



FortiSandbox - AWS Guide

Version 3.2

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



April 30, 2020

FortiSandbox 3.2 AWS Guide

34-32-622454-20200430

TABLE OF CONTENTS

Overview	5
Deployment models	5
FortiSandbox VM basic deployment model	5
FortiSandbox VM advanced deployment model	6
Deploying FortiSandbox on AWS	7
Setting up basic AWS network	7
Creating a Virtual Private Cloud (VPC)	7
Creating the subnet for FortiSandbox firmware	8
Creating an internet gateway	10
Creating a route table	10
Creating a security group	12
Launching a FortiSandbox virtual instance in EC2	13
Choosing an Amazon Machine Image (AMI) and the instance type	13
Configuring the instance	14
Adding storage	15
Adding tags	15
Reviewing the instance launch	15
Configuring FortiSandbox network settings	17
Assigning an Elastic IP to the instance	17
Accessing the FortiSandbox web GUI	18
Configuring the DNS	19
Accessing FortiSandbox CLI	19
Testing FortiSandbox	19
FortiSandbox dashboard and contract information	19
Submit on-demand test using remote VM	20
FortiSandbox VM and WindowsCloudVMs topology	22
FortiSandbox VM Port Usage	23
Setting up an AWS account for FortiSandbox	23
Creating an IAM group	23
Attaching policies	24
Creating IAM users and an AWS API key	27
IAM Users	27
AWS API Key	29
Configuring the FortiSandbox GUI for AWS	30
Preparing network connection for FortiSandbox VM	31
Optional: Using a custom VM on AWS	32
Preparing the network interface for custom VM	33
Installing a custom VM using CLI	33
Test the installation	36
Interaction with a custom VM clone during scan	36
Optional: Using HA-Cluster	40
Launching an HA-Cluster	40
Configuring an HA-Cluster	41

Use Case: Instantaneous IOC Intelligence Sharing Across Multi-Clouds	43
Use Case: Fabric-Based Deep Analysis for Zero-Day Malware Detection	44
Adaptive Notification and Remediation	44
Use Case: FSA Cloud Scan Automation	45
S3 Bucket Scanning	46
Use Case: MTA Adapters	47
Change Log	50

Overview

Fortinet's FortiSandbox on AWS enables organizations to defend against advanced threats in the cloud. It works with network, email, endpoint, and other security measures, or as an extension of on-premise security architecture to leverage scale with complete control.

FortiSandbox is available on the AWS Marketplace.

You can install FortiSandbox on AWS as a standalone zero-day threat prevention or you can configure it to work with your existing FortiGate, FortiMail, or FortiWeb AWS instances to identify malicious and suspicious files, ransomware, and network threats.

Deployment models

You can configure your FortiSandbox VM on AWS using an advanced or basic deployment model.

FortiSandbox VM basic deployment model

The FortiSandbox basic deployment model is the fastest and easiest way to deploy a FortiSandbox VM on AWS. Basic deployment uses the AWS setup wizard to guide you through the setup process with step-by-step instructions. Deployment takes approximately 10 minutes.

Advantages

- A single setup wizard page where you can enter all the information for launching a FortiSandbox VM.
- Only simple information is required: VM region, EC2 instance type, and your EC2 keypair.
- HA features are supported by adding a second NIC during setup using the wizard.

Limitations

- The FortiSandbox VM can only have a maximum of two network interfaces when setup with the wizard.
- Supports sandboxing analysis using Windows Cloud VMs only.
- Does not support DHCP options and NAT Gateway that are required to run custom Windows VMs.

FortiSandbox VM advanced deployment model

To use the advanced features of the FortiSandbox VM including custom VMs and HA features, use the advanced deployment model. Advanced deployment requires you to manually create all the resources you need. This model is recommended for people who have experience working with AWS and the cloud. Deployment takes approximately one hour.

Advantages

- Gives you full control to customize the resources required to deploy the VM.
- Supports custom Windows VMs.
- Supports HA features.

Limitations

- Takes longer to deploy.
- Requires advanced knowledge of deploying VMs in AWS.
- Must deploy all components manually in AWS.
- Must follow instructions carefully for a successful deployment.

Deploying FortiSandbox on AWS

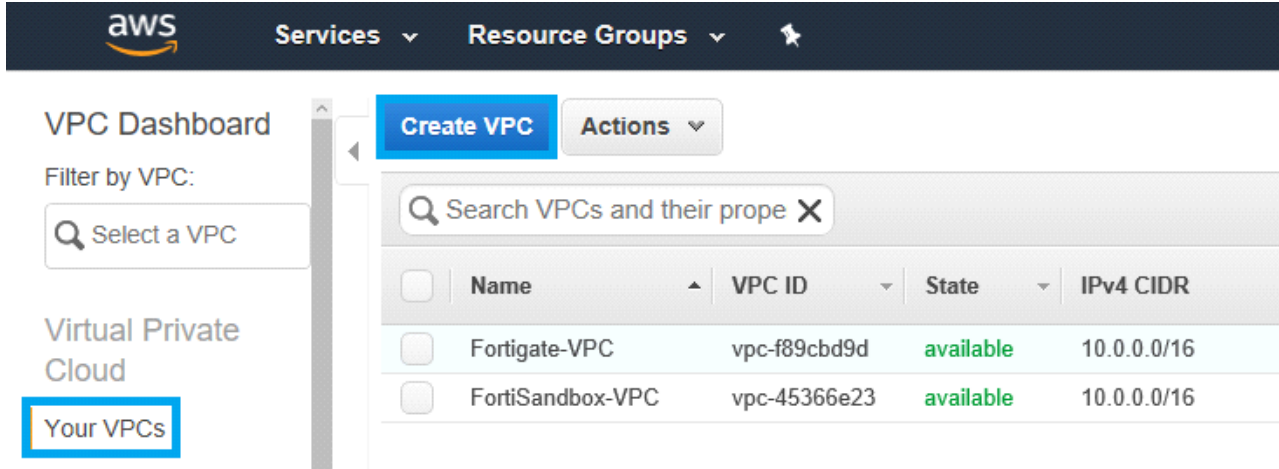
These procedures deploy FortiSandbox on AWS:

1. Setting up basic AWS network
2. Launching a FortiSandbox virtual instance in EC2
3. Configuring FortiSandbox network settings
4. Testing FortiSandbox
5. Setting up an AWS account for FortiSandbox
6. Preparing network connection for FortiSandbox VM
7. Optional: Using HA-Cluster
8. Optional: Using a custom VM on AWS

Setting up basic AWS network

Creating a Virtual Private Cloud (VPC)

1. Go to *VPC Dashboard > Your VPCs* and click *Create VPC*.



The screenshot shows the AWS VPC Dashboard. On the left, the 'Your VPCs' tab is selected. At the top, there is a 'Create VPC' button. Below it, a search bar is present. The main area displays a table of VPCs:

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR
<input type="checkbox"/>	Fortigate-VPC	vpc-f89cbd9d	available	10.0.0.0/16
<input type="checkbox"/>	FortiSandbox-VPC	vpc-45366e23	available	10.0.0.0/16



Create a new VPC even though there is a default VPC.

2. Enter the following information, then click *Yes, Create*.
 - For *Name tag*, enter a name. For example, *FortiSandbox*.
 - For *IPv4 CIDR block*, enter *10.0.0.0/16*. This helps ease scale-out issues in the future.

- For *IPv6 CIDR block*, select *No IPv6 CIDR Block*.
- For *Tenancy*, select *Default*.

Create VPC ✕

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag ⓘ

IPv4 CIDR block* ⓘ

IPv6 CIDR block* ☒ No IPv6 CIDR Block ⓘ
☐ Amazon provided IPv6 CIDR block

Tenancy ⓘ

Cancel Yes, Create

Creating the subnet for FortiSandbox firmware

If you do not use Custom VMs, you don't have to create a private subnet. Even without a private subnet, you can still use the remote VM for file analysis.

- Public subnet with IPv4 CIDR 10.0.0.0/24, which is connected to the FSA-VM management interface.
- Private subnet with IPv4 CIDR 10.0.1.0/24, which is connected to all VM clones and FSA-VM.
- HA-Cluster subnet is optional for HA-Cluster.

To create the public subnet:

1. Click *Subnets > Create Subnet*.
2. In the *Create Subnet* dialog box, enter the following information, then click *Yes, Create*.
 - For *Name tag*, enter a name. For example, *Public_FortiSandbox*.
 - For *VPC*, select the VPC you just created.
 - For *IPV4 CIDR block*, enter *10.0.0.0/24* (public subnet).

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tagPublic_FortiSandbox

VPCvpc-13818f7a | FortiSandbox

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

Availability ZoneNo Preference

IPv4 CIDR block10.0.0.0/24

Cancel

Yes, Create

To create the private subnet:

1. Click *Subnets > Create Subnet*.
2. In the *Create Subnet* dialog box, enter the following information, then click *Yes, Create*.
 - For *Name tag*, enter a name. For example, *Private_FortiSandbox*.
 - For *VPC*, select the VPC you just created.
 - For *IPv4 CIDR block*, enter *10.0.1.0/24* (private subnet).

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tagprivate_FortiSandbox

VPCvpc-13818f7a | FortiSandbox

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

Availability ZoneNo Preference

IPv4 CIDR block10.0.1.0/24

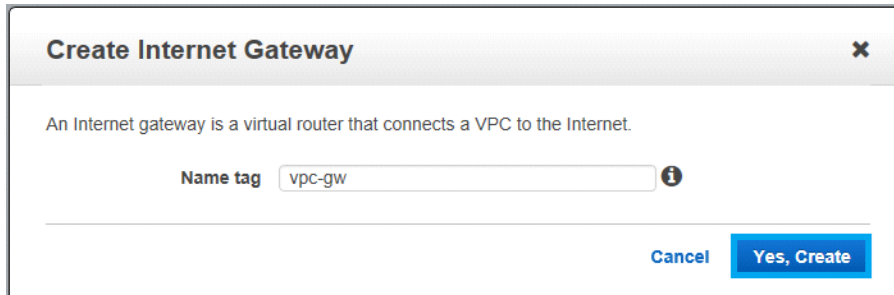
Cancel

Yes, Create

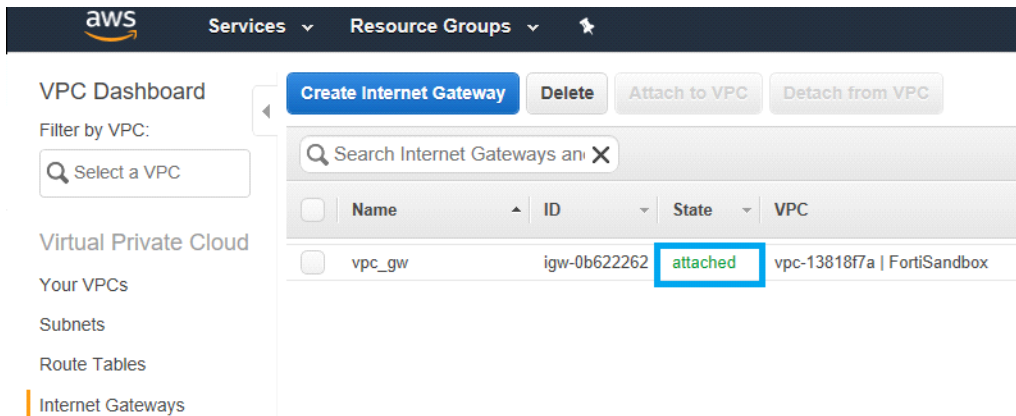
3. If you want, repeat the above steps to create an HA-Cluster subnet.

Creating an internet gateway

1. Under *Virtual Private Cloud > Internet Gateways*, click *Create Internet Gateway*.
2. For *Name tag*, enter a name. For example, *vpc-gw* and click *Yes, Create*.



3. When the Internet Gateway is created, click *Attach to VPC*.
4. Select the VPC and click *Yes, Attach*.

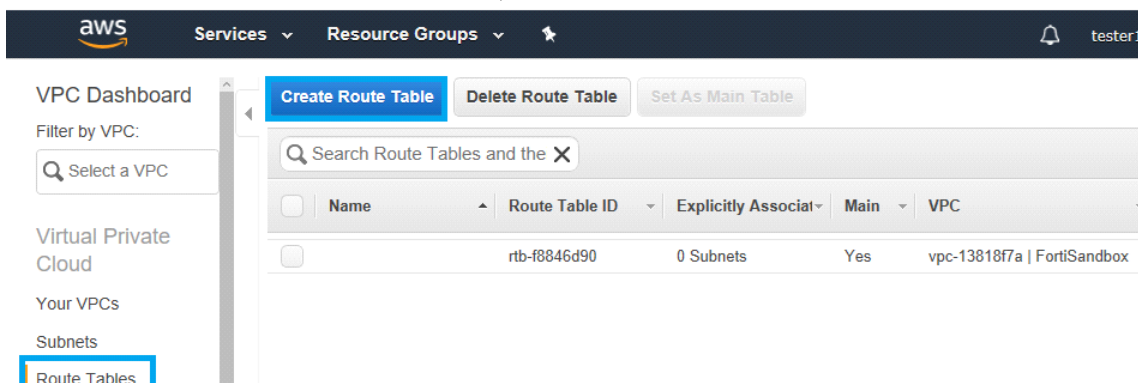


The screenshot shows the AWS VPC Dashboard. On the left, the 'Internet Gateways' link is highlighted in the navigation menu. The main panel shows a table of Internet Gateways. One gateway is listed with the name 'vpc-gw', ID 'igw-0b622262', and state 'attached'. The 'Attach to VPC' button is highlighted in blue.

Name	ID	State	VPC
vpc-gw	igw-0b622262	attached	vpc-13818f7a FortiSandbox

Creating a route table

1. Under *Virtual Private Cloud > Route Tables*, click *Create Route Table*.



The screenshot shows the AWS VPC Dashboard. On the left, the 'Route Tables' link is highlighted in the navigation menu. The main panel shows a table of Route Tables. One route table is listed with the name 'rtb-f8846d90', ID 'rtb-f8846d90', and state '0 Subnets'. The 'Create Route Table' button is highlighted in blue.

Name	Route Table ID	Explicitly Associat	Main	VPC
rtb-f8846d90	rtb-f8846d90	0 Subnets	Yes	vpc-13818f7a FortiSandbox

- In the *Create Route Table* dialog box, enter the following information, then click *Yes, Create*.
 - For *Name tag*, enter a name. For example, *route_FortiSandboxTest*.
 - For *VPC*, select the VPC you created.

Create Route Table ✕

A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Name tag ?

VPC ?

Cancel
Yes, Create

- Go to *Subnet Associations > Edit*, select the public subnet you created, then click *Save*.

rtb-474aa32f | route_FortiSandbox(public)

Summary
Routes
Subnet Associations
Route Propagation
Tags

Cancel
Save

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input checked="" type="checkbox"/>	subnet-1e41d853 Public_FortiSandbox	10.0.0.0/24	-	rtb-474aa32f route_FortiSandbox(public)
<input type="checkbox"/>	subnet-c245dc8f Private_fortisandbox	10.0.1.0/24	-	rtb-77769f1f route_Fortisandbox(private)

- Go to *Routes > Add Another Route*, enter the following information, then click *Save*.

