azure File System on page 101. • Azure Blob Storage. See Azure Blob Storage on page 101. For domain-based DFS namespace, ensure the domain name can be resolved with the system Primary DNS server.
Network Share Name	Network share name.
Server Name/IP	Server FQDN or IP address.
Share Path	File share path in the format `/path1/path2`.
Scan Files Of Specified Pattern	Include or exclude files which match a file name pattern.
File Name Pattern	File name pattern.
Username, Password, Confirm Password	Username and password. For domain users, use the format `domain_name\user_name`.
Scan Job Priority	When multiple network share scans run at the same time, higher priority scans get more scan power.
Keep A Copy Of Original File On FortiSandbox	Keep a copy of the original file on FortiSandbox.
Skip Sandboxing for the same unchanged files	To improve scan speed, you can skip sandboxing scan on existing files (if applicable) and only do sandboxing scan on new files. Existing files are only scanned by AntiVirus engine and Community Cloud query.
Enable Quarantine of Malicious Files	Quarantine files with a Malicious rating in the selected location. Quarantined files are put in a folder with the name of the Job ID and each file is renamed with the Job ID for that file and a meta file with more information.
Enable Quarantine of Suspicious - High Risk files	Quarantine suspicious files with a High Risk rating in the selected location. Quarantined files are put in a folder with the name of the Job ID and each file is renamed with the Job ID for that file and a meta file with more information.
Enable Quarantine of Suspicious - Medium Risk files	Quarantine suspicious files with a Medium Risk rating in the selected location. Quarantined files are put in a folder with the name of the Job ID and each file is renamed with the Job ID for that file and a meta file with more information.
Enable Quarantine of Suspicious - Low Risk files	Quarantine suspicious files with a Low Risk rating in the selected location. Quarantined files are put in a folder with the name of the Job ID and each file is renamed with the Job ID for that file and a meta file with more information.
Enable Quarantine of Other rating files	Quarantine suspicious files with a Other rating in the selected location. Quarantined files are put in a folder with the name of the Job ID and each file is renamed with the Job ID for that file and a meta file with more information.

Enable copying or moving clean files to a sanitized location	Copy or move files with a Clean rating to another location. By default, a new folder is created for each scheduled scan job in the sanitized location and all clean files are copied into it with the original folder structure. To save space, uncheck *Keep a complete copy of clean files for every scheduled scan* so that files of the same path have only one copy in the sanitized location.
Enable Scheduled Scan	Enable scheduled scan and specify the schedule type.
Description	Optional description for the network share entry.
Send notification email after each scan	Email a summary report for each network share scan to the specified users.

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

Conserve Mode:

FortiSandbox goes into Conserve Mode once it has copied 10,000 files to the local device.

In Conserve Mode, FortiSandbox stops copying files from the remote Network Share and continues processing the copied files until the *Pending* count is 5000 for a Standalone node or 5000 or more for a node in an HA Cluster.

A warning level system log entry alerts you of the event.

To run a network share scan immediately:

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

To test network share connectivity:

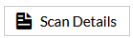
1. Go to *Security Fabric* > *Network Share*.
2. Select a share.
3. Click *Test Connection* to test connectivity with the network share.

Scan Details

The *Scan Details* page shows scheduled scans for the selected network share.

To view the Scan Details:

1. Go to *Security Fabric* > *Network Share* and select a network share.
2. In the toolbar, click *Scan Details*.



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.

To view the job details, click a numbered link and then click the *Job Detail* button. Please keep the following in mind:

- Job details are not displayed if the job information was deleted based on the settings in the *Scan Profile* > *General* page.
- Scan jobs are deleted when system triggers a reboot.

All the Netshare Scan records will be deleted when the Primary node in a HA-Cluster reboots. In Standalone Mode, an unfinished Netshare Scan will not resume after system boots up.

Quarantine

Create and edit quarantine locations in the Security Fabric. Quarantine supports SMB, NFS, AWS, and Azure mount types. To view the quarantine information, go to *Security Fabric* > *Quarantine* .

Quarantine is only available in the Primary node of an HA cluster

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	Test the selected entry's connection. The result is displayed in the banner at the bottom right corner.

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 *Security Fabric* > *Quarantine*.
2. Click the *Create New* button from the toolbar.

3. Configure the following options:

Enabled	Select to enable quarantine location.
Quarantine Name	Enter the quarantine name.
Mount Type	Select the mount type from the dropdown list. The following options are available: • CIFS (SMB v1.0, v2.0, v2.1 and v3.0) • NFSv2, NFSv3, NFSv4 • AWS S3, AWS S3 BJ, AWS S3 NX • Azure File Share • Azure Blob Storage
Server Name/IP	Enter the server fully qualified domain name (FQDN) or IP address.
Share Path	Enter the file share path. In the format `/path1/path2`.
Username	Enter a user name. For a domain user, use the format `domain_name\user_name`.
Password	Enter the password.
Confirm Password	Enter the password a second time for verification.
Keep Original File At Current Location	Select to keep the original file at the current location when a file is quarantined from a network share. By default, the original file is kept at its current location when being moved.
Description	Enter an optional description for the quarantine location entry.

4. Select *OK* to save the entry.

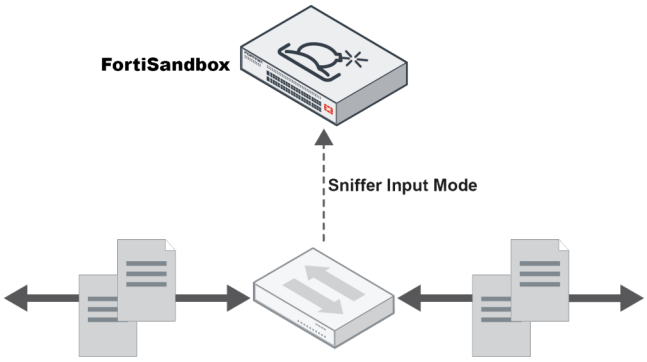
To edit a quarantine:

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

Sniffer

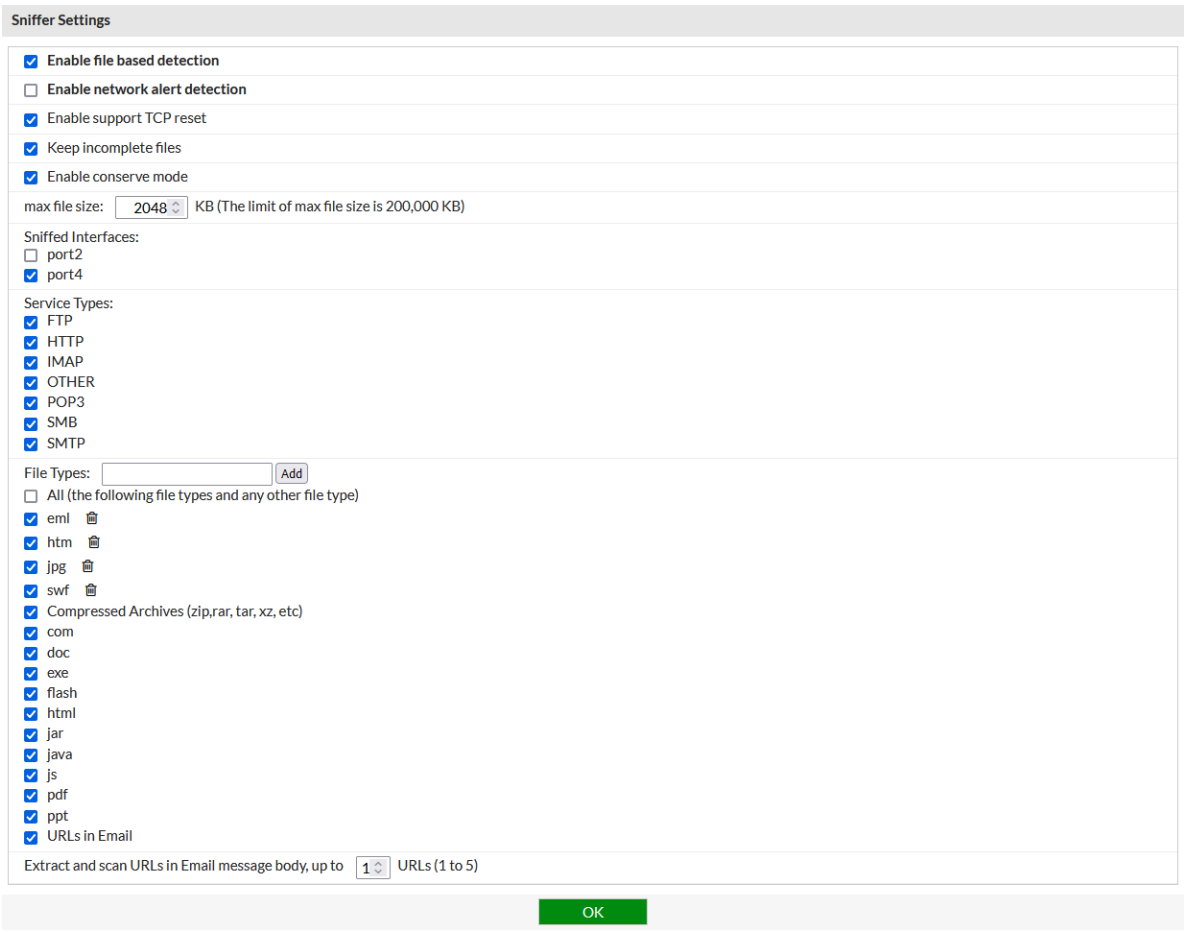


Sniffer mode relies on inputs from spanned switch ports. It is the most suitable infrastructure for adding protection capabilities to existing threat protection systems from various vendors.

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

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

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



Configure the following settings:

Enable file based detection	Select the checkbox to enable file based detection.
Enable network alert detection	Select the checkbox to enable network alerts detection. This feature detects sniffed live traffic for connections to botnet servers and intrusion attacks and visited suspicious web sites with Fortinet IPS and Web Filtering technologies. Alerts can be viewed in the *Network Alerts* page. For URL visits, certain categories can be treated as benign in *Scan Policy and Object* > *Web Category*. Enabling *Network Alert Detection* disables *TCP Reset*.
Enable support TCP reset	View Sniffer generated TCP RST packages from *Scan Policy and Object* > *TCP RST Package*. Only HTTP URL are supported. Enabling *TCP Reset* disables *Network Alert Detection*. Enable *Send client a warning message with comfort page when TCP is disconnected* to notify the user the URL is blocked and cannot be downloaded. Click the edit icon to customize the font size, background and font color with the HTML editor. Source code must contain "`%%URL%%`" to display the blocked URL.

Keep incomplete files	Keep files without completed TCP sessions. Select the checkbox to keep incomplete files. Sometimes incomplete files can be useful to detect known viruses.
Enable Conserve mode	When conserve mode is enabled, the sniffer might enter conserve mode if it is too busy, such as when there are too many jobs in the pending queue (250K), sniffed traffic exceeds optimal throughput, or HDD/RAM disk usage is too high. In conserve mode, the sniffer only extracts executable (.exe) and MS Office files. Optimal traffic throughput: • FSA-2000E: 4 Gbps • FSA-3000E: 8 Gbps • FSA-VM00: 1Gbps
Max file size	The maximum size of files captured by sniffer. Enter a value in the text box. The default value is 2048kB and the maximum file size is 200000kB. Files that exceed the maximum file size are not sent to FortiSandbox.
Sniffed Interfaces	Select the interface to monitor.
Service Types	Select the traffic protocol that the sniffer will work on. Options include: *FTP*, *HTTP*, *IMAP*, *POP3*, *SMB*, *OTHER* and *SMTP*. The *OTHER* service type is for raw TCP protocol traffic.
File Types	Select the file types to extract from traffic. When *All* is checked. all files in the traffic will be extracted. Users can also add extra file extensions by putting it in *File Types* field and clicking *Add* > *OK*. The user can delete it later by clicking the *Trash* can icon beside it and clicking *OK*. When *URLs in Email* type is selected, URLs embedded inside Email body will be extracted and scanned as WEBLink type. User can define the number of URLs to extract for each Email, from 1 to 5.

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

FortiNDR

FortiSandbox can use FortiNDR as one method to generate verdicts. If FortiNDR rates a file as clean, and all other methods gives that file a clean verdict, then FortiSandbox will not go into VM scan. If FortiNDR rates a file as malicious or high risk, then FortiSandbox will also rate it as malicious or high risk. For all other FortiNDR ratings, FortiSandbox follows the regular scan flow and give a final verdict after using all methods including VM scan.

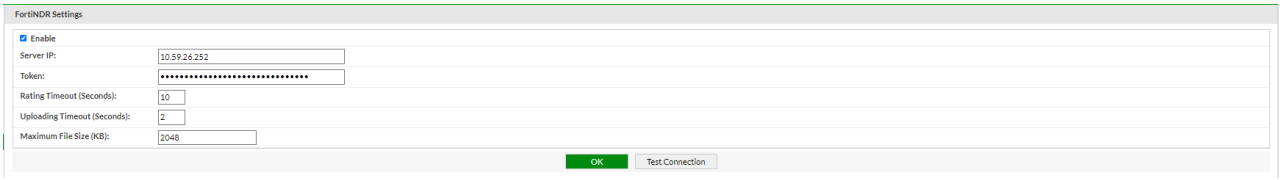
Prerequisites

- FortiNDR server is installed and licensed.
- FortiNDR is higher than v1.5.0 build 0104.
- You have the token from FortiNDR *System* > *Administrator* > *Edit* > *API Key*.

FortiNDR v1.5.0 -1.5.3 is named *FortiAI*. For more information, see the FortiAI product page in the Fortinet Document Library.

To configure FortiNDR as a verdict method:

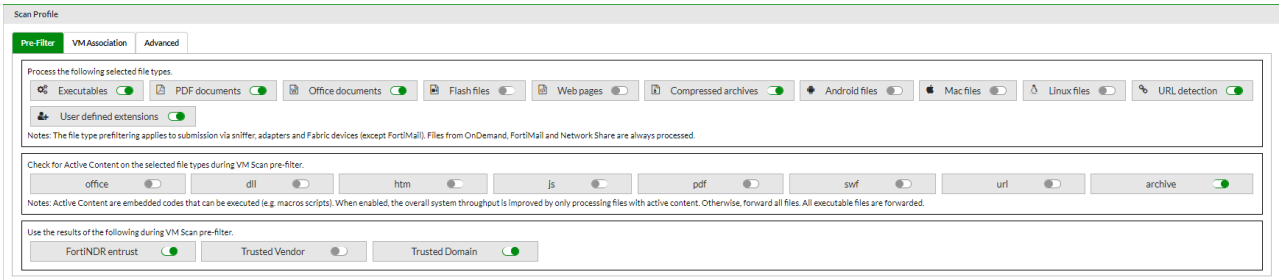
1. Go to *Security Fabric* > *FortiNDR*.
2. Click *Enable*.



3. Configure the following options.

Server IP	IP address of FortiNDR server.
Token	The token from FortiNDR *System* > *Administrator* > *Edit* > *API Key*.
Rating Timeout (Seconds)	The maximum time to wait for FortiNDR to give a verdict. If a file does not get a verdict from FortiNDR by this time, the file goes into normal scan flow.
Uploading Timeout (Seconds)	The maximum time to upload a file to FortiNDR. If a file does not upload to FortiNDR by this time, the file goes into normal scan flow.
Maximum File Size (KB)	The maximum file size to upload to FortiNDR. Oversize files are not sent to FortiNDR, they continue with regular scan flow.

4. Go to *Scan Policy and Object* > *Scan Profile* > *Pre-Filter*.
5. Enable *FortiNDR entrust* and click *Apply*.



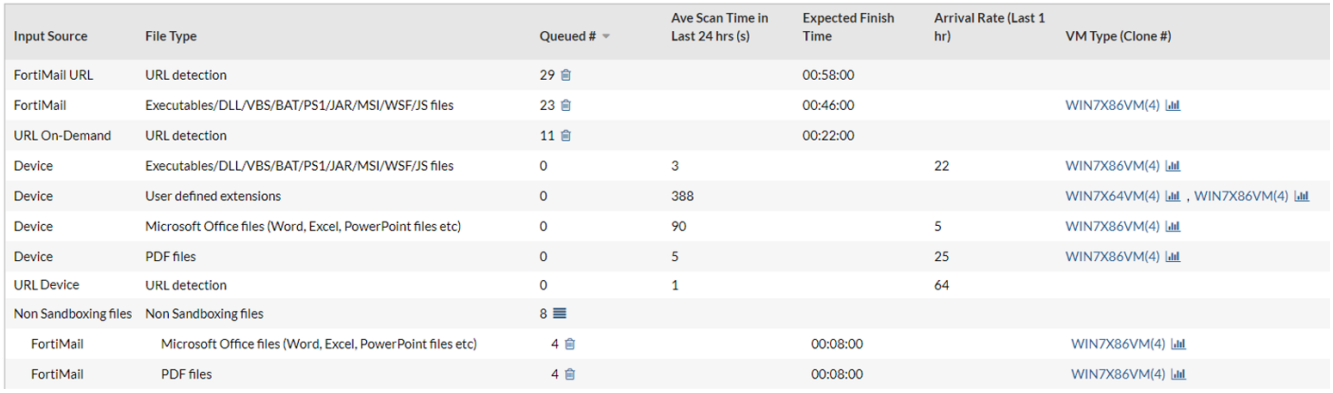
Scan Job

Job Queue

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

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

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



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

The following options are available:

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

The following information is displayed:

Input Source	The type of Input Source. Input source types can be the following values: • On-Demand • File RPC • Device • Sniffer • Adapter • Network Share • URL On-Demand • URL RPC • URL Device

	• URL Adapter
File Type	File types can be one of the following values: • Executables /DLL/VBS/BAT/PS1/JAR/MSI/WSF files • Microsoft Office files (Word, Excel, Powerpoint etc) • Adobe Flash files • Archive files (extensions: .7z, xz, .bz2, .gz, .tar, .zip, .Z, .kgb, .ace, etc.) • PDF files • Static Web files • Android files • MACOSX files • URL detection • User defined extensions • Job Queue Assignment Pending files (files received from input sources and not yet processed) • Non Sandboxed files (files that do not enter the Sandboxing scan step according to the current Scan Profile settings. If the Scan Profile settings are changed, they may enter the Sandboxing scan step eventually.)
Queued #	Current pending job number. A *Trash Can* appears beside the pending job number. Clicking on the *Trash Can* icon purges the job queue. Select the icon next to the *Non Sandboxing files* Input Source to expand the selection to view and purge non-sandboxing files separately.
Ave Scan Time in Last 24 hrs (s)	Average scan time of one file in the last 24 hours, in seconds.
Expected Finish Time	The expected time when the pending jobs will finish.
Arrival Rate (Last 1 hr)	Files put in the Job Queue in the last hour.
VM Type (Clone #)	The VM type with its clone number. A *Chart* icon appears beside the VM Type (Clone#). If you click on the *Chart* icon, the VM's usage chart appears. This chart shows a rough percentage of used clones of this VM type across time. If the usage percentage is consistently at a high level across time, the user should consider allocating more clone numbers to it.

VM Jobs

Go to *Scan Job* > *VM Jobs* to view files currently scanned inside the VM. The page displays the file name and progress. To view a screenshot of the running scan, click the VM *Screenshot* button and then the *PNG Link* button.

If the scan allows VM interaction, click the VM Interact icon to interact with the scan. To stop an interactive scan, click the trash icon.

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

File Job Search

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

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

The following options are available:

Refresh		Click the *Refresh* icon to refresh the entries displayed after applying search filters.
Search Field		Enter the detection time frame and click to add additional search filters for Device, File MD5, Filename, File SHA1, File SHA256, Job ID, Malware, Rating, Service, Source, User, Device, Infected OS, Rated by, Submit User, Submit Filename, Suspicious Type, or Scan Unit. When the search criteria is a *Filename*, click the = sign to toggle between the exact and pattern search.
Time Period		Select a time period to apply to the search.
Export to Report		Select to open the Report Generator dialog box. Select to generate a PDF or CSV report. You can wait until the report is ready to view, or navigate away and find the report later in *Log & Report* > *Report Center* page.
Customize		Click the *Customize* icon to customize the Job View settings page. For more information, see Job View Settings on page 189.
Action		
	View Details	Click the *View Details* icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
	Archived File	The icon displays that the file as an archived file.
	FortiGuard Advanced Static Scan	The icon displays that the file is rated by user's overridden verdict or FortiGuard advanced static scan.
	File Inside Archive	The icon displays that the file is a file extracted from an archive file.
	Rescan Job	The icon displays that the job is Malicious from an AV Rescan or a rescan of the Malicious file.
	Video	Click the *Video* button to play the video of the scan. Scan videos are available in On-Demand scans if the user has the privilege.
	Perform Rescan	Click the icon to rescan the entry. In the *Rescan Configuration* dialog box, you can skip *Static Scan*, *AV Scan*, *Cloud Query*, and *Sandboxing*. Click *OK* to continue. This feature is only available for files with a *Malicious* rating and the suspicious jobs detected by *Static Scan*, *AV Scan*, *Cloud Query* and the yara engine. The rescan job is in *Scan Job* > *File On-Demand*.
Pagination		Use the pagination options to browse entries displayed.

The following information is displayed:

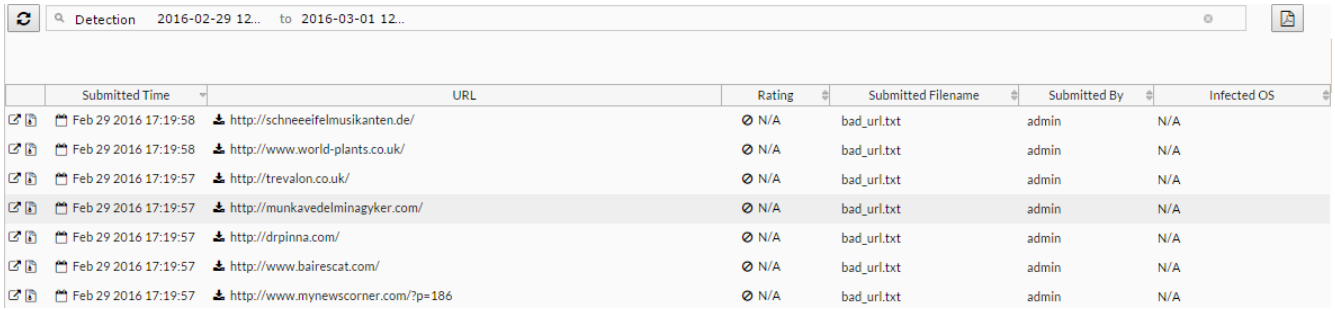
Total Jobs	The number of jobs displayed and the total number of jobs.

The displayed columns are determined by settings defined in *System* > *Job View Settings* > *File Detection Columns* page. For more information, see Job View Settings on page 189.

URL Job Search

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

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



The following options are available:

Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.
Search Field	Enter the detection time frame and click to add additional search filters for Destination, Device, Infected OS Job ID, Job Status, Rated By, Rating, Scan Unit, Submit User, Submitted Filename and URL. When the search criteria is *Submitted Filename*, click the = sign to toggle between the exact and pattern search.
Time Period	Select a time period to apply to the search.
Export to Report	Select to open the Report Generator dialog box. Select to generate a PDF or CSV report. During generation, do not close the dialog box or navigate away from the page. You can wait till the report is ready to view, or navigate away and find the report later in *Log & Report* > *Report Center* page.
Customize	Click the *Customize* icon to customize the Job View settings page. For more information, see Job View Settings on page 189.
Action	
View Details	Click the *View Details* icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.

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

The following information is displayed by default:

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

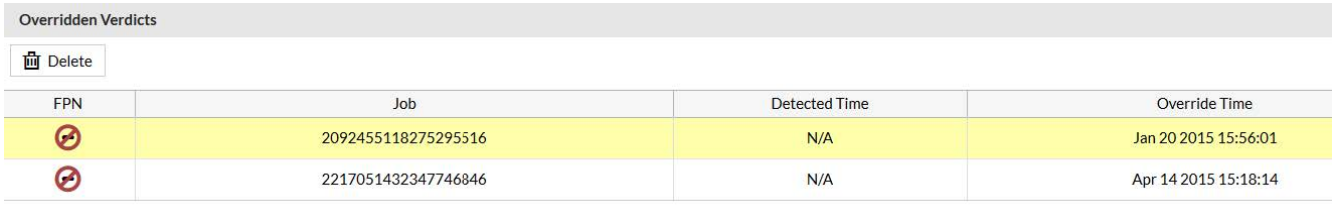
The displayed columns are determined by settings defined in *System* > *Job View Settings* > *URL Detection Columns* page. For more information, see Job View Settings on page 189.

Overridden Verdicts

The *Overridden Verdicts* page displays jobs that users have manually marked as *False Positive* or *False Negative*. *Job IDs*, *Comment*, *Job Finish Time*, and the time that the user manually marked the verdict will be displayed. If the job's

detailed information is still available, the user can click on *Job ID* to display them.

You can easily delete a FP/FN verdict in this page by selecting an entry and clicking the *Delete* button, or use `CTRL+click` to select and delete multiple entries at the same time.



File On-Demand

To view on-demand files and submit new files to be sandboxed, go to *Scan Job* > *File On-Demand*. You can drill down for details and apply search filters. You can select to create a PDF or CSV format report for on-demand files.

Use *File On-Demand* to upload different file types directly to FortiSandbox. You can then view the results and decide whether to install the file on your network.

FortiSandbox has a rescan feature. When a Suspicious or Malicious file is detected, you can click the *ReScan* icon to rescan the file. This is useful when you want to understand the file's behavior when run on the Microsoft Windows host. You can force the file to do Sandboxing scan even if was detected in former steps of Static Scan, AV Scan, Cloud Query, or stopped from entering VM by Sandboxing-prefilter setting. All rescanned jobs are listed on the *File On-Demand* page.

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

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

File On-Demand page - level 1

The following options are available:

Submit File	Click the button to submit a new file. You can upload a regular or archived file. Six levels of file compression is supported. All files in the archive will be treated as a single file.
Show Rescan Job	Jobs generated from manual rescan can be shown/hidden by this option.
Search	Show or hide the search filter field.
Add Search Filter	Click the search filter field to add search filters. Click the cancel icon to the left of the search filter to remove the specific filter. Click the clear all filters icon in the search filter field to clear all filters. When the search filter is Filename, select the equal icon to toggle between exact search and pattern search.

Refresh	Click the refresh icon to refresh the entries displayed after applying search filters.
Clear all removable filters	Click the *trash can* icon to clear all removable filters.
Export Data	Click the *Export Data* button to create a PDF or CSV snapshot report. The time period of included jobs in the report depends on the selection of Time Period dropdown. You can wait until the report is ready to view, or navigate away and find the report later in *Log & Report* > *Report Center*.
View Jobs	Click the icon to view the scan jobs associated with the entry. You can view detailed information for files scanned. If the file is an archive file, all files in the archive are displayed in this page.
Pagination	Use the pagination options to browse entries displayed.

This page displays the following information:

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

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

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

1. Click the *View Jobs* icon. The view jobs page is displayed.

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

2. This page displays the following information and options:

Back	Click the *Back* button to return to the On-Demand page.
Search	Show or hide the search filter field.
Refresh	Click the *Refresh* icon to refresh the entries displayed after applying search filters.
Add Search Filter	Click the search filter field to add search filters. Click the *Cancel* icon to the left of the search filter to remove the specific filter. When the search filter is Filename, select the *Equal* icon to toggle between exact search and pattern search.
View Details	Click the *View Details* icon to view file information. The information displayed in the view details page is dependent on the file type and risk level.
Scan Video	When the scan is submitted, if *Record scan process in video* is selected, a video icon is displayed. Clicking it will allow the user to select one VM type in which the scan is done and recorded. Select the VM type to play the video or save it to a local hard disk. The order of displayed columns is determined by the settings defined in the *System* > *Job View Settings* > *File Detection Columns* page. For more information, see Job View Settings on page 189.
Pagination	Use the pagination options to browse entries displayed.

3. Click the *View Details* icon to view file details. The *View Details* page will open a new tab. For information on the *View Details* page, see Job Details page reference on page 235.
4. Click the parent job ID icon to view rescan file details.
   If the parent job is an archive file, the childrens' file names are included in the Archive Files dropdown list. Select a child's file name to view its detail.
5. Close the tab to exit the *View Details* page.

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

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

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

To submit a file to FortiSandbox:

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

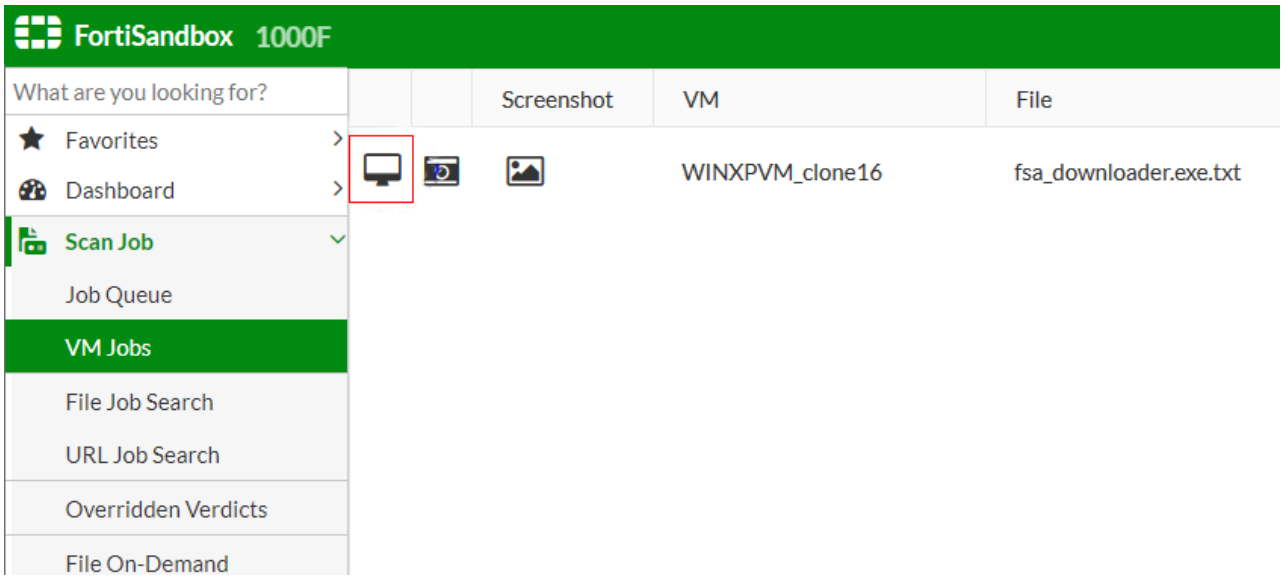
Select a File	Click the *Browse* button and locate the sample file or archived sample file on your management computer.
Possible password(s) for archive/office file	List all possible passwords to extract password protected archive file, or open password protected Microsoft Office file. One password per line. Default password list set in the Scan Policy and Object > General Settings page will also be used to extract the archive files.
Comments	Optional comments for future reference.
Force to scan the file inside VM	Enable to select advanced options.
Follow VM Association Settings in Scan Profile	If the sandboxing step is not skipped, the file will be sent to its associated VMs defined in Scan Profile.
Force to Scan Inside the Following VMs	Overwrite VM association settings in Scan Profile by selecting one or more of the enabled VMs.
Allow Interaction	Select the *Allow Interaction* checkbox to interact with the Windows VM. For more information, see To use the Allow Interaction feature: on page 92.
Record scan process in video if VMs involve	Select to enable video recording. After scan finishes, a video icon will show in the File On-Demand second level detail page. Clicking it will trigger a download or play the video.
Add sample to threat package	If result matches malware package requirement, add scan result to threat package.
Enable AI	Use AI engine to scan the file.

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

To use the Allow Interaction feature:

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

4. Go to the *Scan Job* > *VM Jobs* page, the job will be launched when a clone of a selected VM is available.



To interact with the windows VM:

1. 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?*
2. Click *Yes* to stop the scan and the VNC session will close after a few seconds. Go back to the *On-Demand* page to check the scan result.

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

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

URL On-Demand

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

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

The following options are available:

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

This page displays the following information:

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

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

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

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

   The reset of displayed columns are determined by settings defined in *System* > *Job View Settings* > *URL Detection Columns*. For more information, see Job View Settings on page 189.
3. Click the *View Details* icon to view file details. The *View Details* page will open a new tab. For information on the *View Details* page, see Job Details page reference on page 235.
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:

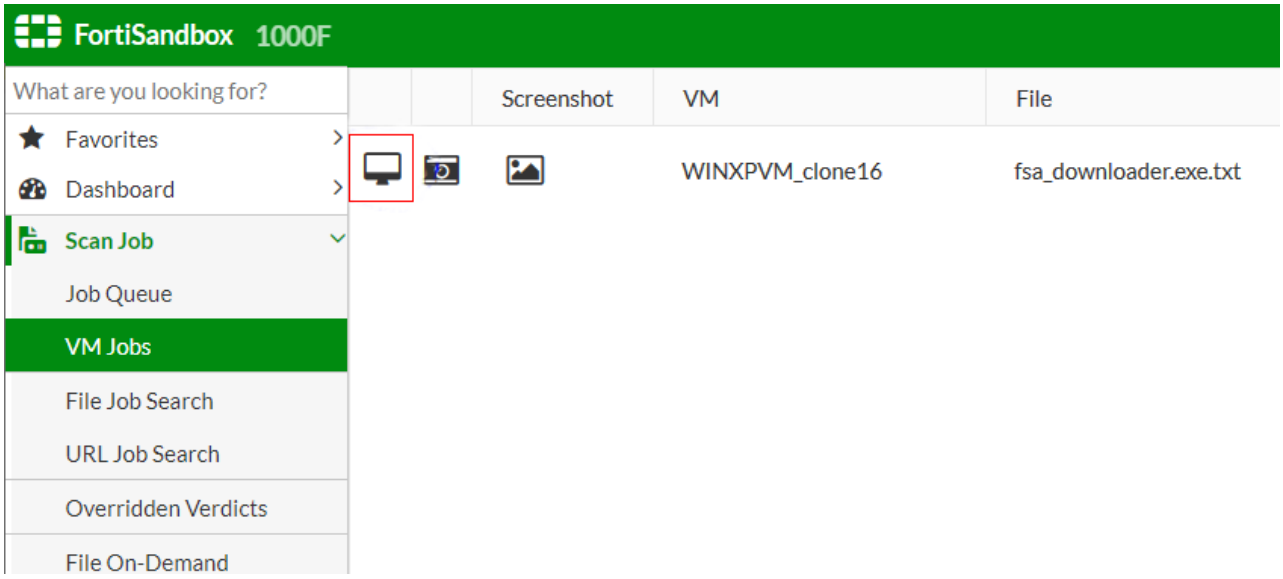
Depth	Enter the *Recursive Depth* in which URLs are examined. The original URL is considered level `0`. A depth of `1` will open all links on the original URL page and crawl into them. The default value is define in the *Scan Policy and Object* > *Scan Profile* page.
Timeout	Enter the *Timeout Value*. The Timeout Value controls how long the device will scan the URL. If the network bandwidth is low, the timeout value should be larger to accommodate higher depth values. The default value is defined in the *Scan Policy and Object* > *Scan Profile* page.
Direct URL	To scan only a single URL, check the *Direct URL* checkbox. Enter the URL in the *Enter a URL* field.
Select a File	Click the *Browse* button and locate the plain-text file on your management computer. The maximum number of URLs in this file is determined *Maximum URL Value in Scan Policy and Object* > *Scan Profile* > *Advanced tab* > *URL content limit*.

