Integrating FortiSandbox into FortiMail

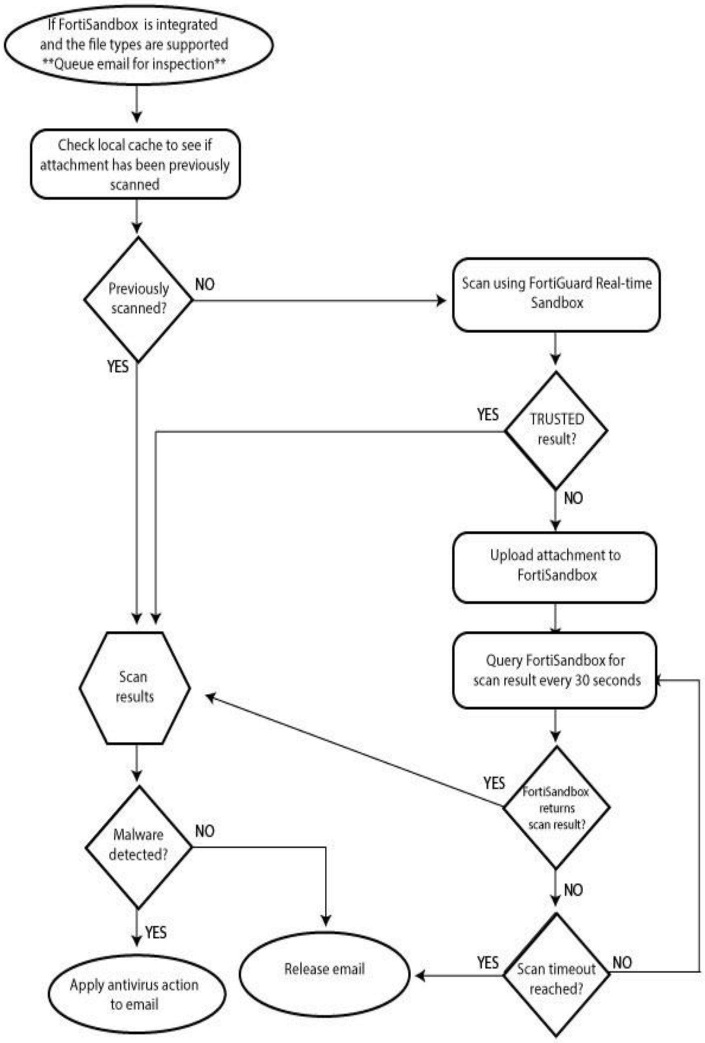
FortiSandbox is a key part of Fortinet's innovative Advanced Threat Protection solution. Recommended by NSS Labs, FortiSandbox is designed to detect and analyze advanced targeted attacks designed to bypass traditional security defenses.

This topic details how FortiSandbox works and guides you through the process of integrating FortiSandbox with FortiMail.

Understanding FortiSandbox

While traditional signature-based systems rely on predefined virus signatures to catch viruses, FortiSandbox looks at the construction of files for characteristics commonly found in viruses and emulates the execution looking for typical virus behavior. As a file is examined, the virus-like attributes are totaled. If a threshold in the number of virus-like attributes is passed, the file is marked as suspicious.

The illustration below details the scanning process.



If FortiSandbox is integrated and the file types are supported **Queue email for inspection**
Check local cache to see if attachment has been previously scanned
Previously scanned?
NO
YES
Scan using FortiGuard Real-time Sandbox
TRUSTED result?
YES
NO
Upload attachment to FortiSandbox
Query FortiSandbox for scan result every 30 seconds
Scan results
FortiSandbox returns scan result?
YES
NO
Malware detected?
NO
YES
Scan timeout reached?
YES
NO
Apply antivirus action to email
Release email

Connecting FortiSandbox

To connect FortiSandbox to FortiMail

1. Go to *AntiVirus* > FortiSandbox > FortiSandbox.
2. Enable *FortiSandbox Inspection*.
3. Enter an email address as the *Notification Email* if you want to be notified of protection activity.
4. Specify how long FortiMail should wait to retrieve high level statistics from FortiSandbox.