- For *Destination*, enter 0.0.0.0/0.
- For *Target*, select the internet gateway for the public subnet.

rtb-474aa32f | route_FortiSandbox(public)

Summary
Routes
Subnet Associations
Route Propagation
Tags

Cancel
Save

View: All rules

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
<input data-bbox="203 1661 500 1696" type="text" value="0.0.0.0/0"/>	<input data-bbox="505 1661 954 1696" type="text" value="igw-0b622262"/>	Active	No	✕

Add another route

Creating a security group

1. Under *Virtual Private Cloud > Security Groups*, click *Create security group*.
2. Enter the following information, then click *Create*.
 - For *Security group name*, enter a name.
 - For *Description*, enter a description.
 - For *VPC*, select the VPC you just created.

[Security Groups](#) > Create security group

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group fill in the fields below.

Security group name* ⓘ

Description* ⓘ

VPC ⓘ

* Required

Filter by attributes

VPC ID	Name tag	Owner
vpc-0cd46d3fe45dd6f2b	vpc10.100	730432517238
vpc-979b7dee	vpc10.0	730432517238
vpc-0aa30ee8fac21ee54	easy10.10	730432517238
vpc-04c716595f063c268	vpc10.200	730432517238

Cancel Create

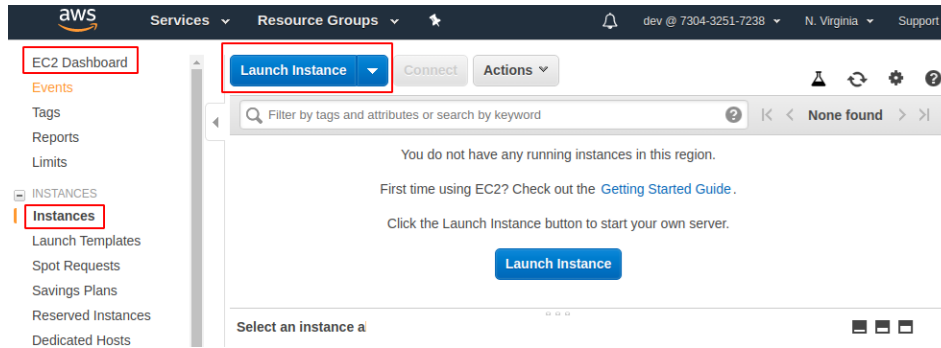
3. Configure the following:

Details	Value
Type	All Traffic. You can select TCP.
Protocol	All. You can select TCP.
Port Range	If you select <i>All</i> for <i>Protocol</i> , the <i>Port Range</i> is automatically selected. If you select TCP, allow all the following: <ul style="list-style-type: none"> • HTTPS (TCP 443) • SSH traffic (TCP 22) • OFTP traffic (TCP 514) • Optional: FTP (TCP 21) • If needed: RDP to VM interaction
Source	Custom. For the <i>SourceIP</i> , enter 0.0.0.0/0.

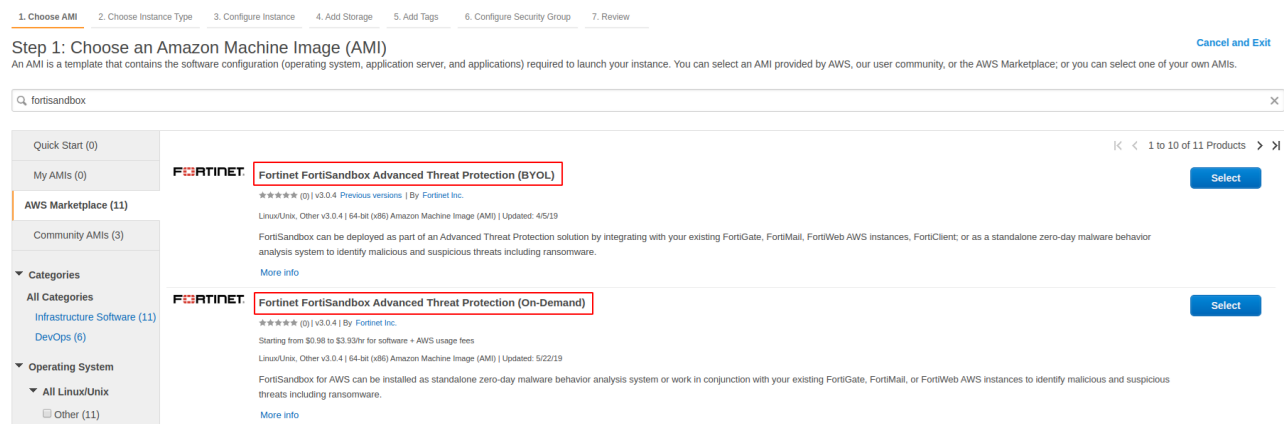
Launching a FortiSandbox virtual instance in EC2

Choosing an Amazon Machine Image (AMI) and the instance type

1. Go to *EC2 > Instances* and click *Launch Instance*.

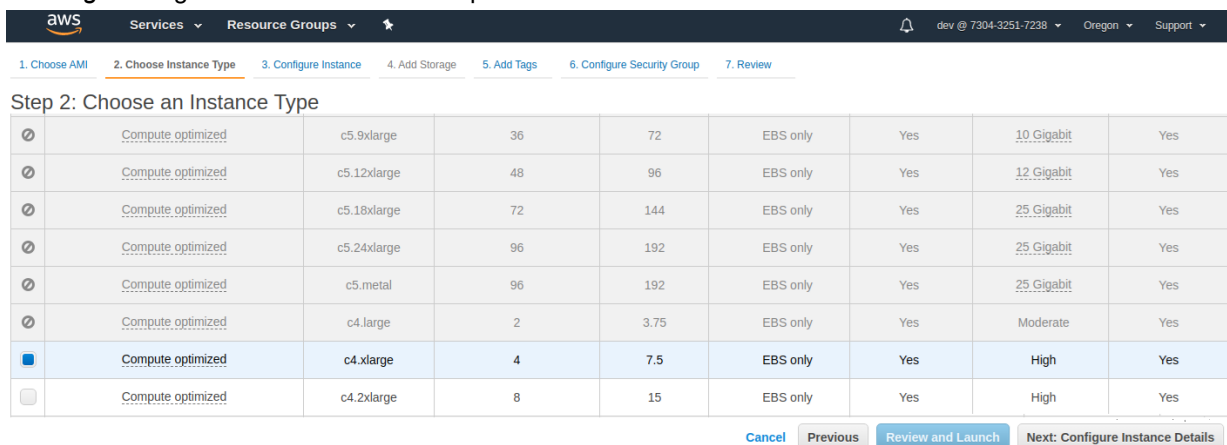


2. In the left panel, click *AWS Marketplace* and search for *fortisandbox* AMI.



3. Select *Fortinet FortiSandbox Advanced Threat Protection (BYOL)* or *Fortinet FortiSandbox Advanced Threat Protection (On-Demand)*.

- If you selected *Fortinet FortiSandbox Advanced Threat Protection (BYOL)*, select an *Instance Type* that is *c4.xlarge* or larger for balanced burstable performance.



- If you selected *Fortinet FortiSandbox Advanced Threat Protection (On-Demand)*, select an *Instance Type* that is *m4.xlarge* or larger for balanced burstable performance.

The screenshot shows the AWS Management Console interface for creating an EC2 instance. The 'Step 2: Choose an Instance Type' screen is active. A table lists various instance types, with 'm4.xlarge' selected. The table columns include instance type, vCPUs, memory (GiB), storage type, EBS only, tenancy, network performance, and on-demand baseline. The 'm4.xlarge' instance is highlighted with a blue selection bar.

Instance Type	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
<input checked="" type="radio"/>	General purpose	m5.8xlarge	32	128	EBS only	Yes	10 Gigabit	Yes
<input checked="" type="radio"/>	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
<input checked="" type="radio"/>	General purpose	m5.16xlarge	64	256	EBS only	Yes	20 Gigabit	Yes
<input checked="" type="radio"/>	General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
<input checked="" type="radio"/>	General purpose	m5.metal	96	384	EBS only	Yes	25 Gigabit	Yes
<input type="radio"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
<input checked="" type="radio"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
<input type="radio"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes

Buttons at the bottom: Cancel, Previous, Review and Launch, Next: Configure Instance Details

4. Click *Next: Configure Instance Details*.

Configuring the instance

Configure the following instance details, then click *Next, Add Storage*.

Details	Values
Number of Instances	1
Purchasing Option	N/A
Network	Select the FortiSandbox VPC you created
Subnet	Select the public subnet you created
Auto-Assign Public IP	Disable
IAM Role:	None
Shutdown Behavior	Stop
Enable Termination Protection	N/A
Monitoring	N/A
Tenancy	Shared - Run a shared hardware instance
eth0	Select the public subnet you created; Auto-Assign (or any IP in that subnet)
eth1	Select the private subnet you created; Auto-Assign (or any IP in that subnet)



If you do not use trial VMs or custom VMs, you can skip adding `eth1`. You can add it back when the instance is stopped.

Adding storage

After configuring the Instance Details, click *Next, Add Storage*.

Adding tags

Do not configure anything on this page. Click *Next, Configure Security Group*. See [Creating a security group on page 12](#).

Reviewing the instance launch

1. Review the instance details, then click *Launch* to open the *Create a New Key Pair* dialog box.
2. Enter a *Key pair name*.
3. Click *Download Key Pair* and save the private key file.

You can import an existing public key for remote access to the running instance.

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.


Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

Fortisandboxkey

Download Key Pair

 You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

4. Click *Launch Instances*.
After launching the instance, the next page shows that the FortiSandbox instance is running.
5. Click *View Instances* to view the instance state.
It takes several minutes for *Status Checks* to change from *Initializing* to *2/2 checks*.

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
<input type="checkbox"/>	FortiSandbox	i-0550184bac6acd53b	t2.medium	us-west-2b	<div>● running</div>	<div>✓ 2/2 checks...</div>	None
<input type="checkbox"/>		i-079847bfb1bf0e096	t2.medium	us-west-2b	<div>● running</div>	<div>⌚ Initializing</div>	None

6. When the instance is running, click the instance and enter a name. For example, *FortiSandbox*.

Launch Instance

Connect

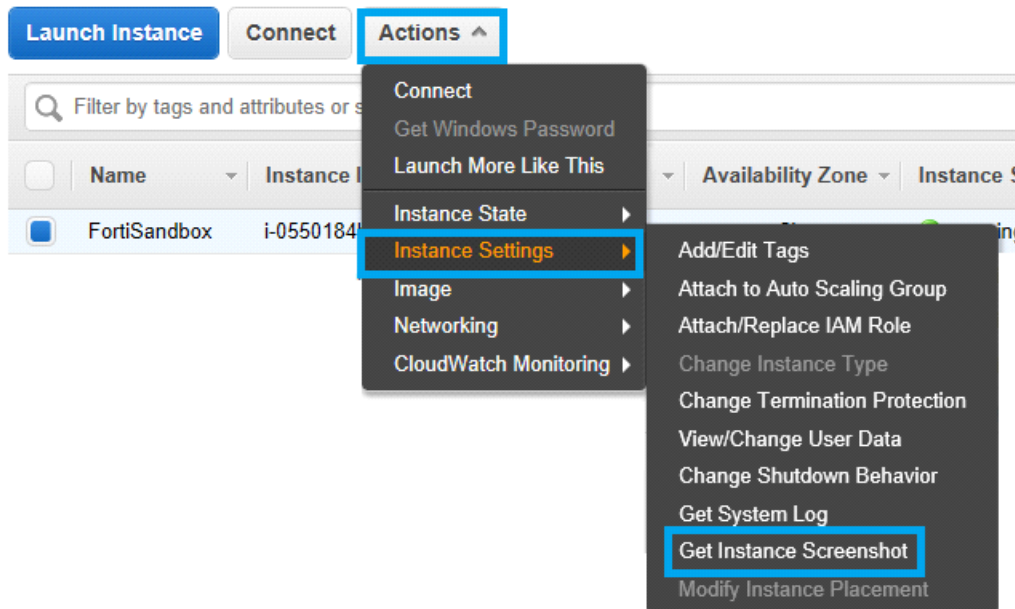
Actions

Filter by tags and attributes or search by keyword

?

<input type="checkbox"/>	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	
<input checked="" type="checkbox"/>	FortiSandbox	i-0550184bac6acd53b	t2.medium	us-west-2b	● running	✓ 2/2 checks...	None	
<input type="checkbox"/>	12/255	i-079847bfb1bf0e096	m3.xlarge	us-west-2a	● stopped		None	

7. Select the created instance and go to *Actions > Instance Settings > Get Instance Screenshot* to view the status of the launched instance.

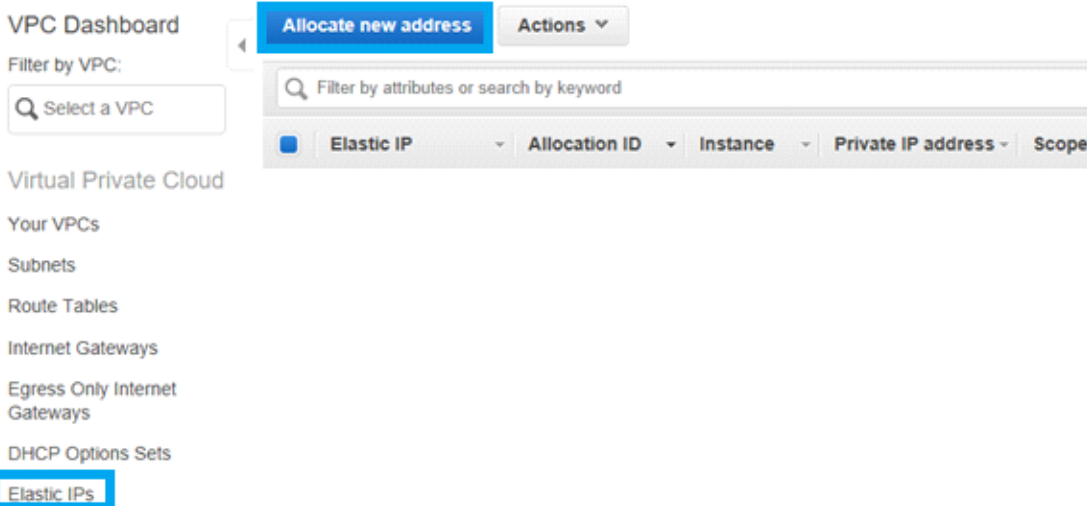


Configuring FortiSandbox network settings

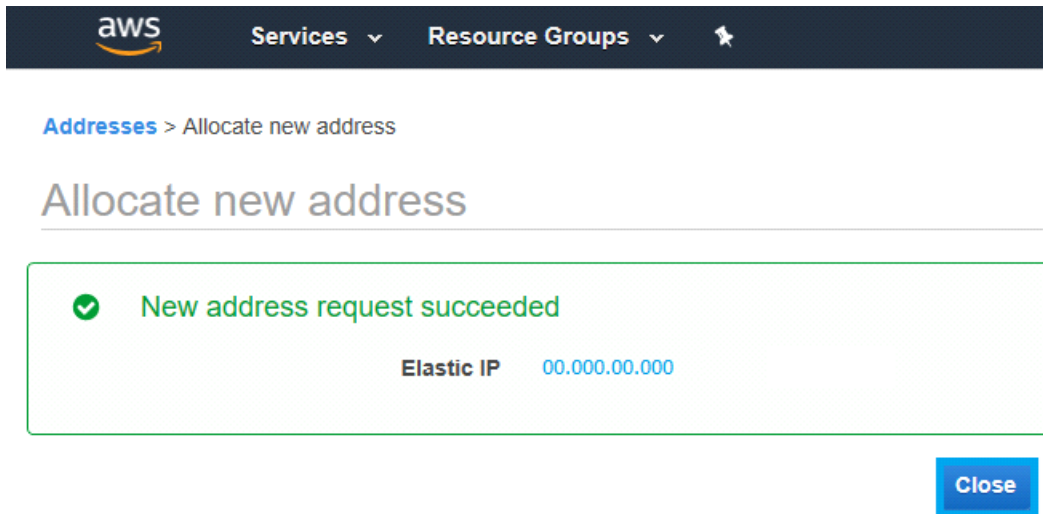
Assigning an Elastic IP to the instance

If necessary, create an Elastic IP (EIP) under Virtual Private Cloud.