Comments	You can choose to enter optional comments for future reference.
Debug Options	To display the advanced options, check the *Debug Options* toggle. Users can choose to follow scan profile settings or specify the VMs.
Follow VM Association settings in Scan Profile	The URL will be sent to its associated VMs for the WEBLink defined in the Scan Profile. Enabled VM means its clone number is larger than `0`. **Note**: To use WindowsCloud VM, you need to purchase the subscription service. URL will be sent to Fortinet Sandboxing cloud to scan.
Force to Scan the URL Inside VM	A VM type must be selected. Settings from the Scan Profile will be overridden and the URL will only be scanned in selected VM types. If VM images are not ready, the VM list will not be displayed.
Allow Interaction	Select the *Allow Interaction* checkbox to interact with the Windows VM. For more information, see To use the Allow Interaction Feature: on page 96.
Record scan process in video	Select to enable video recording. After scan finishes, a video icon will show in the second level detail page. Clicking it will trigger a download or play the video.
Add URL sample to threat package	Select to add the sample to malware package, if the result meets settings in Package Options
Enable AI	Use AI engine to scan the file.

3. Click *Submit*.

To use the Allow Interaction Feature:

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



To interact with the Windows VM:

1. Click the *Interaction* icon to use web based VNC client.
2. 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.

Cloud Storage

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

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

The following options are available:

Create New	Click to create a new cloud storage connection.
Edit	Select an entry from the list and then click *Edit* in the toolbar to edit the entry selected.
Delete	Select an entry from the list and then click *Delete* in the toolbar to remove the entry selected.
Scan Now	Select an entry from the list and then click *Scan Now* in the toolbar to scan the entries.
Scan Details	Select an entry from the list and then click *Scan Details* in the toolbar to view the scheduled scan entries.
Test Connection	Test the selected entry's connection. The result is displayed in the banner at the bottom right corner.

The following information is displayed:

Name	The name of the cloud storage.
Scan Scheduled	The scan scheduled status. Scheduled network scans are done in parallel.
Type	The mount type.
Share Path	The cloud storage access URI.
Quarantine	Displays if quarantine is enabled.

Enabled	Displays if the cloud storage scan is enabled. If a cloud storage scan is disabled, its scheduled scan will not be executed.
Status	Displays the cloud storage connection status. The states are: • Network is Accessible • Network Down • *Azure Blob Storage* connection status will always be . *Test Connection* will show the connection status

To create a new cloud storage scan:

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

Enabled	Select to enable network share configuration. If network share is not enabled, its scheduled scan will not run.
Network Share Name	Enter the network share name.
Mount Type	Select the mount type from the dropdown list. Depending on the type selected, you will be asked for different information required to access your cloud storage. The following options are for cloud storage: • Azure File Share • AWS S3 • Azure Blob Storage
AWS S3 Settings	See AWS S3 Settings on page 100.
Azure FS Settings	See Azure File System on page 101.
Scan Files Of Specified Pattern	Select to include or exclude files which match a file name pattern.
File Name Pattern	Enter the file name pattern.
Scan Job Priority	When multiple network share scans run at the same time, the higher priority scans will get more scan power compared to those having lower priority. The priority can be set to *High*, *Medium* (default), or *Low*.
Keep A Copy Of Original File On FortiSandbox	Select to keep a copy of the original file on FortiSandbox.
Skip Sandboxing for the same unchanged files	Select to skip Sandboxing scan on existing files (if applicable) and only Sandboxing scan new files. Existing files will only be scanned by AntiVirus engine and Community Cloud query. This is to improve scan speed.
Enable Quarantine of Malicious Files	Select to enable quarantine then select the quarantine location from the dropdown list. Files with a Malicious rating will be quarantined in the quarantine location.

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

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

4. Select *OK* to save the entry.

To run a network share scan immediately:

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

AWS S3 Settings

FortiSandbox can scan files stored on cloud using AWS S3.

The following AWS S3 settings are available when creating a new Network Share, Quarantine, and Job Archive:

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

Azure File System

FortiSandbox can scan files stored on cloud using Azure File System.

Azure File Share

The following Azure file share settings are available when creating a new Network Share, Quarantine, and Job Archive:

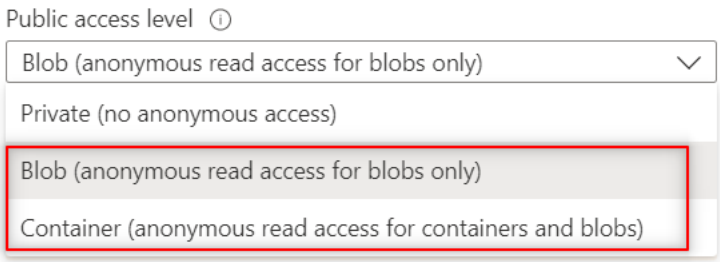
Domain of the Share URL	Enter the Azure file share URL's domain name, found in the Azure server's menu at *Storage Accounts* > *storage account name* > *Settings* > *Properties* > *URL*.
Path of the Share URL	Enter the path of the URL, found in the Azure server's menu at *Storage Accounts* > *storage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

Azure Blob Storage

1. Set up the container for FSA on Azure

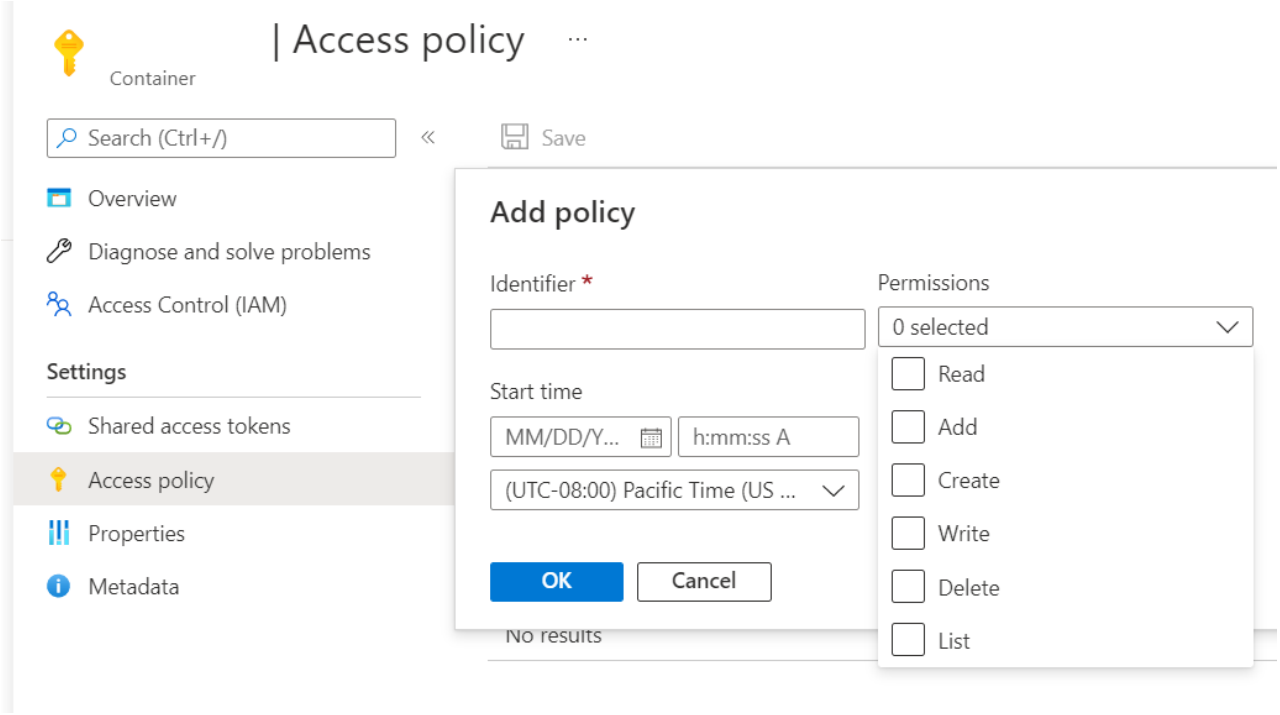
1. Log into the Azure Portal and go to the *Storage Account* for FortiSandbox.
2. In left menu, click *Containers* then click the + *Container* icon to create a new container:

   For *Public access level*, you can select either *Blob* or *Container*.



3. Go to *Access policy* > *Add policy* and locate the to the newly created container.

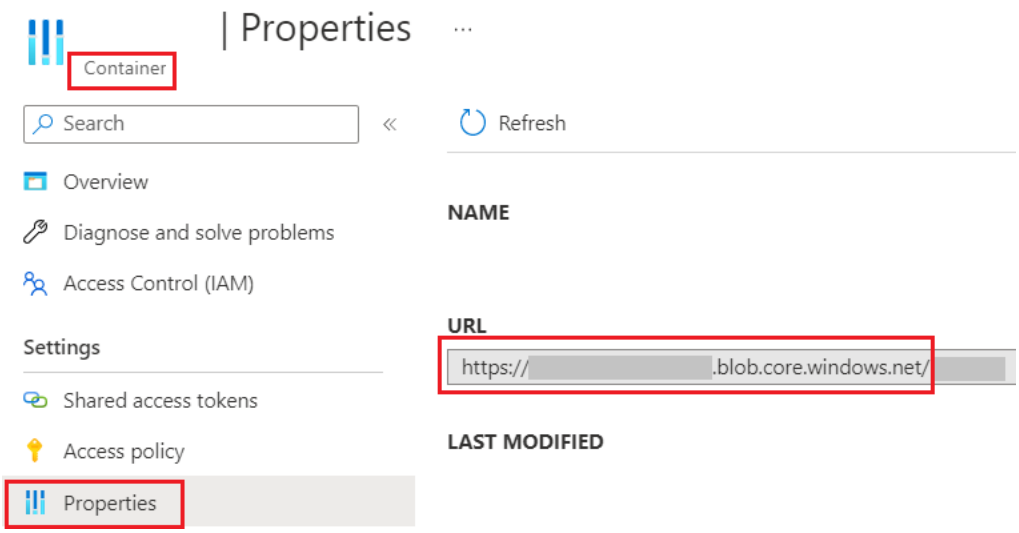
4. Under *Permissions* select *Read* and *Write* permissions, then click *Save*.



2. Setup the Azure Blob Storage on FSA

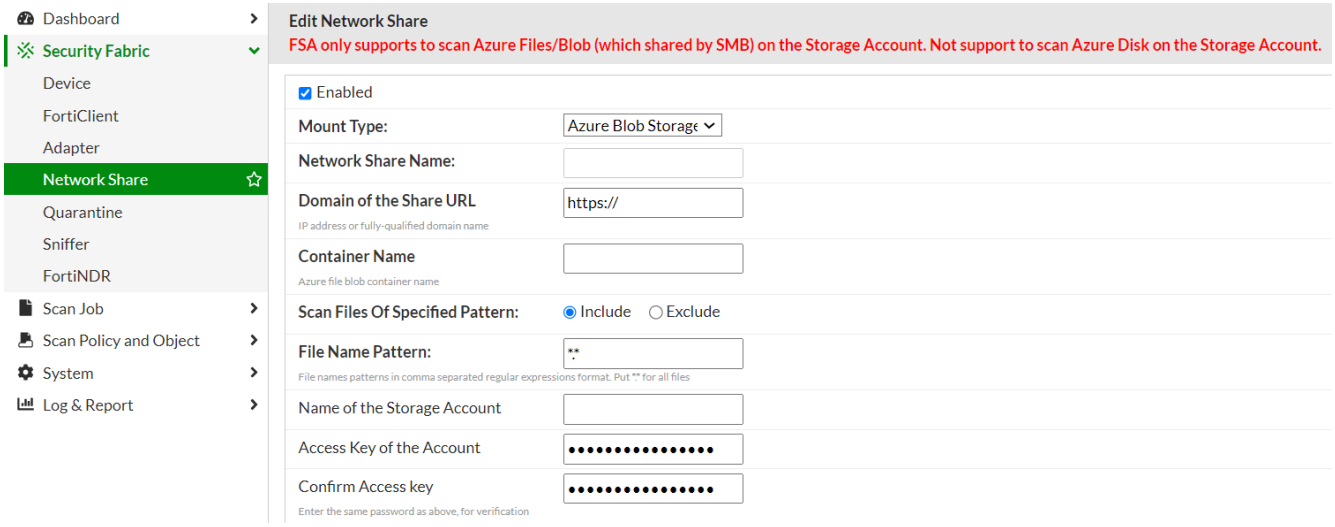
1. On FortiSandbox go to Security Fabric > Network Share.
2. The following *Azure Blob Storage* settings are available when creating a new *Network Share*, *Quarantine*, and *Job Archive*:

Mount Type	Select *Azure Blob Storage*.
Domain of the Share URL	Enter the URL of the storage account which ends with `.net`. For example, `https://storage_account.blob.core.windows.net`. This can be found on the *Properties* page of the container (see the image below).
Container Name	Enter the container name.
Name of the Storage Account	Enter the name of the Storage Account.
Access Key of the Account	Enter the Access Key of the Storage Account.

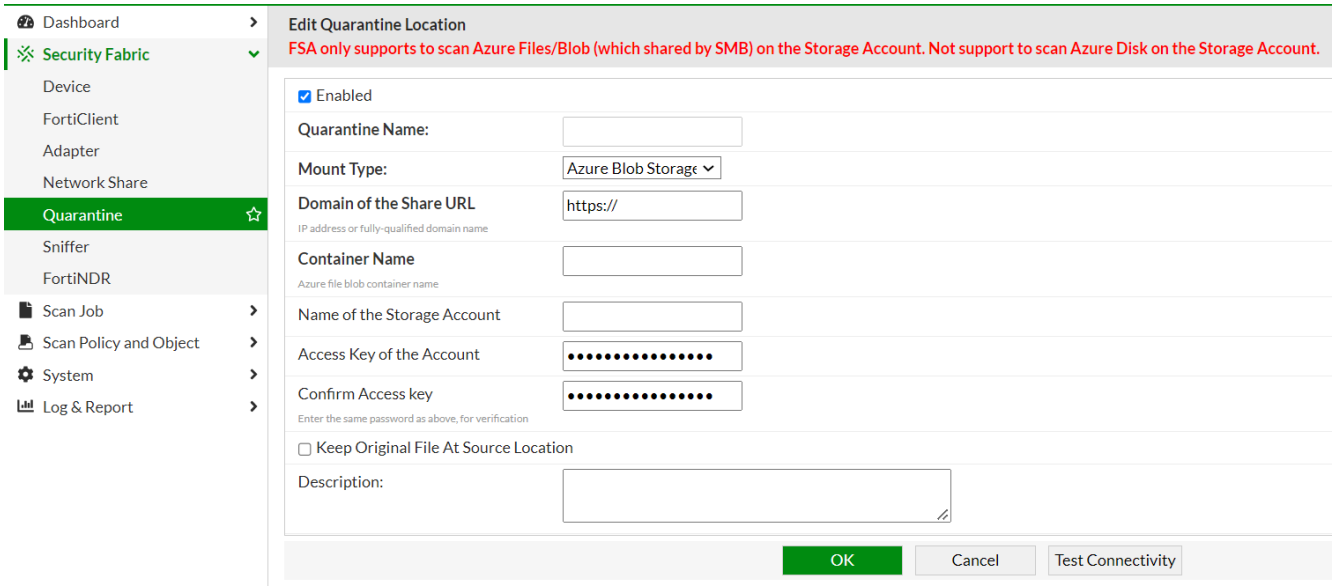


Configuration examples:

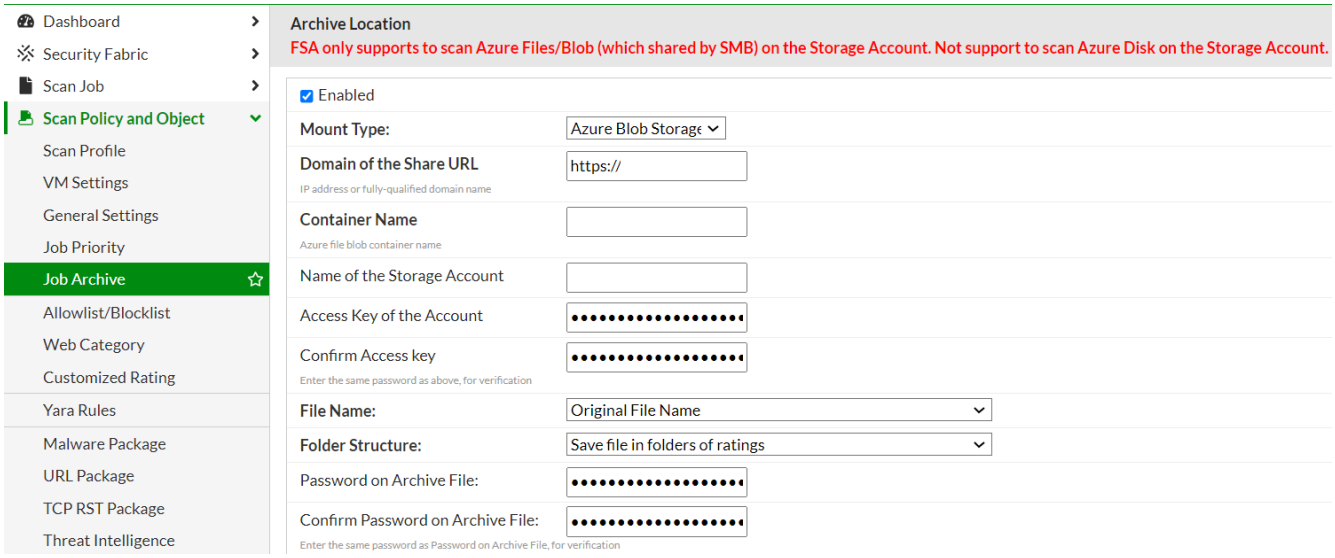
Network Share configuration



Quarantine configuration



Job Archive configuration

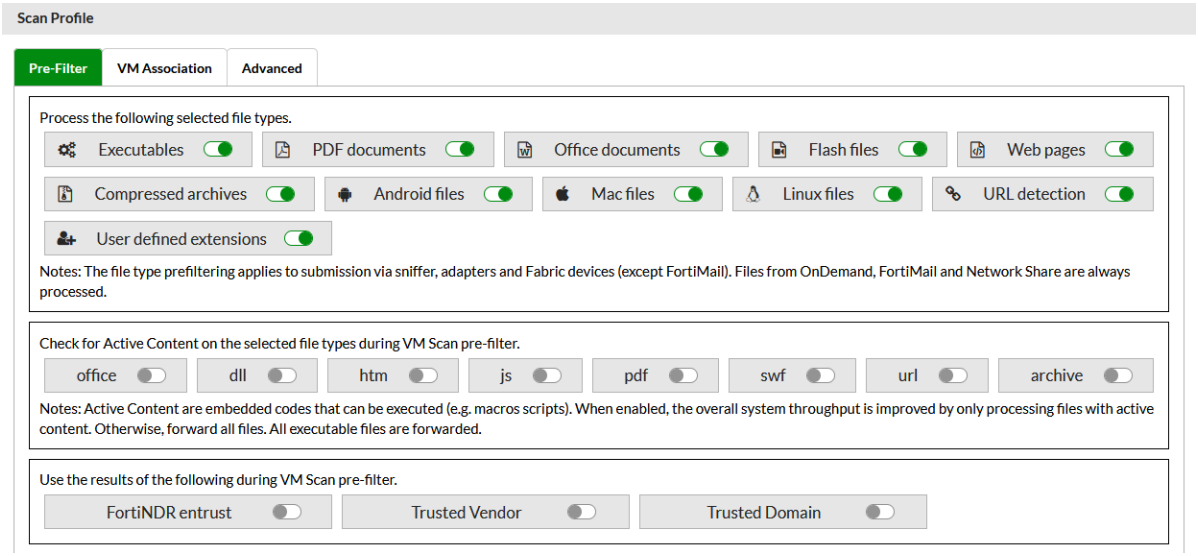


Scan Policy and Object

Scan Profile

Use the *Scan Profile* page to do the following:

- Configure the types of files that are put into the job queue.
- Configure the VM image to scan pre-defined file types and user defined file types.
- Enable adaptive VM scan.
- Enable parallel VM scan.
- Configure VM scan ratio.



File types

FortiSandbox supports the following file types by default.

Executables	BAT, CMD, DLL, EML, EXE, JAR, JSE, MSI, PS1, UPX, WSF, and VBS. Most DLL files cannot be executed within a VM. You can enable pre-filtering with the following CLI command: `sandboxing-prefilter -e -tdll` Only the DLL files which can be executed inside a VM are put into the Job Queue.
Archives	ZIP, GZ, BZ2, 7Z, TGZ,XZ, TAR, RAR, Z, CAB, KGB, LZH, ACE, ISO and ARJ. Archive files are extracted up to six levels (default) and each file inside is scanned according to the Scan Profile settings. The following are the default number of files extracted. You can change the default value using `prescan-config`. • On-Demand input: 10000

	• JSON API: 1000 • All other input sources: 100
Microsoft Office	Word, Excel, PowerPoint, Outlook, and more.
Adobe	PDF, SWF, and Flash.
Static Web Files	HTML, JS, URL, and LNK.
Android File	APK.
MACOSX Files	Mac (MACH_O, FATMACH, XAR, and APP files) and dmg (DMG) files.
WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.

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

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

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

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

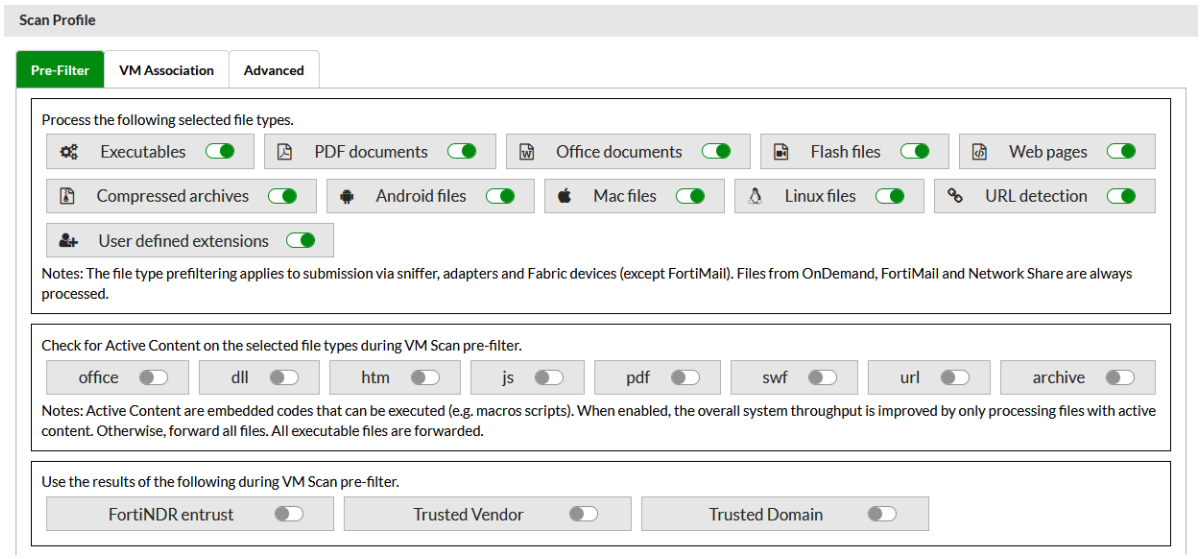
By default, FortiMail holds a mail item for a time to wait for the FortiSandbox verdict. Before FortiSandbox scans a file or URL sent from FortiMail, it checks if FortiMail still needs the verdict as FortiMail might have already released the email after time out. If not, FortiSandbox gives the job an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

Use the CLI command `fortimail-expired` to enable or disable this expiration check.

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

Scan Profile Pre-Filter Tab

Use the *Pre-Filter page* file type panel to define file types and URLs that are allowed to enter the job queue if they are from a sniffer, adapter, or device other than FortiMail.



Files or URLs submitted through On-Demand, RPC JSON API, network share, or FortiMail are always put into the job queue even if their file types are not set to enter the job queue.

To allow a file type to enter the job queue:

Click the toggle button to enable it. If the button is grayed out, files of that type are dropped.

To enable pre-filter for selected file types:

Click the toggle button to enable it. If the button is enabled, only suspicious files or unrated URLs are forwarded for VM Scan. The files and URLs will still go through the Static Scan stage. Enabling the prefilter can improve the scan performance. For more information, see Improving Scan Performance in the FortiSandbox *Best Practices and Troubleshooting Guide*.

To use trust results from trusted resources during pre-filter:

Click the toggle button to enable it. If the button is enabled, files rated by that resources are pre-filtered.

When *FortiNDR entrust* is enabled, files rated by FortiNDR as clean skip the sandboxing VM scan step.

When *Trusted Vendor* is enabled, executable files from a small internal list of trusted vendors skip the sandboxing scan step.

When *Trust Domain* is enabled, files downloaded from a small internal list of trusted domains skip the sandboxing scan step.

Trusted domains:

- http://www.google.com
- http://www.microsoft.com

Trusted vendors:

- Microsoft
- Fortinet Technologies
- Adobe Systems
- Google
- Apple

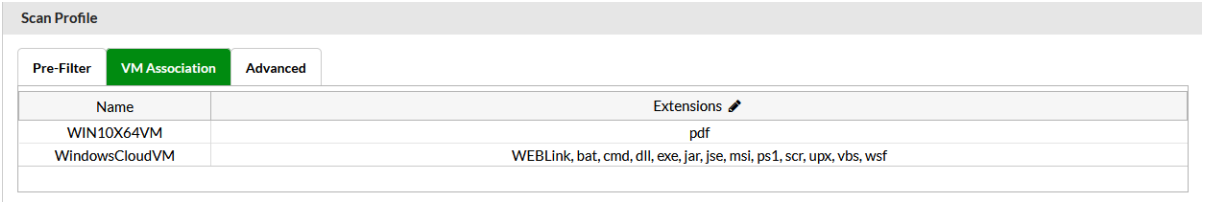
If there is a long queue of pending jobs, consider turning off some file types to the job queue. For example, in most networks, many files are static web files (JavaScript, html, aspx files) and Adobe Flash files. When you have performance issue, consider turning them off.

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

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

Scan Profile VM Association Tab

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



To configure VM association:

Click the edit icon. The left panel shows installed applications and the right panel shows current associated file types.

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

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

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

To improve the system scan performance, you can turn on the sandbox pre-filtering of a file type through the `sandboxing-prefilter` CLI command. For example, you can associate web files to VM types. If the `sandboxing`

`pre-filtering` is *OFF* for `js/html` files, all of them will be scanned inside associated VM types. This may use up system's sandboxing scan capacity because web files are usually large in amount. It is recommended to enable `sandboxing pre-filtering` for web files. For more details, refer to the *FortiSandbox 4.2.4 CLI Reference Guide*.

To edit an associated file type:

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

Add a user defined extension:

Make sure the user defined extension is enabled.

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

Finalizing the list of Scanned File Types:

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

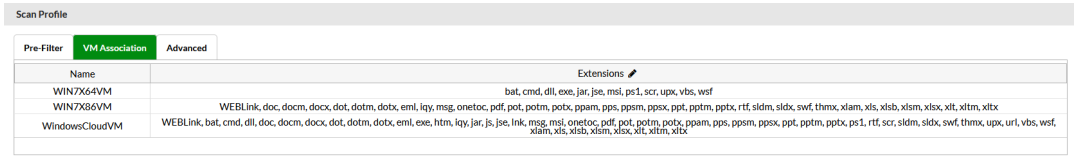
For files with a user defined extension, they will be scanned by a VM image no matter what file types they really are. Only a file's extension counts.

HA-Cluster

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

In a cluster environment, it is highly recommended that all cluster nodes have the same enabled VM, although it is not enforced. If cluster nodes do not have the same list of enabled VM types, a warning message will show up on top of the Scan Profile page for five seconds.

HA-Cluster Scan Profile VM Association Tab



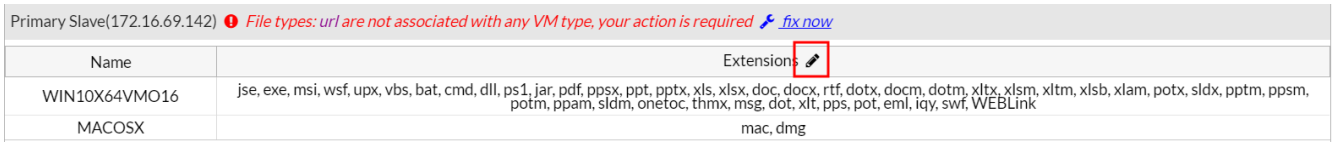
This page displays all cluster nodes enabled VM images and their enabled extensions. If the clone number is 0, the VM type is disabled. In this case, the enabled simulator VM is not listed.

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

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

To configure associations for the HA-Cluster:

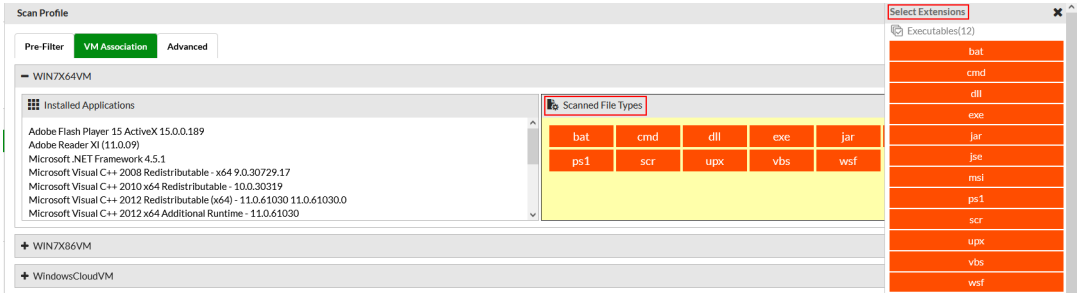
Click the pencil icon or the *fix now* link to edit the corresponding HA node.



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

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

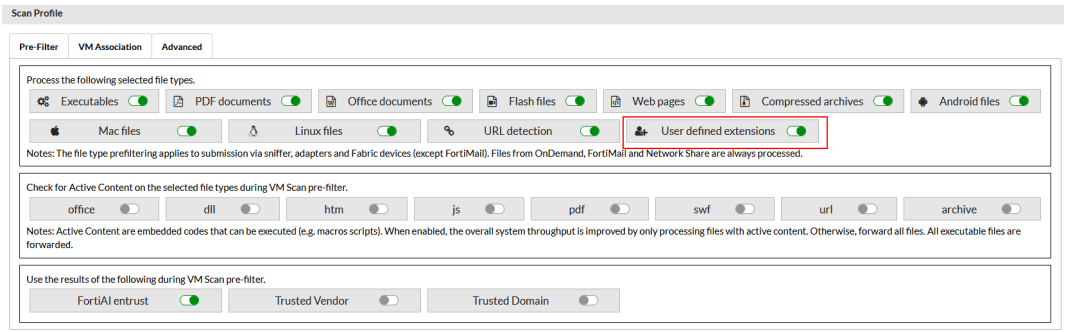
1. Click the *Scanned File Types* area. The *Select Extensions* pane is displayed.



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

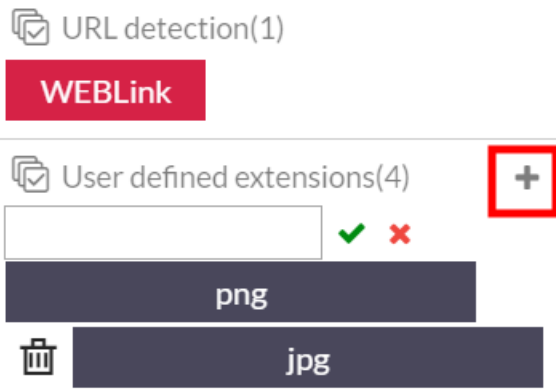
To add a user-defined extension for the HA-Cluster:

First, make sure the user-defined extension is enabled in the *Pre-Filter* tab.



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

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



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

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

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

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

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

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

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

Scan Profile Advanced Tab

Use the *Advanced* tab to define advanced features for file/URL detection.

Enable Adaptive VM Scan

Enable this option to dynamically adjust the number of clones of enabled local VMs. Local VMs include default VMs, optional VMs, and customized VMs.

Enabling this option does not affect the number of remote MacOS or WindowsCloudVMs.

In an HA-Cluster, only the primary node can enable this option and the setting is immediately synced to all nodes.

A VM's clone number is increased when its usage is higher than a threshold and there are assignable clones or reassignable clones.

A VM's clone number is reduced when it has reassignable clones and there are other VMs requiring more clones.

An enabled local VM has at least one clone. The number of assignable clones cannot be less than *0* at any time.

FortiSandbox-AWS, FortiSandbox-Azure, and FortiSandbox-HyperV do not support Adaptive Scan.

Enable Parallel VM Scan

Enable this option to allow FortiSandbox to run multiple VMs at the same time for a job. Normally, a job is scanned in the VM in sequence if the file type is associated with a different VM.

The parallel VM scan only happens when a job needs two or more VM scans and those VMs have a free clone. If there are no free clones, then parallel VM scan does not happen.

In an HA-Cluster, only the primary node can enable this option and the setting is immediately synced to all nodes.

Enhance VM Scan Ratio

Enable this option to allow a customized ratio for jobs that are scanned in the VM. The ratio is a low bound for the jobs that need to be scanned, meaning the percentage of jobs scanned in the VM can be equal to or higher than the preset ratio.

This option:

- Is an extra filter that sends a job to the VM. When disabled, the VM scan is skipped.
- Does not affect jobs that should normally be scanned in the VM. Those jobs are still VM scanned.

To configure this option:

Enable *Set customized sandboxing ratio* and set a ratio between *1* and *100*.

In the system log, FortiSandbox creates a job event log (debug level) every 5 minutes for VM scan ratio statistics for jobs in approximately the last hour. This lets you see how many files were scanned in the VM in the last hour.

VM scan ratio calculation

The ratio is recalculated for each job based on the total old jobs from one hour ago to the current job submission time.

Example 1. The preset ratio is 60%, there are 100 total jobs in the last hour before the current job, and 60 of 100 have been sent to VM scan. The ratio before the current job is 60*100.0/100 = 60% (<=60%). So the current job will be sent to the VM.

Example 2. You submit another job after the above example. The scan ratio is (60+1)*100.0/(100+1) = 60.39% (>60%). So this job won't be sent to the VM.

Because the VM scan takes time and there are jobs rated by cache, AV, allowlist/blocklist, Static Scan, and so on, the ratio of jobs finished in VM scan over all finished jobs in the last hour can be different from the ratio set for this feature.

In an HA-Cluster, only the primary node can enable this option and the setting is immediately synced to all nodes. Each node uses its local scan jobs to calculate the latest VM scan ratio, and then compare the universal ratio to decide whether to send a current job to VM.

Cache Dynamic Scan Results

Enable this option to allow VM scan cache.

VM Scan timeout for non-executable file

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

Currently, MAC OSX and Windows Cloud VM do not support file detection timeout.

To configure file detection timeout:

1. Go to *Scan Policy and Object* > *Scan Profile* > *Advanced*.
2. Enable *VM Scan timeout for non-executable file* and enter a timeout value.
   A shorter *Default Timeout* value provides better performance and faster scan speed, but lower accuracy. For a balance of speed and accuracy, use a value that falls in the middle of the 60-180 second range for normal model. Higher-end models (2000E/3000E/3000F/2000G), allows 30-180 second range.
3. Click *Apply*. The Scan results shows the VM Scan time.

When *VM Scan timeout for non-executable file* is, the non-executable files will display the timeout value in Job Detail Overview page, for `Timeout Value:111 seconds`.

VM Scan timeout for URL

When URL detection is enabled, FortiSandbox scans URLs (WEBLinks). You can also specify the timeout setting (from 30 to 1200 seconds).

