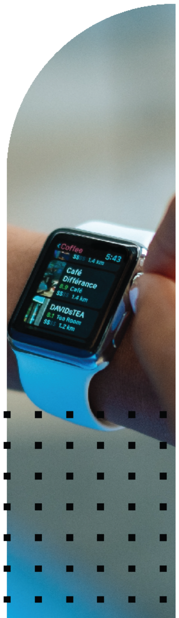
AWS Guide

FortiSandbox 4.2



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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 19, 2022
FortiSandbox 4.2 AWS Guide
34-421-829779-20221019

TABLE OF CONTENTS

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.

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

This document conaitns images from the AWS interface. Some images and text strings may not reflect the current AWS version. Where possible, we have noted the version the image is based on.

For the most accurate AWS information, please refer to the product documentation.

Prepare the AWS environment

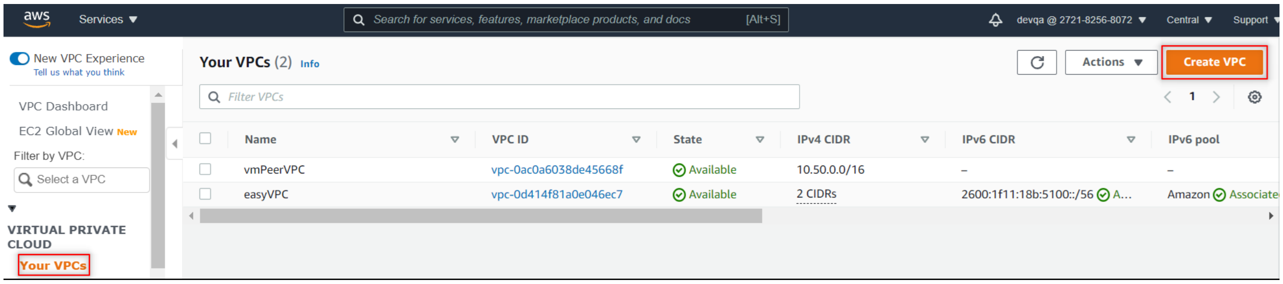
Before deploying a FortiSandbox instance, some basic steps are required to setup and run the AWS environment.

Start by logging into the AWS management console with a user account that has enough privileges to create a new Virtual Private Cloud (VPC).

Set up the basic AWS environment for FortiSandbox

Create a Virtual Private Cloud (VPC)

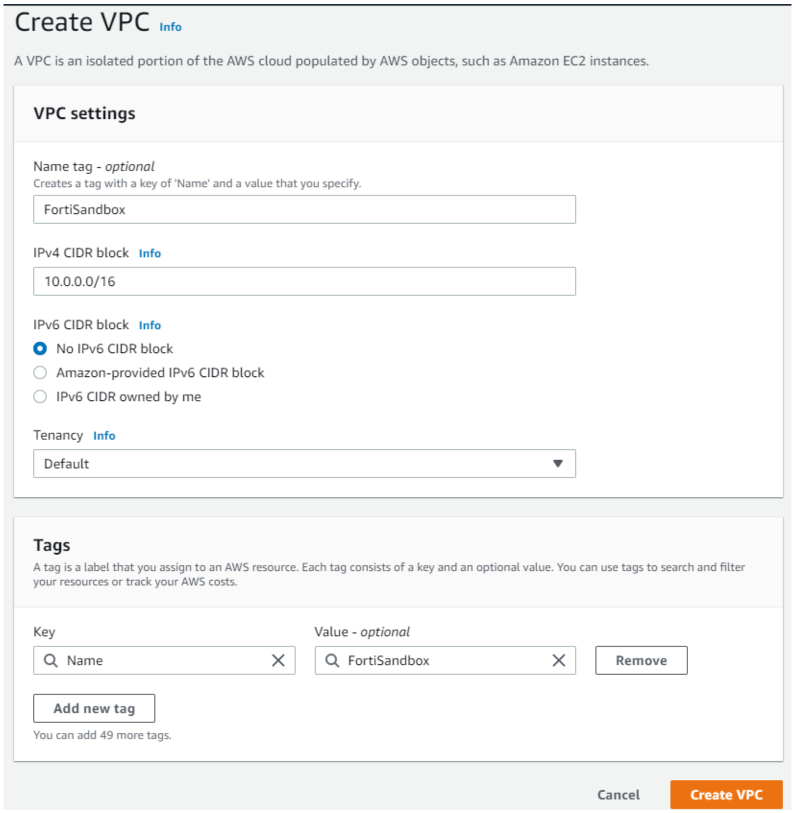
1. Go to *VPC Dashboard* > *Your VPCs* and click *Create VPC*.



□	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool
□	vmPeerVPC	vpc-0ac0a6038de45668f	Available	10.50.0.0/16	–	–
□	easyVPC	vpc-0d414f81a0e046ec7	Available	2 CIDRs	2600:1f11:18b:5100::/56 A...	Amazon Associate

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

2. Enter the following information, then click *Create VPC*.
   - For *Name tag*, enter a name. For example, *FortiSandbox*.
   - For *IPv4 CIDR block*, enter a subnet such as 10.0.0.0/16 that will cover the IP ranges this VPC will use.
   - For *IPv6 CIDR block*, enter a valid IPv6 CIDR block that will cover IP ranges this VPC will use, or select *No IPv6 CIDR Block* if IPv6 IP address is not used.
   - For *Tenancy*, select *Default*.