1. Click *Elastic IPs* > *Allocate new address*.



2. Click *Allocate new address* to get the new EIP Address.
3. When you see the new *Elastic IP* address, click *Close*.



4. Select the new Elastic IP address you just created and click *Actions* to associate the EIP with FortiSandbox port1.
5. On the Associate Elastic IP Address page:
 - In the *Resource type* section, select *Network Interface*.
 - In the *Network Interface* section, select the FortiSandbox port1.
 - In the *Private IP address* section, select the FortiSandbox port1 private IP address.
 - In the *Reassociation* section, clear the *Allow this Elastic IP address to be reassociated* checkbox.

EC2 > Elastic IP addresses > Associate Elastic IP address

Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (52.39.221.107)

Elastic IP address: 52.39.221.107

Resource type
Choose the type of resource with which to associate the Elastic IP address.

☐ Instance

☒ Network interface

Network Interface
eni-0f420ed98d60b04b2

Private IP address
The private IP address with which to associate the Elastic IP address.
10.0.0.20

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

☐ Allow this Elastic IP address to be reassociated

Cancel Associate

- Click **Associate**.

Accessing the FortiSandbox web GUI

- Copy the *IPv4 Public IP* address from the created instance.

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
<input type="checkbox"/>	FortiSandbox	i-0550184bac6acd53b	t2.medium	us-west-2b	running	2/2 checks...	None		00.00.00.000
<input checked="" type="checkbox"/>	FortiSandbox_test	i-079847bfb1bf0e096	t2.medium	us-west-2b	running	2/2 checks...	None		00.000.00.00

- Paste the copied IP address into a browser window to log into the FortiSandbox GUI.
The default username is *admin* and the default password is your Instance ID. You can find this in the EC2 Management Console.

Configuring the DNS

1. Go to *Network > System DNS*.
2. Configure the following:

Detail	Value
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4

3. Click *OK*.

Accessing FortiSandbox CLI

You can use CLI commands in the FortiSandbox console or use an SSH or TELNET client. Before logging in, convert the saved `pem` file you downloaded when you created the key pair `ppk` file.

If you did not choose the *Without Key Pair* option, log in using the *Instance ID* as the password.

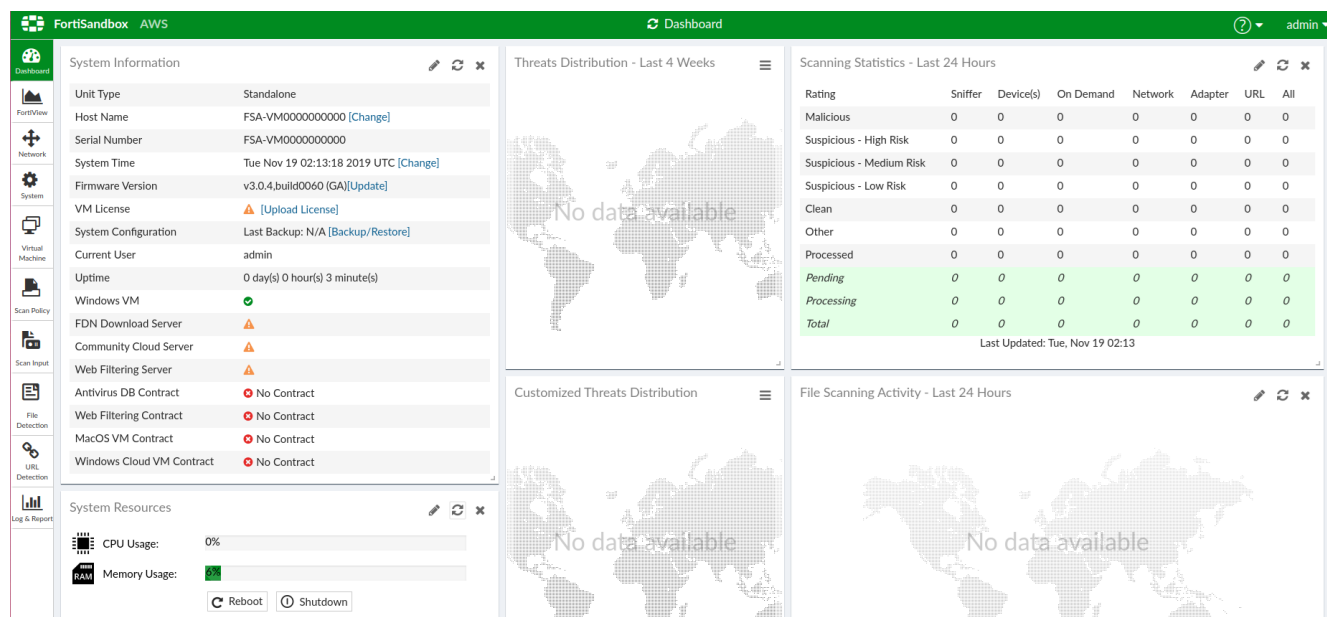
For more information, see [Connecting to Your Linux Instance Using SSH](#) and [Connecting to Your Linux Instance from Windows Using PuTTY](#).

Testing FortiSandbox

FortiSandbox dashboard and contract information

Upload the FortiSandbox license for AWS FortiSandbox BYOL.

VM license is not needed for AWS FortiSandbox On-Demand.



Submit on-demand test using remote VM

Starting with version 2.5.1, FortiSandbox AWS supports the WindowsCloudVM remote VM type.

You can change the maximum number of the remote VMs in *Virtual Machine > VM Images*.

Virtual Machine VM Status VM Images Scan Policy Scan Input File Detection	Optional VMs (0/0)							
	Customized VMs (0)							
	Remote VMs (2)							
	MACOSX	0	activated		2	0	mac dmg	
	WindowsCloudVM	0	activated		6	8	exe php tiff gif png tn mov doc mp3 rm doc pptm ppsm potm ppa pps pot upx WEBLink	
								Apply

To submit on-demand test using remote VM:

1. Go to *Scan Input > File On-Demand > Submit File*.
2. Click *Choose File* and upload the `fiddler2setup.exe` file.
3. Click *Submit*.

If the uploaded file is not malicious or suspicious, the rating is *Clean*.

FortiSandbox AWS

Dashboard
FortiView
Network
System
Virtual Machine
Scan Policy
Scan Input
File On-Demand
URL On-Demand
Job Queue
Device
FortiClient
Adapter
Network Share
Quarantine
Malware Package
URL Package

Submit New File

Please upload sample file or archived sample files. The following archive formats are supported: .tar, .z, .xz, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .tar.Z, .7z, .rar, .lzh, .ace

Skip:

- ☒ Static Scan
- ☒ AV Scan
- ☒ Community Cloud Query
- ☐ Sandboxing

Overwrite Scan Profile settings to Scan in VM type:

- ☐ MACOSX
- ☒ WindowsCloudVM

Select a file: No file selected.

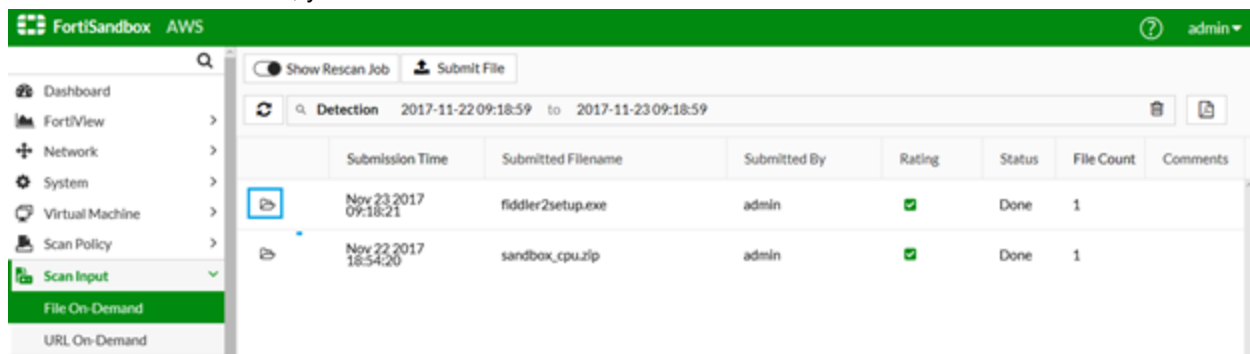
☐ Allow Interaction

☐ Add sample to threat package

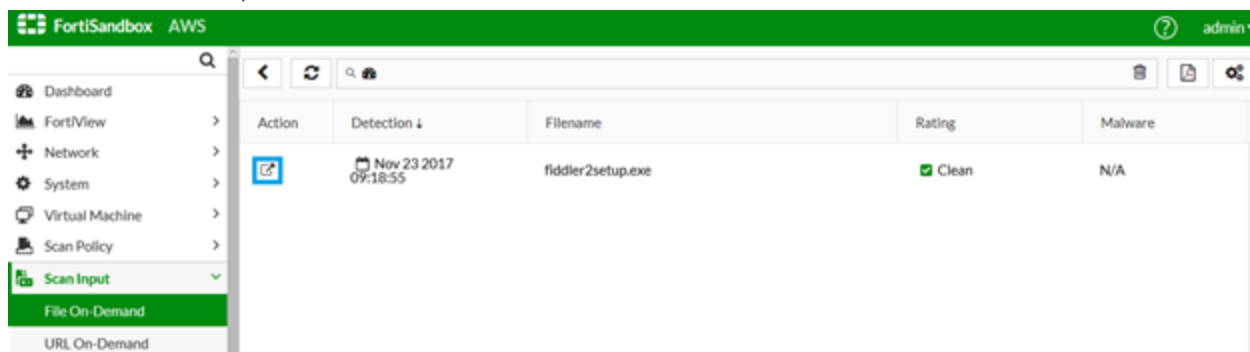
Possible password(s) for archive file:

Comments:

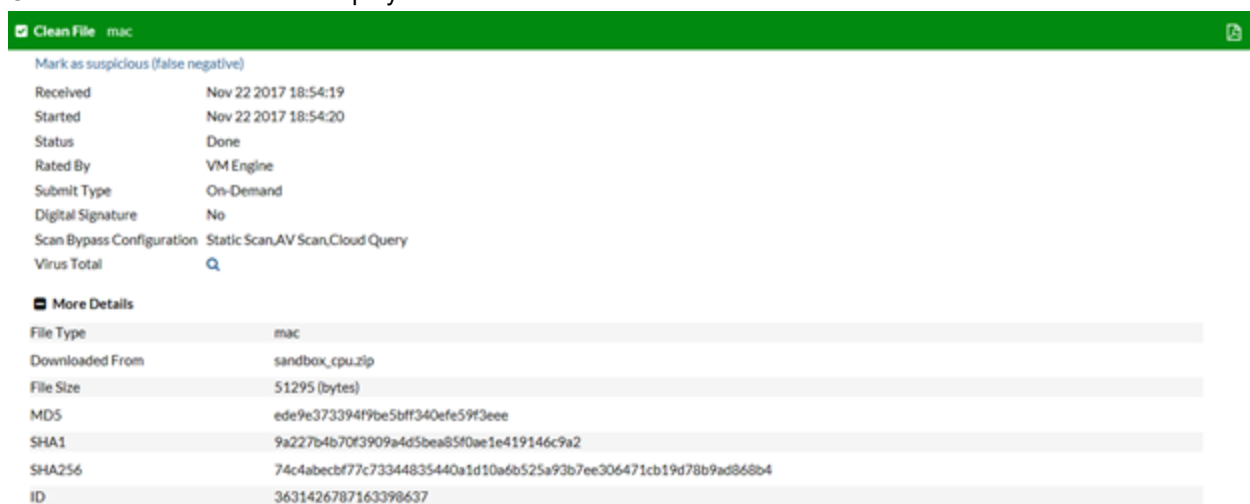
4. When the scan is finished, you can view files in *File On-Demand*.



5. In the *Action* column, click the *View File* icon.

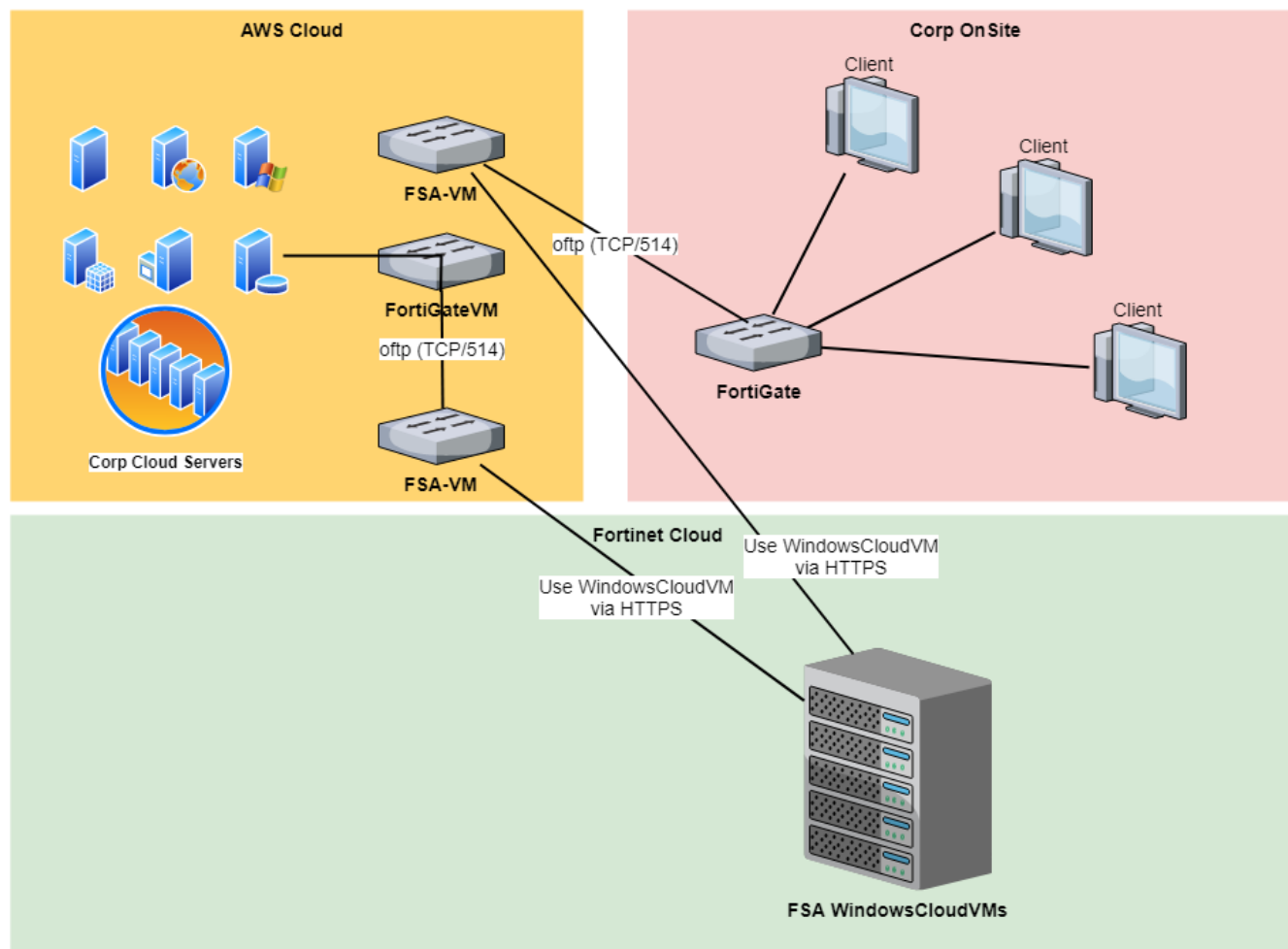


6. Check the file details that is displayed.



Detection Time	Nov 22 2017 18:59:09
Scan Time	289 seconds
Scan Unit	
Specified VMs	MACOSX
Launched OS	MACOSX
Behavior Summary	
This file modified files	
This file deleted files	
This file dropped files	
This file spawned process(es)	
Analysis Details	
MACOSX	
Original File	
Files Created (4)	
Files Deleted (2)	
Files Modified (4)	
Launched Processes (10)	
Tracer Package Version: 02005.00503	
Rating Package Version: 02005.00506	