When this option is disabled, the default timeout is 60 seconds.

URL depth limit

Enable this option to examine the recursive depth of URLs (from 1 to 5).

When this option is disabled, only the URL itself is examined.

URL content limit

Enable this option to specify the maximum number of URLs from 1 to 10000.

When this option is disabled, the maximum number of URLs is unlimited.

Enable Rating Cloud Service

Enable this option to enhance the rating of the submission to provide a better detection rate by utilizing the Rating Engine and supervised Machine Learning in the cloud. When enabled, the local verdict and rating log are sent to the cloud. The original submitted file is not included.

Enable Code Emulator

Enable this option to forward the Windows executable submitted file for emulation to find traces of malicious code.

Enable Pipeline Mode

Enable this option to improve performance and accelerate the scan by reducing the time spent on VM instance starts and shutdowns. This means that jobs can be scanned in a VM instance one at a time without shutting down the instance.

A guest VM instance can only be reused when the scanning job won't change the VM instance status. If the guest VM status has been changed, the VM instance will be shut down and restored for the next job.

If a job is rated *malicious* or *suspicious* in a pipeline mode VM instance, the job is rescanned in a fresh restored VM to secure a final rating.

When a file is scanned in Pipeline Mode VM clone, the Job Details overview page will indicate the launched pipeline mode clone, (for example, *Pipeline mode OS:WIN7X86VM*).

If *debug* level log is enabled, *Job Event* will show the number of jobs scanned in Pipeline Mode VM clone, (for example, *WIN7X86VM_clone065 is in pipeline and has scanned 2 jobs*. See, Logging Levels.

FortiSandbox-AWS and FortiSandbox-Azure do not support Pipeline Mode.

File Scan Priority

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

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

File Scan Flow

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

1. Filtering and Static Scan
   In this step, the file is scanned by the AntiVirus engine and the YARA rules engine. Its file type is compared with the *Scan Profile page* > *Pre-Filter* tab settings to decide if it should be put in the job queue. If yes, it is compared with the allowlist and blocklist and overridden verdict list.

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

2. Community Cloud Query
   The file will be queried against the Community Cloud Server to check if an existing verdict is available. If yes, the verdict and behavior information are downloaded. This makes the malware information shareable amongst the FortiSandbox Community for fast detection.
3. Sandboxing Scan
   If the file type is associated with a VM type, as defined in the *Scan Profile page* > *VM Association*, the file is scanned inside a clone of that VM type. A file that is supposed to be scanned inside a VM might skip this step if it's filtered out by sandboxing prefiltering. For more information, see the *FortiSandbox CLI Guide* for the `sandboxing-prefiltering` command.

URL Scan Flow

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

1. Static Scan.
   In this step, the URL is checked against the user uploaded *Allowlist* or *Blocklist* and the *Overridden Verdicts* list.
2. Sandboxing Scan.
   If WEBLink is associated with a VM type as defined in the *Scan Profile page* > *VM Association* tab, the URL is scanned inside a clone of that VM type. If the *URL* type is enabled with the `sandboxing pre-filtering` command, only URLs whose webfiltering category is *UNRATED* is scanned inside a VM.
   For more information, see the the `sandboxing-prefiltering` command in the *FortiSandbox CLI Guide*.

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

VM Settings

Go to *Scan Policy and Object* > *VM Settings* to view all installed VM images and configure the number of instances of each image.

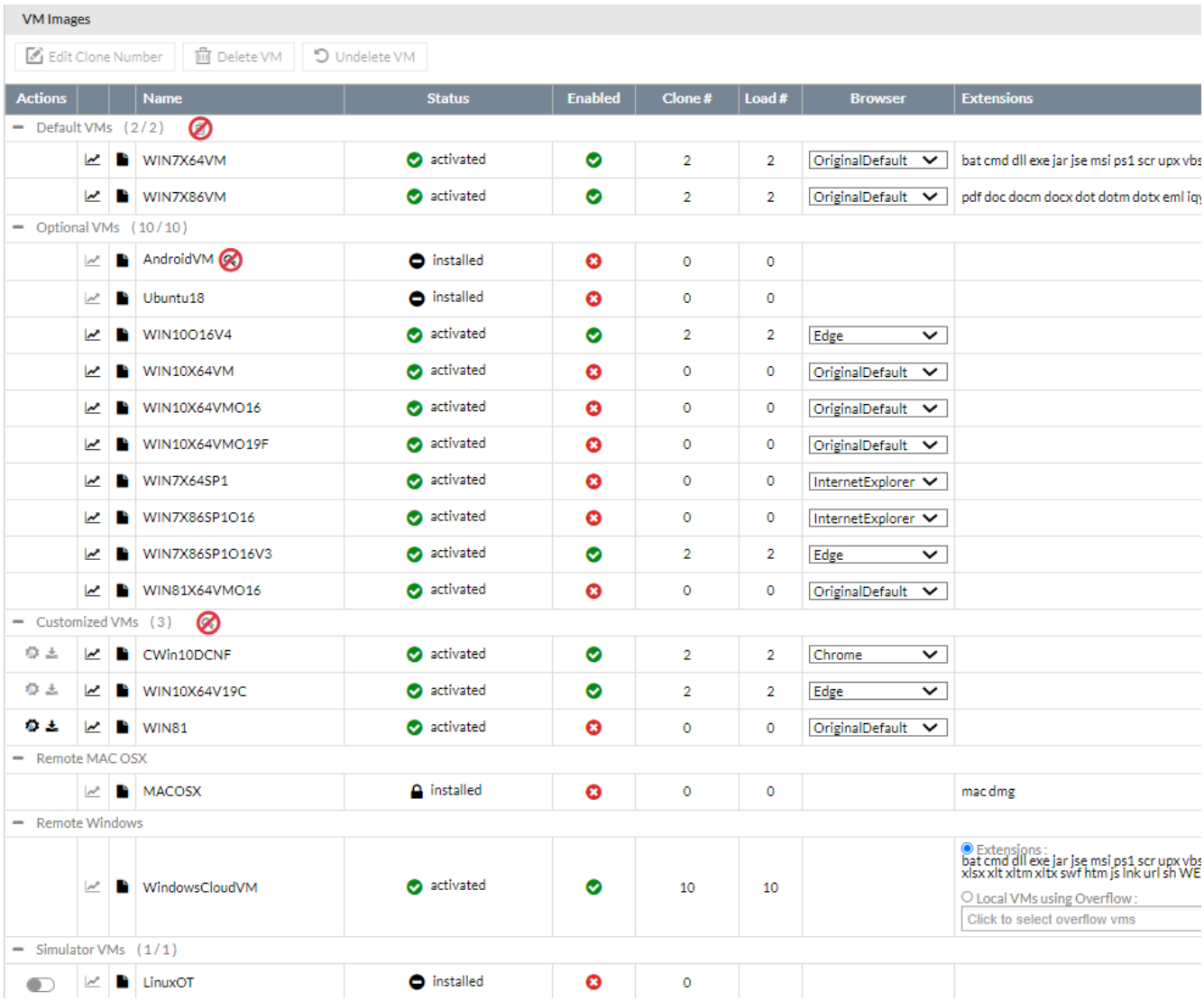
VM images are grouped into the following categories:

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

Remote MACOSX	Fortinet supports MACOSX remote VMs. You can purchase subscription services from Fortinet to reserve clone numbers in the FortiSandbox Cloud. There is no trial license for MACOSX VM. In cluster mode for MACOSX remote VMs, all cluster nodes share a collected pool of reserved clones from each unit. This means that even if a node has no remote VM contract, it can still upload files to the cloud for scanning. For the cluster as a whole, the number of files being scanned on the cloud cannot exceed the total number of reserved clone numbers at any given moment.
Remote Windows	Fortinet supports WindowsCloudVM as remote VMs. You can purchase subscription services from Fortinet to reserve clone numbers in the FortiSandbox Cloud. Besides normal use of WindowsCloudVM, overflow mode is supported. All activated local windows can be configured to overflow to WindowsCloudVM. When *Local VM to use overflow* is selected, jobs that have utilized all local clones for selected VMs will be scanned to WindowsCloudVM instead of waiting for another local clone. In a cluster, each unit in the cluster can purchase WindowscloudVM seat counts. The cloud VM seats are local to each unit and is not shared. Configuration to use overflow mode is also local to each unit.
Remote VMs	Fortinet supports *MACOSX* and *WindowsCloudVM* as remote VMs. You can purchase subscription services from Fortinet to reserve clone numbers in the FortiSandbox Cloud. There is no trial license for MACOSX VM. In cluster mode for MACOSX remote VMs, all cluster nodes share a collected pool of reserved clones from each unit. This means that even if a node has no remote VM contract, it can still upload files to the cloud for scanning. For the cluster as a whole, the number of files being scanned on the cloud cannot exceed the total number of reserved clone numbers at any given moment. In cluster mode for WindowsCloudVM, VM00 units in the cluster can purchase WindowscloudVM seat counts. These cloud VM clones are local to the VM00 unit and are not shared.
Simulator VMs	Fortinet provides LinuxOT VM. For information, see Simulator VMs on page 124

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

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



The following options are available:

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

The following information is displayed:

Enabled VM Types	The maximum number of VM types that can concurrently run. The maximum is four on models other than FSA-3000E. The maximum is six on FSA-3000E.
Keys	Maximum number of keys including used key numbers and installed key numbers.
Clone Number	Maximum clone number and the number of the installed Windows license. For example: • FSA-3000E, the maximum clone number is 56. • FSA-2000E, the maximum clone number is 24. • FSAVM00, the maximum clone number is 8.To expand the unit's scan power, you can purchase cloud Windows VM subscription. Files can be sent to Fortinet Cloud Sandboxing to scan.
Name	Name of the VM image. The name is unique in the system. If you upload a new VM image of the same name, the current installation is replaced. To see the VM's usage chart, click the *Chart* icon beside the *Name*.
Status	VM image status such as: • Ready to Download • Ready to Upgrade • Downloading (shows a progress bar) • Ready to Install (Install or Remove downloaded image) • Installing • Installed (Disabled) • Installed (No Keys Available) • Activated
Enabled	If an image's clone number is 0, it is disabled. Otherwise it is enabled.
Clone#	VM clone number. Double-click the number to edit it and then click the green checkmark to save the new number. Click *Apply* to apply the change. The VM system re-initializes. The total clone number of all VM images cannot exceed the number of installed Windows licenses. For example, for FSA-2000E, the maximum clone number is 24. We recommend applying more than 8+clone_number*3 of memory on your FSA unit.
Load#	The used VM clone number. For example, if a cluster primary node is set to use 50% of sandboxing scan power, the load # is half of clone #.
Browser	Set the default browser in Local Windows and Custom VMs. The default browser is Microsoft Internet Explorer.
Extensions	List of all the file types the VM image is associated with. It means files of these types will be scanned by this VM if these types are determined to enter the job queue. The system decides if they need to be sandboxed. If the sandbox prefiltering is turned off for a file type, it will be scanned inside each associated VM type. If sandbox prefiltering is turned on, files of this file type will be statically scanned first by an advanced analytic engine and only suspicious ones will be scanned inside associated VM types. You can define file type and VM association in *Scan Policy and Object* > *Scan Profile*. You can double-click the value to access the *Scan Profile* page to edit the list.

When Windows Cloud VM is used in normal mode, file extensions can be modified and displayed. If it is used in overflow mode, only selected local windows VMs will be displayed.

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

Virtual Machine

The FortiSandbox VM host is based on a modified hypervisor.

Model, License, and VM Information

Model	Base License*	Default VMs	Number of VM Hosts Supported
FSA-3000F	Windows 7 Windows 10 Office 2019	WIN7X64SP1O16 (with Office)	Supports 2 VM hosts by default, maximum up to 74 VM hosts. For Cloud expansion, you can subscribe up to 200 Windows Cloud VMs.
FSA-3000E	Windows 7 Windows 8.1 Windows 10 Office 2016	WIN7X86VM (with Office) WIN7X64VM	Supports 8 VM hosts by default, maximum up to 56 VM hosts. For Cloud expansion, you can subscribe up to 200 Windows Cloud VMs.
FSA-2000E	Windows 7 Windows 8.1 Windows 10 Office 2016	WIN7X86SP1O16 (with Office)	Supports 4 VM hosts by default, maximum up to 24 VM hosts. For Cloud expansion, you can subscribe up to 200 Windows Cloud VMs.
FSA-1000F	Windows 7 Windows 10 Office	WIN7X64SP1O16 (with Office)	Supports 2 VM hosts by default, maximum up to 14 VM hosts. For Cloud expansion, you can subscribe up to 200 Windows Cloud VMs.
FSA-500F	Windows 7 Windows 10 Office	WIN7X64SP1O16 (with Office)	Supports 2 VM hosts by default, maximum up to 6 VM hosts. For Cloud expansion, you can subscribe up to 200 Windows Cloud VMs.
FSAVM00	None	WIN7X86SP1O16 (with Office**) WIN10X64VM (available for download**)	No VM host by default, maximum up to 8 VM hosts. For Cloud expansion, you can subscribe up to 200 Windows Cloud VMs.

*Licenses pre-installed on the appliance.

**Both WIN7X86SP1O16 and WIN10X64VM will be listed as the default VM after the `VM00_base.pkg` is manually installed. Please refer to the deployment guide for more details.

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

You can download and use optional images from *VM Settings* > *Optional VMs*. The VM name shows the OS type. *O16* in the name means Microsoft Office 2016 is installed.

The following software is installed on each pre-installed Windows guest image:

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

Android VM is free to download and use.

You can build custom VM images but you must have software licenses for your custom images.

Other OS versions:

MacOS	Mac OS X 10.11
Android	Android OS 4.2.2
Linux	Ubuntu 18 and Redhat 8

Clone Number for VM Image

The following is the default clone number for VM images.

Model	VM Image	Number of Clones
FSA-3000F	WIN10X64VMO16	8
FSA-3000E	WIN7X64VM	4
	WIN7X86VM	4
FSA-2000E	WIN7X86SP1O16	4
FSA-1000F	WIN7X64SP1O16Z	2
FSA-500F	WIN7X64SP1O16Z	2

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

You can change the default settings to suit the majority of file types in your environment. For example, if most file types are Office files and WIN7X86VM is associated with Office files, you can decrease the clone number of other VM images and increase the clone number of the WIN7X86VM image.

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

VM Screenshot

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

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

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

Configure a custom VM

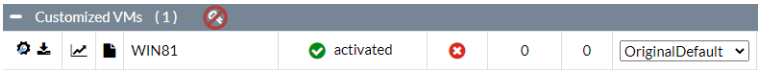
Custom VM modification is supported on the appliance-based and private cloud. It is not supported on cloud deployments such as FortiSandbox on AWS and Azure and FortiSandbox Cloud. Admins must have "Read Write" privileges to modify a custom VM.

Please refer to the FortiSandbox *Custom VM Guide* when developing your Custom VM. This guide is available to FortiSandbox customers with access to the Fortinet Developer Network or is available upon request from Customer Support.

A Custom VM requires a perpetual license. Once the license is registered with FortiCloud, download it from the support site and then upload it to FortiSandbox. If successful, the *License* widget in the *Dashboard* will display a green icon indicating the VM is enabled and ready to use.

To modify a custom VM:

1. Go to *Scan Policy and Object* > *VM Settings*.
2. Under *Customized VMs*, ensure the *Clone #* is zero.

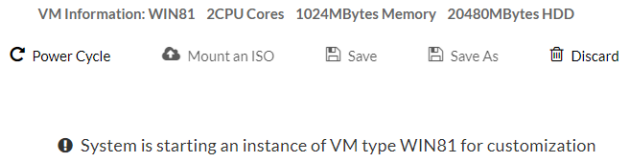


3. Click the *Customize VM* icon .
4. Configure the VM settings that will be used for the VNC session only. FortiSandbox uses pre-defined VM resources for the Dynamic Scan.

VM Name	The name cannot exceed 15 characters. Only letters and numbers are supported.

CPU Cores	Default is *1*. Maximum of two cores are supported. Once VNC terminates the CPU value reverts to default.
Memory	Default is *1024*. Maximum of 2048 MB memory is supported. Once VNC terminates the Memory value reverts to default.

5. Click *Start*. The system starts an instance of the VM type. This may take some time to complete.



6. Click *Mount an ISO* to install the software. Only ISO format is supported.

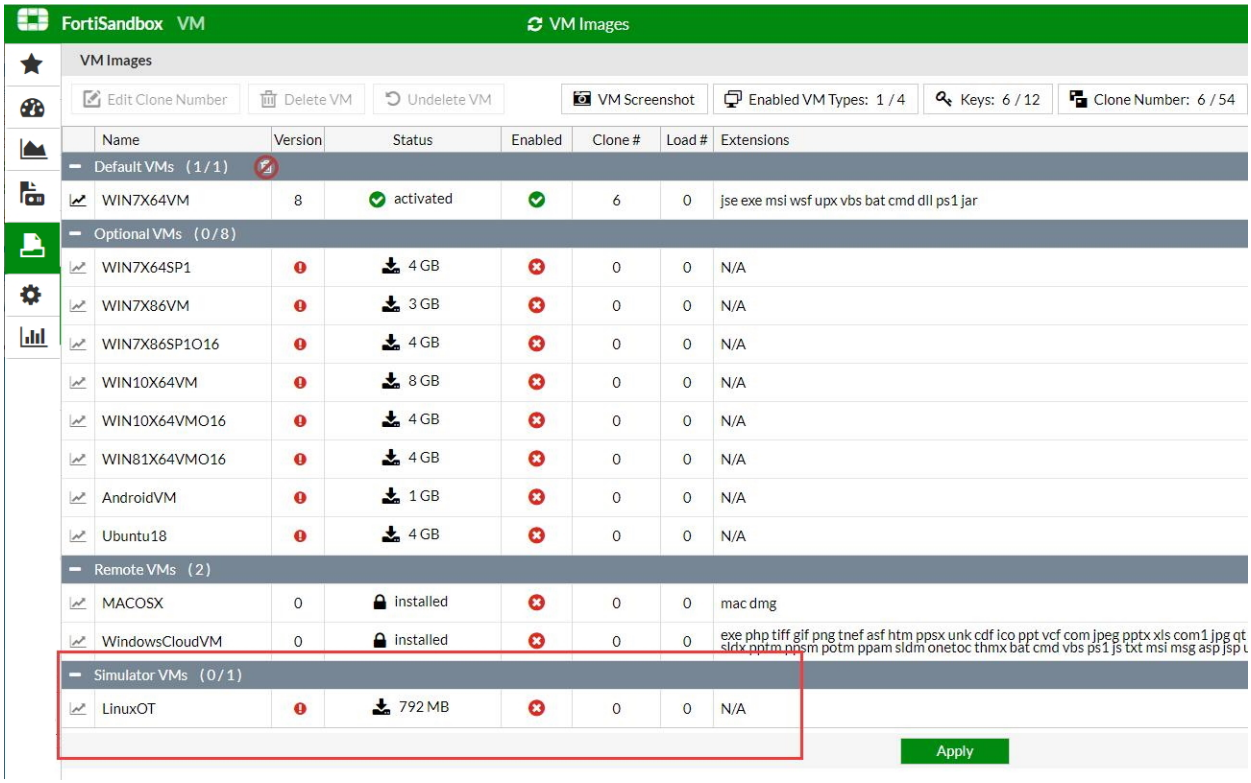
   The mounted ISO will be connected as CD drive. Alternatively, you can transfer files via file sharing site over the Internet. YOu should only visit a trusted site to avoid any unexpected changes on your VM.

7. Click *Power Cycle* to restart the instance.
8. To save your modifications, shutdown first the custom VM instance via VNC.
   - Click the *Save* icon to save all changes.
   - Click the *Save As* icon to save changes and then assign the current instance under a new name.
9. (Optional) Return to *VM Settings* and click the *Download* icon to download the VDI of all un-used custom VM(s).

Simulator VMs

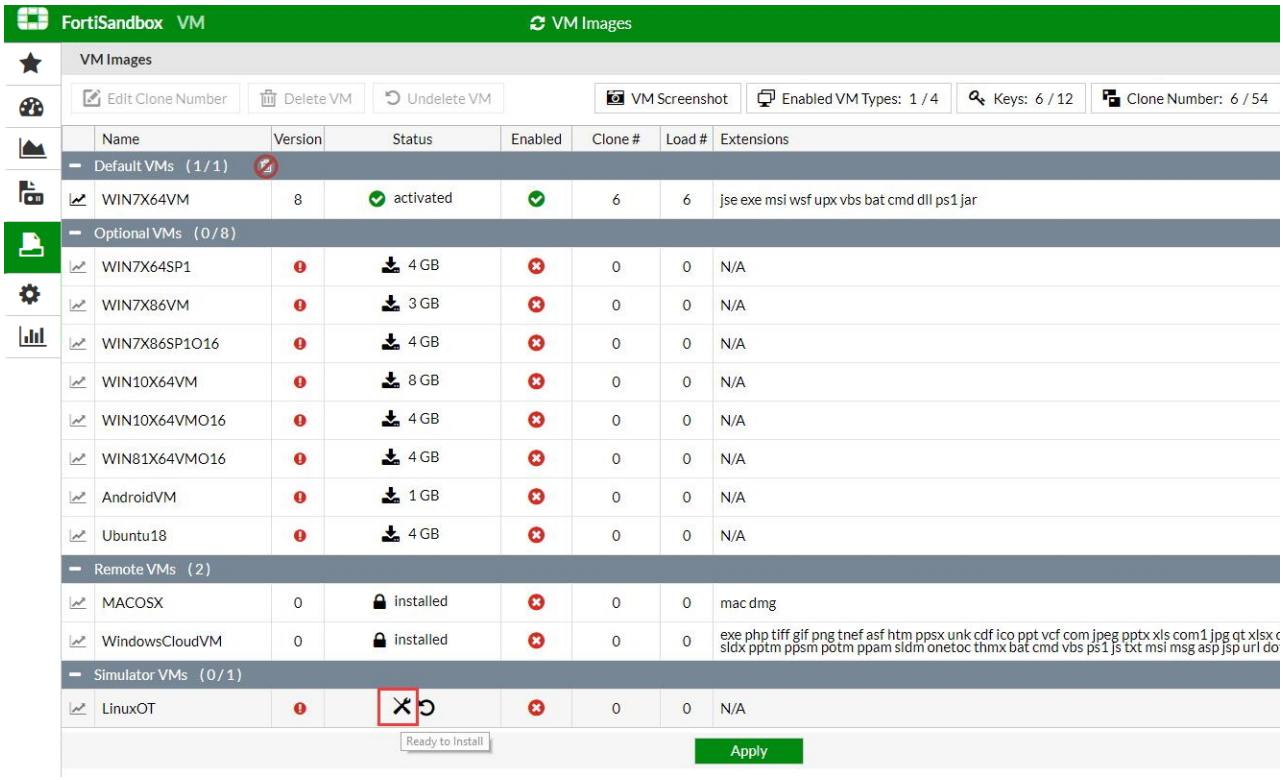
Preparing the OT Simulator VM on FortiSandbox

1. In *Dashboard* > *Status* > *Licenses* widget, check that the Industrial Security Service contract is valid.
2. Go to the VM Image page and find *LinuxOT* under the *Simulator VMs* table.

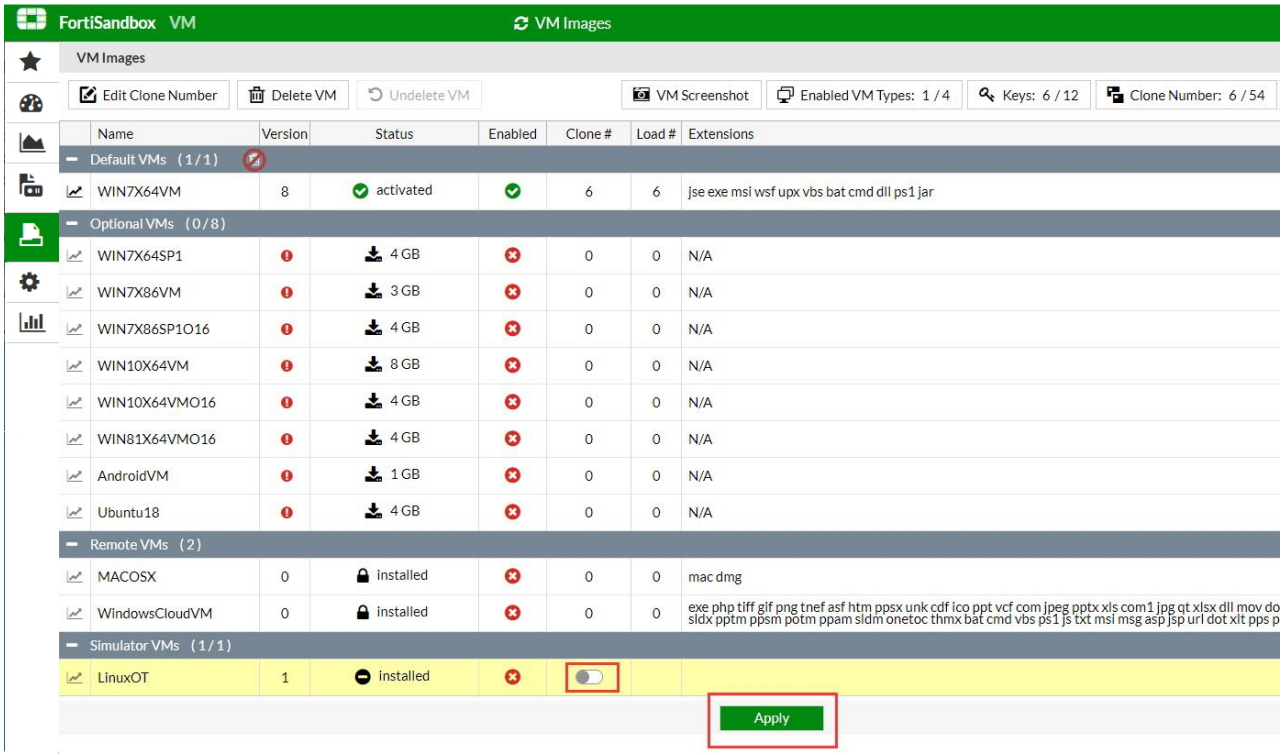


3. Click the download icon in the status column of the *LinuxOT* row.

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

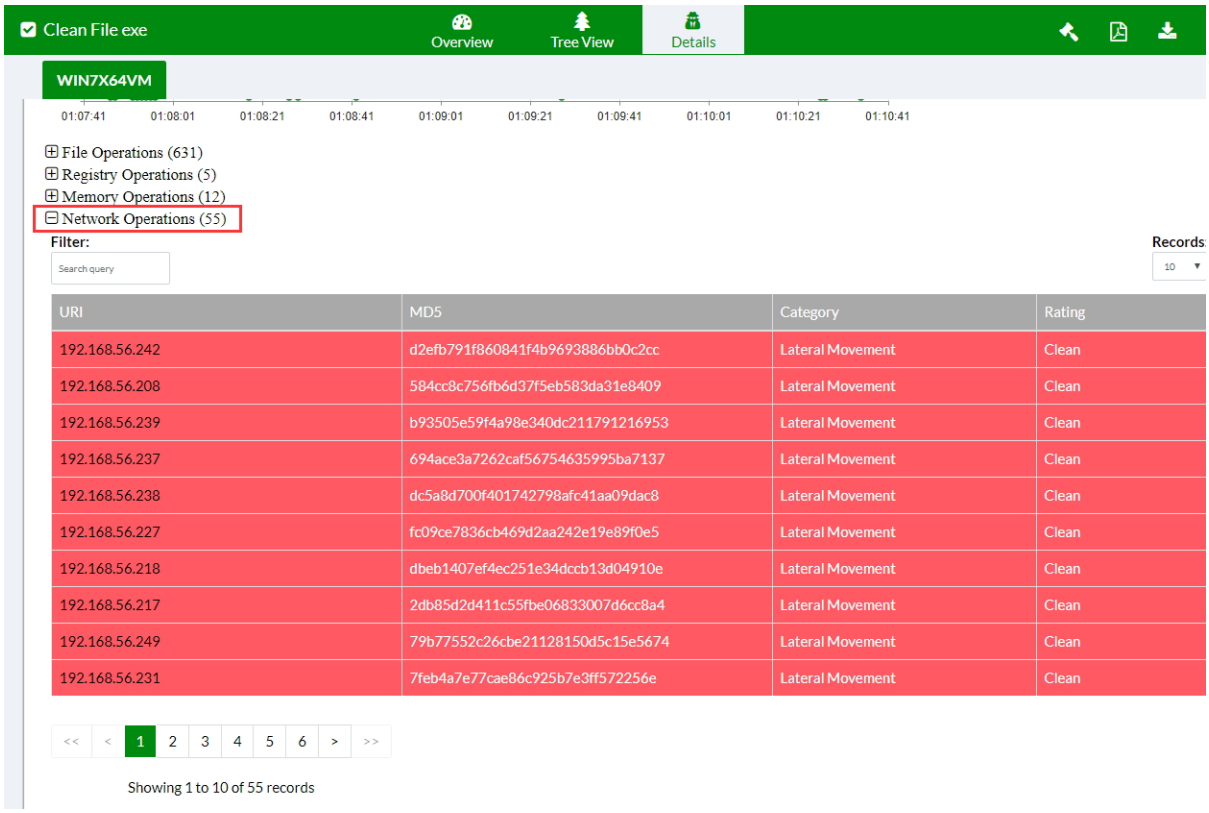


5. After rebooting, the *LinuxOT VM* is installed with clone disabled.
6. Toggle the switch in the *Clone #* column to enable it then press *Apply* to save the changes.



Scanning the files with the Simulator VM enabled

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



Set the default browser

Set the default browser in Local Windows and Custom VMs. The default browser is Microsoft Internet Explorer.

Supported Browsers and minimum required version:

- Google Chrome v75.0.3770.80
- Mozilla Firefox v90.0
- Microsoft Edge v86.0.622.61
- Microsoft Internet Explorer

Local Windows VM:

Chrome, FireFox and Edge are not listed if the installed version on the VM is lower than minimum required.

Optional VM:

The *Browser* setting is only available in the following Optional VMs. These VMs are only available in version 4.2:

- WIN10O16V4
- WIN7X86SP1O16V3
- WIN10O19V1

Download the applicable VM and apply a Windows license accordingly.

Custom VM:

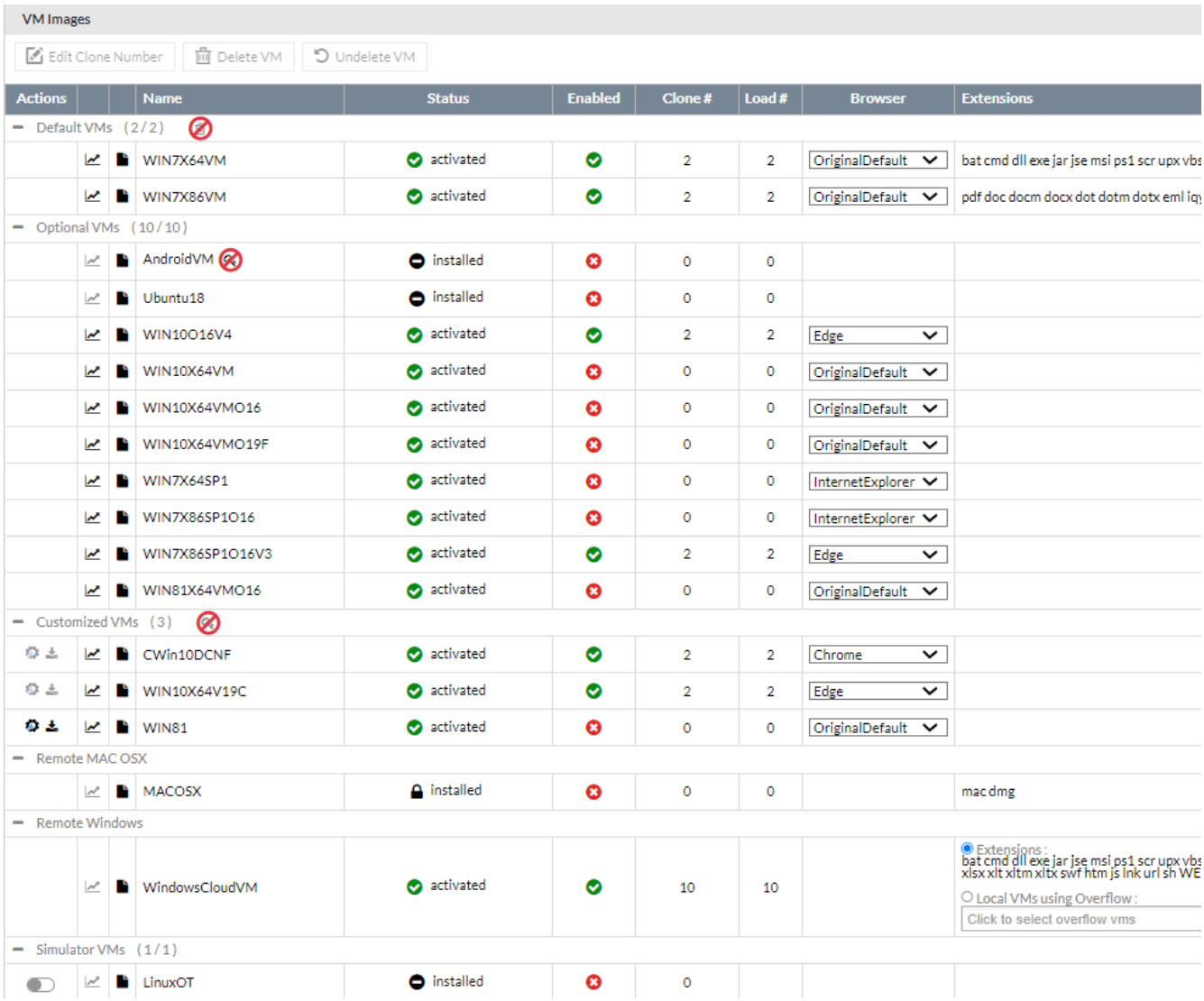
All browsers are listed regardless of whether the browser is installed on the VM. If the configured browser is not installed, the URL will be opened by the default browser. If the configured browser is installed but does not meet the required version, the URL will opened but cannot be scanned properly.

On the *Job Detail*, the browser used in the VM can be viewed in the *Process Information* under the *Tree View* tab.

To set the default browser in a Custom VM:

1. Go to *Scan Policy and Object* > *VM Settings*.
2. In the *Browser* column, click the *OriginalDefault* dropdown, and select a browser from the list.