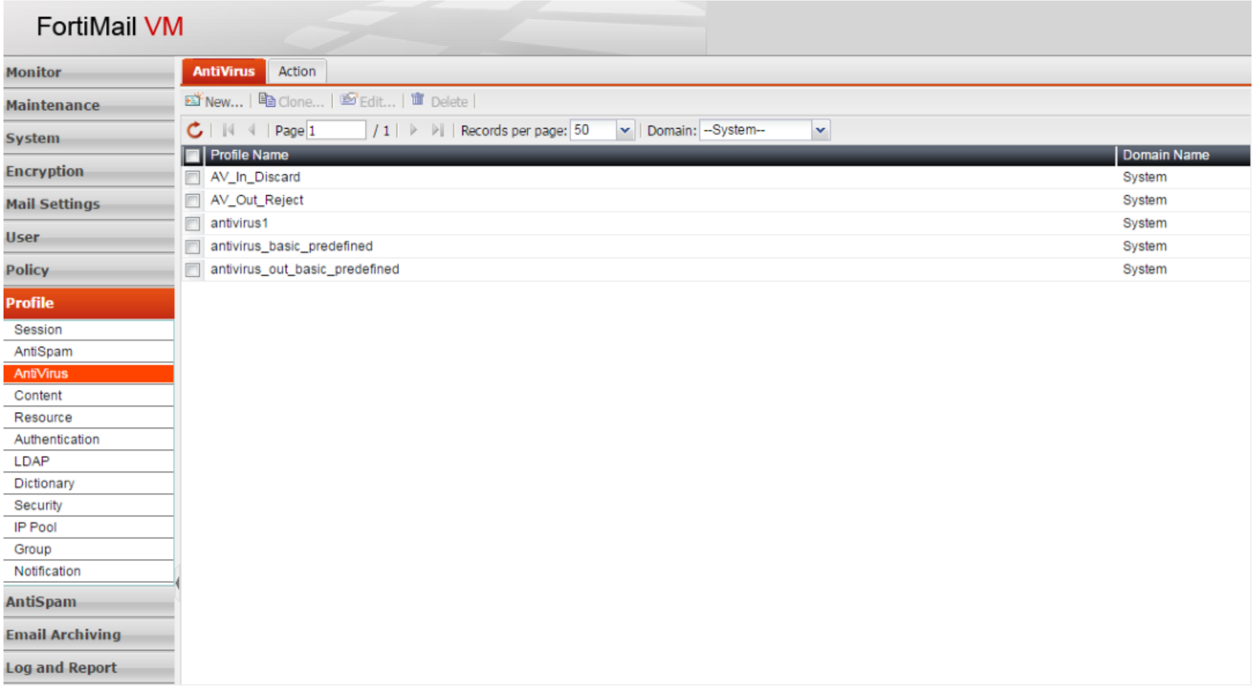
   Note: The statistics include the number of malware detected, and how many files are clean among the total number of files submitted.

Profile and Creation

Once FortiSandbox is connected, you'll need to create an AntiVirus profile that uses FortiSandbox.