FortiSandbox VM and WindowsCloudVMs topology



FortiSandbox VM Port Usage

Type	Service	Port
FortiGate	OFTP	TCP/514
FortiClient	File analysis	TCP/514
Others	SSH CLI management	TCP/22
	Telnet CLI management	TCP/23
	Web admin	TCP/80, TCP/443
	OFTP communication with FortiGate and FortiMail	TCP/514
	Third-party proxy server for ICAP servers (ICAP)	TCP/1344
	Third-party proxy server for ICAP servers (ICAPS)	TCP/11344
FortiGuard	FortiGuard distribution servers	TCP/8890
	FortiGuard web filtering servers	UDP/53, UDP/8888
FortiSandbox Community Cloud	Upload detected malware information	TCP/443, UDP/53
FortiSandbox WindowsCloudVMs	Serving WindowsVM on cloud for FSA-VM to perform sandboxing	TCP/443

Setting up an AWS account for FortiSandbox

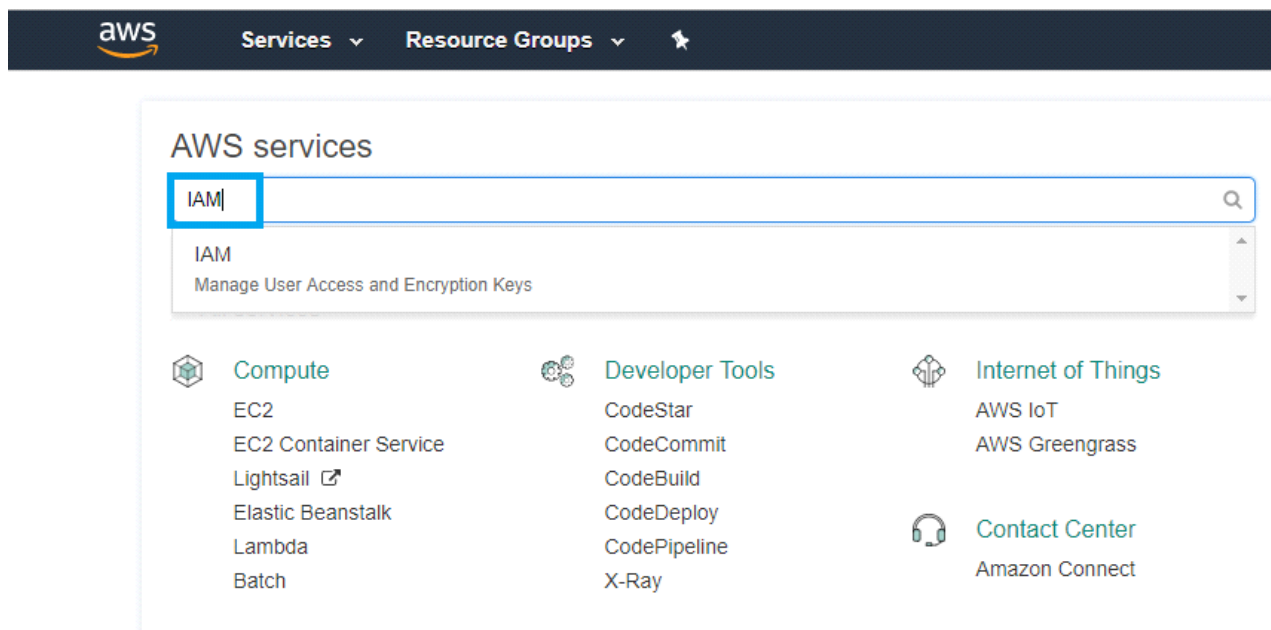
These procedures set up an AWS account for FortiSandbox:

1. [Creating an IAM group](#)
2. [Attaching policies](#)
3. [Creating IAM users and an AWS API key](#)
4. [Configuring the FortiSandbox GUI for AWS](#)

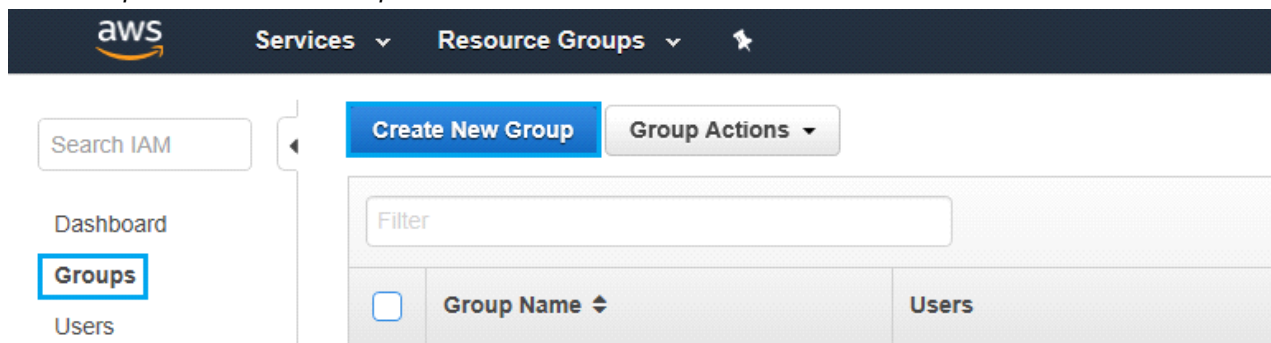
Creating an IAM group

1. In the *AWS Management Console*, create one or more IAM users.
2. Log into the AWS Console.

3. Click *Search* and search for *IAM*.



4. Click *Groups* > *Create New Group*.



5. In the *Group Name* field, enter a name, for example, *QA_FortiSandboxTest*.

Attaching policies

You must have the correct permissions to attach policies to a group. Add the following policies to the group you created (QA_FortiSandbox).

- AmazonEC2FullAccess
- IAMFullAccess
- AmazonS3FullAccess
- AdministratorAccess
- AmazonVPCFullAccess
- AWSImportExportFullAccess
- VMImportExportRoleForAWSConnector
- AmazonRoute53FullAccess

1. Click *Filter* and enter *AmazonEC2FullAccess*.
2. Select the checkbox beside *AmazonEC2FullAccess*.

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type Showing 1 results

	Policy Name	Attached Entities	Creation Time	Edited Time
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530

3. Repeat this for all policies.
4. After reviewing, click *Create Group* to list the group under *Groups*.

Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

Review

Review the following information, then click **Create Group** to proceed.

Group Name	Policies
QA_FortiSandboxTest	arn:aws:iam::aws:policy/PowerUserAccess arn:aws:iam::aws:policy/AmazonEC2FullAccess arn:aws:iam::aws:policy/AWSConfigUserAccess arn:aws:iam::aws:policy/IAMFullAccess arn:aws:iam::aws:policy/IAMUserSSHKeys

Cancel Previous **Create Group**

5. Check the group you created (*QA_FortiSandbox*) to review the group summary.

Search IAM

Dashboard

Groups

Users

Roles

Policies

Create New Group Group Actions

Filter

	Group Name	Users	Inline Policy
<input checked="" type="checkbox"/>	QA_FortiSandboxTest	1	✓

6. In the *Permissions* tab, review the attached policies; then under *Inline Policies*, click *Create Group Policy*.

The screenshot shows the AWS IAM console interface. On the left, the 'Groups' menu item is highlighted. The main content area shows the 'QA_FortiSandboxTest' group details. The 'Permissions' tab is selected, displaying a list of managed policies attached to the group. Below this, the 'Inline Policies' section is visible, and the 'Create Group Policy' button is highlighted.

Policy Name	Actions
AmazonEC2FullAccess	Show Policy Detach Policy Simulate Policy
IAMFullAccess	Show Policy Detach Policy Simulate Policy
AmazonS3FullAccess	Show Policy Detach Policy Simulate Policy
AdministratorAccess	Show Policy Detach Policy Simulate Policy
AmazonVPCFullAccess	Show Policy Detach Policy Simulate Policy
AWSImportExportFullAccess	Show Policy Detach Policy Simulate Policy

7. Select *Custom Policy* and use the policy editor to customize your own set of permissions.

The screenshot shows the 'Set Permissions' page in the AWS IAM console. The 'Custom Policy' option is selected under the 'Policy Generator' section. The 'Select' button is highlighted.

8. Enter a policy name and code.

9. Click *Validate Policy*. If validation is successful, click *Apply Policy*.

Customize permissions by editing the following policy document. For more information about the access guide. To test the effects of this policy before applying your changes, use the [IAM Policy Simulator](#).

This policy is valid.