Fortinet Ex. 2003 - Page 127 of 245



Remote VM:

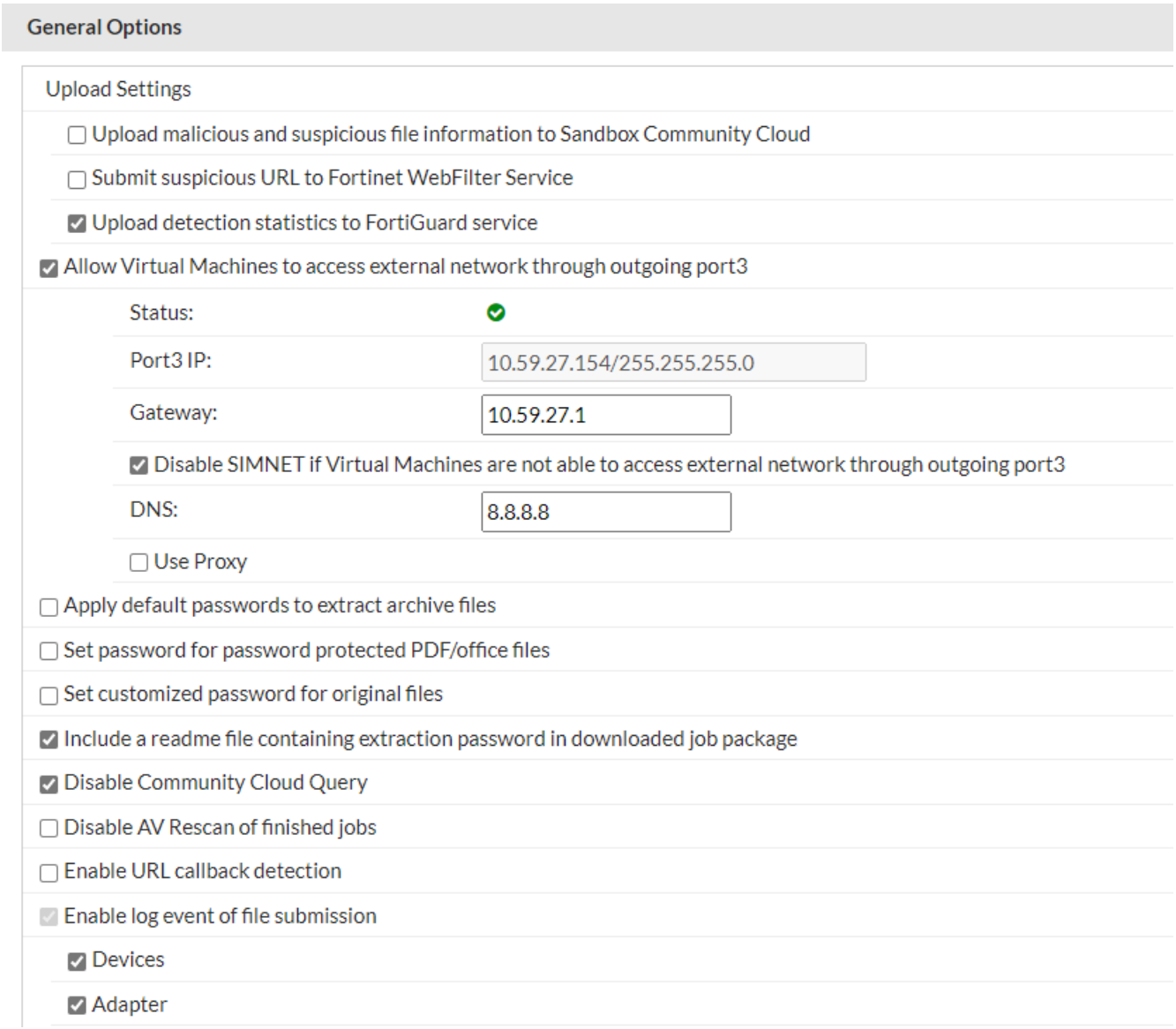
This feature is not supported in Remote (Windows, MacOS and Android Cloud VMs) and Local Linux VMs.

Deploying for Static Scan

When deploying FortiSandbox VM00 for Static Scan only, use firmware version 4.2.2 or later. You can leave the clone number at zero. For this deployment, the *Sandbox Threat Intelligence* plus *FortiCare Premium* subscriptions are required. Windows expansion licenses are not required.

General Settings

Go to *Scan Policy and Object* > *General Settings* 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 and URL information to the Sandbox Community Cloud. If enabled, the original file/URL, file/URL checksum, tracer log, verdict, submitting device serial number, and downloading URL are uploaded.
Submit suspicious URL to Fortinet WebFilter Service	Enable to submit malware downloading URL to the FortiGuard Web Filter Service.

Upload detection statistics to FortiGuard service	Enable to upload statistics to FortiGuard. If enabled, the following are uploaded: submitting device serial number and firmware, job-related results and statistics.
Allow Virtual Machines to access external network through outgoing port3	Enable to allow Virtual Machines to access external network through the outgoing port3. For further details, refer to the *port3 (VM outgoing interface)* topic in Interfaces on page 165.
Status	Port3 status to access the Internet.
Gateway	Enter the next hop gateway IP address. The *System* and VM cannot use the same gateway to access the Internet.
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 *FortiGuard* menu.
Proxy Type	Select the proxy type from the dropdown list. The following options are available: • HTTP Connect • SOCKS v4 • SOCKS v5; requires DNS UDP protocol is not supported.
Server Name/IP	Enter the proxy server name or IP address.
Port	Enter the proxy server port number.
Proxy Username	Enter a proxy username.
Proxy Password	Enter the proxy password.
Apply default passwords to extract archive files	User can define a list of passwords that can be tried to extract archive files. Input passwords line by line.
Set password for password protected PDF and office files	User can define one password for PDF and Office files.

Set customized password for original files	User can define their own password for the original sample when downloaded from FortiSandbox.
Disable Community Cloud Query	Cloud Query sends checksums to query any previously known rating from other FortiSandbox devices that contribute to the Community Cloud. Cloud Query is enabled by default. We recommend keeping this option enabled to utilize known rating for faster detection. 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 sniffed traffic are frequently queried against Web Filtering service.
Enable log event of file submission	Enable to log the file submission events of an input source.
Devices	Select to log the file submission events of a device, like FortiGate, FortiMail, or FortiClient.
Adapter	Select to log the file submission events from an adapter like a Carbon Black server.
Network Share	Select to log the file submission events when they are from a network share.
ICAP	Select to log the file submission events from an ICAP client.
BCC Adapter	Select to log the file submission events from a BCC client.
MTA Adapter	Select to log the file submission events from a MTA client.
Reject duplicate file from device	Enable to reject duplicate files from devices.
Delete original files of Clean or Other rating after	Enable to delete original files of Clean or Other ratings after a specified time. If the time is 0, the original files with either Clean or Other ratings will not be kept on the system. Original files of Clean or Other rating can be kept in system for a maximum of 4 weeks.
Day	Enter the day.
Hour	Enter the hour.
Minute	Enter the minute.
Delete original files of Malicious or Suspicious rating after	Enable to delete original files of Malicious or Suspicious ratings after a specified time.
Day	Enter the day.

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

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

Job Priority

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

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

Job Queue Priority

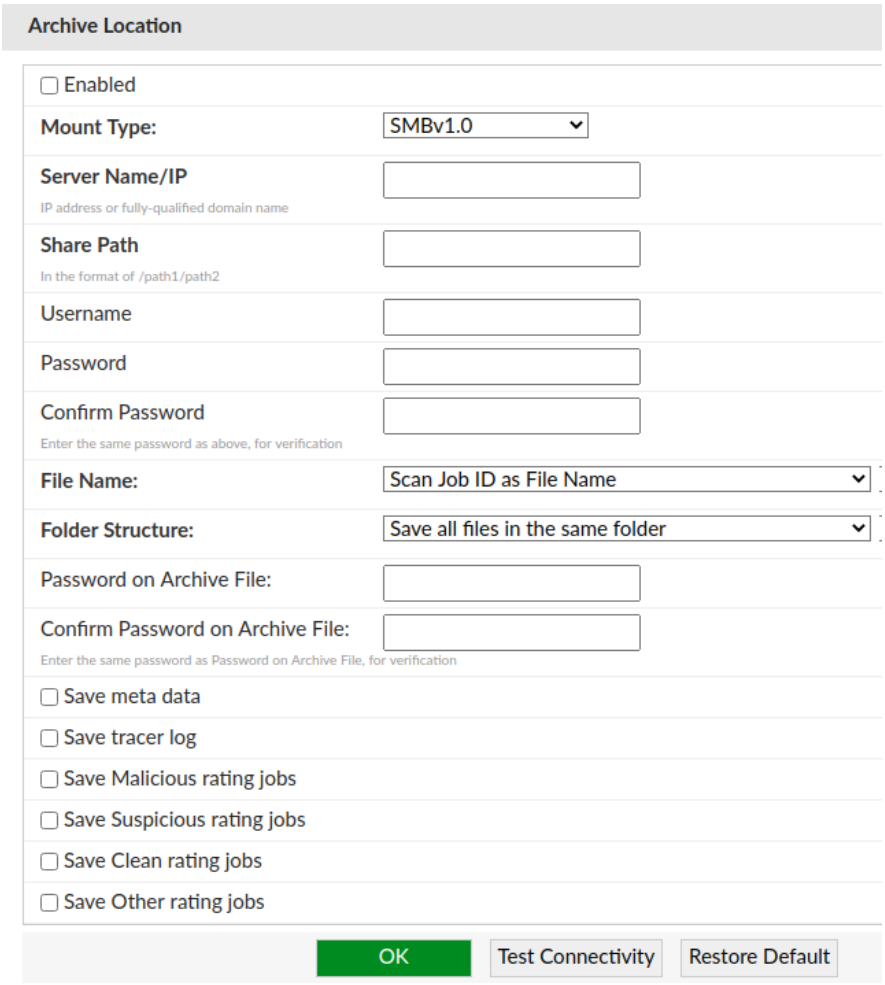
#	Input Source	File Type
1	OD On-Demand	EXE Executables/DLL/VBS/BAT/PS1/JAR/MSI/WSF files
2	OD On-Demand	USER User defined extensions
3	OD On-Demand	PDF PDF files
4	OD On-Demand	DOC Microsoft Office files (Word, Excel, PowerPoint files etc)
5	OD On-Demand	SWF Adobe Flash files
6	OD On-Demand	WEB Static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

Job Archive

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

The Job Archive is only available in the Primary node of an HA cluster.

To view the *Archive Location* page, Go to *Scan Policy and Object* > *Job Archive* .



The following options can be configured:

Enabled	Select to enable the job archive feature.
Mount Type	Select the mount type of the network share folder: • SMB v1.0 • SMB v2.0 • SMB v2.1 • SMB v3.0 • NFSv2 • NFSv3 • NFSv4 • Azure File Share • Azure Blob Storage • AWS S3 • AWS S3 BJ • AWS S3 NX

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

Allowlist and blocklist

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

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

- If an allowlist entry is hit, the job rating will be *Clean* with a local overwrite flag.
- If a blocklist entry is hit, the job rating will be *Malicious* with a local overwrite flag. Malware names will be FSA/BL_

DOMAIN, FSA/BL_URL, FSA/BL_MD5, FSA/BL_SHA1, or FSA/BL_SHA256.

- If the same entry exists on both lists and is hit, the blocklist will take priority and the file will be rated *Malicious*.

To manage the allowlist and blocklist manually:

1. Go to *Scan Policy and Object* > *Allowlist/Blocklist*.
2. Click the menu icon beside *Allowlists* or *Blocklists* to see its menu items.
3. Click the + button to add a new entry.

The URL pattern has a higher rating priority than a domain pattern. For example, if you enter `*.microsoft.com` in a domain allowlist and `http://www.microsoft.com/*abc/bad.html` in a URL blocklist, a file from `http://www.microsoft.com/1abc/bad.html` will be rated as `Malicious`.

4. Click *OK*.

To manage the allowlist and blocklist through files:

1. Go to *Scan Policy and Object* > *Allowlist/Blocklist*.
2. Beside *Allowlists* or *Blocklists*, click the menu icon and select the *Manage lists by uploading files* icon.
3. Select the list type from the dropdown menu:
   - *MD5*
   - *SHA1*
   - *SHA256*
   - *Domain*
   - *URL*
   - *URL REGEX*
4. Select the *Action* from the dropdown menu:
   - *Append*: Add checksums to the list.
   - *Replace*: Replace the list.
   - *Clear*: Remove the list.
   - *Download*: Download the list to the management computer.
   - *Delete*: Delete an entry from the list if the entry is in the uploaded file.
5. If the action is *Download*, click *OK* to download the list file to the management computer.
6. If the action is *Append* or *Replace*, click *Choose File*, locate the checksum file on the management computer, then click *OK*.
7. If the action is *Clear*, click *OK* to remove the list.

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

The total number of URL REGEXs in allowlist and blocklist must be less than 1000.

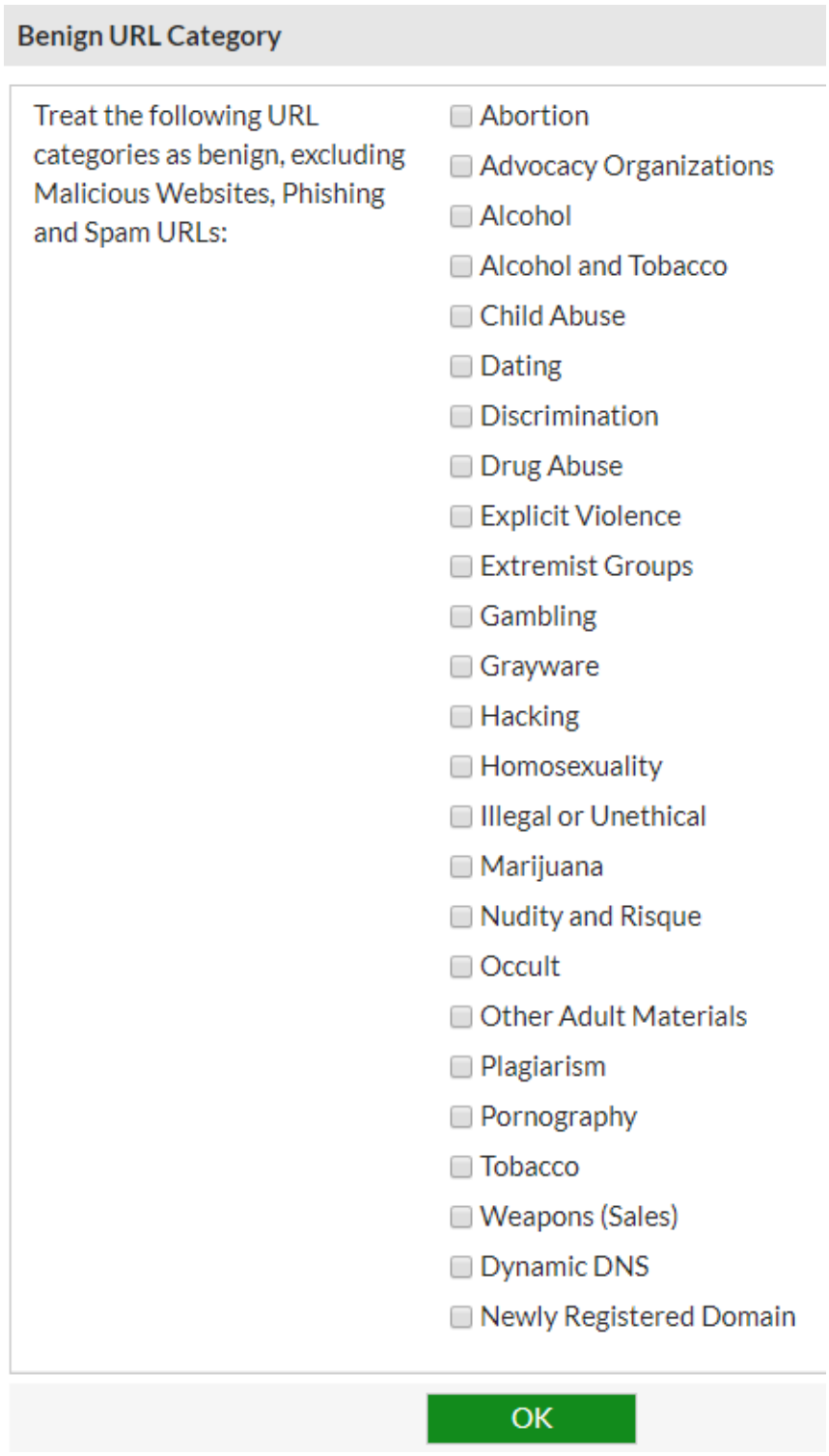
The total number of domains plus URLs in allowlist and blocklist must be less than 50000.

The total number of MD5+SHA1+SHA256 in allowlist and blocklist must be less than 50000.

Web Category

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

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



Working Together With URL Pre-Filtering

By default, URL scanning is done inside a VM. However, if performance is a concern, you can enable *URL Pre-Filtering*.

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

Scenarios

URL Sandboxing Pre-Filtering is Enabled

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

URL Sandboxing Pre-Filtering is Disabled

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

Customized Rating

Use the Customized Rating page to set verdicts for the following cases: VM Timeout, Tracer Engine Timeout, Unextractable Encrypted Archive, and URL whose return code is not *200*.

By default, all customized ratings are set as *Not Applied*. For any other value, the customized rating is always take higher priority if it applies.

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: • Not Applied • 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: • Not Applied • Unknown

	• Clean • Malicious • Low Risk • Medium Risk • High Risk
Unextractable Encrypted Archive	The archive file is password protected and cannot be extracted with a predefined password list set in the *Scan Policy and Object* > *General Settings* page. Select one of the following ratings: • Not Applied • Unknown • Clean • Malicious • Low Risk • Medium Risk • High Risk
URL whose return code is not 200	Block any URL sent to FortiSandbox which returns anything other than *200 OK*. You can disable this option by selecting *Not Applied*. Select one of the following ratings: • Not Applied • Unknown • Clean • Malicious • Low Risk • Medium Risk • High Risk

YARA Rules

YARA is a pattern matching engine for malware detection. It can be applied for files as well as downloaders. 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.

For more information about writing YARA rules, see the product documentation.

FortiSandbox supports following Yara modules:

Cuckoo, Magic, Dotnet, PE, ELF, Hash, Math and Time. For information about YARA modules, see the production documentation.

The following options are available:

Import	Select to import a YARA rule file. You can apply one YARA rule to multiple file types.

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

The following information is displayed:

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

To upload YARA Rule File:

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

YARA Rule Name	Enter a name for the YARA rule set.
Default Description	Enter a description of the YARA rule set.
Rules Risk Level	Select a rule risk level between 1-10. • *0-1*: Clean • *2-4*: Low Risk • *5-7*: Medium Risk • *8-10*: High Risk All the YARA rules inside the YARA rule file will share the same risk level.
File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
YARA Rule File	Choose a text file containing YARA rules.

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

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

To edit a YARA Rule set:

1. Go to *Scan Policy and Object* > *YARA Rules*.
2. Select a YARA Rule.
3. Click the *Edit* button from the toolbar.
4. Configure the following options:

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

5. Click OK to apply changes.

To delete a YARA rule set:

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

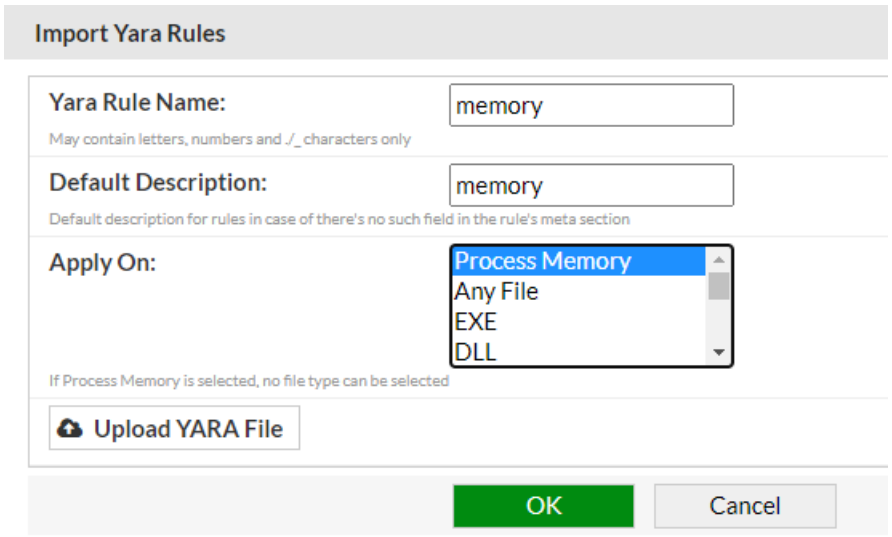
To change the status of a YARA rule set:

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

To import a process memory YARA Rule:

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

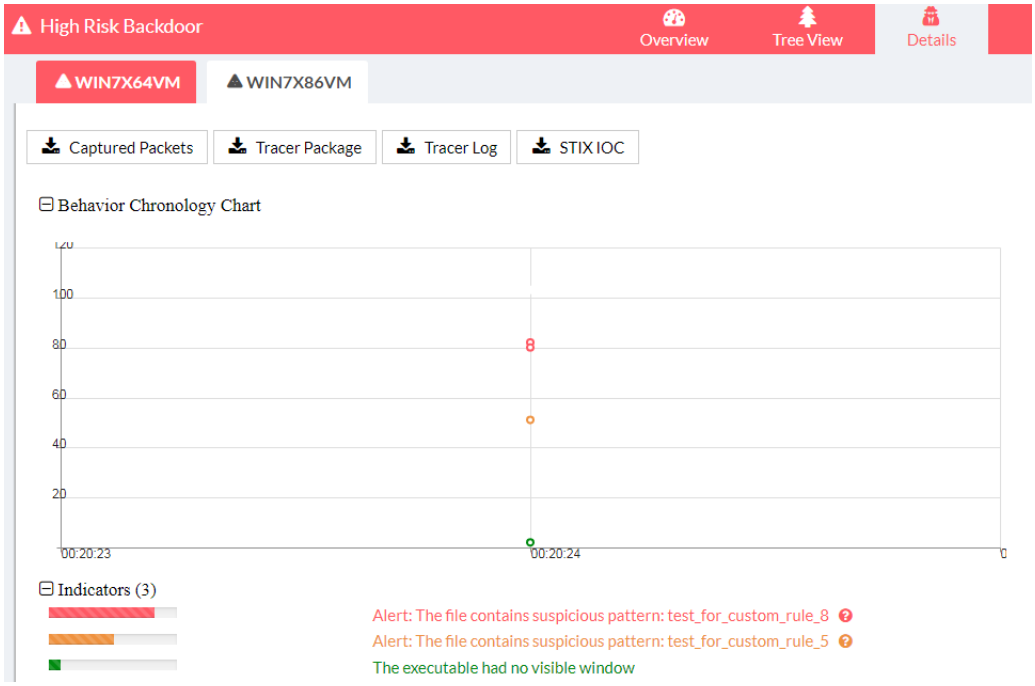
1. Go to *Scan Policy and Object* > *YARA Rules*.
2. Click the *Import* button.
3. Input a YARA rule name in the *Yara Rule Name* field.
4. Add a description for the YARA Rule if there is no corresponding field contained in the rule's *meta* section.
5. In the *Apply On:* field, click *Process Memory*.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



6. Click *Upload YARA File* and select the YARA Rule file.
7. Click *OK*.

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

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



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

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

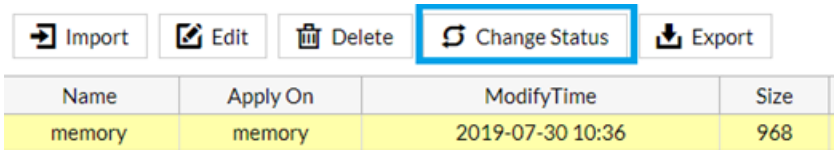
Format guidelines for process memory YARA Rules:

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

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

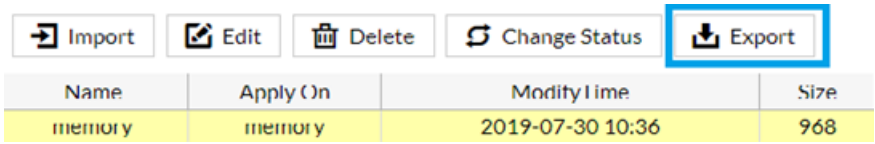
To activate the process memory YARA Rule

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



To export a YARA rule:

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



Malware Package

Go to *Scan Policy and Object* > *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 Policy and Object* > *URL Package* to view the URL Package list.

The following options are available:

Refresh	Refresh the URL Package list.
View	Select a package version number and click the *View* button from the toolbar. The following information is shown: • Job Detail: View the downloaded file's detailed information. If the unit is joining a global threat information sharing network, only local detection has the Job Detail button available. • Mark the URL as False Positive: If marked, the URL will be removed from future URL packages. If the unit is joining a global threat information sharing network, the change is also reported to the *Collector* and is shared by all units in the network. A new package will generate after removing the entry. • Detected: The time and date that the item was detected. • URL: The URL in the package. • Rating: The risk rating of the downloaded file.

	• Serial Number: From which unit the threat information is from. • Global/Local: If this threat information is from a local unit, or from another unit.
Download URL	Download a text file which contains URLs in the package.

This page displays the following:

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

FortiSandbox only keeps URL packages generated in last 7 days.

TCP RST package

Go to *Scan Policy and Object* > *TCP RST Package* to view the FortiSandbox Sniffer TCP RST list.

The following options are available:

Refresh	Refresh the TCP RST Package list.
View	Select a package version number and click the *View* button from the toolbar. The following information is displayed: • **Job Detail**: View the downloaded file's detailed information. • **Remove from TCP RST package**: If marked, the URL will be removed from future TCP RST packages. • **Detected**: The date and time that the item was detected. • **Host/IP**: From where the URL is from. • **URL**: The URL in the package. • **Rating**: The risk rating of the downloaded file.
Package Options	Configure how the packages are generated.
Download Blocklist	Download the *FSA Detected Blocklist* or *Custom Blocklist*.

Upload Custom Blocklist	Upload a user-defined blocklist to FortiSandbox.
	File requirements:
	• Text files are supported
	• One URL per line
	• URLs, IPs and domains are supported
	Example:
	`http://www.example.com`
	`www.test.net`

	`http://66.77.88.99`
	`11.22.33.44`
	After the file is uploaded it will overwrite previous versions of the custom blocklist if there are any.
	In an HA Cluster , the custom blocklist will only be synced to a new primary node when failover occurs.

Delete Custom Blocklist	Delete a user-defined blocklist.

The *TCP RST Package* page displays the following information:

Version	The TCP RST package version.
Release Time	The TCP RST package release time.
Total	The total number of URLs inside the package.

To configure a TCP RST package:

1. Go to *Scan Policy and Object* > *TCP RST Package*.
2. Click *Package Options* and configure the following settings.

Includes past 14 day(s) of data	Enter a value between 1-365 days.
Includes job data of the following ratings	Select *Malicious*, *High Risk* or *Medium Risk*.

3. Click *OK*.

Threat Intelligence

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

Malware and URL Package Options

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

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

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

Because of size limitations, the following limits are in effect:

- Malware packages can have a maximum of 100K entries.
- URL package can have a maximum of 1000 entries.

The URL package contains downloaded URLs of detected malware.

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

Include past __ day(s) of data. (1-365 days)	Enter the number of days.
Include the job data of the following ratings	
Malicious	Include malware with malicious ratings.
High Risk	Include downloaded URLs of malware with high risk ratings and URLs sent by FortiMail devices of high risk ratings and whose scan depth is 0.
Medium Risk	Include downloaded URLs of malware with medium risk ratings and URLs sent by FortiMail devices of medium risk ratings and whose scan depth is 0.
Download STIX	Download most recently generated URL STIX IOC package.

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 v2 format. Two types of IOC packages are generated:

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

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

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

```
        <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">File Hash
             Watchlist</indicator:Type>
        <indicator:Observable id="FortiSandbox:Observable-723483db-a3e0-4de0-93cd-
             5bd37b3c4611">
           <cybox:Object id="FortiSandbox:File-3d9e7590-b479-4352-9a11-8fa313cee9f0">
              <cybox:Properties xsi:type="FileObj:FileObjectType">
                 <FileObj:Hashes>
                    <cyboxCommon:Hash>
                       <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-
                            1.0">SHA256</cyboxCommon:Type>
                       <cyboxCommon:Simple_Hash_Value
                            condition="Equals">0696e7ec6646977967f2c6f4dcb641473e76b4d5c9beb6
                            e433e0229c2accec5d</cyboxCommon:Simple_Hash_Value>
                    </cyboxCommon:Hash>
                 </FileObj:Hashes>
              </cybox:Properties>
           </cybox:Object>
        </indicator:Observable>
        <indicator:Indicated_TTP>
           <stixCommon:TTP idref="FortiSandbox:ttp-afa9d28b-9602-4936-8b94-93e29cc8830c"
                xsi:type='ttp:TTPType'/>
        </indicator:Indicated_TTP>
   </stix:Indicator>
</stix:Indicators>
<stix:TTPs>
   <stix:TTP id="FortiSandbox:ttp-afa9d28b-9602-4936-8b94-93e29cc8830c" timestamp="2016-08-
        12T18:25:52.674181+00:00" xsi:type='ttp:TTPType'>
        <ttp:Title>Suspected High Risk - Riskware</ttp:Title>
        <ttp:Behavior>
           <ttp:Malware>
              <ttp:Malware_Instance>
                 <ttp:Type xsi:type="stixVocabs:MalwareTypeVocab-1.0">Exploit Kits</ttp:Type>
                 <ttp:Name>Suspected High Risk - Riskware</ttp:Name>
              </ttp:Malware_Instance>
           </ttp:Malware>
        </ttp:Behavior>
   </stix:TTP>
</stix:TTPs>
</stix:STIX_Package>
```

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

Global Network

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

This feature requires that:

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

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

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

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

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

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

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

Alias	Enter the network Alias name.
Authentication Code	Enter the authentication code for Contributor to join the network.
Contributors	List the units who are in the network.
Local Malware Package Options	These options define how each unit generates local packages after it has threat information. For more information, see Threat Intelligence on page 147.
Local URL Package Options	
Enable Local STIX IOC Package	

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

Collector IP Address	Enter the Collector's IP address.
Alias	Enter the global network Alias name.

Authentication Code	Enter the authentication code to join the network.
Local Malware Package Options	These options define how each unit generates local packages after it has threat information. For more information, see Threat Intelligence on page 147.
Local URL Package Options	
Enable Local STIX IOC Package	
Scan Profile is Managed by Manager	By enabling this option, the unit can choose to allow its scan profile to be managed by the Collector. The Collector will combine all VM types from the Contributors. After you configure a scan profile on the Collector, the configurations will be downloaded by each Contributor. A unit can join global threat network as *Contributor* to allow the *Collector* to control its *Scan Profile*, or it can work as *Collector* to manage *Scan Profile* of all units in the network. Only a standalone unit or primary node in a cluster can join the network.

4. Click *OK* to save the settings.

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

CLI

Use FortiSandbox CLI commands for initial device configuration and troubleshooting. After initial device configuration, use the GUI for most FortiSandbox functions. The GUI has a CLI Console which you can use as a CLI.

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

You can enable SSH and Telnet access on the port1 (administration) interface or any other administrative port set through the CLI command `set admin-port` and access the CLI through SSH or Telnet to troubleshoot the device including RAID related hard disk issues. You can also connect to the CLI through the console port.

To connect to the CLI through the console port:

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

Serial line to connect to	COM1

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

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

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

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

For more information on FortiSandbox CLI commands, see the *FortiSandbox CLI Reference Guide* in the Fortinet Document Library.

System

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

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

Administrator	Configure administrator user accounts.
Admin Profiles	Configure user profiles to define user privileges.
Device Groups	Add devices to a device group and assign it to multiple device users.
Interfaces	Configure the Interface Status, IP Address / Netmask, and Access Rights.
DNS	Configure Primary and Secondary DNS servers.
Static Route	Configure the Destination IP/Mask, Gateway, and Device for a Static Route
LDAP Servers	Configure LDAP Servers.
RADIUS Servers	Configure RADIUS Servers.
Mail Server	Configure the Mail Server.
SNMP	Configure SNMP.
FortiGuard	Configure FortiGuard.
Certificates	Configure CA certificates.
Login Disclaimer	Configure the Login Disclaimer.
Settings	Configure the idle timeout, the GUI language, and whether the left menu is expanded or compact. You can also reset all widgets to their default state.
Job View Settings	Define columns and orders of job result tables.
Event Calendar Settings	Define what kind of events to display in *Event Calendar* page.

Administrators

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

Users with a *Device* Admin Profile under *System* > *Admin Profiles* can only view and edit their own information.

Only the default admin account can see and access that account. Other users cannot see the default admin account in the GUI. Only administrators with *Super Admin* profile can see all scan jobs, while other users can only see their own jobs.

The following options are available:

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

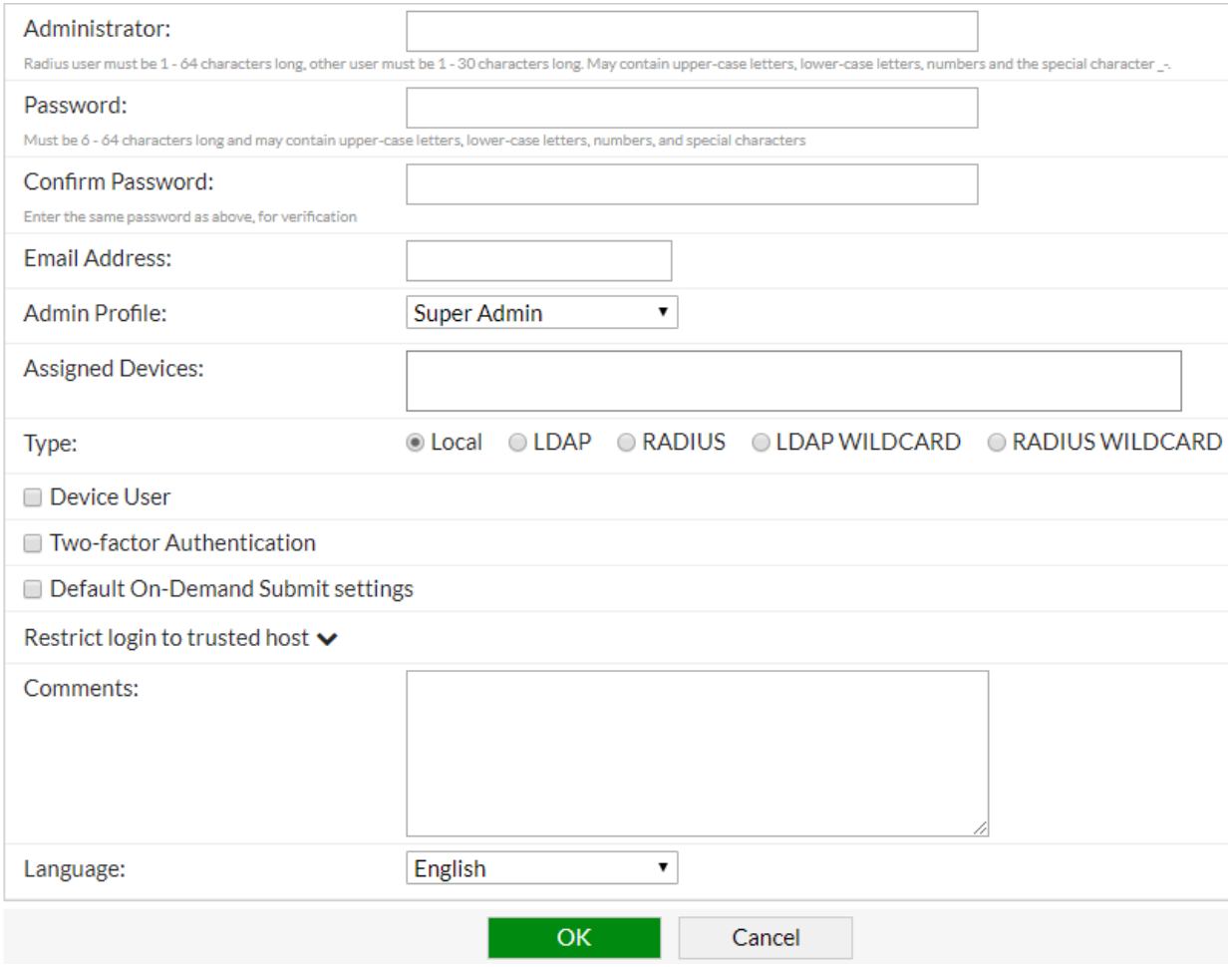
The following information is displayed:

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

To create a new user:

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

2. Click *Create New*.



3. Configure the following and click *OK*.

Administrator	Name of the administrator account. • *Local* and *LDAP*: Name must be 1 - 30 characters and may contain upper/lower-case letters, numbers, periods (.), underscores (-) and hyphens (-). • *RAIDIUS*: Name must be 1 - 64 characters and may contain upper/lower-case letters, numbers, periods (.), underscores (-) and hyphens (-).
Password, Confirm Password	This field is only available when *Type* is *Local*. Password of the account. The password must be 6 to 64 characters using uppercase letters, lowercase letters, numbers, or special characters.
Email Address	Email address for contact information.
Phone Number	Phone number for contact information. Phone number must start with *+1*.
Admin Profile	Select the Admin Profile for the user: *Super Admin*, *Read Only*, or *Device*.