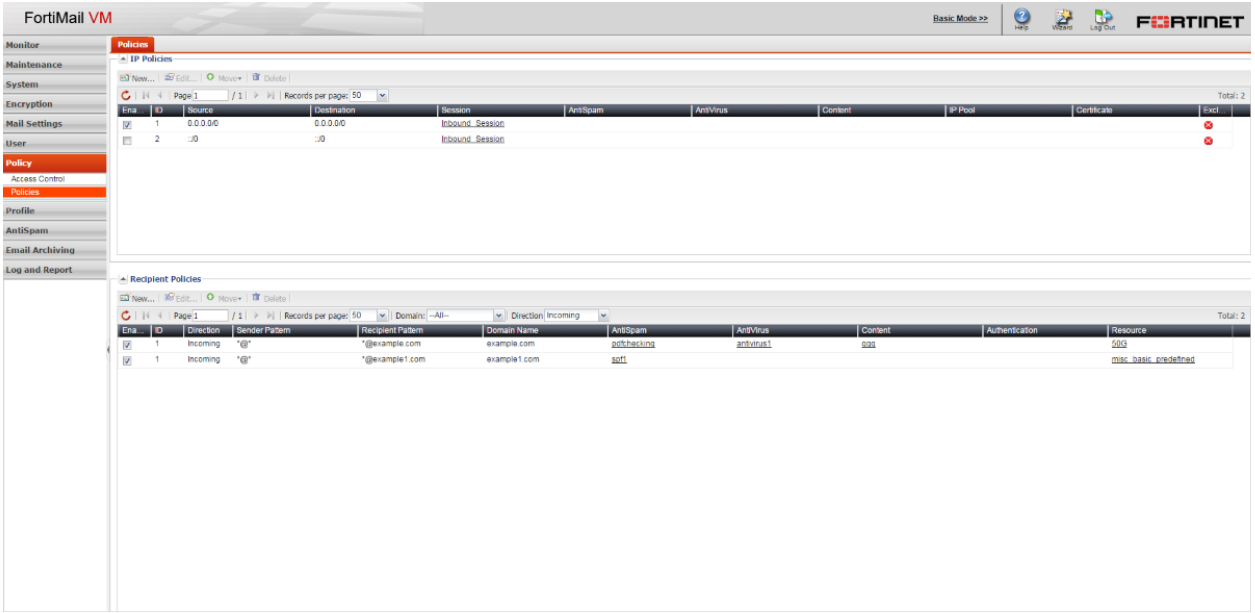
To create an AntiVirus profile:

1. Go to *Profile* > *AntiVirus* > *AntiVirus*.
2. Select *New*.



Profile Name	Domain Name
AV_In_Discard	System
AV_Out_Reject	System
antivirus1	System
antivirus_basic_predefined	System
antivirus_out_basic_predefined	System

3. Enter a name for the new profile and select a default action that FortiMail will take when encountering a threat.
4. Enable the *FortiSandbox* option. This enables FortiMail to send potentially harmful attachments to FortiSandbox for further analysis.
5. Specify the action to take if the FortiSandbox analysis determines that an email message includes a threat by selecting the appropriate action from the dropdown menu.
6. Go to *Policy* > *Policies*.



IP Policies

Page 1 / 1 | Records per page: 50 | Total: 2

Ena...	ID	Source	Destination	Session	AntiSpam	AntiVirus	Content	IP Pool	Certificate	Excl...
☑	1	0.0.0.0/0	0.0.0.0/0	Inbound_Session						✖
□	2	::/0	::/0	Inbound_Session						✖

Recipient Policies

Page 1 / 1 | Records per page: 50 | Domain: --All-- | Direction Incoming | Total: 2

Ena...	ID	Direction	Sender Pattern	Recipient Pattern	Domain Name	AntiSpam	AntiVirus	Content	Authentication	Resource
☑	1	Incoming	"@"	"@example.com	example.com	pdfchecking	antivirus1	ggg		50G
☑	1	Incoming	"@"	"@example1.com	example1.com	sof1				misc_basic_predefined

7. Select *New* under either the *IP Policies* or *Recipient Policies* section to create a new policy.
8. Select the newly created antivirus profile from the *AntiVirus* dropdown menu under the *Profiles* section.
9. Select **Create.**

Supported File Types

The list of files which FortiMail submits to the FortiSandbox for inspection is largely dependent on what files the FortiSandbox can support. The list of supported files is continuously growing. Below is the list of files currently supported in FortiMail 5.2.3 (FortiSandbox 2.0 or later).

- MS Word: docx, dotx, docm, dotm
- MS Excel: xlsx, xlsm, xltm, xlsb, xlam
- MS PowerPoint: pptx, ppsx, potx, sldx, pptm, ppsm, potm, ppam, sldm
- MS OneNote: onetoc
- MS Theme: thmx

- JAR
- SWF
- PDF
- Java script file
- Windows executable files such as .scr, .dll, .com, and .exe
- Archive files: .RAR and .ZIP