Policy Name

testinlinepolicy

Policy Document

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:CreateRole",
8         "iam:PutRolePolicy",
9         "iam:ListRoles"
10      ],
11      "Resource": [
12        "*"
13      ]
14    }
15  ]
16 }
```

☒ Use autoformatting for policy editing

Cancel Validate Policy Apply Policy

10. Under *Inline Policies*, you can review the created policy names.

Creating IAM users and an AWS API key

IAM Users

To create an IAM user:

- Go to *Users* and click *Add User*.
- Configure the following and then click *Next: Permissions*.
 - For *User name*, enter a username.
 - For *Access type*, select *AWS Management Console access*.
 - For *Console Password*, select *Custom password* and enter a password.

Add user

1

Details

2

Permissions

3

Review

4

Complete

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* ☐ Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
☒ AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

Console password* ☐ Autogenerated password
☒ Custom password

☐ Show password

Require password reset ☒ User must create a new password at next sign-in
Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.

* Required

[Cancel](#)

[Next: Permissions](#)

3. Search for the *Group Name* you created (*QA_FortiSandbox*) and then click *Next: Review*.

Services
Resource Groups

Fortinet AWS
Global

Details
Permissions
Review
Complete

Set permissions for tester1

Add user to group

Copy permissions from existing user

Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Create group

Refresh

Q Search

Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> QA_FortiSandboxTest	AmazonEC2FullAccess and 5 m

[Cancel](#)
[Previous](#)
[Next: Review](#)

4. When you have added the group, click *Create User*.
5. Click *Close*.

6. Click *Groups* to view the user you created.

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

IAM > Groups > QA_FortiSandboxTest

Summary

Group ARN: arn:aws:iam::777823085352:group/QA_FortiSandboxTest

Users (in this group): 1

Path: /

Creation Time: 2017-10-23 13:05 UTC+0530

Users Permissions Access Advisor

This view shows all users in this group: 1 User

User	Actions
tester1	Remove User from Group

7. Log out of AWS and log in as the user you created.
8. Reset the password and click *Confirm* to change the password.

AWS API Key

API Gateway supports multiple mechanisms of access control including metering or tracking API use by clients using API keys.

To create an AWS API key:

1. Go to *IAM > Users > created user > Security credentials* and click *Create access key*.

aws Services Resource Groups

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Users > tester1

Summary

User ARN: arn:aws:iam::777823085352:user/tester1

Path: /

Creation time: 2017-10-23 14:12 UTC+0530

Permissions Groups (1) **Security credentials** Access Advisor

Sign-in credentials

Console password: Enabled [Manage password](#)

Console login link: <https://fortigate.signin.aws.amazon.com/console>

Last login: 2017-11-28 02:05 UTC+0530

Assigned MFA device: No

Signing certificates: None

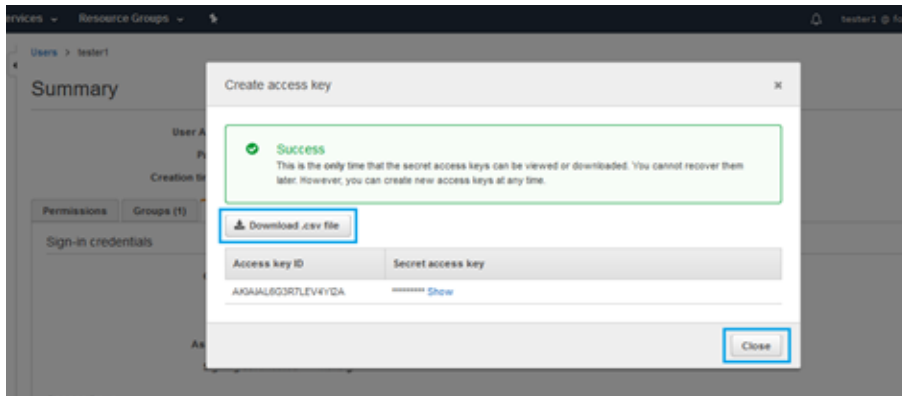
Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)

Create access key

Access key ID	Created	Last used	Status
---------------	---------	-----------	--------

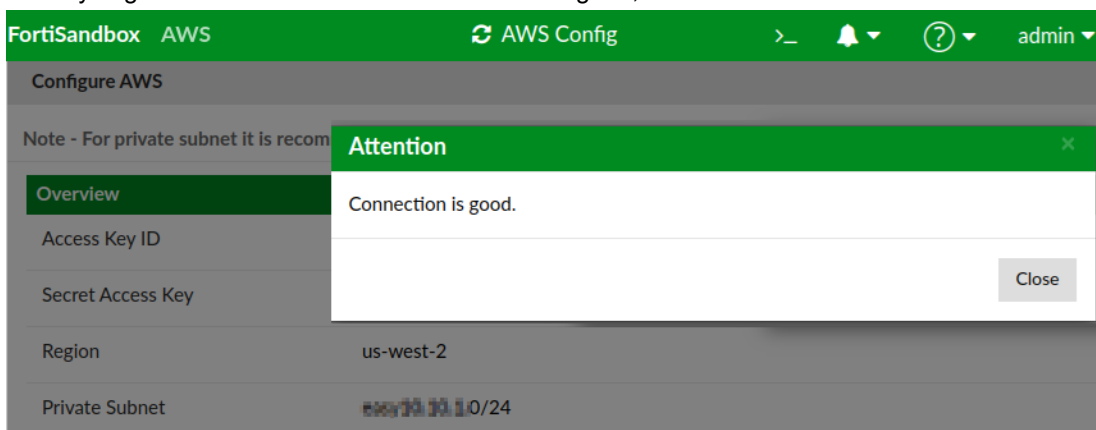
2. In the *Create access key* dialog box, click *Download.csv file* to save the *Access key ID*.



3. Click *Close*.

Configuring the FortiSandbox GUI for AWS

1. Go to *System > AWS Config* and enter the AWS API key information in the setup wizard.
2. Select *Local VM Instance Type* and then select the recommended *t2-medium*.
3. Click *Next*.
4. For *VPC ID*, select the VPC you created.
5. For *Private Subnet*, select the private subnet for VM.
For example, the private subnet with *IPv4 CIDR 10.0.1.0/24* which is connected to all VM clones and FSA-VM.
6. For *Security Groups*, select the security group.
7. Click *Save*.
8. Click *Connection Test*.
9. When you get a confirmation that the connection is good, click *Close*.



Preparing network connection for FortiSandbox VM

The Private Subnet (IPv4 CIDR 10.0.1.0/24) is connected to all VM clones and FSA-VM.

To create a private subnet:

1. Click *Create Subnet* and configure the following information.
 - For *Name tag*, enter a name. For example, `private_FortiSandbox`.
 - For *VPC*, select the VPC you created.
 - For *IPv4 CIDR block*, enter `10.0.1.0/24` (for private subnet).

The screenshot shows the AWS Management Console interface. On the left, the 'Subnets' link is highlighted under 'Your VPCs'. The main area displays a list of subnets. A 'Create Subnet' modal dialog is open, showing the following configuration:

- Name tag:** `private_FortiSandbox`
- VPC:** `vpc-13818f7a | FortiSandbox`
- VPC CIDRs:**

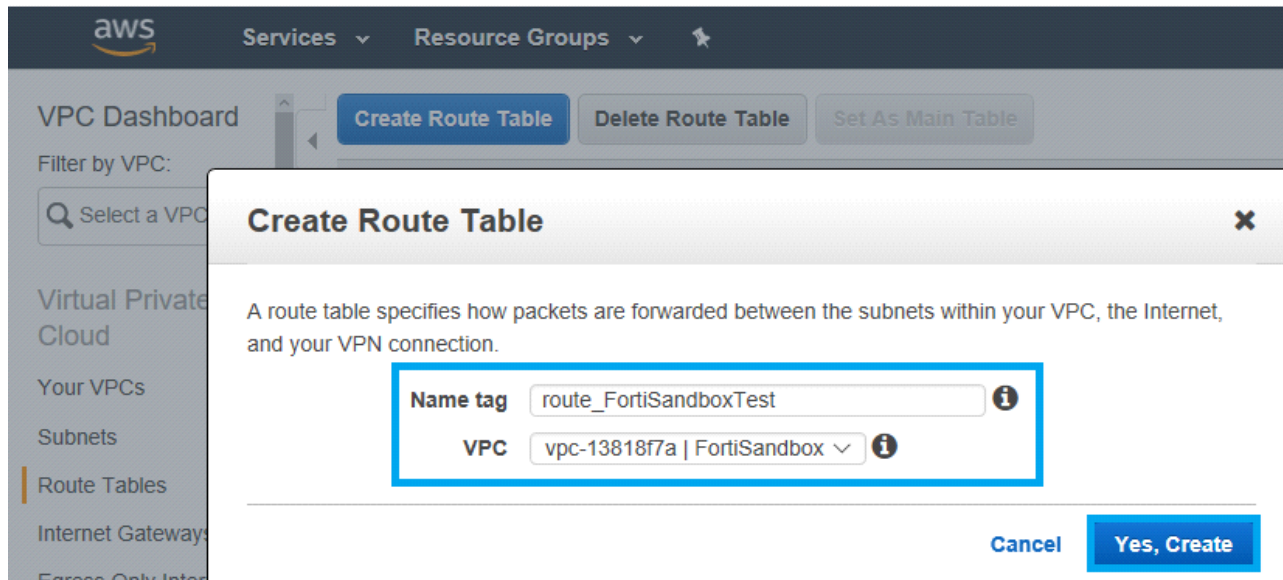
CIDR	Status	Status Reason
10.0.0.0/16	associated	
- Availability Zone:** `No Preference`
- IPv4 CIDR block:** `10.0.1.0/24`

At the bottom right of the dialog are 'Cancel' and 'Yes, Create' buttons.

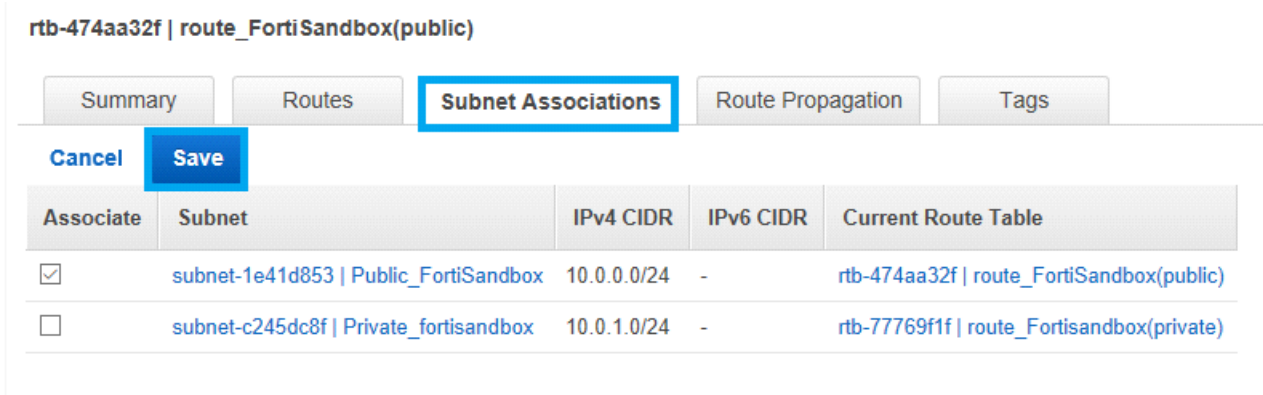
2. Click *Yes, Create*.

To create a route table:

1. Under *Virtual Private Cloud*, select *Route Tables*.
2. Click *Create Route Table* and configure the following. Then click *Yes, Create*.
 - For *Name Tag*, enter a name.
 - For *VPC*, select the VPC you created.



3. Go to *Subnet Associations*.
4. Click *Edit*, select the public subnet, then click *Save*.



5. Go to *Routes* and click *Add Another Route*.
 - For *Destination*, enter 0.0.0.0/0.
 - For *Target*, select the *Internet Gateway* for public subnet you created.
6. Click *Save*.
7. Repeat these steps to create a route table for your private subnet, and, if needed, for your HA-Cluster.

Optional: Using a custom VM on AWS

FortiSandbox AWS supports custom VMs. You can provide a VHD image of a custom VM and the FortiSandbox firmware can load the VM image and use it for sample analysis.

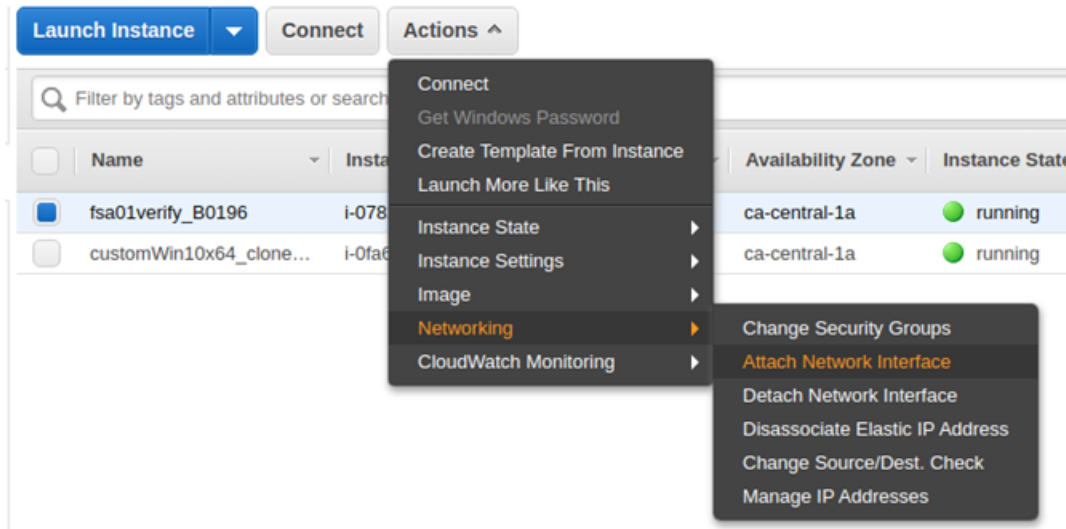
For information on setting up a custom VM on AWS, see the custom VM image section in the *FortiSandbox Administration Guide* to do the following:

- Create a custom VHD image using virtualization software such as VirtualBox.
- Prepare the OS installation package.

- Install software and components on the custom VM image.
- Set up the VM image environment.

Preparing the network interface for custom VM

1. Create a network interface under `private_subnet` (10.0.1.x) and assign a private IP address.
2. Attach this network interface to FortiSandbox AWS.



3. Reboot the FortiSandbox instance.
4. Go to **Network > Interfaces** to verify that the network interface is attached.

FortiSandbox AWS							
Interfaces							
Regular Mode							
admin							
+ Create New Edit Delete							
Interface	IPv4	IPv6	Interface Status	Link Status	Access Rights	PCAP	
port1 (administration port)	10.10.0.13/255.255.255.0		⬢	⬢	HTTPS,SSH	⬢	
port2	10.10.1.13/255.255.255.0		⬢	⬢		⬢	

Installing a custom VM using CLI

Convert the saved `pem` file which you downloaded while creating the key pair to a `ppk` file.

If you did not choose the *without key pair* option, log in using `<InstanceID>` as the password.



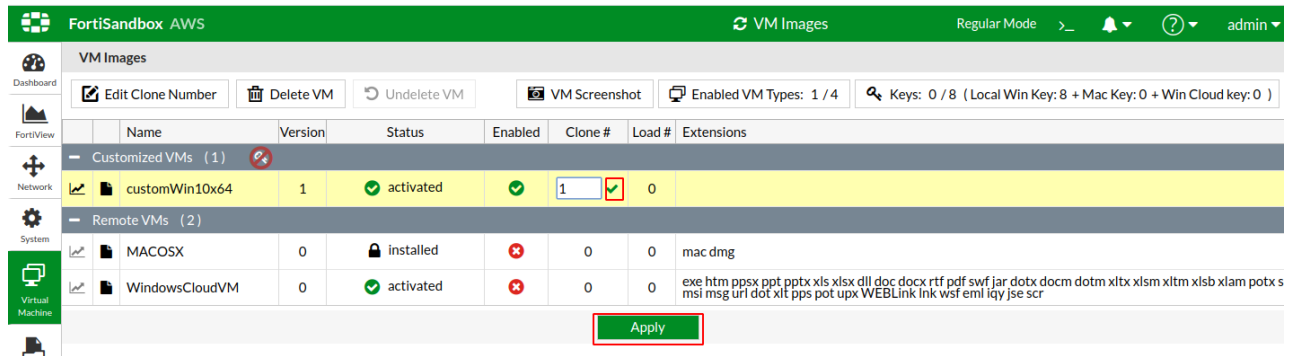
- Use a meaningful custom VM name and keep the name the same as `VM_image_name`.
- Do not use special characters in the name.
- Do not use reserved FortiSandbox VM names starting with `WIN7`, `WIN8`, or `WIN10`.



Do not use the `set admin-port` command to set `port2` as the administrative port.

To install a custom VM on AWS:

1. Go to the FortiSandbox firmware CLI.
2. Import the VHD image using the CLI command `vm-customized`.
For more information about the `vm-customized` command, see the FortiSandbox CLI Reference Guide in the [Fortinet Document Library](#).
3. In the FortiSandbox GUI, go to *Virtual Machine > VM Images* and change *Clone #* to 1 or higher.



4. In a new CLI window, check the VM clone initialization using the `diagnose-debug vminit` command.

5. In the FortiSandbox GUI, go to the *Dashboard* to verify there is a green checkmark beside *Windows VM*.

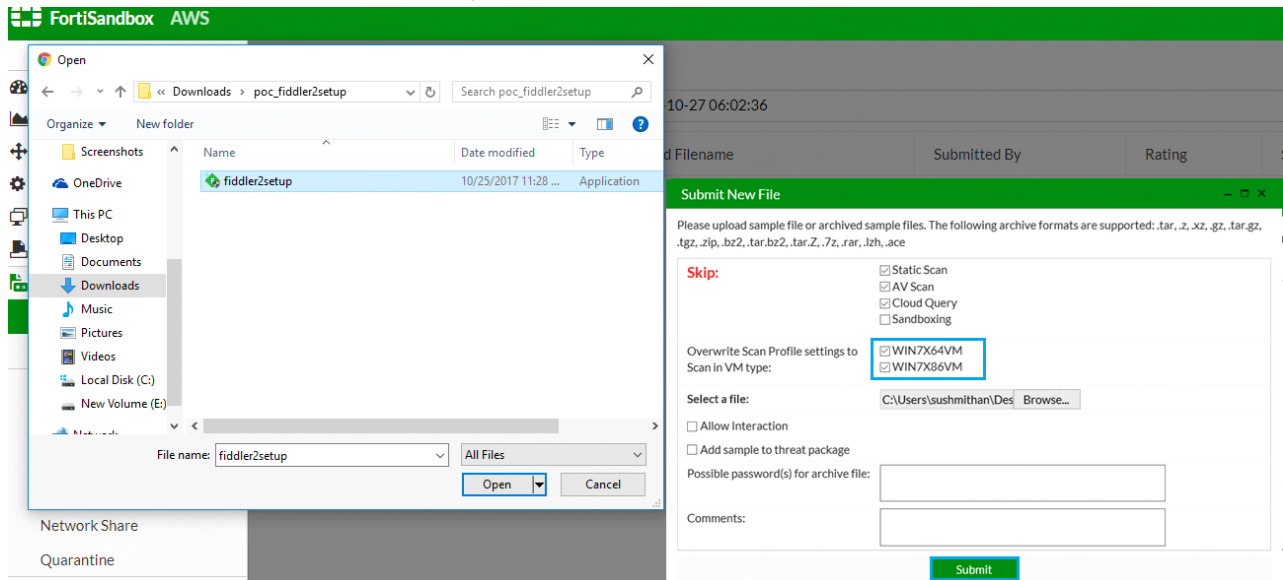
The screenshot shows the FortiSandbox AWS Dashboard. The left sidebar contains navigation icons for Dashboard, FortiView, Network, System, Virtual Machine, Scan Policy, Scan Input, and File Detection. The main content area is titled 'System Information' and displays various system details. The 'Windows VM' row is highlighted with a red box and shows a green checkmark, indicating it is successfully installed.

System Information	
Unit Type	Standalone
Host Name	FSAVM0I000013068 [Change]
Serial Number	FSAVM0I000013068