Assigned Devices	Assign devices and/or VDOMs/Protected Domains to the user. This applies if you enable *Device User*. Click in the *Assigned Devices* box to display the *Available Devices* panel which lists all available devices and VDOMs/Protected Domains. Use this panel to select or add devices.
Type	Select administrator type.
LDAP	When *Type* is *LDAP*, select the *LDAP Server*. For more information, see LDAP Servers on page 172.
RADIUS	When *Type* is *RADIUS*, select the *RADIUS Server*. For more information, see RADIUS Servers on page 174.
LDAP WILDCARD	When *Type* is *LDAP WILDCARD*, select the *LDAP Server*. The *Administrator* is *LDAP_WILDCARD* and cannot be edited. For more information, see Wildcard Admin Authentication on page 162.
RADIUS WILDCARD	When *Type* is *RADIUS WILDCARD*, select the *Radius Server*. The *Administrator* is *RADIUS_WILDCARD* and cannot be edited. For more information, see Wildcard Admin Authentication on page 162.
Device User	Enable this option to assign devices to the user. When the user logs in, only jobs belonging to the assigned devices or VDOMs/Protected Domains are visible. You can create device groups in *System* > *Device Groups* and then assign them to a device user. You can also assign devices on the fly by selecting *self assigned* in the *Device Group* dropdown list.
Two-factor Authentication	When administrator *Type* is *Local*, you can use two-factor authentication. Select an *Authentication Type* of *Email*, *SMS*, or *FTM* (FortiTokenMobile). Two-factor Authentication is only available for FortiSandbox appliances, and FSA-VM0T when FortiToken Cloud service purchased.
Default On-Demand Submit settings	This option is available to administrators whose *Administrator Profile* > *Scan Job* has *Read Write* access. Use this option to set the default settings in *Scan Job* > *File On-Demand* and *URL On-Demand*. Each administrator can have their own default settings. For information on these settings, see File On-Demand on page 89 and URL On-Demand on page 93.
Restrict login to trusted host	Expand to configure trusted hosts.
Trusted Host #1 **Trusted Host #2** **Trusted Host #3**	Enter up to 50 IPv4 trusted hosts. Only users from trusted hosts can access FortiSandbox.
Trusted IPv6 Host #1 **Trusted IPv6 Host #2**	Enter up to 50 IPv6 trusted hosts. Only users from trusted hosts can access FortiSandbox.

Trusted IPv6 Host #3	
Comments	Optional description comment for the administrator account.
Language	GUI language for the user: *English*, *Japanese*, or *French*.

Setting trusted hosts for administrators limits which computers an administrator can log into from FortiSandbox. When you configure a trusted host, FortiSandbox only accepts the administrator's login from the configured IP address or subnet. Any attempt to log in with the same credentials from any other IP address or any other subnet are dropped.

To edit a user account:

1. Login as an user whose Admin Profile has *Read/Write* privileges under *System* > *Admin Profiles*, and go to *System* > *Administrators*.
2. Select the user you want to edit and click *Edit*.
   Only the *admin* account can edit its own settings.
   When editing the *admin* account, you must enter the old password before you can set a new password.
3. Edit the account and then retype the new password in the confirmation field.
4. Click *OK*.

To test LDAP/RADIUS user login:

1. Login as an user whose Admin Profile has *Read/Write* privileges under *System* > *Admin Profiles*, and go to *System* > *Administrators*.
2. Select an LDAP/RADIUS user to test.
3. Click *Test Login*.
4. In the dialog box, enter the user's password.
5. Click *OK*.
   If an error occurs, a detailed debug message appears.

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

Admin Profiles

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

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

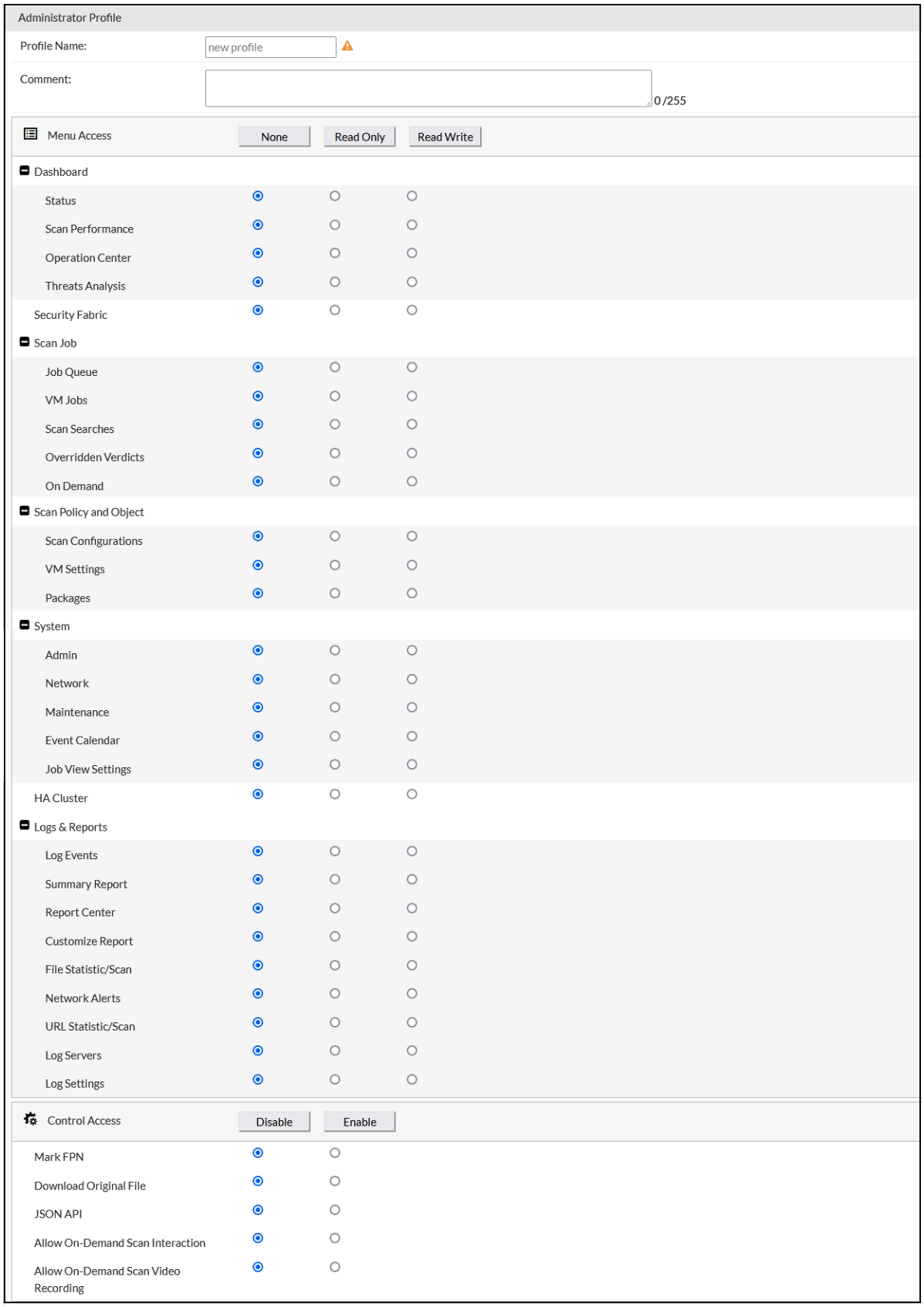
- *Super Admin*: All functionalities are accessible.
- *Read Only*: Can view certain pages but cannot change any system setting.
- *Device*: Can view certain pages about assigned devices, but cannot change any system setting.

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

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

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

Fortinet Ex. 2003 - Page 159 of 245


Administrator Profile
Profile Name:
new profile
Comment:
0/255
Menu Access
None
Read Only
Read Write
Dashboard
Status
Scan Performance
Operation Center
Threats Analysis
Security Fabric
Scan Job
Job Queue
VM Jobs
Scan Searches
Overridden Verdicts
On Demand
Scan Policy and Object
Scan Configurations
VM Settings
Packages
System
Admin
Network
Maintenance
Event Calendar
Job View Settings
HA Cluster
Logs & Reports
Log Events
Summary Report
Report Center
Customize Report
File Statistic/Scan
Network Alerts
URL Statistic/Scan
Log Servers
Log Settings
Control Access
Disable
Enable
Mark FPN
Download Original File
JSON API
Allow On-Demand Scan Interaction
Allow On-Demand Scan Video Recording

Menu Access		Description
Dashboard	**Status**	Grant access to *Dashboard* > *Status*.
	Scan Performance	Grant access to *Dashboard* > *Scan Performance*. See Scan Performance (dashboard) on page 37.
	Operation Center	Grant access to *Dashboard* > *Operation Center*. See Operation Center on page 38
	Threats Analysis	Grant access to *Dashboard* > *Threats by Topology, Threats by Hosts, Threats by Files, Threats by Device*.
Security Fabric		Grant access to *Security Fabric* > *Device, FortiClient, Adapter, Network Share, Quarantine, Sniffer, FortiNDR*. See Security Fabric on page 50.
Scan Job	**Job Queue**	Grant access to *Scan Job* > *Job Queue*. See Job Queue on page 84.
	VM Jobs	Grant access to *Scan Job* > *VM Jobs*. See VM Jobs on page 85.
	Scan Searches	Grant access to *Scan Job* > *File Job Search, URL Job Search*. See File Job Search on page 86 and URL Job Search on page 87.
	Overridden Verdicts	Grant access to *Scan Job* > *Overridden Verdicts*. See Overridden Verdicts on page 88.
	On Demand	Grant access to *Scan Job* > *File On-Demand, URL On-Demand*. See File On-Demand on page 89 andURL On-Demand on page 93.
Scan Policy and Object	**Scan Configurations**	Grant access to *Scan Policy and Object* > *Scan Profile, General Settings, Job Priority, Job Archive, Allowlist/Blocklist, Web Category, Customized Rating, Yara Rules, Threat Intelligence, Global Network*. See Scan Policy and Object on page 105.
	VM Settings	Grant access to *Scan Policy and Object* > *VM Settings*. See VM Settings on page 116
	Packages	Grant access to *Scan Policy and Object* > *Malware Package, URL Package, TCP RST Package*. See Malware Package on page 144, URL Package on page 145, and TCP RST package on page 146.
System	**Admin**	Grant access to *System* > *Administrator, Admin Profile, Device Group, LDAP Servers, RADIUS servers, Certificates* . See Administrators on page 154 and Admin Profiles on page 158.
	Network	Grant access to *System* > *Interfaces, DNS, Static Route*.
	Maintenance	Grant access to *System* > *Mail Servers, FortiGuard, Login Disclaimer, SNMP, System Recovery, Settings*.
	Event Calendar	Grant access to *System* > *Event Calendar, Event Calendar Settings*. See Event Calendar on page 188
	Job View Settings	Grant access to *System* > *Job View Settings*. See Job View Settings on page 189.

Menu Access		Description
HA Cluster		Grant access to the *HA-Cluster* settings. See HA-Cluster on page 193.
Logs & Reports	**Log Events**	Grant access to *Log & Report* > *Events* > *All Events, System Events, VM Events, Job Events, Notification Events*. See Log Categories on page 213
	Summary Report	Grant access to *Log & Report* > *Summary Report*. See Summary Reports on page 217.
	Report Center	Grant access to *Log & Report* > *Report Center*. See Report Center on page 218.
	Customize Report	Grant access to *Log & Report* > *Customize Report*. See Customize Report on page 219.
	File Statistic/Scan	Grant access to *Log & Report* > *File Statistics*, *File Scan*. See File Statistics on page 222 and File Scan on page 220.
	Network Alerts	Grant access to *Log & Report* > *Network Alerts*. See Network Alerts on page 227.
	URL Statistic/Scan	Grant access to *Log & Report* > *URL Statistic, URL Scan*. See URL Scan on page 224.
	Log Servers	Grant access to *Log & Report* > *Log Servers*. See Log Servers on page 231.
	Log Settings	Grant access to *Log & Report* > *Log Settings*. See Local Log on page 232
Control Access		Click to Disable or Enable all the *Control Access* settings.
Mark FPN		Allow the profile to override a false positive or negative.
Download Original File		Enable to download the original file from the *Job Detail* page. See FortiGuard on page 178.
JSON API		Grant the profile JSON API privileges.
Allow On-Demand Scan Interaction		Enable to use *VM interaction* during the On-Demand scan or take scan snapshots in the *VM Status* page.
Allow On-Demand Scan Video Recording		Allow the profile to take a video during the On-Demand scan and watch it later in the On-Demand page.

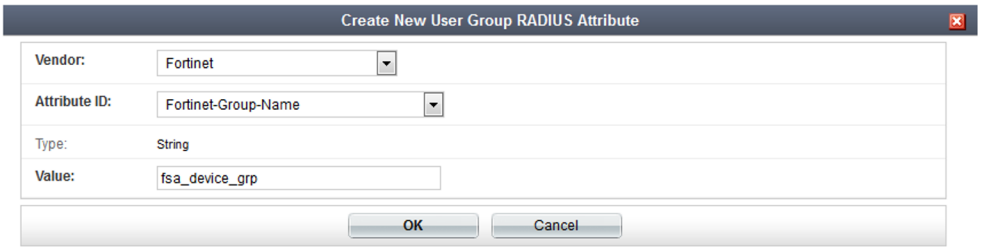
Wildcard Admin Authentication

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

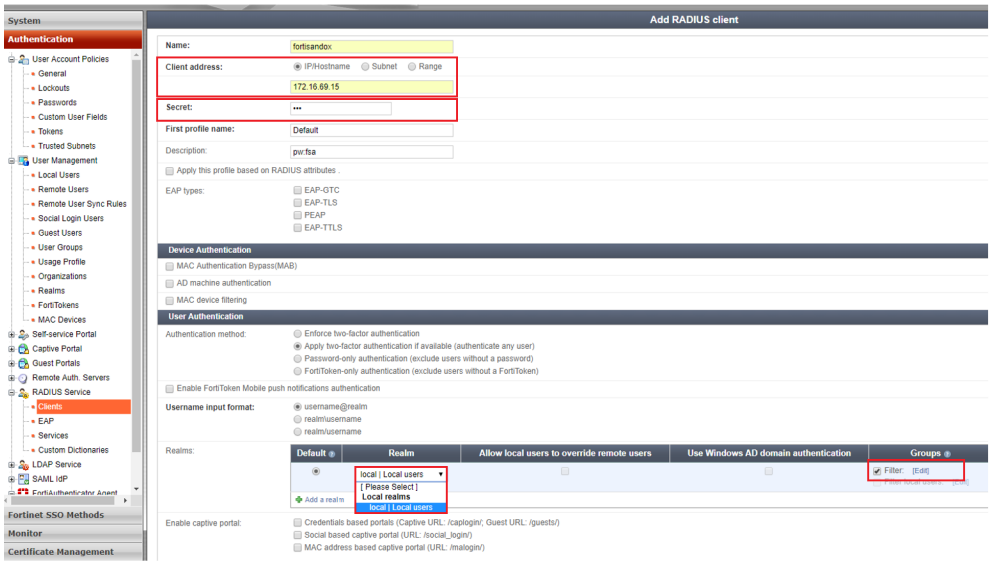
To add accounts on a RADIUS server:

This example uses FortiAuthenticator as the RADIUS server.

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



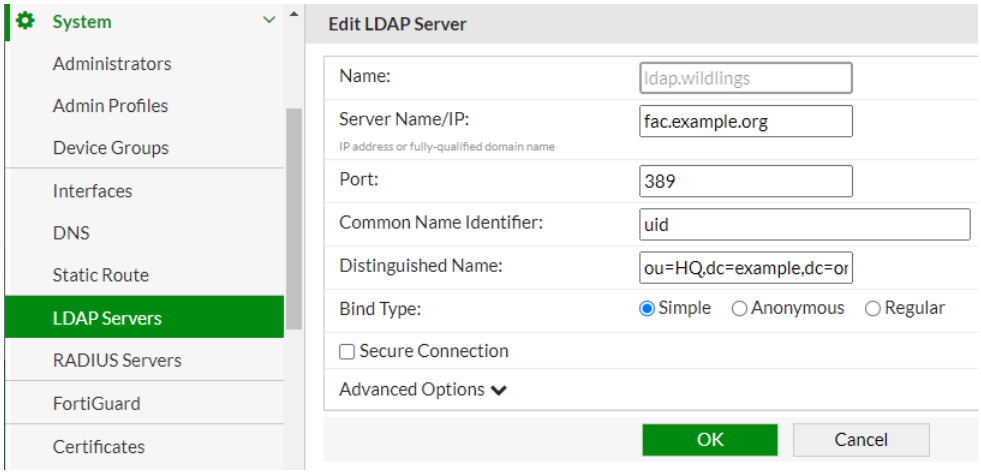
3. Create a new RADIUS service client.
   a. Set the client address as the FortiSandbox IP address.
   b. Enter the secret key in the *Secret* field.
   c. Configure profiles and add the user groups whose users will log into the FortiSandbox.



4. On FortiSandbox, set up the RADIUS server in *System* > *RADIUS Servers*.
   See RADIUS Servers on page 174.
5. Create a new administrator in *System* > *Administrators*.
   a. Select *RADIUS WILDCARD* as the type.
   b. Select the *RADIUS Server* created in the previous step.
   c. The administrator name is RADIUS_WILDCARD and it cannot be changed. The administrator can be a device user, however, the assigned device group will be overridden if the RADIUS user group has defined the *Attribute ID* as *Fortinet-Group-Name*.

To add accounts on an LDAP server:

1. On the FortiSandbox, set up the LDAP server in *System* > *LDAP Servers*.
   See LDAP Servers on page 172.
   In this example, all users from OU=HQ under the LDAP tree dc=example, dc=org will be able to log into FortiSandbox.



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

Device Groups

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

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

To create a device group:

1. Go to *System* > *Device Groups* and click *Create New*.
2. Enter a group name.
3. Enter a comment to identify this device group if required.
4. Select the devices to be included in the device group.
5. Click *Save*.
   The device group is now available to select when modifying or creating a new administrator with device user privileges enabled.

Device groups are also used in LDAP/RADIUS wildcard authentication.
See Wildcard Admin Authentication on page 162.

Interfaces

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

This page displays the following information and options:

Interface	The interface name and description, where applicable. The failover IP includes the description: *(cluster external port)*.
port1 (administration port)	port1 is hard-coded as the administration interface. You can enable or disable HTTP, SSH, or Telnet access rights on port1. HTTPS is enabled by default. You can use port1 for Device mode, although a different, dedicated port is recommended.
port2	You can use port2 for Sniffer mode, Device mode, or inter-node communication within a cluster.
port3 (VM outgoing interface)	port3 is reserved for outgoing communication triggered by the execution of the files under analysis. FortiSandbox uses port3 to allow scanned files to access the Internet. The Internet visiting behavior is an important factor to determine if a file is malicious. As malicious files are infectious, ensure that the connection for port3 is isolated but can also access the Internet. Do not allow this connection to belong to or be able to access any internal subnet that needs to be protected. Fortinet recommends placing this interface on an isolated network behind a firewall. FortiSandbox VM accesses external networks through port3. Configure the next hop gateway and DNS settings in *Scan Policy and Object* > *General Settings* > *Allow Virtual Machines to access external network through outgoing port3*. This allows files running inside VMs to access the external network. One special type of outgoing communication from a guest VM is to connect to the Microsoft activation server to activate the Windows Sandbox VM product keys. Office licenses are verified through VM machines so internet access via port3 is required to contact Microsoft for license activation. If the VM cannot access the outside network, a simulated network (SIMNET) starts by default. SIMNET provides responses to popular network services like `http` where some malware is expected. If the VM internet access is down, the SIMNET status is displayed beside the down icon. Click that icon to go to the VM network configuration page. SIMNET is not a real internet. This can affect catch rate. Do not use an IP address from the production IP pool for the IP assignment on port3 because it might get put on the blocklist.

port4	You can use port4 for Sniffer mode, Device mode, or inter-node communication within a cluster.
port5/port6	You can use port5 and port6 for Sniffer mode, Device mode, or inter-node communication within a cluster. On FortiSandbox 2000E and 3000E devices, port5 and port6 are 10G fiber ports. We recommend using these ports on a primary or secondary node as communications ports with cluster workers.
port7/port8	You can use port7 and port8 for Sniffer mode, Device mode, or inter-node communication within a cluster.
IPv4	IPv4 IP address and subnet mask of the interface.
IPv6	IPv6 IP address and subnet mask of the interface.
Interface Status	State of the interface: • Interface is up • Interface is down • Interface is being used by sniffer
Link Status	Link status: • Link up • Link down
Access Rights	Access rights associated with the interface. HTTPS is enabled by default on port1 and any other administrative port set by the CLI command `set admin-port`. You can select to enable HTTP, SSH, and Telnet access on the administrative port.
PCAP	Click the PCAP icon to sniff the traffic of an interface for up to 60 seconds. Click *Capture & Download* to download the PCAP file as a zip file. Maximum file size is 100MB file size. You can define the tcpdump filter such as host 172.10.1.1 or TCP port 443. You can only run one capture at a time for each port. Sniffing ports are combined and treated as a single port.
Create New	Create an interface.
Edit	Edit the selected interface.

For more, see Port and access control information on page 22.

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

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

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

Edit an interface

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

To edit an IPv4 or IPv6 address:

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

Edit administrative access

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

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

To edit administrative access:

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

Create an aggregate interface

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

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

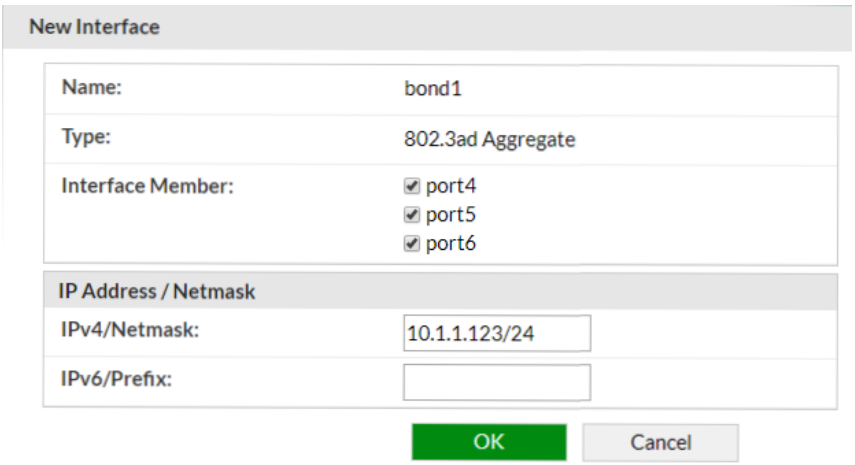
A network interface must meet all the following conditions to be added to an aggregate interface:

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

To create an aggregate interface:

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

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



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

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

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

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

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

```
set admin-port bond1
```

System > *Interfaces* shows that *bond1* has the same access rights as *port1*.
When you change the *port1* access rights, the *bond1* access right is automatically synchronized.

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

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

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

Additional information

- LACP supports static mode only.
- There is no CLI command to create or delete the LACP 802.3ad interface.
- The bond interface does not support PCAP.
- You cannot delete an admin LACP bond.
- You cannot add a new interface to an existing bond.
- You cannot remove an interface member from an existing bond.
- For FortiSandbox VM, including KVM, Hyper-V, AWS, and Azure, implement the LACP support on the virtual server first, then create the aggregate interface.

Failover IP

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

The primary and secondary node local IP will be kept locally during failover.

Example:

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

```
> show
Configured parameters:
Port 1 IPv4 IP: 172.16.69.145/24 MAC: 14:18:77:52:37:72
Port 1 IPv6 IP: 2620:101:9005:69::145/64 MAC: 14:18:77:52:37:72
Port 2 IPv4 IP: 1.1.7.5/24 MAC: 14:18:77:52:37:73
Port 3 IPv4 IP: 192.168.199.145/24 MAC: 14:18:77:52:37:74
IPv4 Default Gateway: 172.16.69.1
> hc-settings -sc -tM -n145 -cdemo-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: FSA3KE3R17000243
Type: Master
Name: 145
HC-Name: demo-cluster
Authentication Code: 1234
Interface: port2
Cluster Interfaces:
port1: 172.16.69.160/255.255.255.0
```

Create an API Interface

You can create an interface that only allows API access through HTTPS port.

Before you create the API interface, be aware that you cannot:

- Set or unset API port with the GUI (CLI only)
- Login to to the API port with the GUI (access will be denied)
- View the api-port in Sniffer settings
- Access the API port through HTTP
- Set the api-port interface as an admin port or HA port
- Set admin-port, port3, sniffer port, or HA port as an api-port

To display the API information with the CLI:

```
show
```

Example

```
IPv4 Default Gateway: 10.59.4.1
Administration interface(s): port1 bond1                                    API
interface(s): port2
```

To add an API port with the CLI:

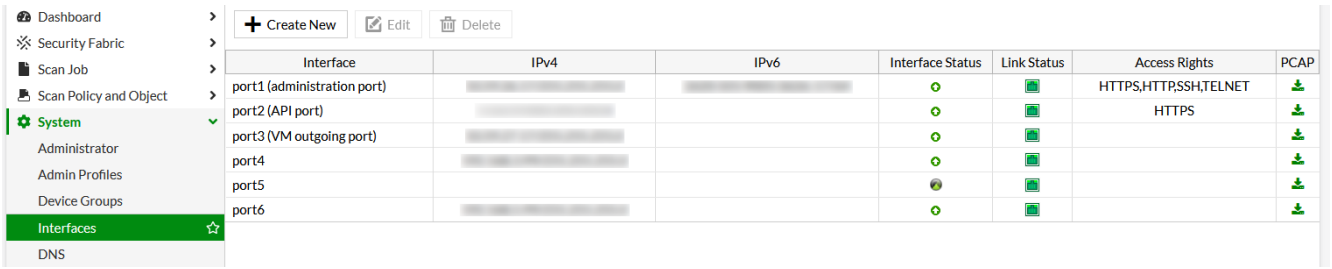
```
set api-port port2
```

To unset an API port with the CLI:

```
unset api-port port2
```

To view an API interface in the GUI:

1. Go to *System* > *Interfaces*.
2. In the *Interface* column, the port is appended with *API port*.



DNS Configuration

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

Static Route

Use this page to manage static routes on your FortiSandbox device. Go to *System* > *Static Route* to view the routing list.

The following options are available:

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

The following information is displayed:

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

To create a new static route:

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

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

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

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

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

To edit a static route:

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

To delete a static route or routes:

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

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

LDAP Servers

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

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

The following options are available:

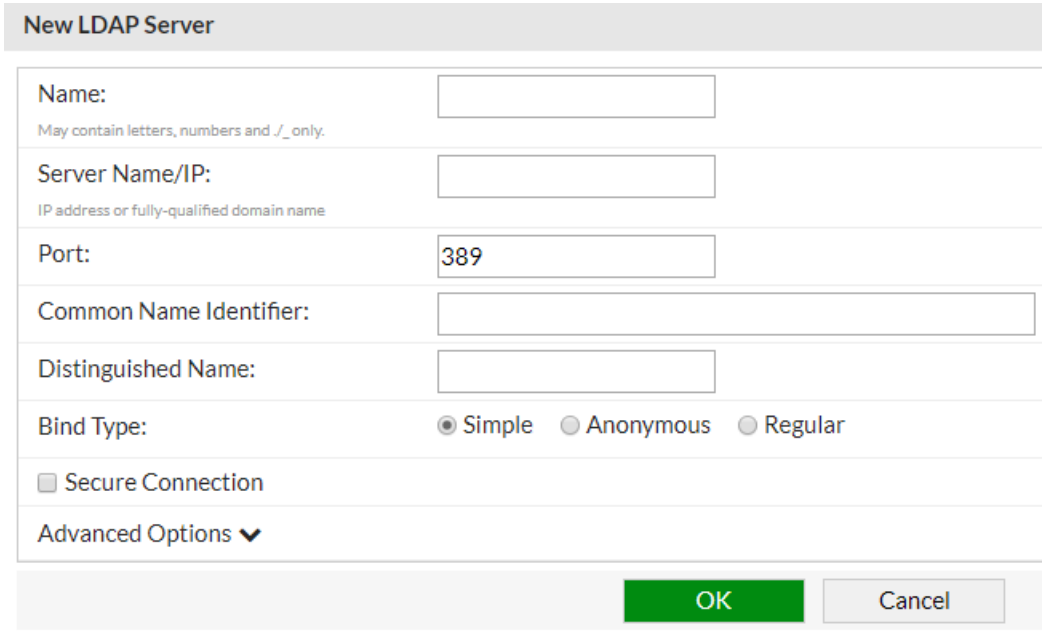
Create New	Add an LDAP server.
Edit	Edit the selected LDAP server.
Delete	Delete the selected LDAP server.

The following information is displayed:

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

To create a new LDAP server:

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



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

Name	LDAP server name. Use a name unique to FortiSandbox.
Server Name/IP	LDAP server IP address or fully qualified domain name.
Port	Port for LDAP traffic. LDAP default port is 389. LDAPS default port is 636.

Common Name Identifier	LDAP common name. Most LDAP servers use `cn`. Some servers use other common name identifiers such as `uid`.
Distinguished Name	LDAP distinguished name used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. For example, you can follow the format `CN=Users,DC=Example,DC=Com`.
Bind Type	LDAP bind type for authentication, including: • Simple • Anonymous • Regular
Username	If *Bind Type* is *Regular*, enter the user distinguished name.
Password	If *Bind Type* is *Regular*, enter the password.
Secure Connection	LDAP connection type.
Protocol	If *Secure Connection* is enabled, select *LDAPS* or *STARTTLS*.
CA Certificate	If *Secure Connection* is enabled, select the CA certificate.
Advanced Options	Expand to configure advanced options.
Attributes	Attributes such as *member*, *uniquemember*, or *memberuid*.
Connect timeout	Connection timeout in milliseconds. Default is 500.
Filter	Filter in the format such as `(&(objectClass=*))`.
Group	Name of the LDAP group. For example, you can follow the format `CN=Group1,DC=Example,DC=Com`.
Memberof-attr	Specify the value for this attribute. This value must match the attribute of the group in LDAP server. All users of the LDAP group with the attribute matching the *memberof-attr* inherit the administrative permissions of the group.
Profile-attr	Specify the attribute for this profile.
Secondary-server	Specify a secondary server for failover in case the primary LDAP server fails. The *Distinguished Name* must be the same.
Tertiary-server	Specify a tertiary server for failover in case the primary and secondary servers fail. The *Distinguished Name* must be the same.

RADIUS Servers

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

If you have configured RADIUS support and require a user to authenticate using a RADIUS server, the FortiSandbox unit contacts the RADIUS server for authentication. To authenticate with the FortiSandbox unit, the user enters a user name and password. The FortiSandbox unit sends this user name and password to the RADIUS server. If the RADIUS server

can authenticate the user, the FortiSandbox unit successfully authenticates the user. If the RADIUS server cannot authenticate the user, the FortiSandbox unit refuses the connection.

The following options are available:

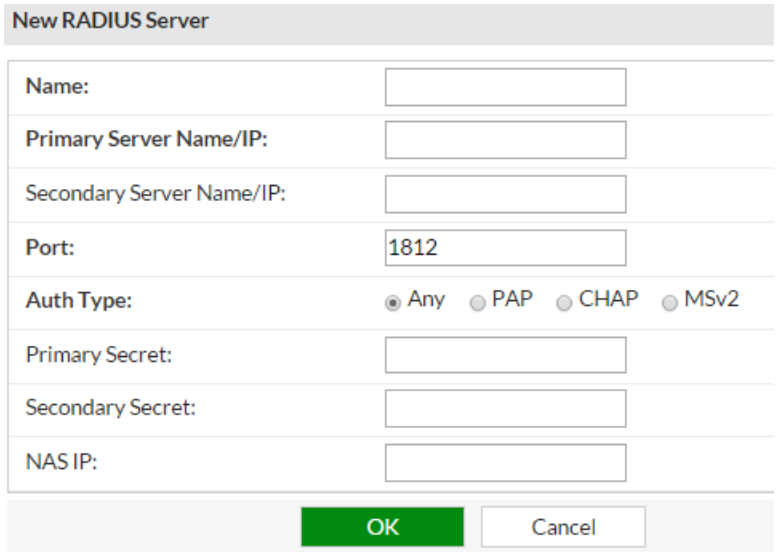
Create New	Select to add a RADIUS server.
Edit	Select a RADIUS server in the list and click *Edit* in the toolbar to edit the entry.
Delete	Select a RADIUS server in the list and click *Delete* in the toolbar to delete the entry.

The following information is displayed:

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

To add a RADIUS server:

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



Fortinet Ex. 2003 - Page 175 of 245

3. Configure the following settings:

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

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

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

Mail Servers

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

The following options are available:

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

Send a notification email to the global email list when Files/URLs with selected rating are detected	Select to enable this feature. When enabled, a notification email is sent to the global email list, individual device, and VDOM/Domain email address when malware is detected.
Global notification mail receivers list (separated by comma)	Enter the email addresses that comprise the global email list.
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*.
Notification mail subject template	Enter the subject line for the notification emails.
Send a notification email to the Device/Domain/VDOM email list when Files/URLs with selected ratings are detected	When a malware from an input device is detected, send a notification email to its admin email address.
What rating of job to send alert email	Select the rating of jobs that will trigger email notification. Options include: *Malicious*, *High Risk*, *Medium Risk*, and *Low Risk*.
Notification mail subject template	Enter the subject line for the notification emails.
Send a notification email to the email list when malicious/suspicious verdict is returned to client device	When enabled, a notification email is sent to an email list when a malicious/suspicious rating is retrieved by a client device.
Use FQDN as unit address for job detail link (default is IP address of Port1)	Use FQDN instead of port1 IP for a job detail link inside alert emails and reports.
FQDN Name	Enter FQDN name.
Send scheduled system resource status report to the email list	When a VM is near the custom threshold, send a usage status email to the admin email address.
System status email receivers list (separated by comma)	Enter the email addresses to get the status email.
Send alert email when:	**CPU Usage >**: Customize threshold of CPU usage. **RAM Usage >**: Customize threshold of RAM usage. **Disk Usage >**: Customize threshold of Disk usage. **Ramdisk Usage**: Customize threshold of VM usage. **Total Pending Jobs**: Customize threshold of total pending jobs. **Average Scan Time**: Customize threshold of average scan time. **System check every (minutes)**: Customize system check schedule. A system status alert email will be sent when any threshold is reached.

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

FortiGuard

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

The following options and information are available:

Module Name	FortiGuard module name such as *AntiVirus Scanner*, *AntiVirus Extreme Signature*, *AntiVirus Active Signature*, *AntiVirus Extended Signature*, *Network Alerts Signature*, *Sandbox System Tools*, *Sandbox Rating Engine*, *Sandbox Tracer Engine*, *Industry Security Signature*, and *Traffic Sniffer*.

	All modules automatically install update packages when they are available on FDN.
Current Version	Current version of the module.
Last Check Time	Date and time that module last checked for an update.
Last Update Time	Date and time that module was last updated.
Last Check Status	Status of the last update attempt.
Upload Package File	Click *Choose File* to select a package file on the management computer, then click *Submit* to upload the package file to FortiSandbox. If the unit has no access to Fortinet FDN servers, go to the Customer Service and Support site to download package files manually.
FortiGuard Server Location	Select FDN servers for package update and Web Filtering query. The default selection is *Nearest* which is the FDN server nearest the unit's time zone. Selecting *US Region* means using only servers in the USA. Selecting *Global* means using global FDN servers via secure connection via HTTPS port 443 to do FDN update.
FortiGuard Server Settings	
Use override FDN server to download module updates	Enable this option to use an override FDN server or FortiManager to download module updates. Enter the override server IP address or FQDN in the text box. Enabling this option disables *FortiGuard Server Location*. Click *Connect FDN Now* to schedule an immediate update check.
Use Proxy	Enable this option to use a proxy. Configure the *Proxy Type* (*HTTP Connect*, *SOCKS v4*, or *SOCKS v5*), *Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
Connect FDN Now	Click *Connect FDN Now* to connect to the FDN server/proxy.
FortiGuard Web Filter Settings	
Secure Connection	FortiSandbox supports secure XOR encrypted connection for FortiGuard web filter settings. When enabled, the system uses secure XOR encrypted mode for the connection.
Use override server for web filtering query	Enable this option to use an override server address for web filtering query using the server IP address or FQDN in the text box. The default is the web filtering server nearest the unit's time zone.
Use Proxy	Enable this option to use a proxy. Configure the *Socks5 Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
VM Image Download Proxy Settings	
Use Proxy	Enable this option to use a proxy. Configure the *Proxy Type* (*HTTP Connect*, *SOCKS v4*, or *SOCKS v5*), *Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
FortiSandbox Community Cloud & Threat Intelligence Settings	

	Use override server for community cloud server query	Enable this option when using FortiManager for FortiGuard upgrades in your environment. When using FortiManager for FortiGuard upgrades, only verdict information is available for malware. The malware's behavior information is not available.
	Use Proxy	Enable this option to use a proxy. Configure the *Socks5 Server Name/IP*, *Port*, *Proxy Username*, and *Proxy Password*.
FortiSandbox WindowsCloud VM Settings		
	Server Regions	This option requires a Windows Cloud VM contract. Select the region where Windows Cloud VMs are used to scan files. You can override the APT server and manually enter the IP address of the APT server which hosts the Windows Cloud VM.

Certificates

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

FortiSandbox does not generate certificates, but does support importing certificates for SSH and HTTPS access to FortiSandbox. The following formats are supported: `.crt` and `.pem`.

The following options are available:

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

The following information is displayed:

Name	The name of the certificate.
Subject	The subject of the certificate.
Status	The certificate status, active or expired.
Service	HTTPS or SSH service that is using this certificate.
Certificate	Download the server certificate.
Sub Certificate	Download the intermediate CA (Certificate Authority) certificate if you are using a certificate chain.
Cacert	Download the CA (Certificate Authority) certificate.

To import a certificate:

1. Go to *System* > *Certificates*.
2. Click *Import* from the toolbar.
3. Enter the certificate name in the text field.
4. Click *Choose File* and locate the certificate and key files on your management computer.
5. Optionally, you can import the intermediate CA certificate by clicking the *Choose File* button for *Sub Certificate*, and locating the intermediate CA certificate file.
6. Click *OK* to import the certificate.

You also have the option to import a Password Protected PKCS12 Certificate. To import a PKCS12 Certificate, check the *PKCS12 Format* box upon importing a new certificate and writing down the possible password. When checking the *PKCS12 Format* box, the other Certificate file selection boxes disappear and are replaced by the *PKCS12 File* selection option because only this type is valid.

To view a certificate:

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

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

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

To download a CA certificate:

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

To delete a CA certificate:

1. Go to *System* > *Certificates*.
2. Select the certificate from the list and click *Delete* from the toolbar.
3. Click *OK* in the *Are You Sure* confirmation page.

Firmware certificate(s) cannot be deleted.

Login Disclaimer

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

If enabled, the Login Disclaimer will appear when a user tries to log into the unit from the GUI or SSH session.

After the message is edited, the SSH daemon needs to restart to display the new message. Users who are logged into FortiSandbox with the SSH client will lose their connection while an admin is editing the Login Disclaimer.

SNMP

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

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

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

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

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

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

Configuring the SNMP agent

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

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

To configure the SNMP agent:

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

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

To create a new SNMP v1/v2c community:

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

3. Configure the following settings:

Enable	Select to enable the SNMP community.
Community Name	Enter a name to identify the SNMP community.
Hosts	The list of hosts that can use the settings in this SNMP community to monitor the FortiSandbox system.
IP/Netmask	Enter the IP address and netmask of the SNMP hosts. Select the *Add* button to add additional hosts.
Queries v1	Enter the port number and select to enable. Enable queries for each SNMP version that the FortiSandbox system uses.
Queries v2c	Enter the port number and select to enable. Enable queries for each SNMP version that the FortiSandbox system uses.
Traps v1	Enter the local port number, remote port number, and select to enable. Enable traps for each SNMP version that the FortiSandbox system uses.
Traps v2c	Enter the local port number, remote port number, and select to enable. Enable traps for each SNMP version that the FortiSandbox system uses.

SNMP Events	Enable the events that will cause the FortiSandbox unit to send SNMP traps to the community.
	• CPU usage is high
	This event is triggered when CPU usage is higher than 90%. The trap is sent every minute.
	• Memory is low
	This event is triggered when memory usage is higher than 90%. The trap is sent every minute.
	• Hard disk usage is high
	This event is triggered when hard disk usage is higher than 80%. The trap is sent every minute.
	• RAID disk information
	The trap message is delivered every hour.
	• Average scan time
	The average scan time is the last hour. The trap is sent every hour.
	• Topology map and health check status for cluster has changed
	• Interface is up or down
	• Power Supply failure (not available on FSA-500F model)
	• Malware is detected
	• License or contract is close to expiry
	This event is triggered 1, 2, 3, 7, 15, and 30 days at 00:00:05 hours before a FortiSandbox license or contract is to expire. For example, an event is triggered:
	  • 30 days at 00:00:05 hours before a VM license is to expire.
	  • 15 days at 00:00:05 hours before a custom VM contract is to expire.

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

To create a new SNMP v3 user:

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

Fortinet Ex. 2003 - Page 185 of 245

3. Configure the following settings:

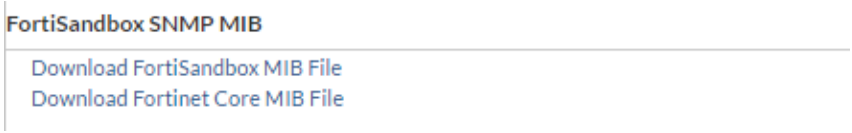
Username	Enter the name of the SNMPv3 user.
Security Level	Select the security level of the user. Select one of the following: • None • Authentication only • Encryption and authentication
Authentication	Authentication is required when *Security Level* is either *Authentication only* or *Encryption and 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 This event is triggered when CPU usage is higher than 90%. The trap is sent every minute. • Memory is low This event is triggered when memory usage is higher than 90%. The trap is sent every minute. • Hard disk usage is high This event is triggered when hard disk usage is higher than 80%. The trap is sent every minute. • RAID disk information The trap message is delivered every hour. • Average scan time The average scan time is the last hour. The trap is sent every hour. • Topology map and health check status for cluster has changed • Interface is up or down • Power Supply failure (not available on FSA-500F model) • Malware is detected

	• License or contract is close to expiry This event is triggered 1, 2, 3, 7, 15, and 30 days at 00:00:05 hours before a FortiSandbox license or contract is to expire. For example, an event is triggered: • 30 days at 00:00:05 hours before a VM license is to expire. • 15 days at 00:00:05 hours before a custom VM contract is to expire.

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

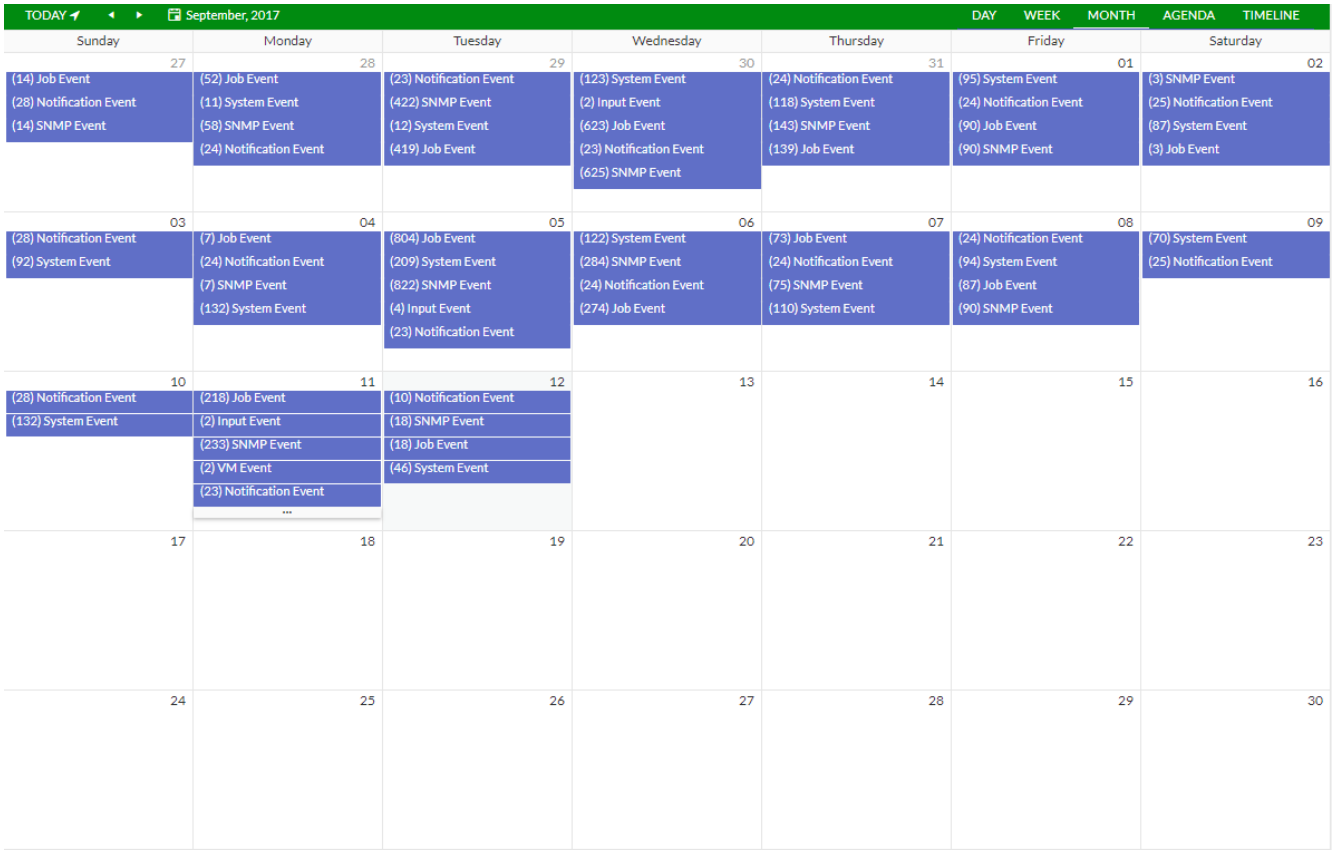
MIB files

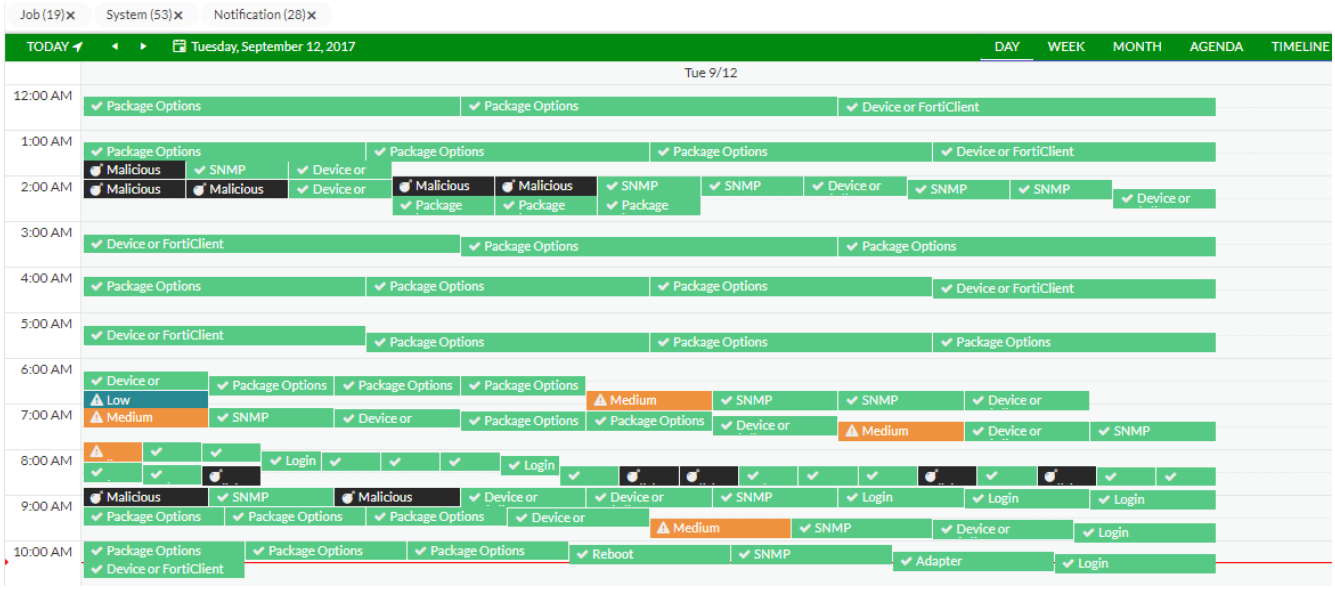
To download MIB files, scroll to the bottom of the SNMP page, and select the MIB file that you would like to download to your management computer.



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.





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.

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

Event Calendar Settings

System > *Event Calendar Settings* allow you to specify which types of events display in *System* > *Event Calendar*. The default displays all available event types.

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

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

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

Job View Settings

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

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

- Pagination
- Infinite Scroll

Job Result pages show job data, including:

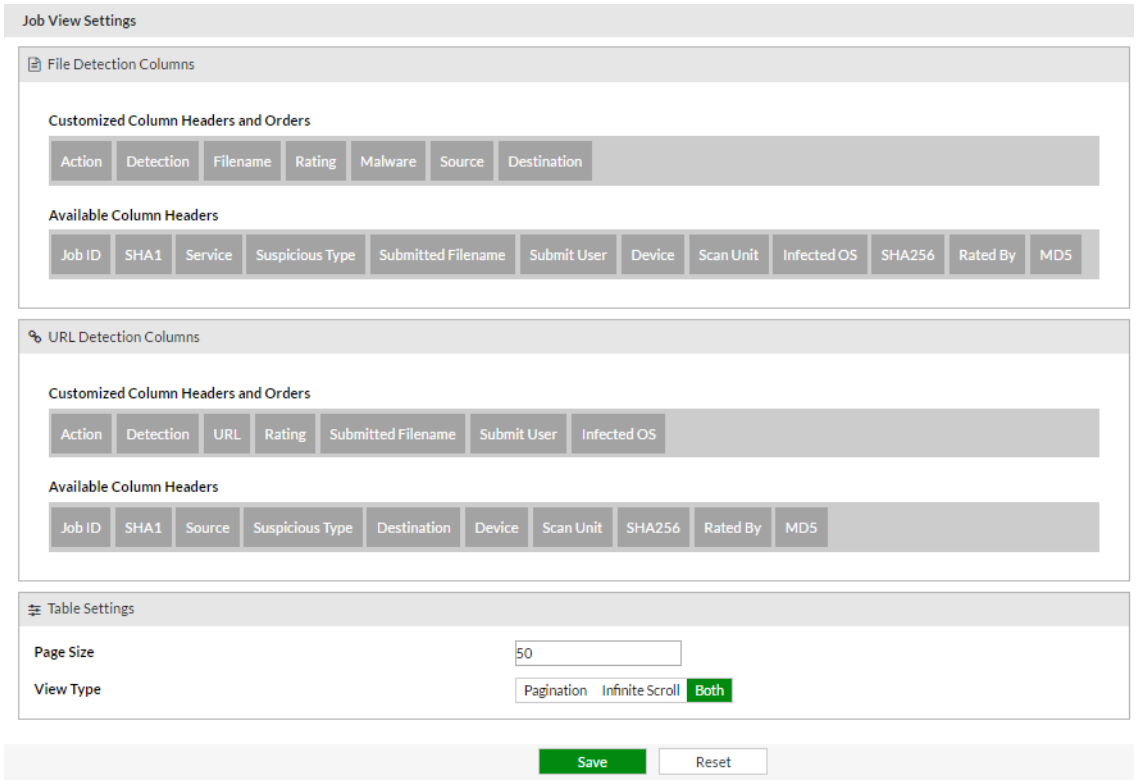
- *Scan Job* > *File Job Search*
- *Scan Job* > *URL Job Search*
- *Log & Report* > *File Scan*
- *Log & Report* > *URL Scan*
- Job links in *Dashboard* > *Status* > *Scan Statistics* widget

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

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

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

You can adjust column width or drag column headers to adjust their order and the change will be saved for future visits. You can also use the *Column Setting* button in the job result page to change settings on the fly and go back to the original page. Column settings are user based, which means different users have their own settings.



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

Action	Extra information, such as showing if a file is an archive file, or if the file is detected through AV Rescan. Users can also view job details or perform a rescan of a Suspicious or Malicious file.
Destination	The IP address of the client that downloaded the file.
Detection	The date and time that the file was detected by FortiSandbox.
Device	The job's input source.
Filename	The file's name.
Infected OS	The OS version of the FortiSandbox VM that was used to make the Suspicious verdict.
Job ID	The ID of the scan job.
Malware	The name of the virus of a Malicious file.
MD5/SHA1/SHA256	The checksum values of the scanned file or URL.
Rated By	The method by which the job is rated, such as the VM Engine.
Rating	The rating of the scan job. It can be one of Malicious, High Risk, Medium Risk, Low Risk, Clean and Unknown.
Scan Unit	The serial number of the FortiSandbox unit which the file is scanned on.
Service	The traffic protocol that file is transferred, such as FTP, HTTP, IMAP, POP3, SMB, OTHER and SMTP.
Source	The IP address of the host where the file was downloaded.
Submitted Filename	The scan job's filename, or a file's parent archive filename, or the submitted filename associated with an On-Demand scan.
Submit User	The user name or IP address who submits the scan file or URL.
Suspicious Type	The malware's type, such Attacker, Riskware or Trojan.
URL	The scanned URL. Only available in URL scan job pages.

Settings

Go to *System* > *Settings* to configure the administrator account settings.

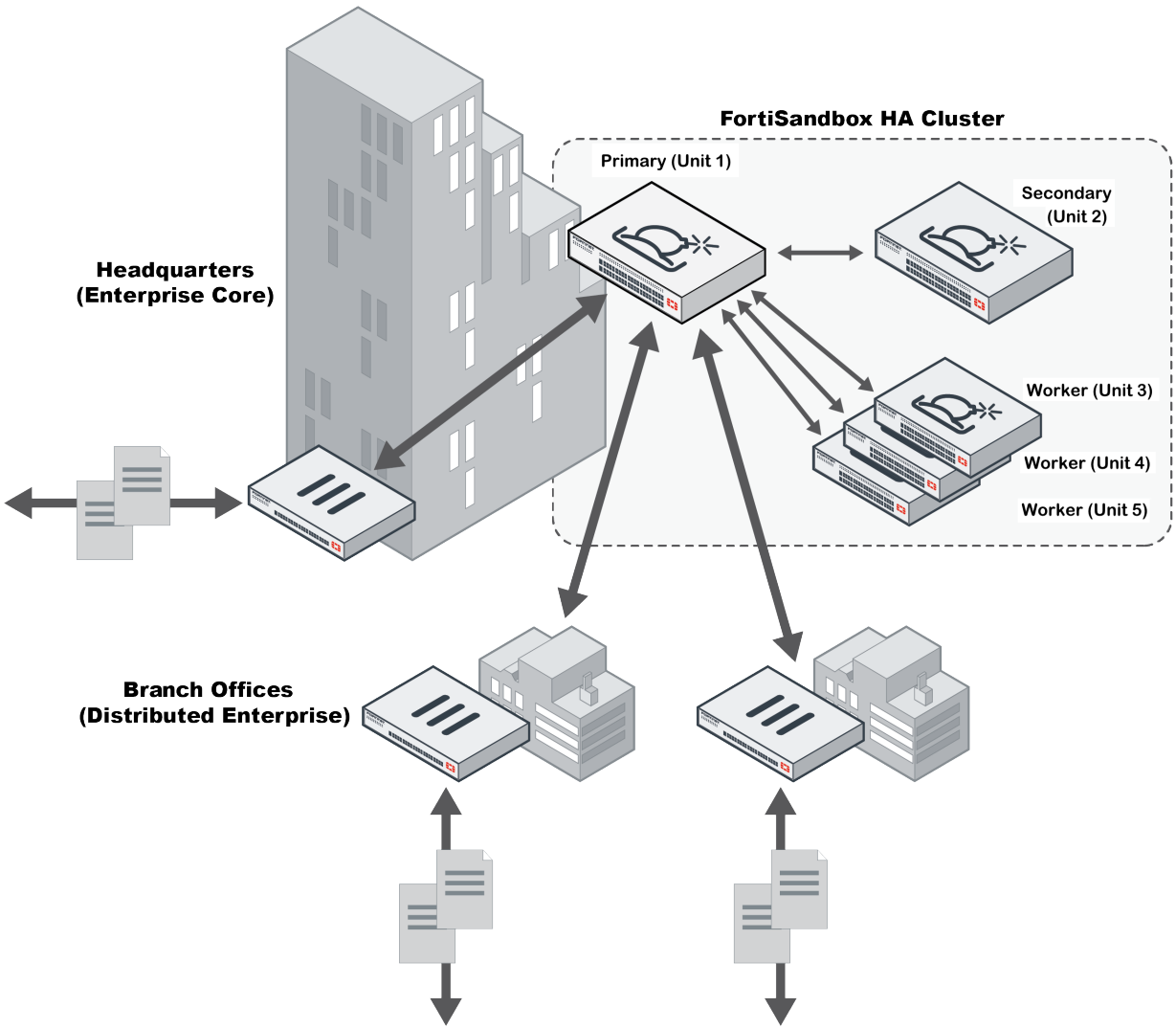
Idle timeout	Length of time before FortiSandbox logs out an inactive user, from 1 to 480 minutes.
Language	Change the GUI language.
Report Saving Days	Length of time to keep reports, from 1 to 28 days.

Show alarms of unprocessed detections in Notifications on Header Bar	Enable this option to show notifications in the top banner. Select the time period and rating of notifications. You must log out and log back in to show notifications. Click the notification to go to *Dashboard* > *Operation Center* to see the details.
Reset all widgets	Reset all widgets in *Dashboard* > *Status*.

HA-Cluster

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

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



Primary	The primary node (Unit 1 in the diagram) manages the cluster, distributes jobs and gathers the results, and interacts with clients. It can also perform normal file scans. All scan-related configuration should be done on the primary node and they will be broadcasted from the primary node to the other nodes. Any scan-related configuration that has been set on a worker node will be overwritten. On the primary node, users can: • Change a worker node's role (secondary and worker)

	• Configure a worker node's network settings • Upgrade worker nodes • View VM Jobs page of worker nodes • Configure FortiGuard settings of worker nodes • Configure VM images of worker nodes, such as setting clone numbers of each VM image • Configure a ping server and/or echo server to frequently check unit's network condition and downgrade itself as a secondary node when necessary to trigger a failover Although all FortiSandbox models can work as a primary node, we recommend using a more powerful model. When the primary and secondary nodes are using a FortiSandbox VM model, you have the option of deploying without VM Clones. See, Deploying primary and secondary nodes without VM Clones on page 202.

Secondary	The secondary node (Unit 2 in the diagram) is for HA support and normal file scans. It monitors the primary node's condition and, if the primary fails, the secondary will assume the role of primary. The former primary will then become a secondary when it is back up.
	To support failover, ensure both the primary and secondary nodes are configured correctly:
	• Both the primary and secondary nodes must be the same model.
	• Both nodes must have the same network interface configuration, including:
	  • The same subnet for port1.
	  • The same subnet for port2.
	  • The same subnet for port3.
	  • The same routing table.
	The secondary node is not required to set up a HA-Cluster but is recommended.
	When the primary and secondary nodes are using a FortiSandbox VM model, you have the option of deploying without VM Clones. See, Deploying primary and secondary nodes without VM Clones on page 202.

Worker	The worker nodes (Units 3–5 in the diagram) perform normal file scans and report results back to the primary and secondary nodes. They can also store detailed job information. Workers should have their own network settings and VM image settings. Workers can be any FortiSandbox model including FortiSandbox VM. Workers in a cluster do not need to be the same model.

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

For heavy job loads, use more powerful FortiSandbox models.

Cluster setup

To save time configuring an HA-Cluster, review cluster pre-requisites. After you have set up the Cluster, you can configure cluster level failover IP for each port except port3 and any ports the sniffer is sniffing. You can also enable *Health Check* to set up a ping server and/or echo server to ensure the network condition between client devices and FortiSandbox is always up.

This section contains the following topics:

- HA-Cluster pre-requisites on page 195
- Example configuration on page 195
- Cluster level failover IP on page 200
- Health Check on page 200
- Using an aggregate interface on page 201

HA-Cluster pre-requisites

- Primary and secondary units are the same model and configuration. We recommend using FortiSandbox 2000E or higher hardware or FortiSandbox VM with SSD drives as primary and secondary nodes in a cluster with multiple worker nodes.
  The worker unit can be a different model and have a different set of Windows VM from the primary or secondary units.
- HA-Cluster requires all nodes to have port1 to be accessible. Nodes use that port to communicate with each other. Port1 is the admin port by default. Other available ports can also be used as the admin port.
- Port3 on all nodes should be connected to the Internet separately.
- All nodes should be on the same firmware build.
- Each node should have a dedicated network port for internal cluster communication.
  Internal cluster communication is encrypted and includes:
  - Job dispatch
  - Job result reply
  - Setting synchronization
  - Cluster topology broadcasting

The system time must be synched on all nodes in the HA cluster. This prevents out-of-sync job results, logs and statistics. It will also prevent the secondary device from becoming the primary device during reboot.

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

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

Example configuration

This example shows the steps for setting up an HA-Cluster using three FortiSandbox units.

Step 1 - Prepare the hardware:

Prepare the following hardware:

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

Put the primary and secondary nodes on different power circuits.

Step 2 - Prepare the subnets:

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

- Switch A: 192.168.1.0/24: For system management.
  - Gateway address: 192.168.1.1
  - External management IP address: 192.168.1.99
- Switch B: 192.168.2.0/24: For internal cluster communications.
- Switch C: 192.168.3.0/24: For the outgoing port (port 3) on each unit.
  - Gateway address: 192.168.3.1
- Switch D: 192.168.4.0/24: For the file submission port (port 4) on the primary and secondary unit.

Step 3 - Setup the physical connections:

1. Connect port 1 of each FortiSandbox device to Switch A.
2. Connect port 2 of each FortiSandbox device to Switch B.
3. Connect port 3 of each FortiSandbox device to Switch C.
4. Connect port 4 of the primary and secondary FortiSandbox device to Switch D.

Step 4 - Configure the primary:

1. Power on the device (Unit A), and log into the CLI (see CLI on page 152).
2. Configure the port IP addresses and gateway address with the following commands:
```
set port1-ip 192.168.1.99/24
set port2-ip 192.168.2.99/24
set port3-ip 192.168.3.99/24
set port4-ip 192.168.4.99/24
set default-gw 192.168.1.1
```
3. Configure the device as the primary node and its cluster failover IP for port1 with the following commands:
```
hc-settings -sc -tM -nPrimaryA -cTestHCsystem -ppassw0rd -iport2
hc-settings -si -iport1 -a192.168.1.98/24
hc-settings -si -iport4 -a192.168.4.98/24
```
4. Review the cluster status with the following command:
```
hc-status -l
```
Other ports on the device can be used for file inputs.

Step 5 - Configure the secondary:

1. Power on the device (Unit B), and log into the CLI.
2. Configure the port IP addresses and gateway address with the following commands:
```
set port1-ip 192.168.1.100/24
set port2-ip 192.168.2.100/24
set port3-ip 192.168.3.100/24
set port4-ip 192.168.4.100/24
set default-gw 192.168.1.1
```
3. Configure the device as the secondary node with the following commands:
```
hc-settings -sc -tP -nSecondaryB -cTestHCsystem -ppassw0rd -iport2
hc-settings -l
hc-worker -a -s192.168.2.99 -ppassw0rd
```
4. Review the cluster status with the following command:
```
hc-status -l
```

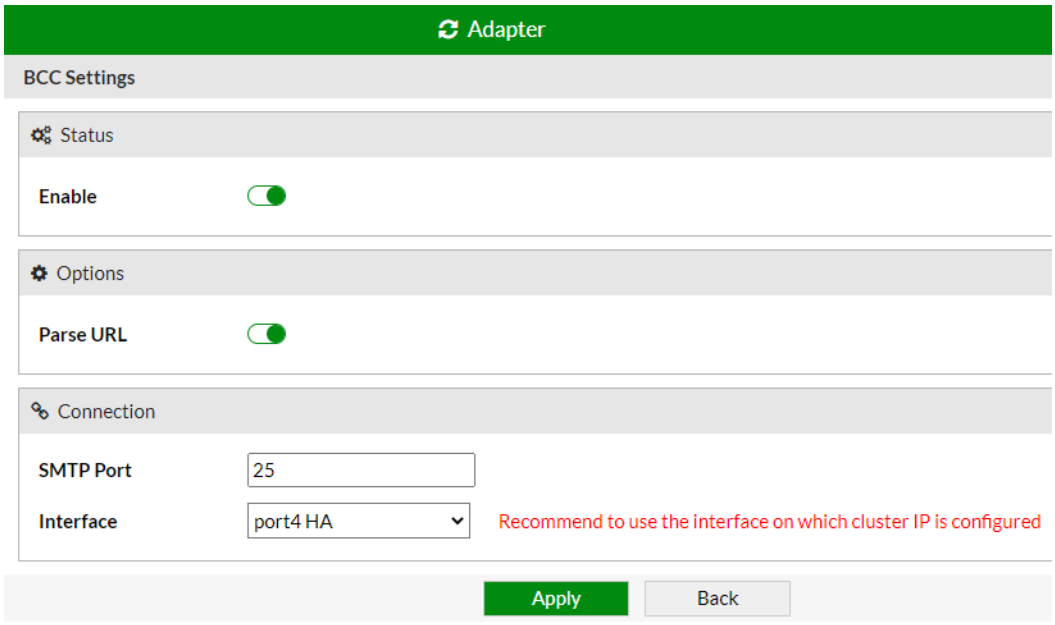
Step 6 - Configure the worker:

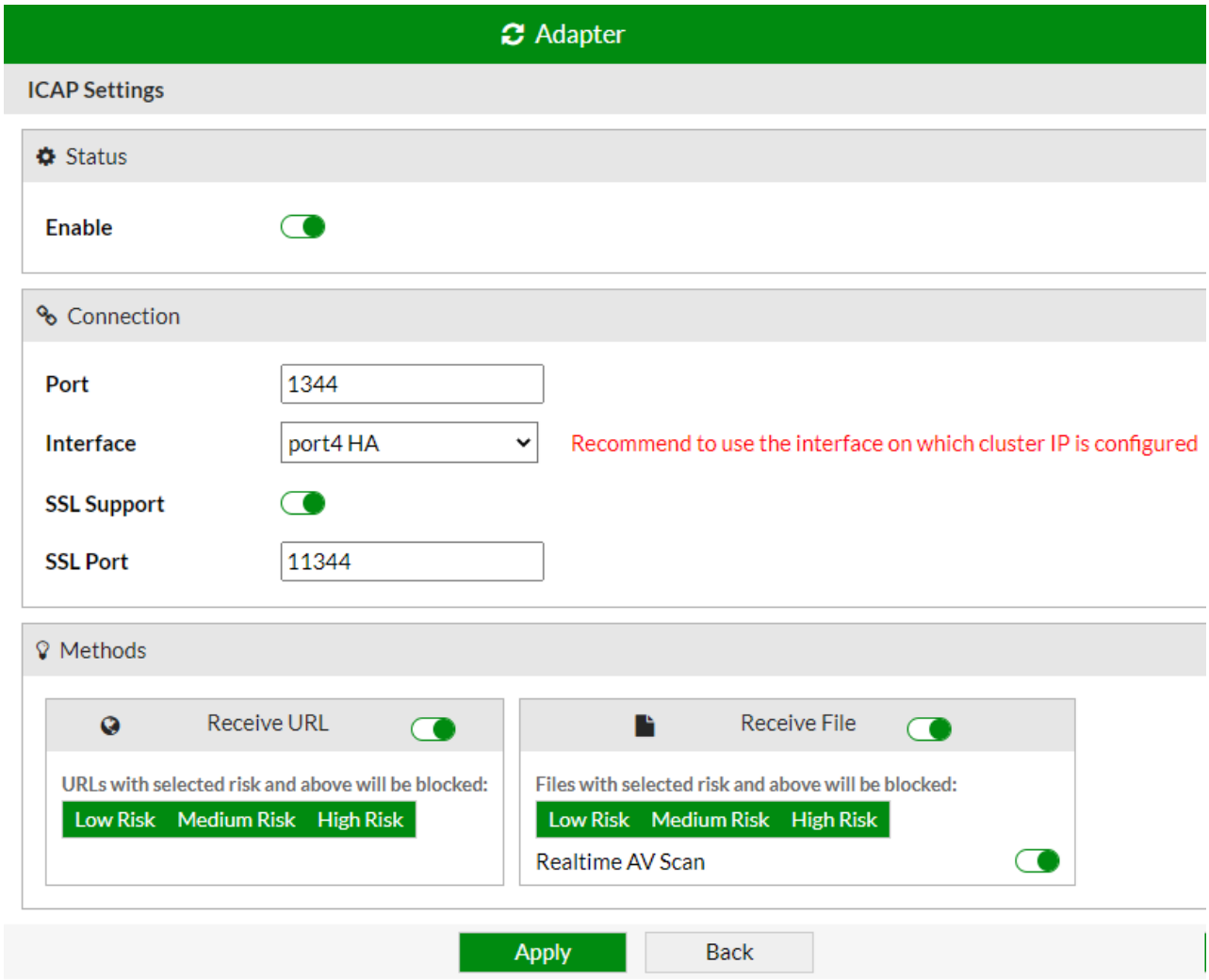
1. Power on the device (Unit C), and log into the CLI.
2. Configure the port IP addresses and gateway address with the following commands:
```
set port1-ip 192.168.1.101/24
set port2-ip 192.168.2.101/24
set port3-ip 192.168.3.101/24
set default-gw 192.168.1.1
```
3. Configure the device as a worker node with the following commands:
```
hc-settings -sc -tR -cTestHCsystem -ppassw0rd -nWorkerC -iport2
hc-settings -l
hc-worker -a -s192.168.2.99 -ppassw0rd
```
4. Review the cluster status with the following command:
```
hc-status -l
```

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

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

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





Step 8 - Configure the following settings on each unit:

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

Scan related settings, such as the scan profile, should be set on primary unit only; they will be synchronized to the worker node. For details, see Primary and worker roles on page 205.