System Time	Fri Mar 27 21:10:29 2020 PDT [Change]
Firmware Version	v3.2.0,build0196 (Interim) [All firmwares]
VM License	✓ [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 2 hour(s) 21 minute(s)
Windows VM	✓
FDN Download Server	✓
Community Cloud Server	✓
Web Filtering Server	✓
Antivirus DB Contract	✓ 2020-07-05
Web Filtering Contract	✓ 2020-07-05

6. To associate file extensions to the custom VM, go to *Scan Policy* > *Scan Profile* to the *VM Association* tab.

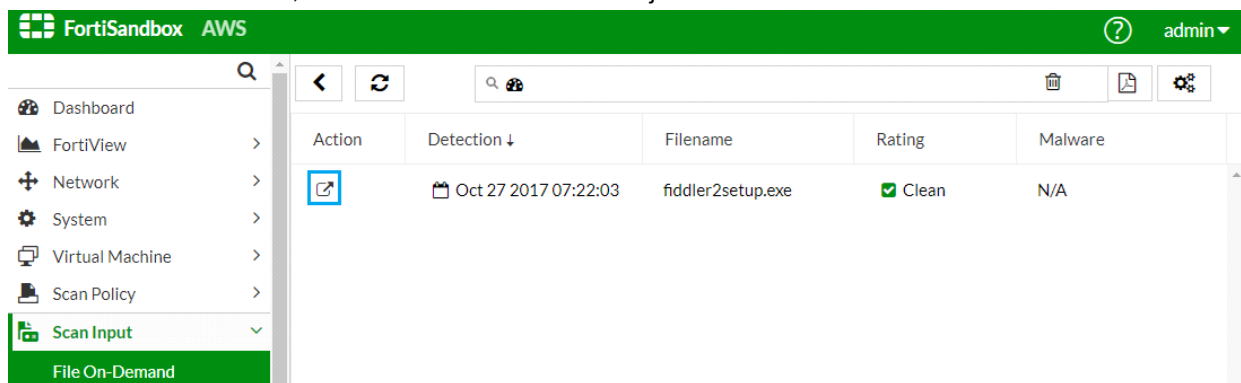
Test the installation

1. Go to *Scan Input > File On-Demand > Submit File*.
2. Select the file and click *Submit*. For example, select `fiddler2setup.exe`.



If the file you send to FortiSandbox is not harmful, the rating is *Clean*.

3. When the scan is finished, click the *View File* icon to view job details.



Interaction with a custom VM clone during scan

1. Go to *Scan Input > File On-Demand* or *URL on-Demand* and click *Submit File* or *Submit File/URL*.
2. Enable *Force to scan the file inside VM* or *Force to scan the url inside VM*.




3. Select *Force to scan inside the following VMs* and select the custom VM.

Submit New File
✕

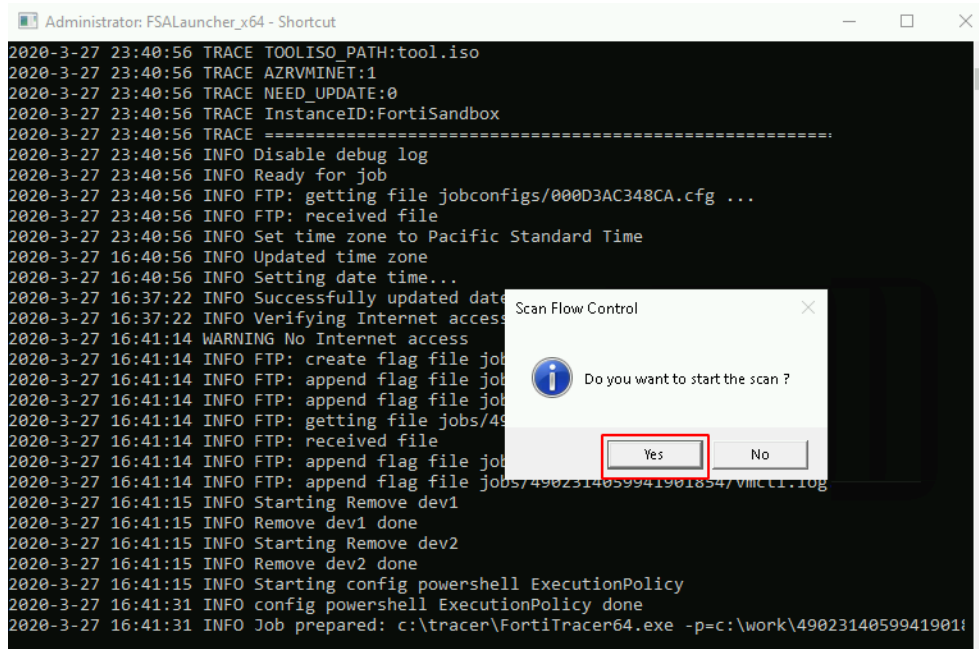
Please upload sample file or archived sample files. The following archive formats are supported: .tar, .z, .xz, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .tar.Z, .7z, .rar, .lzh, .ace

Select a file:	<input type="button" value="Choose file"/> FSAVM4713450316.pdf <small>Maximum 200 MBs</small>
Possible password(s) for archive/office file:	<input style="width: 100%;" type="text"/> <small>One possible password for each line. Please use ASCII format password without empty space.</small>
Comments:	<input style="width: 100%;" type="text"/> <small>Optional comments for later reference</small>
Skip result of:	<input type="checkbox"/> Static Scan <input type="checkbox"/> AV Scan <input type="checkbox"/> Community Cloud Query
<input checked="" type="checkbox"/> Force to scan the file inside VM	
<input type="radio"/> Follow VM Association settings in Scan Profile <input checked="" type="radio"/> Force to scan inside the following VMs <div style="border: 2px solid red; padding: 5px; margin-left: 20px;"> <input checked="" type="checkbox"/> customWin10x64 </div>	
<input type="checkbox"/> Add sample to threat package <small>Add file to Malware Package if it meets settings in Package Options</small>	
<input type="checkbox"/> Enable AI <small>Enable AI mode for this scanning</small>	

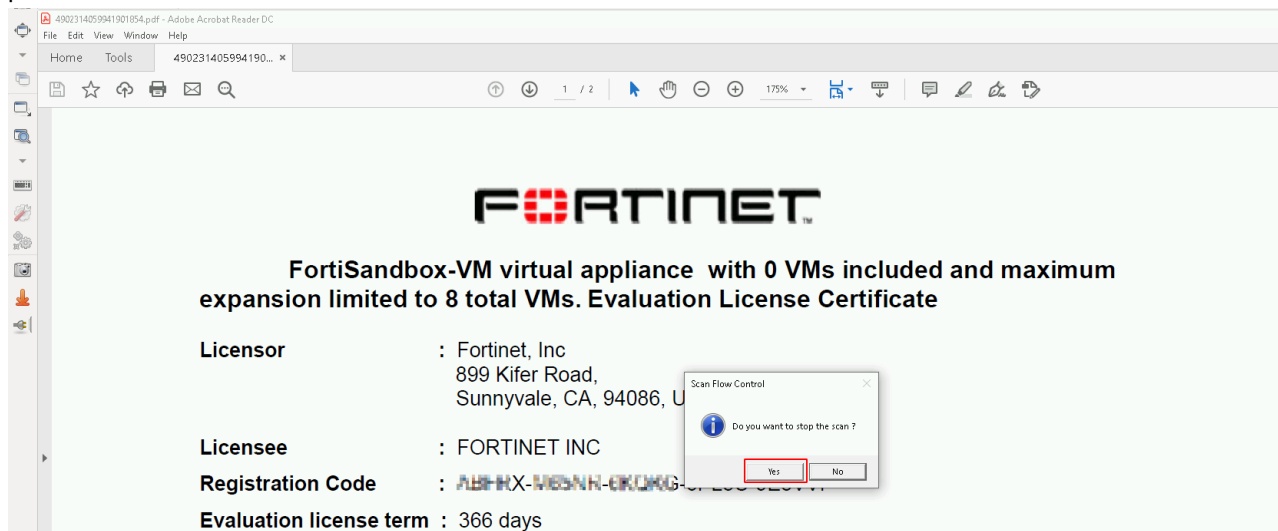
4. Click *Submit*.
5. Go to *Virtual Machine > VM Images* and click *VM Screenshot*.
6. When the icon in the *Interaction* column is enabled, click the icon to establish an RDP tunnel.

VM ScreenShot ↻ 🔗 ✕			
Name	Interaction	ScreenShot	PNG Link
customWin10x64_clone000	<div style="border: 2px solid red; padding: 2px; display: inline-block;"></div>		

7. Click Yes to manually start the scan process with VM Interaction.



8. When the FortiSandbox tracer engine displays the PDF sample, you can click Yes to manually stop the scan process.



9. When the scan is finished, go to the job details page to view the scan results.

☒ Clean File pdf

Overview

Tree View

Details

Basic Information

Received:	Mar 27 2020 16:37:12
Started:	Mar 27 2020 16:37:15-07:00
Status:	Done
Rated By:	VM Engine
Submit Type:	On-Demand
Digital Signature:	Yes
AI Mode:	OFF
SIMNET:	OFF
Virus Total:	Q

Details Information

Downloaded From:	FSAVM4713450316.pdf
File Size:	11678 (bytes)
MD5:	448fedf13fb3827fdc6a8270eacfbaf
SHA1:	0c5fb95ef3c93d7bf7fd2b8a3b37cd16512f5940
SHA256:	a5c42d83c9fe80bd31e8da8f4e985b60ca85c61c87128883449fae2be6cc05e7
ID:	4902314059941901854
Submitted By:	admin
Submitted Filename:	FSAVM4713450316.pdf
Filename:	FSAVM4713450316.pdf
Received:	Mar 27 2020 16:37:12
Scan Start Time:	Mar 27 2020 16:37:15-07:00
VM Scan Start Time:	Mar 27 2020 16:37:22-07:00
VM Scan End Time:	Mar 27 2020 16:52:25-07:00
VM Scan Time:	903 seconds
Scan End Time:	Mar 27 2020 16:52:43-07:00
Total Scan Time:	928 seconds
Scan Unit:	FSAVM01000014855
Specified VMs:	customWin10x64
Launched OS:	customWin10x64

☒ Clean File pdf

Overview

Tree View

Details

customWin10x64

STATIC_SCAN

Process Related

Process Created

Process Injected

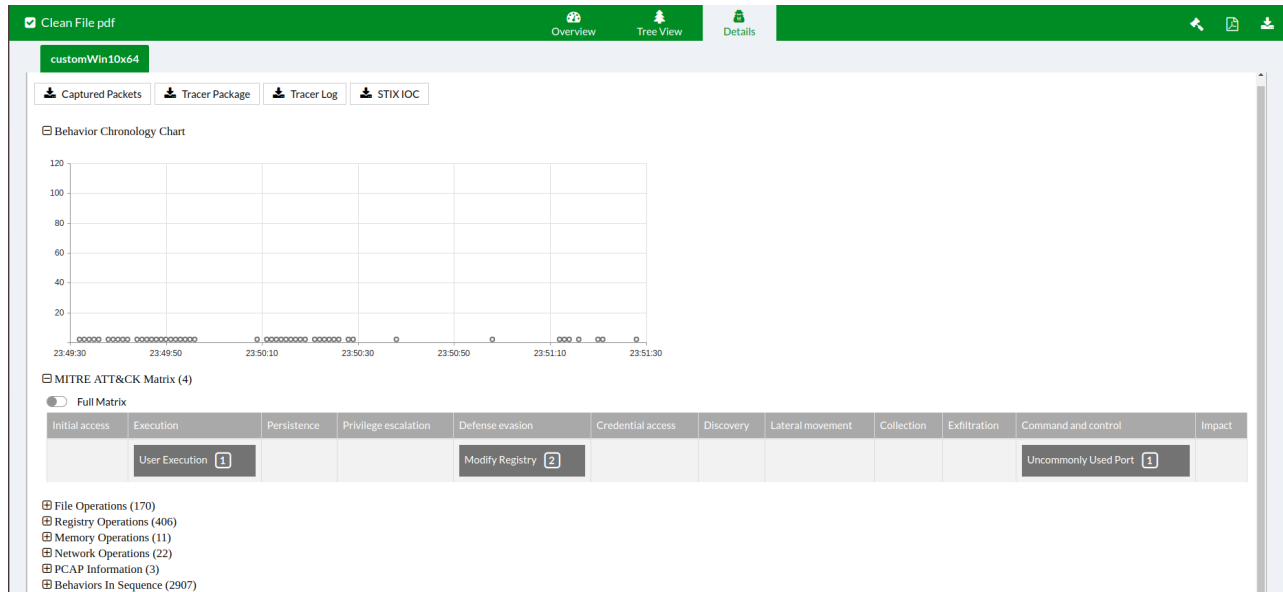
Process Created and Injected

Process Information

File Operation

Registry Operation

PID: 5952	File Type: unknown	MD5: 761efc843f05ab74ed358713dd51c1b	digital_signed: true	signers: Adobe Inc.	CompanyName: Adobe Systems	FileVersion: 1.824.35.0289
-----------	--------------------	--------------------------------------	----------------------	---------------------	----------------------------	----------------------------



Optional: Using HA-Cluster

You can set up multiple FortiSandbox instances in a load-balancing HA (high availability) cluster.

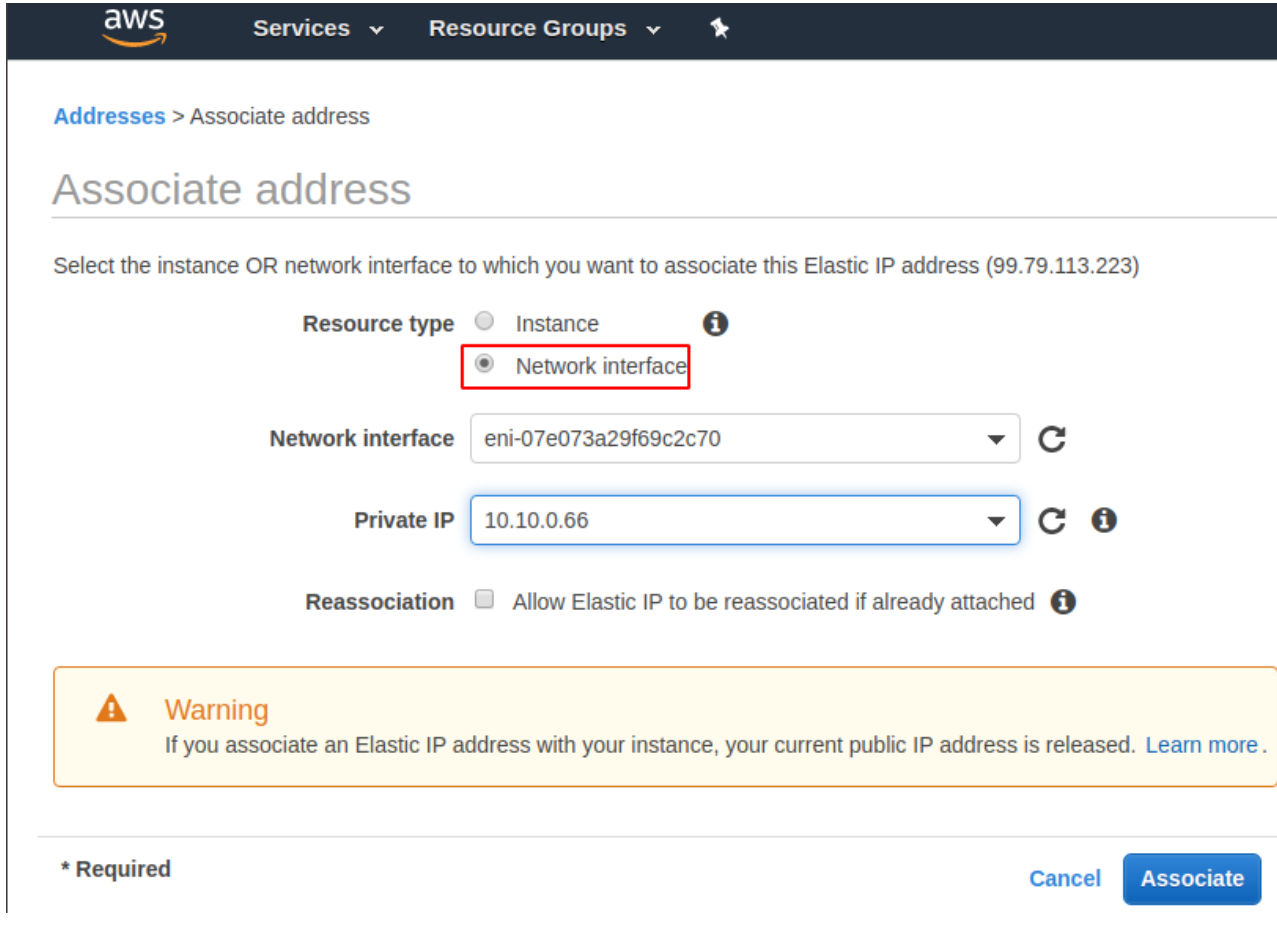
For information on using HA clusters, see the FortiSandbox Administration Guide.

Launching an HA-Cluster

To launch FortiSandbox instances on AWS:

1. On the *AWS Launch Instances* page, launch FortiSandbox primary (formerly master) instances from the marketplace.
2. On the *Configure Instance Details* page of the setup wizard, assign *eth0* to the FortiSandbox firmware subnet of port1 (10.0.0.x).
3. First launch the secondary (formerly primary slave) instance and then launch the worker (formerly slave or regular slave) instances.
If you are using HA-Cluster without failover, the secondary node is optional.
4. Create two additional network interfaces under dedicated subnets for all HA-Cluster nodes.
 - a. Create *private_subnet* (10.0.1.x) for custom VM.
 - b. Create *HA-Cluster_subnet* (10.0.2.x) for HA-Cluster communication.
5. In Network security group, open the following ports for HA-Cluster communication:
 - TCP 2015 0.0.0.0/0
 - TCP 2018 0.0.0.0/0
6. On the AWS Console, add a secondary IP address on the primary node as an external HA-Cluster communication IP address.
 - a. Select the primary node's port1 network interface.
 - b. Go to *Action > Manager IP Addresses* and assign the new IP address.

- c. Optional: you can associate a new EIP address for external HA-Cluster communication. In a failover, this HA-Cluster IP address will be used on the new primary node.



Addresses > Associate address

Associate address

Select the instance OR network interface to which you want to associate this Elastic IP address (99.79.113.223)

Resource type ☐ Instance ☒ Network interface

Network interface eni-07e073a29f69c2c70

Private IP 10.10.0.66

Reassociation ☐ Allow Elastic IP to be reassigned if already attached

Warning

If you associate an Elastic IP address with your instance, your current public IP address is released. [Learn more](#).

* Required

Cancel Associate



Do not use the `set admin-port` command to set the internal HA-Cluster communication port.

7. Attach network interfaces to all HA-Cluster nodes and reboot all nodes after attaching.
8. Import AWS settings into FortiSandbox HA-Cluster.
 - a. Log into each FortiSandbox HA-Cluster node using the EIP address.
 - b. Configure the *AWS Config* page for the primary and worker nodes.

Configuring an HA-Cluster

If you are using HA-Cluster without failover, the secondary is optional.

Ensure the HA-Cluster meets the following requirements:

- Use the same scan environment on all nodes. For example, install the same set of Windows VMs on each node so that the same scan profiles can be used and controlled by the primary node.
- Run the same firmware build on all nodes.

- Set up a dedicated network interface (such as port2) for each node for custom VMs.
- Set up a dedicated network interface (such as port3) for each node for internal HA-Cluster communication.

In this example, 10.20.0.22/24 is an external HA-Cluster communication IP address. The secondary node's private IP address is on the primary node's port1 network interface.

To configure an HA-Cluster using FortiSandbox CLI commands:

1. Configure the primary node:

- `hc-settings -sc -tM -nMyHAPrimary -cClusterName -p123 -iport3`
- `hc-settings -si -iport1 -a10.20.0.22/242`

2. Configure the secondary node:

- `hc-settings -sc -tP -nMyPWorker -cClusterName -p123 -iport3`
- `hc-slave -a -sPrimary_Port3_private_IP -p123`

3. Configure the first worker node:

- `hc-settings -sc -tR -nMyRWorker1 -cClusterName -p123 -iport3`
- `hc-slave -a -sPrimary_Port3_private_IP -p123`

4. If necessary, configure consecutive worker nodes:

- `hc-settings -sc -tR -nMyRWorker2 -cClusterName -p123 -iport3`
- `hc-slave -a -sPrimary_Port3_private_IP -p123`

To check the status of the HA-Cluster:

On the primary node, use this CLI command to view the status of all units in the cluster.