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

If you use the GUI to change a role from worker to standalone, you must remove the worker from the primary using the CLI command `hc-primary -r<serial number>`; then use `hc-status -l` to verify that the worker unit has been removed.

Cluster level failover IP

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

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

Health Check

HA-Cluster > *Health Check* is only available on the primary node. You can use the *Health Check* to set up a ping server and/or echo server to ensure the network condition between client devices and FortiSandbox is always up. If not, the primary node downgrades itself to a secondary node if there is at least one secondary node, a failover occurs after the configured period elapses. If no secondary node exists, the primary node keeps its primary role.

The following options are available:

Create New	Create a new health check ping server and/or echo server.
Edit	Edit a health check ping server and/or echo server.
Delete	Delete a health check ping server and/or echo server.

This page displays the following information:

Interface	The interface port to connect to the ping server and/or echo server. Port3 cannot be used.
Remote Server	IP address or fully-qualified domain name of the remote ping server and/or echo server.
Ping	Enable or disable sending the ping packet to the remote server to ensure the network connection is up.
TCP Echo	Enable or disable sending TCP Echo packet to ensure the network connection to the remote sever is up.
Interval	Time interval in seconds (30-180 seconds) to send a ping or TCP Echo packets.
Failover Threshold	Failover threshold (3-120 times). After a certain number of consecutive missing responses of ping or TCP Echo packets, the primary node will downgrade itself as a secondary if there is an existing secondary node.

To create a new HA Health Check:

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

To edit a HA Health Check:

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

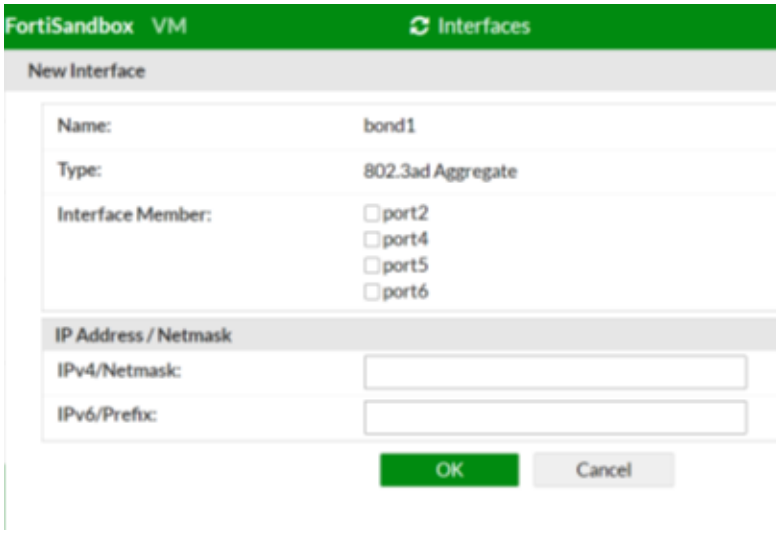
To delete a HA Health Check:

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

Using an aggregate interface

To configure IP addresses on an aggregate interface using the GUI:

1. Go to *System* > *Interfaces* and click *Create New*.



2. Select the *Interface Member*s and set up the IPv4 address and netmask.
3. Click *OK*.
   A new interface called *bond1* is created.

To configure IP addresses on an aggregate interface using the CLI:

1. Use the `show` command to display information about all interfaces.
2. Enter the following command.

```
hc-settings  -si -ibond1 -a<External IP/NetMask>
```

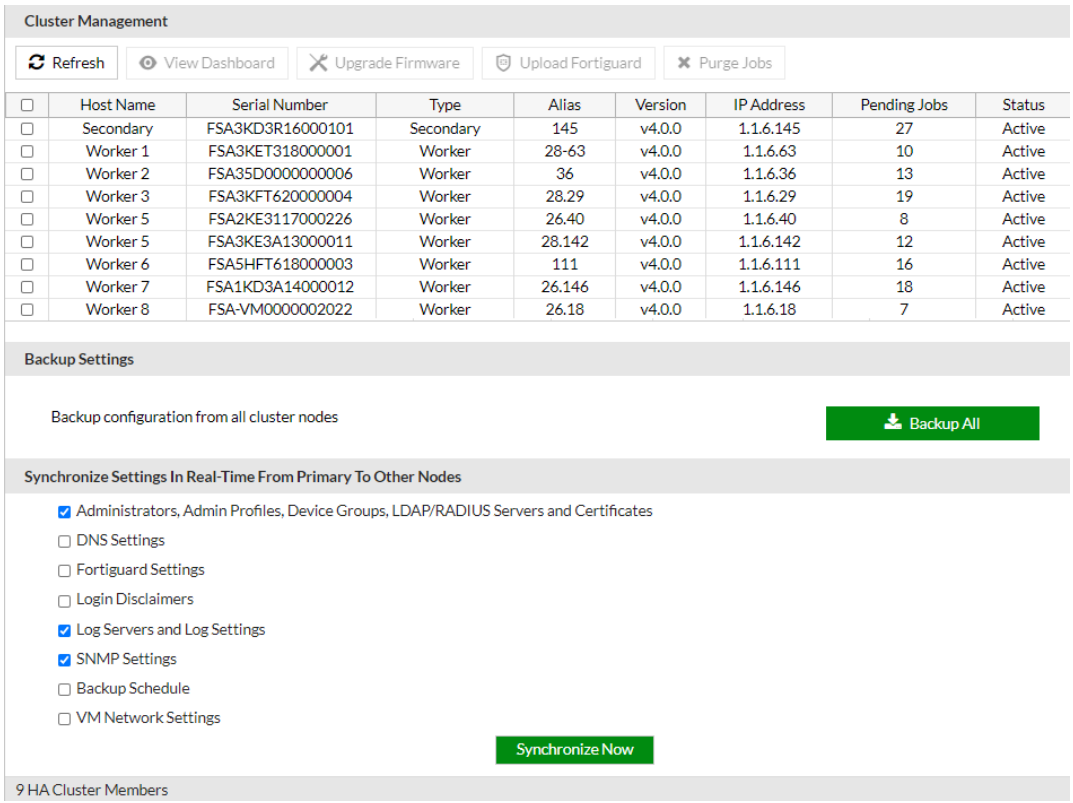
3. Enter the `show` command again to see the new external IP address.
   In the GUI, *System* > *Interfaces* also displays the new external IP address.

Deploying primary and secondary nodes without VM Clones

When the primary and secondary node are using a FortiSandbox VM00 model, you have the option of deploying without VM Clones (i.e. dispatcher). That VM00 deployment dedicates its full VM resources for HA support, receiving incoming files and distribution of files to the worker nodes. There is no scan performed on the VM00. On this type of VM00 deployment, only the *FortiCare Premium Support* subscription is necessary as all the scans are performed on the worker nodes.

Cluster Management

Use *HA-Cluster* > *Cluster Management* to view the basic information of cluster nodes and to manage the cluster.



Host Name	Serial Number	Type	Alias	Version	IP Address	Pending Jobs	Status
Secondary	FSA3KD3R16000101	Secondary	145	v4.0.0	1.1.6.145	27	Active
Worker 1	FSA3KET318000001	Worker	28-63	v4.0.0	1.1.6.63	10	Active
Worker 2	FSA35D0000000006	Worker	36	v4.0.0	1.1.6.36	13	Active
Worker 3	FSA3KFT620000004	Worker	28.29	v4.0.0	1.1.6.29	19	Active
Worker 5	FSA2KE3117000226	Worker	26.40	v4.0.0	1.1.6.40	8	Active
Worker 5	FSA3KE3A13000011	Worker	28.142	v4.0.0	1.1.6.142	12	Active
Worker 6	FSA5HFT618000003	Worker	111	v4.0.0	1.1.6.111	16	Active
Worker 7	FSA1KD3A14000012	Worker	26.146	v4.0.0	1.1.6.146	18	Active
Worker 8	FSA-VM0000002022	Worker	26.18	v4.0.0	1.1.6.18	7	Active

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

The *Cluster Management* section displays all the secondary and worker nodes.

The following information is shown:

Host Name	The host name of the device in the cluster.

Serial Number	The serial number of the device.
Type	The type of the device: *Primary*, *Secondary*, or *Worker*.
Alias	The device's alias.
Version	The software version of the device.
IP Address	The device's internal communication IP address.
Pending Jobs	The number of pending jobs of the device.
Status	The status of the device: *Active* or *Inactive*.

Use the buttons in this section to manage the cluster.

To manage the cluster:

1. Go to *HA-Cluster* > *Cluster Management*.
2. Click Refresh to get the latest cluster information.
   - Select one unit and click *View Dashboard* to display that unit's Dashboard.
   - Select one or more units and click *Upgrade Firmware* to upload a firmware image to upgrade the selected units. The firmware image must be in `.out` or `.deb` format.
   - Select one or more units and click *Upload Fortiguard* to upload a package file to the selected units.
   - Click *Backup All* to back up the configuration file of all cluster units (including the primary unit) to an archive file. The backup archive file is named with the cluster name and the date and time.
   - Select one or more units and click *Purge Jobs* to delete the selected units' pending jobs.
   - If a node is running a different version from the primary node, there is an information icon which tells you that the firmware version is not compatible with the primary node.

Synchronization

Use the *Synchronize Settings In Real-Time From Primary To Other Nodes* section to set synchronization options.

To set cluster synchronization options:

1. Go to *HA-Cluster* > *Cluster Management*.
2. In the *Synchronize Settings In Real-Time From Primary To Other Nodes* section, select what to synchronize with secondary and worker nodes.
3. Click *Synchronize Now*.

Access privilege

To set access privilege for the Cluster Management page:

1. Go to *System* > *Admin Profiles* to the *HA Cluster* section.
2. Set the privilege for *Cluster Management/Status*.
   Read Write privilege allows access to all functions on this page.
   Read Only privilege only displays this page.

Job Summary

HA-Cluster > *Job Summary* shows job statistics data of each node in a cluster. It is only available on the primary node.

To view a HA Job Summary:

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

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

Select a number from the Malicious, Suspicious, Clean, or Other columns to view details about those specific files.

Managing worker nodes

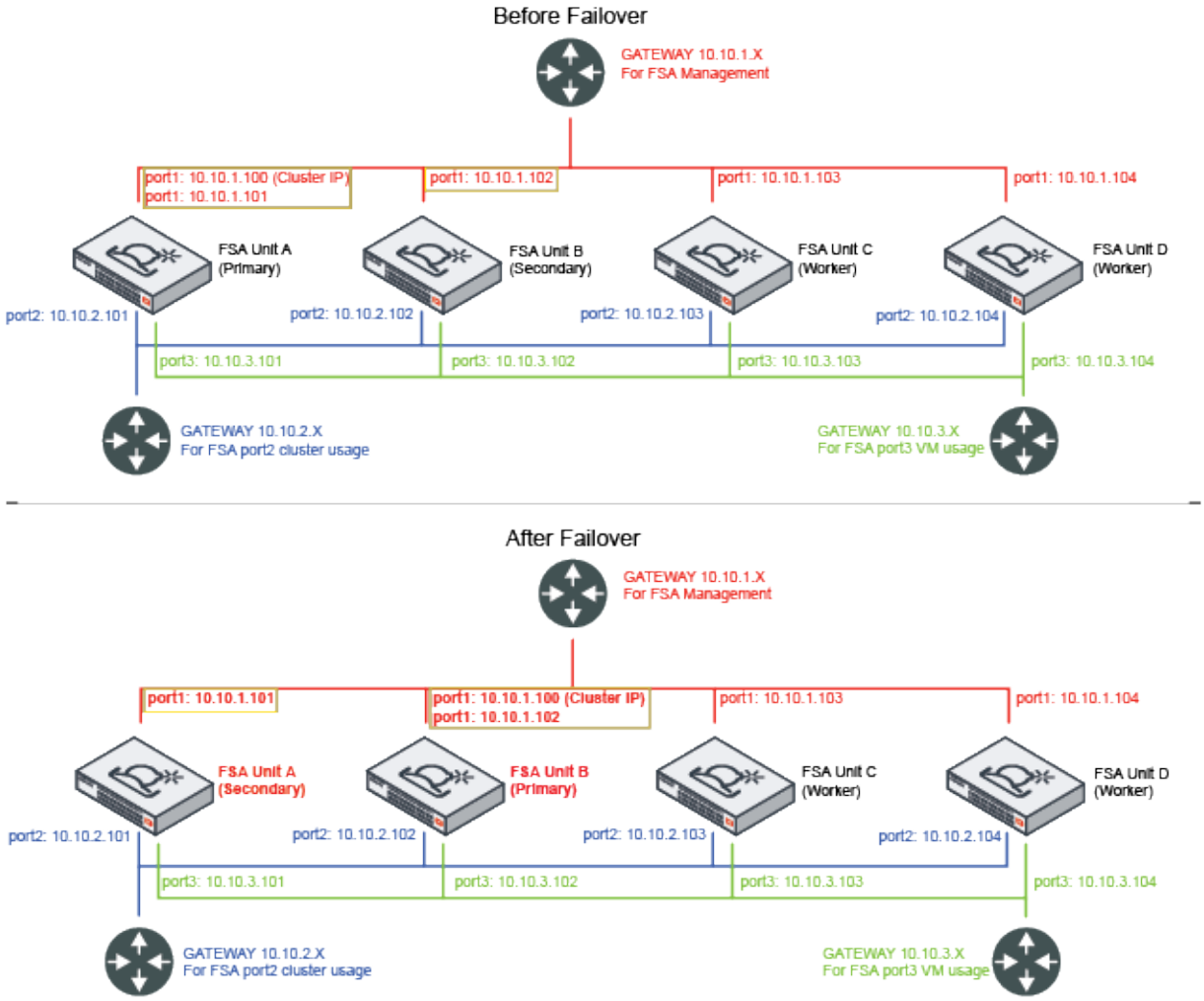
On a primary node, you can select a worker to view and manage information pertaining to that worker. In *Dashboard* > *Status*, the following widgets are displayed: *System Information*, *Scan Statistics*, *System Resources* including *Disk Usage*.

To manage worker nodes on the primary node:

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

HA Roles, Synchronization and Failover

The primary node and secondary node send heartbeats to each other to detect if its peers are alive. If the primary node is not accessible, such as during a reboot, a failover occurs. You can also configure a ping server and/or echo server to regularly check the unit's network condition and downgrade itself to secondary type to trigger a failover. In a failover, the secondary and primary switch roles and the cluster IP addresses change, as indicated by the boxes in the lower image.



In a cluster, there is only one copy of a job, which is in the unit that the primary assigned it to. Jobs that are assigned to the "old" primary will not be scanned in another cluster unit after failover.

Primary and worker roles

On the primary node, all functionality is available based on your licenses and contracts. This includes accepting files from different input sources, sending alert emails, and generating malware packages. Scan profiles should also be

configured on the primary node and will be synchronized to other nodes.

The following table below lists the features and its synchronization settings.

- **Failover** – the related settings are synchronized from primary to secondary during failover.
- **Realtime** – the related settings are synchronized as soon as changes are applied.
- **Realtime*** – the related settings are synchronized in realtime only if configured.

Feature	Secondary	Worker
Dashboard > Status		
Widget settings	Failover	
NTP Server settings	Failover	
Security Fabric		
Device, including FortiClient	Failover	
Adapter	Failover	
Network Share, including network share scans	Failover	
Quarantine	Failover	
Sniffer	Failover	
FortiNDR	Realtime	Realtime
HA-Cluster		
Health Check	Failover	
Scan Job		
Overridden job verdicts	Realtime	Realtime
Scan Policy and Object		
Scan Profile > Pre-Filter	Realtime	Realtime
Scan Profile > Advanced	Realtime	Realtime
General > Allow VMs outbound port3	Realtime*	Realtime*
General > Upload	Failover	
General > Job Archive	Failover	
General > Password/Clean up schedule settings	Realtime	Realtime
Job Queue Priority	Realtime	Realtime
Allowlist/Blocklist	Realtime	Realtime
YARA Rules	Realtime	Realtime
Web Category	Realtime	Realtime
Customized Rating	Realtime	Realtime

Feature		Secondary	Worker
	Global Network settings	Failover	
	Threat Intelligence > Generation Settings	Failover	
System			
	Administrators	Failover/Realtime*	Realtime*
	Device Groups	Failover/Realtime*	Realtime*
	Certificates	Failover/Realtime*	Realtime*
	LDAP Servers and RADIUS Servers	Failover/Realtime*	Realtime*
	Network settings (DNS)	Realtime*	Realtime*
	Mail Server, including Scheduled Report Configuration	Failover	
	SNMP	Failover/Realtime*	Realtime*
	FortiGuard	Realtime*	Realtime*
	Login Disclaimer	Realtime*	Realtime*
	System Recovery	Failover/Realtime*	Realtime*
	Settings	Failover	
	Admin Profiles Failover	Realtime*	Realtime*
Log & Report			
	Log Servers	Realtime*	Realtime*
	Local Log	Realtime*	Realtime*
CLI only configuration			
	AI Mode	Realtime	Realtime
	Device Low-Encryption	Failover	
	Device Authorization	Failover	
	File size limit configuration	Realtime	Realtime
	FortiMail expired timeout	Failover	
	Network settings (proxy and routing tables)	Realtime*	Realtime*
	HA Cluster settings (encryption)	Realtime	Realtime
	OFTPD conserve mode	Failover	
	Primary node scan power	Failover	
	Prescan configuration	Realtime	Realtime
	Remote authentication timeout	Failover	

Feature	Secondary	Worker
TLS version	Realtime	Realtime
Sandboxing embedded URL	Realtime	Realtime
FortiMail Url Recheck	Realtime	Realtime

Although you can assign different VM types to each node in a cluster, we recommend all nodes share the same VM types. VM types are collected from all nodes and are displayed in the primary node's *Scan Profile* > *VM Association* page where VM associations can be configured and synchronized for the entire cluster. If an association for a VM type is missing on the worker node, the sandbox scan cannot be completed.

For example, if you associate WIN10X64VM to scan all executable files when configuring the Scan Profile on the Primary node, but do not enable WIN10X64VM on a Worker node, all executable files distributed to that worker are not scanned by VM.

Heartbeat Synchronization

Primary and secondary nodes in a cluster send heartbeats to each other every half second. When a secondary node fails to receive a single heartbeat from the primary node, it will consider the primary node to be off-line or unreachable. This can happen on the primary node due to a network problem or when it is rebooting. When the primary is unreachable, a selection process for a new primary node will be triggered. The selection is promptly performed and decided based on the health of the nodes. When a secondary node is selected, all other secondary nodes will treat it as the new primary node and the failover process will start.

The heartbeat can also fail due to an issue with the secondary node. In that case, the selection process is still triggered but the primary node remains the same.

Failover scenarios

The failover logic handles two different scenarios:

Objective node available	The objective node is a worker (either secondary or worker) that can decide the new primary. For example, if a cluster consists of one primary node, one secondary node, and one worker node, the worker node is the objective node. After a secondary node takes over the primary role, the original primary node will accept the decision when it is back online. After the original primary is back online, it will become a secondary node.
No Objective node available	When there is no objective node in the cluster, the cluster topology is not stable and the failover process may take several rounds of role changes. This occurs when there is no communication between nodes because the cluster's internal communication is down . During the failover process, the final roles of primary and secondary are decided by three principal factors: the internal connections, the health check, and the serial number. **Internal Connections**

The internal connections in a cluster involve two ports: port1 and the cluster internal port, typically port2 depending on your configuration.

Port1 is used when a node prompts itself to be the primary and needs confirmation from other nodes.

The cluster internal port is used for cluster nodes to detect whether its connection to other nodes in the cluster is available or not, and is used to ask the secondary to failover when its health check fails.

Health Check

The health check is used to check the connection with the ping server and/or echo server. If this connection fails in the primary node, it triggers a failover.

Serial Number

Once the port1 connection is recovered, the unit with the newer serial number will keep the primary role and the unit with the older serial number will become the secondary.

When the new primary is decided, it will:

1. Build up the scan environment.
2. Apply all the settings synchronized from the original primary except the port3 IP and the internal communication port IP of the original primary.

After a failover occurs, the original primary might become a secondary node.

It keeps its original port3 IP and internal cluster communication IP. All other interface ports are shut down as it becomes a worker node. Some functionality is turned off such as email alerts. If you want to reconfigure settings, such as the interface IP, you must do that through the CLI command or the primary's Central Management page.

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

As the new primary takes over the port that client devices communicate with will switch to it. As the new primary needs time to start up all the services, clients may experience a temporary service interruption.

Performance tuning

Setting primary node processing capacity

Primary node requires enough dedicated processing power for job distribution and cluster management. We recommend that for every 5 VM clones on the worker nodes, 1 VM should be removed from the Master.

Example:

You are using two FSA3KE units to setup a cluster. One FortiSandbox works as Primary node and the other works as the Worker node.

The Worker node operates 56 VM clones, so the Primary node should remove 11 clones from its processing capacity. In this example, the Primary node should be running 45 (56 – 11) VM clones.

The CLI command `hc-master -s80` will take the Primary node to 80% of its VM processing power, which is 45 clones. This means that even if you configure the Primary node to run 56 clones, at any moment, no more than 45 clones can be running.

Upgrading or rebooting a cluster

Upgrading or rebooting a cluster has to be done by logging into each device or through the primary unit's *Cluster Management* page. You must upgrade the cluster in the following order:

1. Workers
2. Secondary
3. Primary

It is highly recommended to setup cluster level failover IP set so the failover between primary and secondary can occur smoothly. If you do not want the failover to happen, you can change the secondary unit role to worker. You can either do this through the UI dashboard or the CLI prior to the failover, then change the role back after the unit boots up.

Main HA-Cluster CLI commands

The table below lists the CLI commands to administer your HA-Cluster.

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

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

Setting primary node processing capacity

Primary node requires enough dedicated processing power for job distribution and cluster management. We recommend that for every 5 VM clones on the worker nodes, 1 VM should be removed from the Master.

Example:

You are using two FSA3KE units to setup a cluster. One FortiSandbox works as Primary node and the other works as the Worker node.

The Worker node operates 56 VM clones, so the Primary node should remove 11 clones from its processing capacity. In this example, the Primary node should be running 45 (56 – 11) VM clones.

The CLI command `hc-primary -s80` will take the Primary node to 80% of its VM processing power, which is 45 clones. This means that even if you configure the Primary node to run 56 clones, at any moment, no more than 45 clones can be running.

Fortinet Ex. 2003 - Page 211 of 245

Log & Report

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

Local logs retain up to 1 GB of overall logs. If this limit is reached, logs are rotated to keep the latest ones.

Log Details

To view more details about a specific log in the log list, simply select that log. A log details pane is available at the bottom of the window.

The log details pane contains the same information as the log message list, except with a full message in lieu of a shortened one.

Logging Levels

FortiSandbox logs can be Emergency (reserved), Alert, Critical, Error, Warning, Information, or Debug. The following table provides example logs for each log level.

Log Level	Description	Example Log Entry
Alert	Immediate action is required.	Suspicious URL visit domain.com from 192.12.1.12 to 42.156.162.21:80.
Critical	Functionality is affected.	System database is not ready. A program should have started to rebuild it and it shall be ready after a while.
Error	An erroneous condition exists and functionality is probably effected.	Errors that occur when deleting certificates.
Warning	Functionality might be affected.	Submitted file AVSInstallPack.exe is too large: 292046088.
Information	General information about system operations.	LDAP server information that was successfully updated.
Debug	Detailed information useful for debugging purposes.	Launching job for file. jobid=2726271637747836543 filename=log md5=ebe5ae2bec3b653c2970e8cec9f5f1d9 sha1=06ea6108d02513f0d278ecc8d443df86dac2885b sha256=d678da5fb9ea3ee20af779a4ae13c402585ebb070edcf20091cb20509000f74b

Raw logs

You can download and save raw logs to the management computer using the *Download Log* button. Raw logs are saved as a text file with the extension *.log.gz*. You can search the system log for more information.

Sample raw logs file content

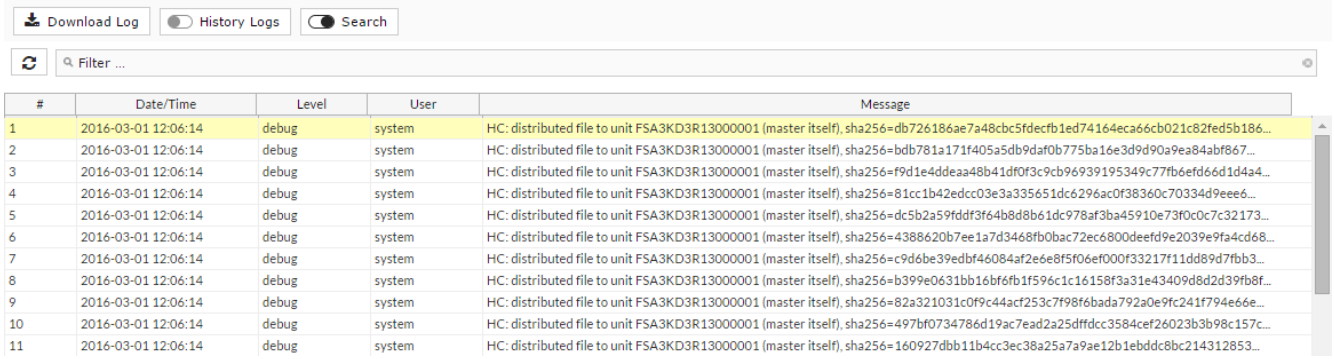
```
itime=1458669062 date=2016-03-22 time=17:51:02 logid=1220000020 type=event subtype=unknown
     pri=alert user=system ui=system action=rating status=success reason=none letype=6
     msg=fname=v32.cab jobid=2725911139058114340
     sha1=f61045626e5f4f74108fb6b15dde284fe0249370
     sha256=f75fca6300e48ec4876661314475cdd7f38d4c73e87dfb5a423ef34a7ce0154f rating=Clean
     scantime=11 malwarename=N/A srcip=204.79.197.200 dstip=208.91.115.250 protocol=HTTP
     device=() url=http://officecdn.microsoft.com/pr/492350f6-3a01-4f97-b9c0-
     c7c6ddf67d60/Office/Data/v32.cab
itime=1458669062 date=2016-03-22 time=17:51:02 logid=0106000001 type=event subtype=system
     pri=debug user=system ui=system action=controller status=success reason=none letype=6
     pid=8605 msg="Sandboxing environment is not available for job 2725913445926977878,
     file type: htm, file extension: htm"
itime=1458669062 date=2016-03-22 time=17:51:02 logid=1220000020 type=event subtype=unknown
     pri=alert user=system ui=system action=rating status=success reason=none letype=6
     msg=fname=0_22_93_0_0_2_0_0_1.html jobid=2725913445926977878
     sha1=098a2ca8d81979f2bb281af236f9baa651d557d5
     sha256=424c62eaaa4736740e43f5c7376ec6f209b0d3df0e0cadcc94324280eafa101f rating=Clean
     scantime=12 malwarename=N/A srcip=125.39.193.250 dstip=208.91.115.12 protocol=HTTP
     device=() url=http://all.17k.com/lib/book/0_22_93_0_0_2_0_0_1.html
```

For detailed log format information, please refer to the *FortiSandbox 4.2.4 Log Reference* available on the Fortinet Document Library.

Log Categories

Logs are group into different categories:

All Events	All logs.
System Events	Logs related to system operation, such as user creation and FDN downloads.
VM Events	Logs related to guest VM systems, such as VM initialization.
Job Events	Logs related to scans. You can trace the scan flow of each file or URL.
HA-Cluster Events	Logs related to cluster configuration and failovers.
Notification Events	Logs related to email alerts and SNMP traps.



The following options are available:

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

The following information is displayed:

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

Viewing logs in FortiAnalyzer

To view FortiSandbox logs in your FortiAnalyzer:

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

The following options are available:

Add Filter		Enter a search term to search the log messages. You can also right-click an entry in a column and select to add a search filter. Click *GO* to apply the filter. Not all columns support the search feature.
Device		Select the device in the dropdown list.
Time Period		Select a time period from the dropdown list. Options include: *Last 30 mins*, *Last 1 hour*, *Last 4 hours*, *Last 12 hours*, *Last 1 day*, *Last 7 days*, *Last N hours*, *Last N days*, or *Custom*.
GO		Select to apply the time period and limit to the displayed log entries. A progress bar is displayed in the lower toolbar.
Column Settings		Select specific columns to be displayed. You can also reset the columns to its default.
Tools		*Tools* has options for changing how to display logs, options for search, and to add or delete column.
	Real-time Log	FortiSandbox does not support *Real-time Log*.
	Display Raw	Select to change view from formatted display to raw log display.
	Download	This option is only available when viewing logs in formatted display. Click to download logs. Select the log file format, then compress with gzip the pages to include and select *Apply* to save the log file on the management computer.
	Case Sensitive Search	Select to enable case sensitive search.
	Chart Builder	Select to create a custom chart.
Display Details button		Detailed information about the log message selected in the log message list. The item is not available when viewing raw logs. *Log Details* are only displayed when enabled in the *Tools* menu.
Search Scope		Select the maximum number of log entries to be displayed from the dropdown list. Options include: *1000*, *5000*, *10000*, *50000*, or *All*.

This page displays the following information:

Logs	The columns and information shown in the log message list will vary depending on the selected log type and the view settings. Right-click various columns to add search filters to refine the logs displayed. When a search filter is applied, the value is highlighted in the table and log details.
Status Bar	Displays the log view status as a percentage.
Pagination	Adjust the number of logs that are listed per page and browse through the pages.

Customizing the log view

The message column can display raw or formatted logs. The columns in the log message list can be customized to show only relevant information in your preferred order.

To View Raw and Formatted Logs

By default, formatted logs are displayed. The selected log view will affect available view options. You cannot customize the columns when viewing raw logs.

To view raw logs:

Go to *Tools* and select *Display Raw* from the dropdown menu from the toolbar.

To view formatted logs:

Go to *Tools* and select *Display Formatted* from the dropdown menu from the toolbar.

Columns

The columns displayed in the log message list can be customized and reordered as needed. Filters can also be applied to the data in a column.

To customize the displayed columns:

1. In the log message list view, click Column Settings in the toolbar.
2. From the dropdown list that is displayed, select a column to hide or display.

The available column settings will vary based on the device and log type selected.

3. To add more columns, select *More Columns*. In the *Column Settings* dialog box that opens, you can show or hide columns by selecting and deselecting the columns.
4. To reset to the default columns, click *Reset to Default*.
5. Click *OK* to apply your changes.

To change the order of the displayed columns:

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

To filter column data:

1. You can filter log summaries by using the *Add Filter* box in the toolbar or by right-clicking an entry and selecting a context-sensitive filter.
2. Specify filters in the *Add Filter* box.
   Use Regular Search. In the selected summary view, click in the *Add Filter* box, select a filter from the dropdown list, and type a value. You can click on an operator to use it, such as greater than (>), less than (<), OR, and NOT. You can add multiple filters at a time, and connect them with "and" or "or".

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

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

To filter log summaries using the right-click menu:

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

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

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

Summary Reports

The *Summary Reports* page lists all Executive Summary and Threat Activity reports including their status, and the user who generated the report. You can download and delete the PDF reports.

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

Generate reports

To generate a summary report on demand, go to *Logs & Reports* > *Summary Report*.

You can generate executive summary and threat activity reports for a specified time period.

The following options are available:

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

This page displays the following information:

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

Report Center

When a report is generated, you have the option waiting until the report is ready to view or viewing the report later on the *Report Center* page.

This *Report Center* page displays the following information:

Status	The status of report generation process: Done, Stopped, or In Progress.
Start Time	The time report generation starts.
Finish Time	The time report is ready.
Report Type	The type of report: PDF or CSV.
Report Size	The size of the report, in kilobytes.
Download Count	The number of times that the report has been downloaded.
Progress	Percentage that the report has finished
Source	The location that the report is scheduled to generate.
Detection Period	The time range of the jobs that this report contains.
Actions	You can view, delete, and download a report.
Pagination	Adjust the number of reports that are listed per page and browse through the pages. When you click on any entry on this page, detailed information about the report is displayed, including the job filtering criteria.

Customize Report

Admins with Read/Write privileges can customize the report title, header and footer. You can also add a logo and background image to your report.

Customized Report settings are supported in the following reports:

- Detail Report
- On Demand Detail Job List Report
- Scan Detail Job List Report
- Scheduled Summary Report
- Network Alerts Report

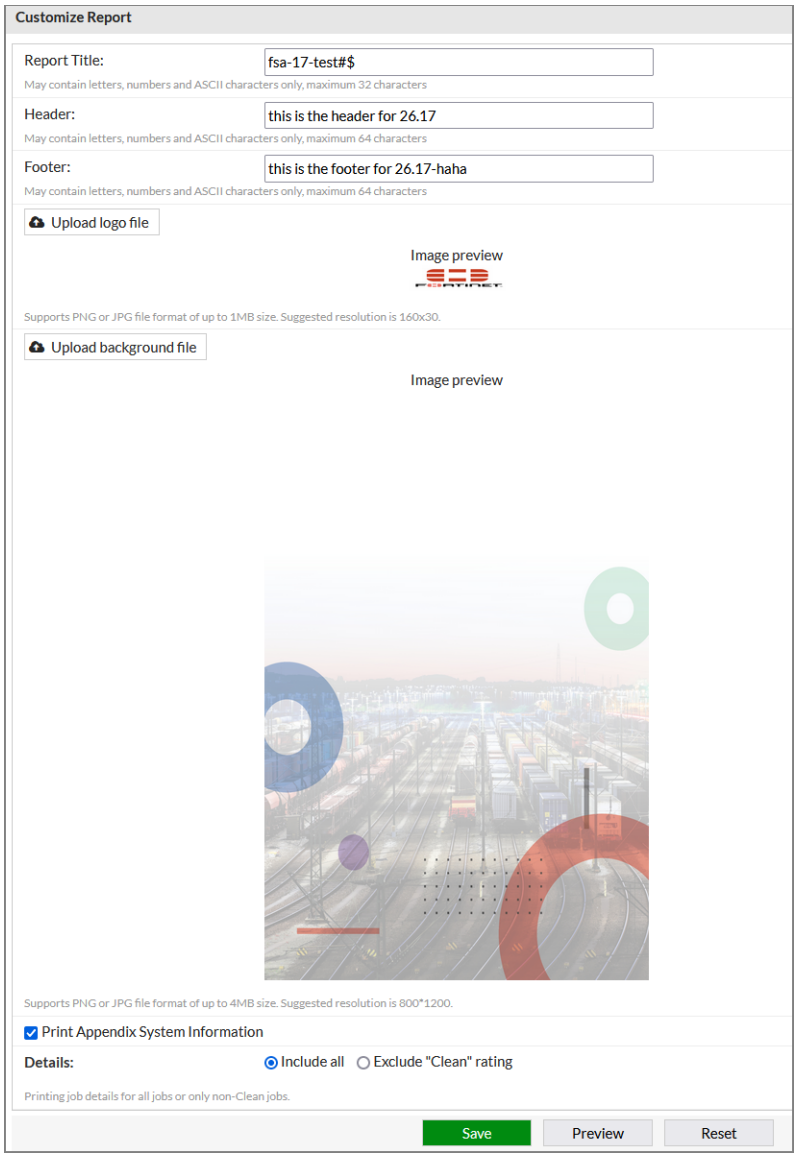
Customize Reports is only available in the Primary node of an HA cluster.

To recover a configuration , go to *System* > *System Recovery* > *View the configurations*.

To customize the report settings:

1. Go to *Log & Report* > *Customize Report*.
2. Configure the report settings and click *Save*.

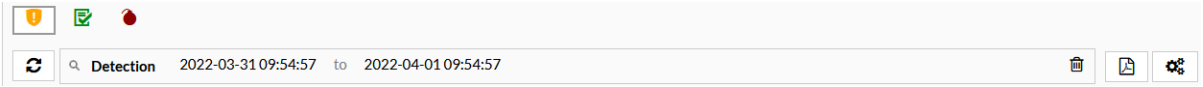
Report Title	Enter the report title.
Header	Enter the header text.
Footer	Enter the footer text.
Upload logo file	Maximum file size is 1MB.
Upload background file	Maximum file size is 4MB.
Print Appendix System Information	• *Include All*: All detailed behavior will be printed including *Malicious*, *Suspicious*, and *Clean* ratings. If no behavior is detected, then *No Behavior was detected* is printed. • *Exclude "Clean" rating*: The detailed behavior for jobs that are rated *Clean* are excluded from the report and *No Behavior was detected* is printed. The behavior for jobs that are rated *Suspicious* or *Malicious* is printed.



File Scan

The *File Scan* page shows file-based job scans grouped by their security ratings. Files submitted through On-Demand are not included. Use this page to view job details and apply search filters. You can also create a PDF or CSV format snapshot report for files based on search filters.

Suspicious jobs are displayed by default. To view *Malicious* and *Clean* jobs, click the icons at the top of the page.



The following options are available:

File Scan Options		
	Suspicious Jobs	Click the *Suspicious Jobs* icon to view the suspicious jobs.
	Clean or Unknown Jobs	Click the *Clean* icon to view the clean or unknown jobs.
	Malicious Jobs	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 *Log & Report* > *File Scan* > *Malicious* and enable *Show Rescan Job Only*.
Refresh		Click the *Refresh* 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 to report		Click the *Export to report* button to create a PDF or CSV snapshot report. The time to generate the report is dependent on the number of events selected. You can wait till the report is ready to view, or navigate away and find the report later on the *Log & Report* > *Report Center* page.
Customize		Click the *Customize* button to customize the Job View Settings. The change will be applied to all file based scan result pages.
Action		
	View Job Detail	Click the *View Details* icon to view the file description and analysis details. The information displayed is dependent on the file selected.
	Customized Rating	Indicates the job was rated by a customized rating.
	Perform Rescan	For malicious jobs, you can also select *Rescan* to manually rescan the file. This way, you can find out the behavior of a known virus. You can select to force the file to do a Sandboxing scan even if it was detected in previous steps of a Static Scan, AV Scan, Cloud Query, or if it was stopped from entering the VM by a Sandboxing-prefilter setting. You can find the job in *Scan Job* > *File On-Demand*.
	Archived File	An icon will appear if the file is an Archived File.
	FortiGuard Static Scan	The icon displays that the file is rated by the user's overridden verdict or FortiGuard advanced static scan.
	File Inside Archive	The icon displays that the file is a file extracted from an archive file.
	Rescan Job	The icon displays that the job is Malicious from an AV Rescan or a rescan job of a Malicious file.

AV Scan	An icon will appear if this job is from an AV Rescan.
Pagination	Use the pagination options to browse entries displayed.

FortiSandbox has an Anti Virus rescan feature. When a new antivirus signature is available, FortiSandbox will perform a second antivirus scan of all the jobs from the last 48 hours whose ratings are *Clean* or *Suspicious* using the new signatures. Detected viruses will be displayed as *Malicious* jobs with the *Rescan* icon beside the *View Details* icon. The original job can still be viewed in the job detail page of the rescanned file by clicking the original job ID.

Virus behavior information is not collected as viruses are detected by the AV scanner. The rescan feature allows you to see how a virus behaves while it is being executed inside a VM.

The displayed columns are determined by settings defined in *System* > *Job View Settings* > *File Detection Columns* page. For more information, see Job View Settings on page 189.

To view file details:

1. Select a file.
2. Click *View Job Detail*. A new tab opens.
   For information on the *View Details* page, see Job Details page reference on page 235.

To rescan a file:

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

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

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

File Statistics

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

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

On-Demand job data is not included.

The following options are available:

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

The following widgets are available:

Scan Statistics	Information about the files scanned for a selected device for a selected time period.
Scan Statistics by Type	Information about file types, rating, and event count for a selected device over a selected time period. To view all the file types, click *Edit* and increase the top count. Default is five.
Top Targeted Hosts	Number of infection events for specific hosts for a selected device over a selected time period. Hover the pointer over a colored portion of a bar in the chart to view the exact number of infection events for that host. Selecting the infected host allows you to drill down to the job details.
File Scan	Number of clean, suspicious, and malicious events at specific times over a selected time period for the selected device. Hover the pointer over a colored portion of a bar in the graph to view the exact number of events for the selected type for that time period.
Top Malware	Number of infection events for specific malware for a selected device over a selected time period. Hover the pointer over a colored portion of a bar in the chart to view the exact number of infection events for that malware. Selecting the malware name allows you to drill down to the job details.
Top Callback Domains	The top callback domains detected over a time period. Callback domains are hosts that files visit when executing in the VM. Hover the pointer over a colored portion of a bar in the chart to view the exact number of infection events for that malware.
Top File Types	The top file types detected over a time period. When *Scanned by Sandboxing* is selected, only files that have finished sandboxing are counted.

Customizing the File Statistics report page

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

To move a widget:

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

To refresh a widget:

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

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

To edit a widget:

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

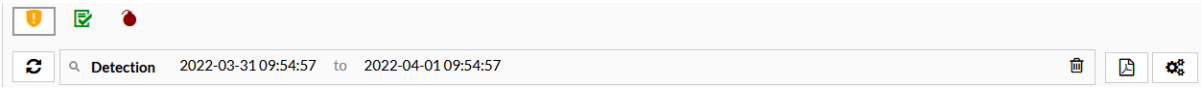
Configure the following information, and then select *OK* to apply your changes:

Custom widget title	Optionally, enter a custom title for the widget. Leave this field blank to use the default widget title.
Refresh interval	Enter a refresh interval for the widget, in seconds. The widgets have default refresh values: • *Scan Statistics*: 3600 seconds • *Scan Statistics by Type*: 3600 seconds • *Top Malware*: 3600 seconds • *Scanning Activity*: 300 seconds • *Top Targeted Hosts*: 10 seconds • *Top Callback Domains*: 3600 seconds
Top Count	Select the number of entries to display in the widget. The top count can be between 5 to 20 entries. This setting is available in all widgets except *Scan Statistics*, *Scan Statistics by Type*, and *Scanning Activity*.

URL Scan

The *URL Scan* page shows file-based job scans grouped by their security ratings. Files submitted through On-Demand are not included. Use this page to view job details and apply search filters. You can also create a PDF or CSV format snapshot report for files based on search filters.

Suspicious jobs are displayed by default. To view *Malicious* and *Clean* jobs, click the icons at the top of the page.



The following options are available:

URL Scan Options		
	Suspicious Jobs	Click the *Suspicious Jobs* icon to view the suspicious jobs.
	Clean or Unknown Jobs	Click the *Clean* icon to view the clean or unknown jobs.
	Malicious Jobs	Click the *Malicious* icon to view the malicious jobs.
Refresh		Click the *Refresh* button to refresh the entries displayed.
Search		Show or hide the search filter field.
Add Search Filter		Click the search filter field to add search filters. When the search criteria is the *Submitted Filename*, click the equals sign to toggle between exact and pattern search. Click the close icon in the search filter field to clear all search filters. Search filters can be used to filter the information displayed in the GUI.
Export Data		Select to create a PDF or CSV snapshot report. The time to generate the report is dependent on the number of events selected. You can wait till the report is ready to view, or navigate away and find the report later on the *Log & Report* > *Report Center* page.
Customize		Click the *Customize* button to customize the Job View Settings.
Action		
	View Details	Click the *View Details* icon to view the file description and analysis details. The information displayed is dependent on the file selected.
	FortiGuard Static Scan	The icon displays that the URL is rated by the user's overridden verdict or FortiGuard advanced static scan.
	Archive File	The icon displays that the URL is from a file through On-Demand scan.
	File Downloading URL	The icon displays that the URL is from FortiMail and its payload is also scanned as a file scan job.
	Perform Rescan	All suspicious items which are not rated by the VM can be rescanned. All malicious files can be rescanned. In the *Rescan Configuration* dialog box, you can customize the new scan's depth and timeout value. You can also force the URL to do Sandboxing scan even if was detected in former steps of the allowlist and blocklist check or stopped from entering VM by a Sandboxing-prefilter setting. Results are in *Scan Job* > *URL On-Demand* and *Scan Job* > *URL Job Search*.
Pagination		Use the pagination options to browse entries displayed.

The displayed columns are determined by settings defined in *System* > *Job View Settings* > *URL Detection Columns* page. For more information, go to Job View Settings on page 189.

To create a snapshot report for all search results:

1. Select to apply search filters.
2. Select the generate to report button. The *Report Generator* window opens.
3. Select either PDF or CSV and click the *Generate Report* button to create the report.

4. When report generation is completed, select the *Download* button to save the file to your management computer.
5. You can wait until the report is ready to view, or navigate away and find the report later on the *Log & Report* > *Report Center* page.

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

URL Statistics

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

The following options are available:

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

The following widgets are available:

Scan Statistics	Information about the URLs scanned per OS. Click the number in the widget to drill down to the job list.
Scan Statistics by Type	Information about URL types, rating, and event count.
Scanning Activity	Number of clean, suspicious, and malicious jobs. Hover the pointer over a colored portion of the graph to view the number of events. You can toggle between hourly data view and daily data view.

Customizing the URL Statistics 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 pointer on the widget's title bar, then click and drag the widget to its new location.

To refresh a widget:

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

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

To edit a widget:

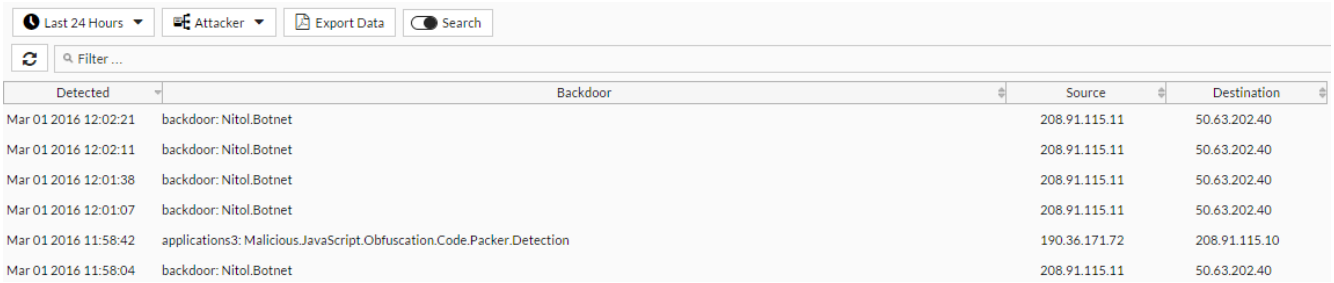
1. Click the edit icon in the widget's title bar to open the edit widget settings window.
2. Configure the following information and then click *OK*.

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

Network Alerts

Network alerts show detected connection attempts to known botnets, attacks to hosts on your network, and harmful websites visited from your network.

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



This page has the following options:

Time Period	Select the time period from the dropdown list. Select one of the following: *24 Hours*, *7 Days*, or *4 Weeks*. You can select the time period to filter the information displayed in the GUI. This selection is also applied to exported data for the snapshot report.
Alert Type	Select Attacker, Botnet, or URL from the dropdown list. You can select the alert type to filter the information displayed in the GUI. This selection is also applied to exported data for the snapshot report.
Attacker	Shows attacks against hosts on your network. When selecting *Attacker* from the dropdown list, the following information is displayed: • Detected: The date and time that the attack was detected by FortiSandbox. • Backdoor: The name of the attack.

	• Source: The attacker's IP address. • Destination: The attacked host IP address. All columns include a filter to allow you to sort the entries in ascending or descending order.
Botnet	Shows detected connections to knows botnets. When selecting *Botnet* from the dropdown list, the following information is displayed: • Detected: The date and time that the botnet contact was detected by FortiSandbox. • Name: The botnet name. • Source: The IP address of the infected host. • Destination: The botnet command and control IP address. The *Detected*, *Name*, and *Source* columns include a filter to allow you to sort the entries in ascending or descending order.
URL	Shows visited suspicious websites from your network. When selecting *URL* from the dropdown list, the following information is displayed: • Detected: The date and time that the malicious URL was visited. • Rating: The severity of the visiting activity. • Category: The URL's web filtering category. • Host: The host IP address. The first level domain name of the URL. • URL: The visited URL address. • Type: The URL type, http or https • Source: The IP address of the host who visited the malicious URL. The *Detected*, *Category*, *Hostname*, *URL*, *Type*, and *Source* columns include a filter to allow you to sort the entries in ascending or descending order. **Tooltip**: Certain URL categories are set as *Benign* by default. To view and change, go to *Scan Policy and Object* > *Web Category*.
Export Data	Select to create a PDF or CSV snapshot report. The time to generate the report is dependent on the number of events selected. You can wait till the report is ready to view, or navigate away and find the report later on the *Log & Report* > *Report Center* page.
Refresh	Click the icon to refresh the log message list.
Search	Show or hide the search filter field.
Add Search Filter	Click the search filter field to add search filters. Click the close icon in the search filter field to remove the search filter. Search filters can be used to filter the information displayed in the GUI.

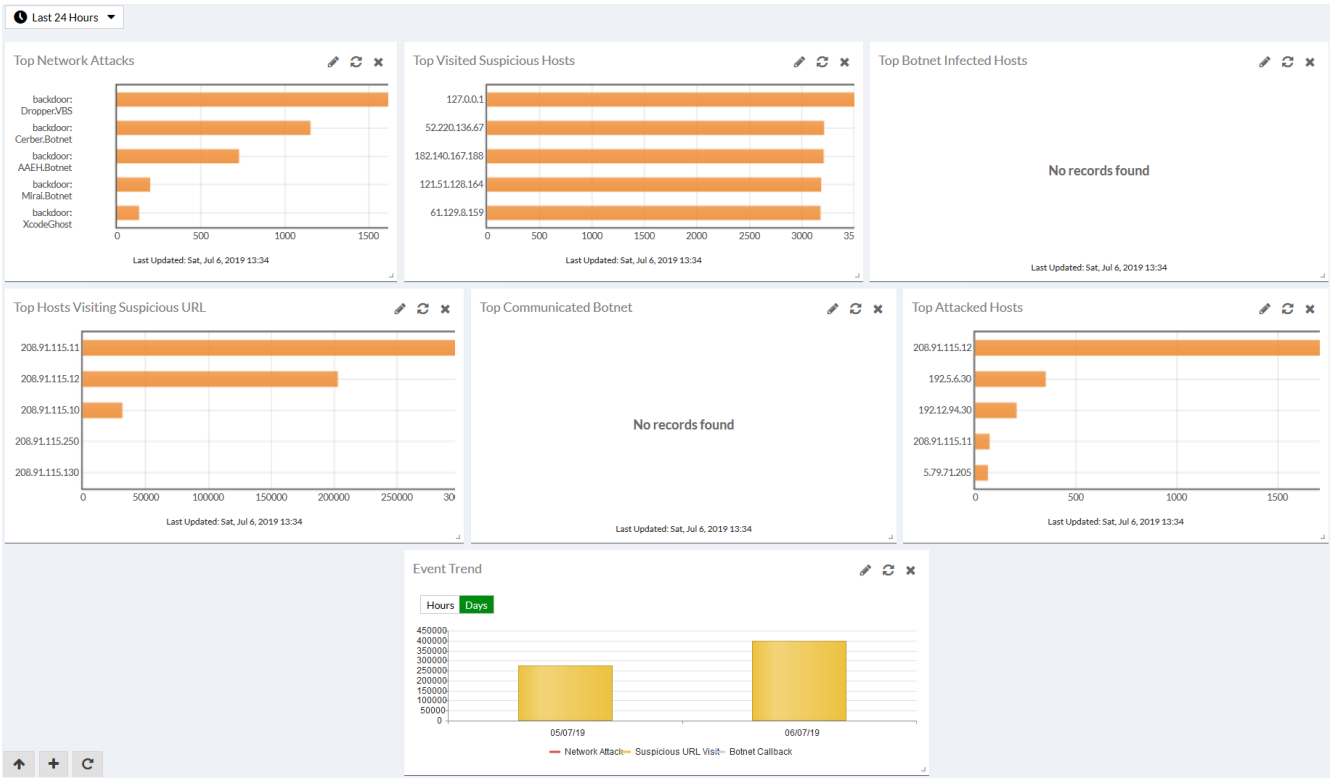
To create a snapshot report for all network alert files:

1. Select a time period from the first dropdown list.
2. Select Attacker, Botnet, or URL from the second dropdown list.
3. Select to apply search filters to further drill down the information in the report.
4. Click the *Export Data* button in the toolbar. The *Report Generator* window opens.
5. Select either PDF or CSV for the report type.

6. Click the *Generate Report* button to create the report.
   When the report generation is completed, select the *Download* button to save the file to your management computer.
7. You can wait till the report is ready to view, or navigate away and find the report later on the *Log & Report* > *Report Center* page.

Network Alerts Statistics

The *Summary Report* page provides a page similar to the system dashboard. You can add and customize widgets in this page. By selecting the time period, you can customize what data is displayed.



The following options are available:

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

The following widgets are available:

Event Trend	Displays a chart providing information about the number of network attacks, suspicious URL visits, and Botnet callbacks over a period of time.

	Hover the pointer over a colored portion of a bar in the graph to view the exact number of events that occurred at that time. You can toggle between hourly data view and daily data view.
Top Network Attacks	Displays a table providing information about the number and type of network attacks. Hover the pointer 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 pointer 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 pointer 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 pointer over a colored portion of a bar in the graph to view the exact number of events that occurred at that time.
Top Visited Suspicious Hosts	Displays a table providing information about the top visited suspicious hosts. Hover the pointer over a colored portion of a bar in the graph to view the exact number of events that occurred at that time.
Top Hosts Visiting Suspicious URL	Displays a table providing information about the top hosts on your network that visit suspicious URLs. Hover the pointer over a colored portion of a bar in the graph to view the exact number of events that occurred at that time.

Customizing the Network Alerts Statistics page

The *Network Alerts Statistics* 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 pointer on the widget's title bar, then click and drag the widget to its new location.

To refresh a widget:

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

To edit a widget:

1. Click the edit icon in the widget's title bar to open the edit widget settings window.
2. Configure the following information and then click *OK*.

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

Log Servers

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

Logs are transmitted instantly. If connectivity to the Log Server is interrupted, FortiSandbox will cache the logs in its buffer and attempt to resend later. The log buffer capacity is 1024 logs. Newer logs are discarded when the buffer is full.

The following options are available:

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

This page displays the following information:

Name	Name of the server entry.
Type	Server type. The following options are available: CEF, syslog (TCP/UDP), or FortiAnalyzer.
Log Server Address	Log server address (IPv4 or IPv6).
Port	Log server port number.

Status	Status of the log server, *Enabled* or *Disabled*.
Secure Connection	Security status of the log server, *Enabled* or *Disabled*.

To create a new server entry:

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

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

4. Click *OK*.

You can forward FortiSandbox logs to a FortiAnalyzer running version 5.2.0 or later.
Syslog server supports IPv6.

To edit or delete a log server:

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

Local Log

As local logs retain up to 1 GB of overall logs, you can turn off logs for specified severity levels.

To turn off logs from specific severity levels:

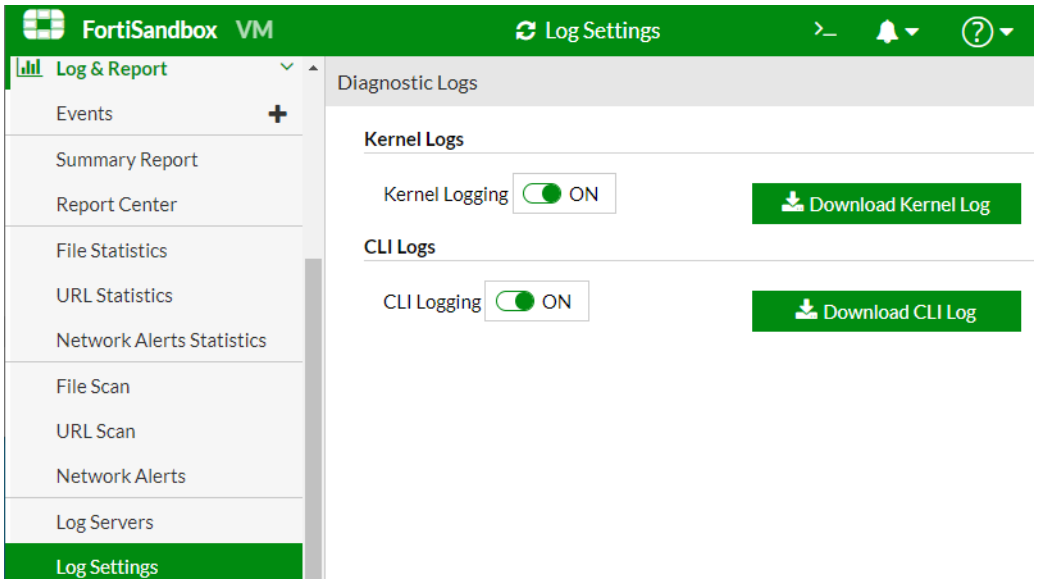
1. Go to *Log & Report* > *Log Settings* >*Local Log*.
2. Uncheck a level to turn off logs from that severity level.

Diagnostic Logs

Diagnostic logs allow the FortiSandbox support team to collect information for troubleshooting purposes. When enabled, users can record and view system internal logs and CLI histories.

To enable or disable Diagnostic Logs:

1. Go to *Logs & Report* > *Log Settings* > *Diagnostic Logs*.
2. Enable or disable *Kernal Logs* or *CLI Logs*.



Appendix A - Advanced deployment scenarios

Deploying primary and secondary nodes without VM Clones

When the primary and secondary node are using a FortiSandbox VM00 model, you have the option of deploying without VM Clones (i.e. dispatcher). That VM00 deployment dedicates its full VM resources for HA support, receiving incoming files and distribution of files to the worker nodes. There is no scan performed on the VM00. On this type of VM00 deployment, only the *FortiCare Premium Support* subscription is necessary as all the scans are performed on the worker nodes.

Deploying for Static Scan

The Static Scan only deployment type provides the highest available performance and lowest scan time to process the samples. Static Scan is comprised of pre-filtering, full antivirus scan, cloud query and Static AI scan. Without the Dynamic Scan, the detection rate is expected to be lower. This mode can be considered when throughput is more important than detection precision. Otherwise, considerthe regular operating mode to ensure the highest available detection precision.

When deploying FortiSandbox VM00 for Static Scan only, use firmware version 4.2.2 or later. You can leave the clone number at zero. For this deployment, the *Sandbox Threat Intelligence* plus *FortiCare Premium* subscriptions are required. Windows expansion licenses are not required.

Deploying for OT Industry

The OT Malware scans for presence of OT related applications and networking protocols. The LinuxOT is a Linux VM to simulate the OT industry deployment. The VM supports the Siemens application and simulates:

- Modbus
- SNMP
- IPMI
- FTP
- TFTP protocols

The Sandbox Threat Intelligence subscription already includes the Industrial Security subscription which allows you to enable the simulation. To scan files, submit them through any Windows VM. If it is an OT Malware, the LinuxOT will capture that lateral movement behavior and access to those application and protocols.

For information, see Simulator VMs on page 124.

Appendix B - Job Details page reference

You can create custom VMs using pre-configured VMs, your own ISO image, or Red Hat VMs on VirtualBox. For more information, contact Fortinet Customer Service & Support.

For information on hard disk hot-swapping procedure, system recovery procedure using Rescue Mode, and password reset procedure, see the FortiSandbox Best Practices and Troubleshooting Guide in the Fortinet Document Library.

When you click the *Job Details* icon, a new browser tab opens showing detailed forensic information of a job. The information is in three tabs: *Overview*, *Tree view*, and *Details*.

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

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

Item	Description
Rated by	The source of the rating decision. The following are the sources by scan module: **Static Scan related:** *AV Scan Engine*, *Sandbox Community Cloud*, *Static Scan Engine*, *Yara Scan Engine*, *Dynamic Scan Cache*, *Allowlist/Blocklist*, *FortiGuard Allowlist/Blocklist*, *Overriden Verdicts*, *AI (Cloud)* and *Fabric Device (FortiNDR)*. **Dynamic Scan related:** *Dynamic Scan (AI off)*, *Dynamic Scan*, *Dynamic Scan (MacOS Cloud)*, *Dynamic Scan (Cloud)*, *Cloud Rating* and *Customized Rating*. The module names have been changed since v4.2.0. If you require the previous module names for mapping, please contact Customer Support.
Submit Type	The input source of the file such as FortiMail.
Source IP	The malware host IP address.
Destination IP	The IP address of the client that downloaded the virus.
Digital Signature	The digital signature availability status of the scanned file.
AI Mode	Whether AI mode is on or off.
Scan Bypass Configuration	When available, the scan bypass configuration will be displayed.
SIMNET	The SIMNET status when the scan is running.
Depth	The URL level to do the recursive scan.
Region	WindowsCloudVM region.
Timeout Value	File/URL scan timeout setting.
Virus Total	By clicking the Virus Total link, a new page will open to query https://www.virustotal.com. Only a limited number of queries per minute is allowed without manual interaction with the Virus Total website.
Child list	For submitted URLs, this field displays a color-coded rating for each child URL, so that you an quickly identify child URLs that have a different rating from the parent URL.
The Original Job of this Rescan Job	Click the link to view the original job if this one is an AV rescan or On-Demand rescan job.
Details Information	View additional file information including the following: Packers, File Type, Downloaded From, File Size, Service, MD5, SHA1, SHA256, ID, Submitted By, Submitted Filename, Filename, Scan Start Time, VM Scan Start Time, VM Scan End Time, VM Scan Time, Scan End Time, Total Scan Time, Scan Unit, Embedded URL number, No VM Reason (reason why sample was not scanned inside VM), VM Reason (reason why sample entered into VM), Launched OS (VM type), Specified Browser, Launched Browser, Pipeline mode OS (if rated by pipeline mode VM), Infected OS, and Anti Evasion Triggers.

Item	Description
	If the sample is from FortiMail, Email related information, such as the Email Sender, Receiver, Client IP, From, To, and Subject will also be shown. If the sample is from Adapter, Adapter IP address and Email related information, such as BCC-Agent Sender and BCC-Agent Receiver will also be shown.
Indicators	A summary of the Malware's behavior indicators if there are any.
Rating	The rating is the final verdict of the FortiSandbox on the scan job based on the collected behavioral activities and static analysis. The assessment of their risk and impact is based on our FortiGuard Threat Intelligence of previously-known malware. Ratings include *Malware*, *High risk*, *Medium risk*, *Low risk*, and *Clean*.
VM Interaction	When *Interaction* mode is enabled before jobs are submitted, *VM Interaction* displays *Raw* and the *Status* is *ON*. When *Interaction* is disabled *VM Interaction* is not displayed in the Overview page.
Video Record	When *Record Video* is enabled, *Video Record* displays *ON*. When *Record Video* is disabled, *Video Record* is not displayed.

The *Tree View* tab shows a tree for file's static structure or file's parent-child process relationship when it executes inside a guest VM. You can drag the tree using the mouse and zoom in or out using the mouse wheel. If there is suspicious activity with one tree node, its label will be colored red. Clicking a node in the tree will open more information in tab format. Suspicious information is shown in the color red, so you can quickly locate it.

The *Details* tab shows analysis details for each detection OS that is launched during the scan. It shows information in a different way from *Tree View* part. The following are details of information displayed:

Item	Description
Analysis Details	View the following analysis details for each Detection OS that is launched during the scan. Each Detection OS's detail will be shown in a separate tab. The Infected OS will have a VM Infected icon in its tab title. If the Malware is detected by non-Sandboxing scan, such as FortiGuard static scan, the tab title is displayed as *N/A*.
Behavior Chronology Chart	View the file's behavior over time and its density during its execution. Clean behaviors: green bubble. Suspicious behaviors: red, blue, or orange bubble. The higher the bubble, the more serious the event is. To view the event details, hover the mouse on top of the bubble. If a file scan is scanned with more than one VM type, the VM tab will dynamically switch to the chart for that type. If the file hits any imported YARA rule, a YARA tab will appear with detailed information. including: • The hit rule • Rule's risk level • Rule set name • Link to original YARA rule file

Item		Description
	Captured Packets	Select the *Captured Packets* button to download the tracer PCAP file to your management computer.The packet capture (PCAP) file contains network traffic initiated by the file. You must have a network protocol analyzer installed on your management computer to view this file. The *Captured Packets* button is not available for all file types.
	Tracer Package	Download the compressed `.tar` file containing the tracer log and related files. The password protected `/backup` folder in the tracer log contains information about the program's execution. The default password for this file is *fortisandbox*. Unzip the tracer log only on a management computer in an analysis environment. To see all dropped files by the file being scanned, use the **-g** argument. This generates a file named filemap.txt in the backup directory of the tracer package.
	Tracer Log	A text file containing detailed information collected inside the Sandbox VM.
	STIX IOC	Download the IOC in STIX2 format.
	Traffic Signature	Displays the signatures of industrial application network traffic that are detected. Click the name to go to its FortiGuard page.
	IPS Signature	Displays IPS signatures that are detected, the signatures are displayed. Click the name to go to its FortiGuard page.
	Screenshot	Download screenshot images when the file was running in the sandbox. This image is not always available.
	YARA Hits	If the file hits FortiSandbox internal YARA rules, detailed information is displayed.
	Office Behaviors	Suspicious indicators detected by FortiGuard advanced Office file static scan engine.
	Virtual Simulator	Suspicious indicators detected by FortiGuard advanced Web file static scan engine.
	Indicators	A summary of behavior indicators, if available. When detailed information is available below, a question mark icon is displayed. When clicked, detailed information is displayed. For some operations, such as File Operations, users can download files in a password protected ZIP format.
	MITRE ATT&CK Matrix	Displays malware's attack techniques and tactics. By default, a light version is displayed. Click the toggle button to swap between the Lite Matrix and Full Matrix.
	Botnet Info	The botnet name and target IP address.
	Files Operations	The file-related operations, includes Created/Deleted/Renamed/Modified/Set Attributes.

Item		Description
	Registry Operations	The registry-related operations, includes Created/Deleted.
	Memory Operations	The memory-related operations, includes Process Related/Process Created/Process Created and Injected/Written.
	Network Operations	Users that are infected by this executable will notice HTTP connections with certain URL/IP addresses. Click the *Network Behaviors* dropdown icon to view the network behavior of the file. This field may not be available for all file types. For certain document files, if they contain malicious URLs, those URLs are displayed here. Users can select a URL to display its detailed information, like rating history and visit volume history.
	Behaviors In Sequence	The executable file's behavior during execution, in time sequence.
	Tracer/Rating Engine Version	The tracer/rating package version is displayed at the bottom of the job detail page and in the PDF Report.
	Video Download Link	Download the video when the *Record Video* is enabled.

Appendix C - Malware types

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

Malware 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.
Stealer	Stealer malware is used to harvest login credentials of standalone systems, networks, FTP, email, game servers and other websites. Once the system is infected, the malware can be customized by the attacker.
Backdoor	Backdoor malware installs a network service for remote access to your network. This type of malware can be used to access your network and install additional malware, including stealer and downloader malware.
Injector	Injector malware injects malicious code into system processes to perform tasks on its behalf.
Rootkit	Rootkit malware attempts to hide its components by replacing vital system executables. Rootkits allow malware to bypass antivirus detection as they appear to be necessary system files.
Adware	Adware malware is a software package which attempts to access advertising websites. Adware displays these unwanted advertisements to the user.
Dropper	Dropper malware is designed to install malicious software to the target system. The malware code may be contained within the dropper or downloaded to the target system once activated.
Downloader	Downloader malware attempts to download other malicious programs.
Trojan	Trojan malware is a hacking program which gains privileged access to the operating system to drop a malicious payload, including backdoor malware. Trojans can be used to cause data damage, system damage, data theft or other malicious acts.
Riskware	Riskware malware has security-critical functions which pose a threat to the computer.
Grayware	Grayware malware is a classification for applications that behave in a manner that is annoying or undesirable. Grayware includes spyware, adware, dialers, and remote access tools that are designed to harm the performance of computers on your network.

Fortinet Ex. 2003 - Page 240 of 245

Malware type	Description
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.

Appendix D - Maximum Values

This topic provides minimum/maximum values for configurations, file size limits, and concurrent client device connections.

- Configuration limits on page 242
- File size limits on page 243
- Client Device Connections

Configuration limits

Job inputs	Min value	Max value	Default value	Configurable
Filename length	1	4096 characters		
Directly URL length	1	3 KB characters		
On Demand job comments lengths	0	255 characters		
Number of children files to unpack from archive file	1	No max	1000 for VM appliance 10,000 for hardware appliance	Y
File size to enter VM		512 MB		
Archive file unpack timeout	1 1	No max	15s for regular file (< 512 MB) 60s for big file (>512 MB)	Y
Allow/Block list	**Min value**	**Max value**	**Default value**	**Configurable**
URL length	1	2048 characters		
Domain name length	1	253 characters		
URL Regex	1	1024 characters		

MD5+SHA1+SHA256 record limit in list	0	50,000		
URL Regex records	0	1,000		
Domain + URL records	0	50,000		
Custom VM				
VM meta file for Installed Applications	0	50 lines		
IOC Package	**Min value**	**Max value**	**Default value**	**Configurable**
Malware/URL/TCP RST package entries counts	0	10,000		
Scan Profile	**Min value**	**Max value**	**Default value**	**Configurable**
URL scan depth	0	5	0	Y
VM Scan timeout for executable file	60s	180s	180s	Y
VM Scan timeout for non-executable file	45s	180s	60s	Y
VM Scan timeout for URL	30s	1200s	60s	Y
System Login	**Min value**	**Max value**	**Default value**	**Configurable**
LDAP/Radius remote authentication	10s	180s	10s	Y
Radius PAP secret		52 characters		
GUI idle time	1 min	480m	30m (For Azure 3m)	Y
User management	**Min value**	**Max value**	**Default value**	**Configurable**
Username length	1	64 characters		
User password	6 characters	64 characters		

File size limits

File size limits are determined by the input type (on-demand, sniffer etc).The default limit for each type is set to 200MB for single file and 500MB for uncompressed archives. You view or change the file-size limit with the CLI.

Hardware	Device	Adapter	Netshare	Sniffer	ICAP	JsonRPC	On-Demand
Single File (MB)	512	1024	1024	1024	1024	1024	1024
Uncompressed Archive (MB)	2048	2048	2048	2048	2048	2048	2048
Virtual (VM00)	**Device**	**Adapter**	**Netshare**	**Sniffer**	**ICAP**	**JsonRPC**	**On-Demand**
Single File (MB)	512	1024	10240	1024	1024	10240	10240
Uncompressed Archive (MB)	2048	2048	10240	2048	2048	10240	10240
FortiSandbox Cloud (PaaS)	**Device**						**On-Demand**
Single File (MB)	1024						1024
Uncompressed Archive (MB)	2048						2024
FortiGate Cloud Sandbox (SaaS)	**Device**						**On-Demand**
Single File (MB)	200						200
Uncompressed Archive (MB)	500						500

To view or change the file size limit with the CLI:

```
filesize-limit
```

For more information, see FortiSandbox CLI Reference Guide in the Fortinet Documents Library.

Client Device Connections

A FortiSandbox system deployed in either a standalone or cluster has a maximum authorized limit of 10,000 FortiGate devices and 50,000 FortiClient endpoints.

The maximum concurrent connection limit from the devices and endpoints is 10,000 connections. The concurrent connection is for file uploading and result query. Note that for ICAP adapter, the concurrent connections from the devices is only 500 connections.

Full capacity will depend on the model and its system capacity.

www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.