```
hc-status -l
```

To use a custom VM on an HA-Cluster:

1. Install the AWS local custom VMs from the primary node onto each worker node using the FortiSandbox CLI command `vm-customized`.
All options must be the same when installing custom VMs on an HA-Cluster, including `-vn[VM name]`.
2. In the FortiSandbox AWS GUI, go to *Virtual Machine > VM Images* and change *Clone #* to 1 for each node. After all VM clones on all nodes are configured, you can change the *Clone #* to a higher number.
3. In a new CLI window, check the VM clone initialization using the `diagnose-debug vminit` command.
4. In the FortiSandbox GUI, go to the *Dashboard* to verify there is a green checkmark beside *Windows VM*.
5. To associate file extensions to the custom VM, go to *Scan Policy > Scan Profile* to the *VM Association* tab.

You can now submit scan jobs from the primary node. HA-Cluster supports VM Interaction on each node.

Use Case: Instantaneous IOC Intelligence Sharing Across Multi-Clouds

In hybrid or multi-cloud environments, it is critical to get first-hand indicators of compromise (IOC) intelligence for zero-day malware protection. FortiSandbox instantly shares session information and IOC related to the malware behavior. If there are multiple FortiSandbox instances (physical, virtualized, or cloud) present, you can identify the synchronization rule for the intelligence update.

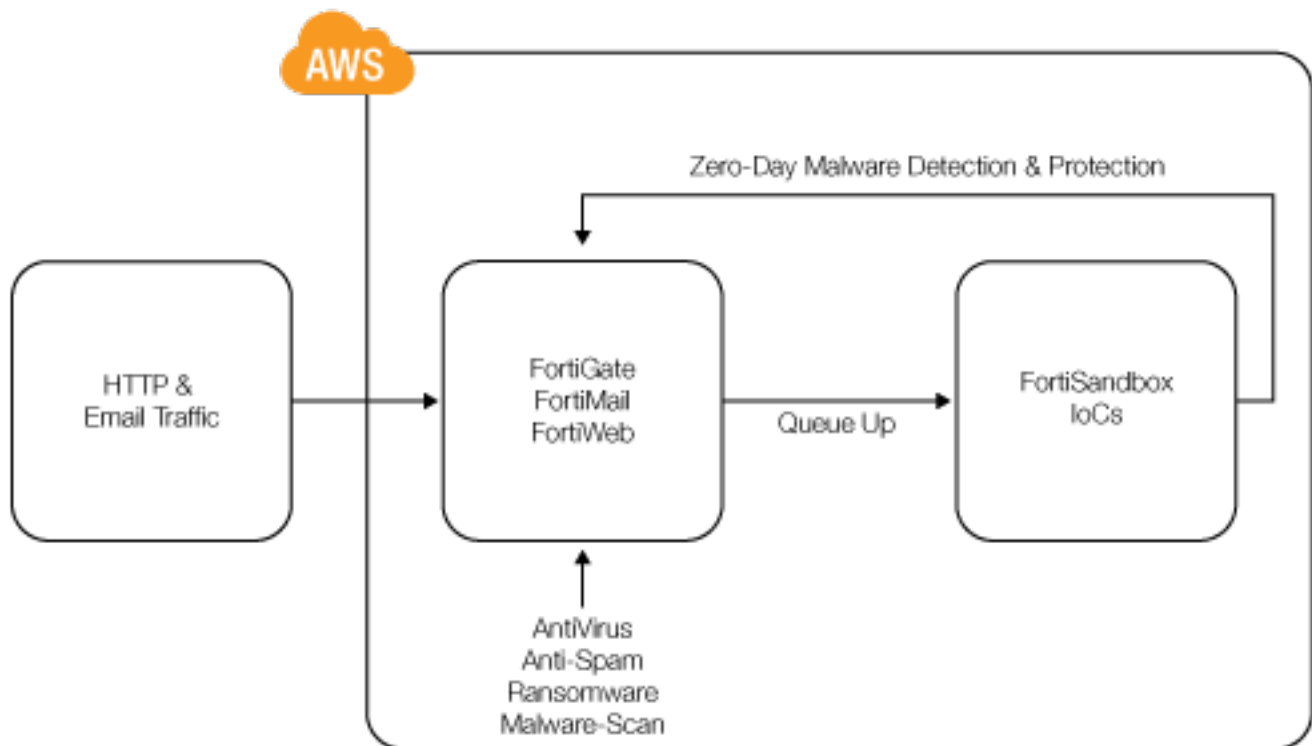


Use Case: Fabric-Based Deep Analysis for Zero-Day Malware Detection

FortiSandbox on AWS introduces elasticity for on-demand sandbox resources when they are needed, which can be very costly in the traditional on premises setting. When working with other Fortinet products like FortiGate, FortiWeb, or FortiMail, FortiSandbox continues to be a powerful use case for public cloud when no prior malware signature exists. When the firewall does not find the AV malicious profile in the HTTP or web traffic, it submits and queues the file sample in FortiSandbox on AWS for in-depth analysis until the verdict is reached.

Adaptive Notification and Remediation

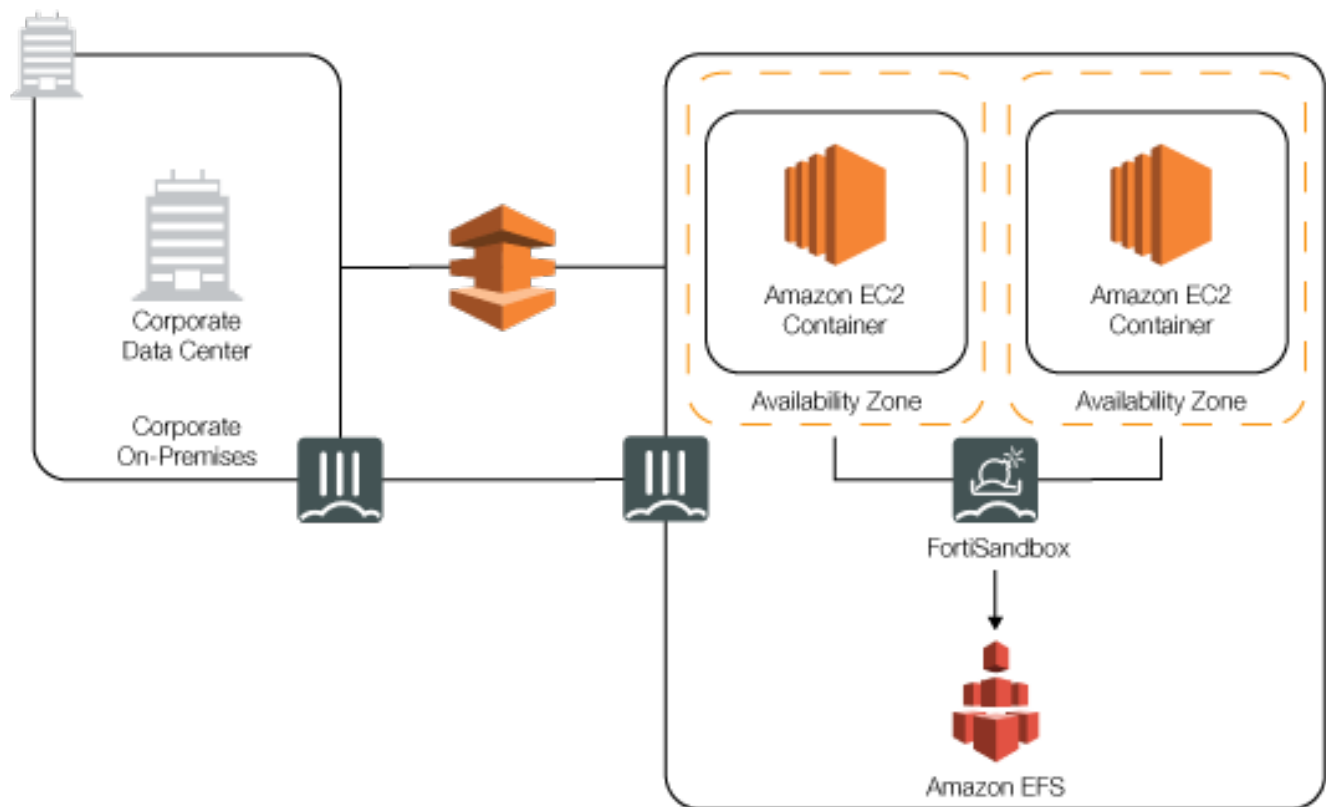
The intelligence is shared across the Fabric. Every signature and IOC that FortiSandbox generates is automatically propagated across all FortiGate firewalls and FortiClient endpoints for immediate blocking or quarantine actions to avoid further damage.



When anticipated traffic is down it can release the AWS compute resources if not needed.

Use Case: FSA Cloud Scan Automation

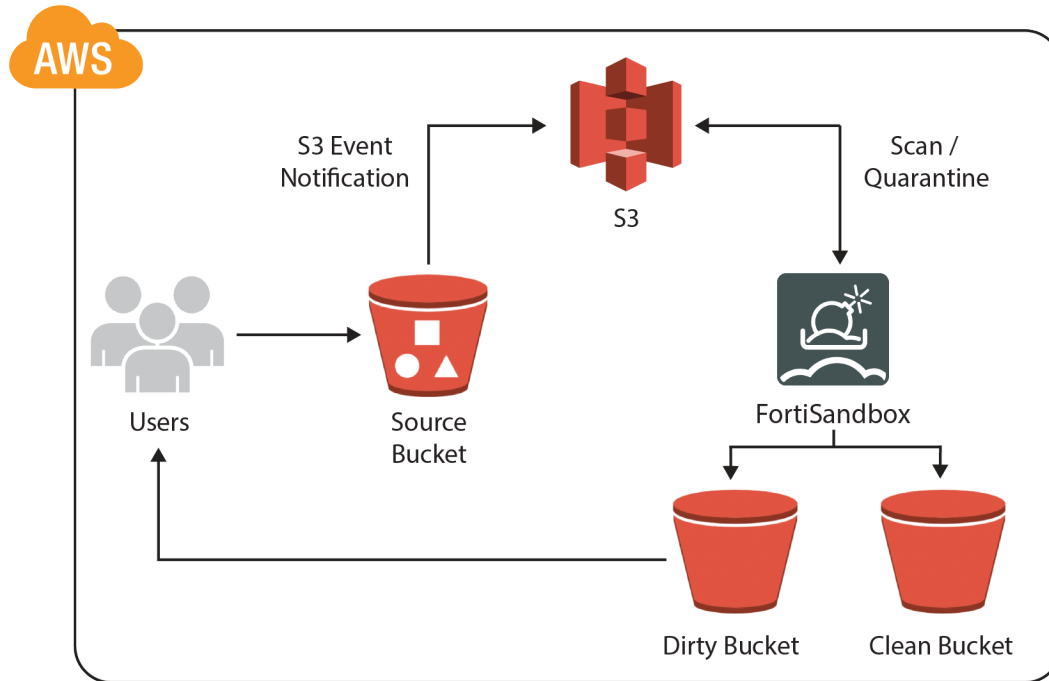
Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud. EFS is used often in cloud migration such as dataset migration, on-demand backup or cloud bursting scenarios. You can mount your Amazon EFS file systems on your on-premises data center servers when connected to your Amazon VPC with AWS Direct Connect or through a FortiGate site-to-site secured connection. In the process, you can insert FortiSandbox on premises or in AWS, or you can perform malware analysis in the EFS-to-EFS backup solution to ensure clean file backup.



S3 Bucket Scanning

The other way to use FortiSandbox through NFS mount is to leverage AWS Storage Gateway. By mounting a file share and mapping it to an Amazon S3 bucket using AWS Storage Gateway, you can configure AWS S3 as the NFS or SMB network share for FortiSandbox malware analysis.

FortiSandbox leverages the AWS API to natively supports S3 bucket scanning. It can quarantine items according to analysis results, and move items into another S3 quarantine bucket based on the Risk level.



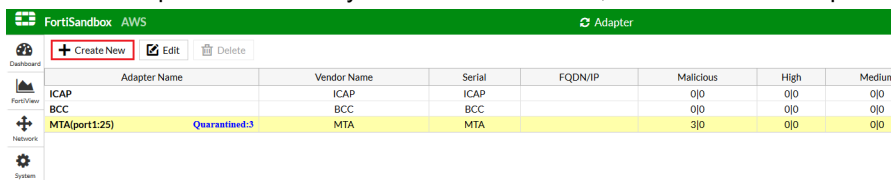
Other use cases such as preventing malware penetration in a closed/isolated network can be considered. Without any external malware signatures, FortiSandbox can help perform zero-day malware analysis instead. For more architecture discussion or if you need to clarify the use cases, email aws@fortinet.com.

Use Case: MTA Adapters

A new MTA adapter has been added to FortiSandbox for FSA_AWS or FSA_VM (where the serial number begins with FSA VM01). FortiSandbox extracts the .EML file, attachment files, and URLs in the email body and then sends them into the job queue.

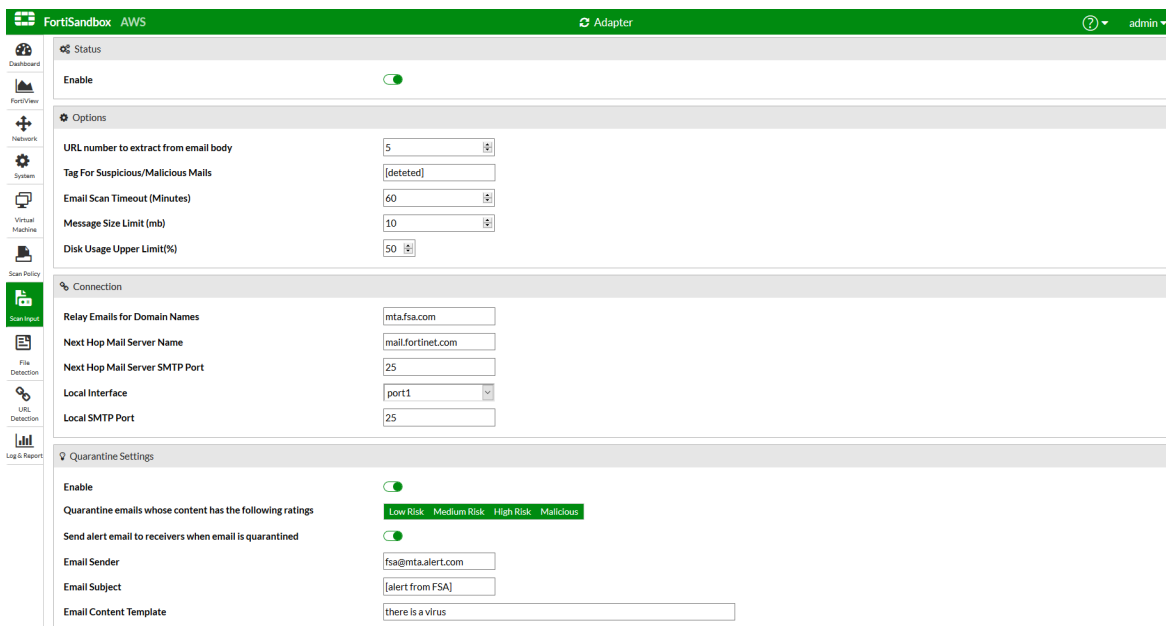
To enable MTA adapters on FSA_AWS or FSA_VM:

1. On the FortiSandbox, go to *Scan Input > Adapter*.
2. The MTA adapter is disabled by default. To activate it, select the MTA adapter from the list and click *Edit*.



Adapter Name	Vendor Name	Serial	FQDN/IP	Malicious	High	Medium
ICAP	ICAP	ICAP		0/0	0/0	0/0
BCC	BCC	BCC		0/0	0/0	0/0
MTA(port1.25)	MTA	MTA		3/0	0/0	0/0

3. Configure the settings under Options and Connection:
 - *Tag For Suspicious/Malicious Mails*: Enter a tag. Malicious and suspicious email are forwarded with the specified tag if Quarantine Settings are disabled.
 - *Relay Domain Name*: FortiSandbox supports multiple domain names separated by a comma.
 - *Next Hop Mail Server Name*: Set as the IP or domain of the target email server.
4. Configure the settings under Quarantine Settings:
 - Email is quarantined by FortiSandbox if the content has the selected ratings, otherwise it is forwarded with the customized tag if the email is rated as malicious or suspicious.
 - Enabling the option to *Send alert email to receivers when email is quarantined* allows you to send customized alert emails when an email is quarantined. The email contains the information of the submission ID (SID) from FortiSandbox.



FortiSandbox AWS Adapter

Status

Enable ☒

Options

URL number to extract from email body: 5

Tag For Suspicious/Malicious Mails: [detected]

Email Scan Timeout (Minutes): 60

Message Size Limit (mb): 10

Disk Usage Upper Limit(%): 50

Connection

Relay Emails for Domain Names: mta.fsa.com

Next Hop Mail Server Name: mail.fortinet.com

Next Hop Mail Server SMTP Port: 25

Local Interface: port1

Local SMTP Port: 25

Quarantine Settings

Enable ☒

Quarantine emails whose content has the following ratings: ☒ Low Risk ☒ Medium Risk ☒ High Risk ☒ Malicious

Send alert email to receivers when email is quarantined ☒

Email Sender: fsa@mta.alert.com

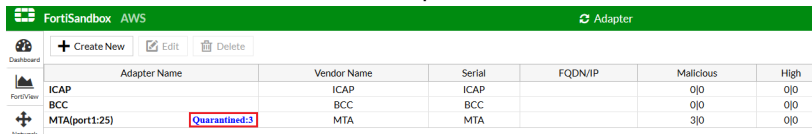
Email Subject: [alert from FSA]

Email Content Template: there is a virus

5. Select *Apply*.

To check and operate suspicious or malicious email quarantined by FortiSandbox:

1. On the FortiSandbox, go to *Scan Input > Adapter*.
2. Click *Quarantine* beside the MTA adapter.

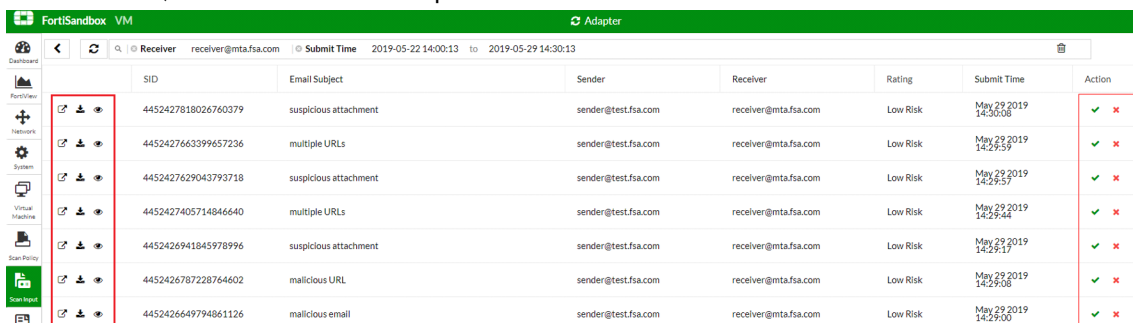


Adapter Name	Vendor Name	Serial	FQDN/IP	Malicious	High
ICAP	ICAP	ICAP		0/0	0/0
BCC	BCC	BCC		0/0	0/0
MTA[port1:25]	MTA	MTA		3/0	0/0

The Quarantine page allows you to view

the quarantined email and apply search filters:

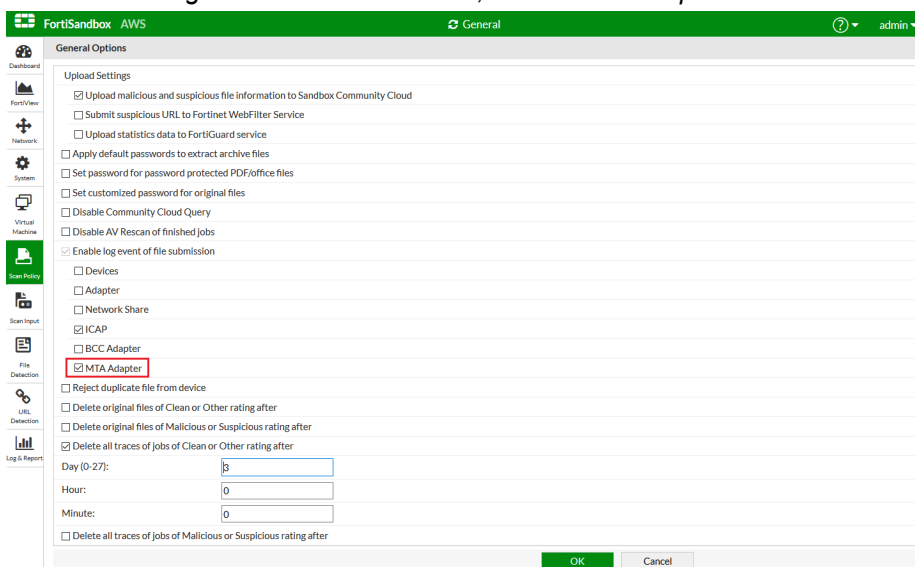
- Click *View Details* to view the Scan Details page for the email.
- Click *Download Email File* to download the original email.
- Click *Preview Email* to preview the email.
- Click *Release Quarantine* to release the email to the receiver.
- Click *Delete Quarantine* to delete the quarantined email from the FortiSandbox database.



SID	Email Subject	Sender	Receiver	Rating	Submit Time	Action
4452427818026760379	suspicious attachment	sender@test.fsa.com	receiver@mta.fsa.com	Low Risk	May 29 2019 14:30:08	✓ ✗
4452427663399657236	multiple URLs	sender@test.fsa.com	receiver@mta.fsa.com	Low Risk	May 29 2019 14:29:59	✓ ✗
4452427629043793718	suspicious attachment	sender@test.fsa.com	receiver@mta.fsa.com	Low Risk	May 29 2019 14:29:57	✓ ✗
4452427405714846640	multiple URLs	sender@test.fsa.com	receiver@mta.fsa.com	Low Risk	May 29 2019 14:29:44	✓ ✗
4452426941845978996	suspicious attachment	sender@test.fsa.com	receiver@mta.fsa.com	Low Risk	May 29 2019 14:29:17	✓ ✗
4452426787228764602	malicious URL	sender@test.fsa.com	receiver@mta.fsa.com	Low Risk	May 29 2019 14:29:08	✓ ✗
4452426649794861126	malicious email	sender@test.fsa.com	receiver@mta.fsa.com	Low Risk	May 29 2019 14:29:00	✓ ✗

To log MTA adapter file submission events:

1. On the FortiSandbox, go to *Scan Policy > General*.
2. Under *Enable log event of file submission*, enable *MTA Adapter*.



FortiSandbox AWS General

General Options

Upload Settings

- ☒ Upload malicious and suspicious file information to Sandbox Community Cloud
- ☐ Submit suspicious URL to Fortinet WebFilter Service
- ☐ Upload statistics data to FortiGuard service
- ☐ Apply default passwords to extract archive files
- ☐ Set password for password protected PDF/office files
- ☐ Set customized password for original files
- ☐ Disable Community Cloud Query
- ☐ Disable AV Rescan of finished jobs
- ☒ Enable log event of file submission
 - ☐ Devices
 - ☐ Adapter
 - ☐ Network Share
 - ☒ ICAP
 - ☐ BCC Adapter
 - ☒ MTA Adapter
- ☐ Reject duplicate file from device
- ☐ Delete original files of Clean or Other rating after
- ☐ Delete original files of Malicious or Suspicious rating after
- ☒ Delete all traces of jobs of Clean or Other rating after
 - Day (0-27):
 - Hour:
 - Minute:
- ☐ Delete all traces of jobs of Malicious or Suspicious rating after

OK Cancel

To view debug logs of the MTA adapter in the CLI:

1. In the CLI console, enter the command `diagnose-debug adapter_mta_relay` and `dignose-debug adapter_mta_mail`.

```
> diagnose-debug -h
Usage: diagnose-debug [netshare|device|adapter] [device_serial_number]
netshare: Network share daemon
device: OFTP daemon for FGT/FML/FCT devices.
adapter_cb: Daemon for third party appliance Bit9 + CARBON BLACK
adapter_icap: Daemon for Internet Content Adaptation Protocol (ICAP)
adapter_bcc: Daemon for BCC
adapter_mta_relay: Daemon for MTA Relay
adapter_mta_mail: Daemon for MTA Mail
```

- Example of `diagnose-debug adapter_mta_relay` command.

```
> diagnose-debug adapter_mta_relay
2019-06-05 21:18:56 FSA-MTA: File from MTA Adapter was submitted.
sha256=010ae06e0085f86dd23614aecd077bb844cc5de59cd5b27ccd172749d60df36f
fname=4463239589762783574 client_ip=10.0.0.128
```

- Example of `diagnose-debug adapter_mta_mail` command.

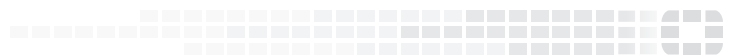
```
> diagnose-debug adapter_mta_mail
Jun  6 04:18:56 FSAVM0I000011483 mail.info postfix/qmgr[31350]: B7E0D3E405A:
from=<jliang@test.fsa.com>, size=327092, nrcpt=1 (queue active)
Jun  5 21:18:56 FSAVM0I000011483 mail.info postfix/smtp[32728]: B7E0D3E405A:
to=<malware@mta.fsa.com>, relay=127.0.0.1[127.0.0.1]:10025, delay=0.61,
delays=0.51/0/0.02/0.07, dsn=2.0.0, status=sent (250 Ok)
Jun  6 04:18:56 FSAVM0I000011483 mail.info postfix/qmgr[31350]: B7E0D3E405A: removed
Jun  5 21:18:56 FSAVM0I000011483 mail.info postfix/smtpd[32498]: disconnect from
unknown[207.102.138.11] ehlo=2 starttls=1 mail=1 rcpt=1 data=1 quit=1 commands=7
.....
```

Change Log

Date	Change Description
2020-04-30	Initial release.



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.