Create VPC Info

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
FortiSandbox

IPv4 CIDR block Info
10.0.0.0/16

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy Info
Default

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	FortiSandbox	Remove

Add new tag
You can add 49 more tags.

Create network subnets for FortiSandbox instance

On AWS, FortiSandbox uses Port1 or any other administrative port set through the CLI command `set-admin-port` as reserved for device management, and Port2 be reserved to communicate with local Windows VM or Linux clones. The other ports are used for file inputs from client devices and inter-communication among cluster nodes. Each port should be on its dedicated subnet.

In a regular setup, these two subnets should be created:

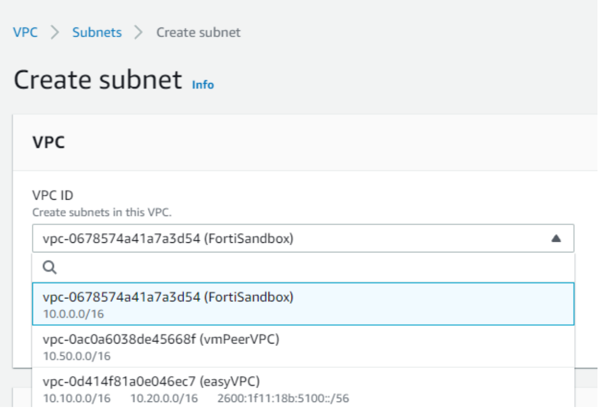
- **Management subnet** on which FortiSandbox management interface listens. Client devices can also connect to this subnet to submit files. We will use *IPv4 CIDR 10.0.0.0/24* as an example in following sections.
- **Local VM clones communication subnet** which FortiSandbox instances use to communicate with local Windows or Linux clones. If you choose to use Windows cloud clones located in Fortinet Data Center, this subnet is not required. We will use IPv4 CIDR 10.0.1.0/24 as example in the following sections.

If needed, you can create more subnets, such as for client devices to submit files, or inter-communications between HA Cluster nodes.

To create a subnet:

1. Click *Subnets* > *Create Subnet*.
2. In the *Create Subnet* dialog box, enter the following information, then click *Create subnet*.
   - For *Name tag*, enter a meaningful name. For example, *Public_FortiSandbox*.
   - For *VPC*, select the VPC you just created.

- For *IPV4 CIDR block*, enter a valid block such as `10.0.0.0/24`.



VPC > Subnets > Create subnet

Create subnet Info

VPC

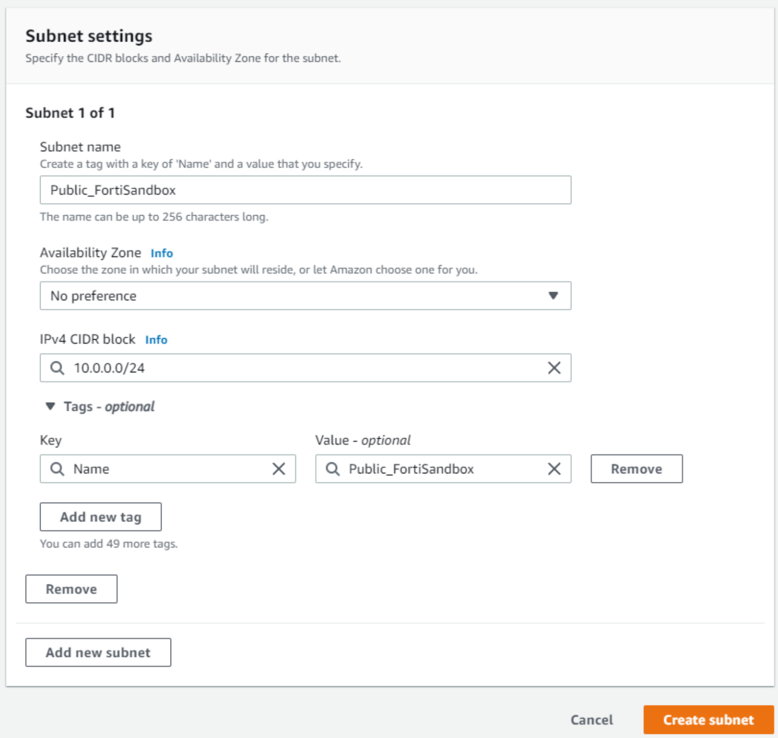
VPC ID
Create subnets in this VPC.

vpc-0678574a41a7a3d54 (FortiSandbox)

vpc-0678574a41a7a3d54 (FortiSandbox)
10.0.0.0/16

vpc-0ac0a6038de45668f (vmPeerVPC)
10.50.0.0/16

vpc-0d414f81a0e046ec7 (easyVPC)
10.10.0.0/16 10.20.0.0/16 2600:1f11:18b:5100::/56



Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Public_FortiSandbox
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

IPv4 CIDR block Info
10.0.0.0/24

Tags - *optional*

Key	Value - *optional*
Name	Public_FortiSandbox

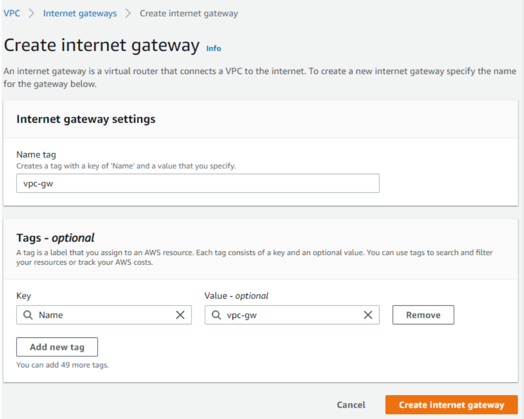
You can add 49 more tags.

Create an internet gateway

If VPC needs to communicate with the Internet, for example, for FortiSandbox instance to get FortiGuard updates from Fortinet, or to access FortiSandbox instance from the Internet, an Internet gateway is needed.

To create 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 *Create internet gateway*.



Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

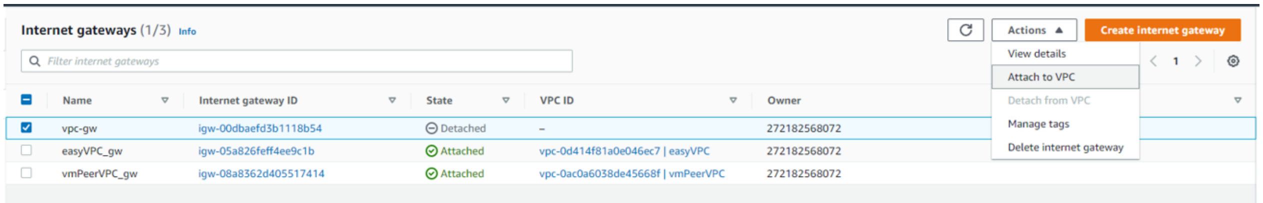
Name tag
Creates a tag with a key of 'Name' and a value that you specify.
vpc-gw

Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name
Value - *optional*: vpc-gw

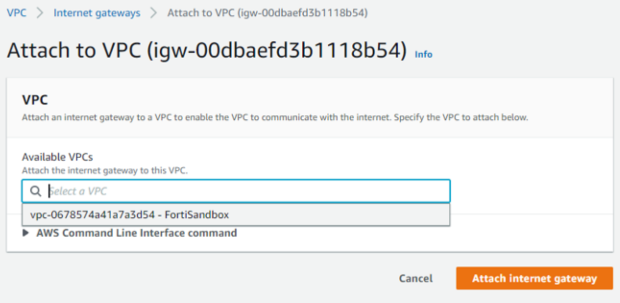
You can add 49 more tags.

3. When the Internet Gateway is created, click *Attach to VPC*.



☐	Name	Internet gateway ID	State	VPC ID	Owner
☑	vpc-gw	igw-00dbaefd3b1118b54	Detached	–	272182568072
☐	easyVPC_gw	igw-05a826feff4ee9c1b	Attached	vpc-0d414f81a0e046ec7 | easyVPC	272182568072
☐	vmPeerVPC_gw	igw-08a8362d405517414	Attached	vpc-0ac0a6038de45668f | vmPeerVPC	272182568072

4. Select the VPC and click *Attach internet gateway*.


VPC > Internet gateways > Attach to VPC (igw-00dbaefd3b1118b54)

Attach to VPC (igw-00dbaefd3b1118b54) Info

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.
Select a VPC
vpc-0678574a41a7a3d54 - FortiSandbox

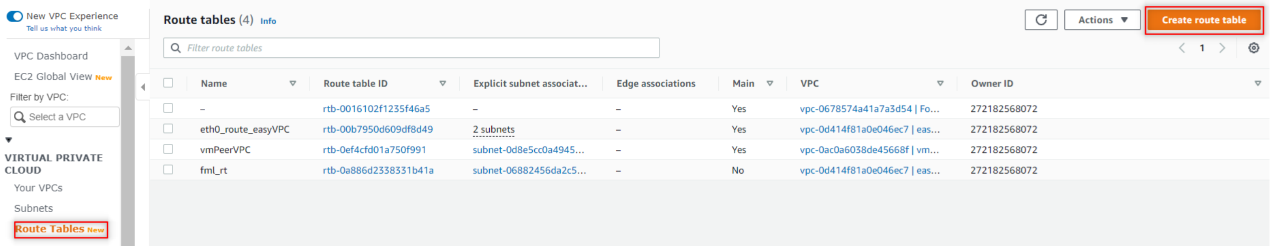
▶ AWS Command Line Interface command
Cancel
Attach internet gateway

Create a route table

Appropriate route table entries are needed for the FortiSandbox instance to communicate with other network entities.

To create route table and entries:

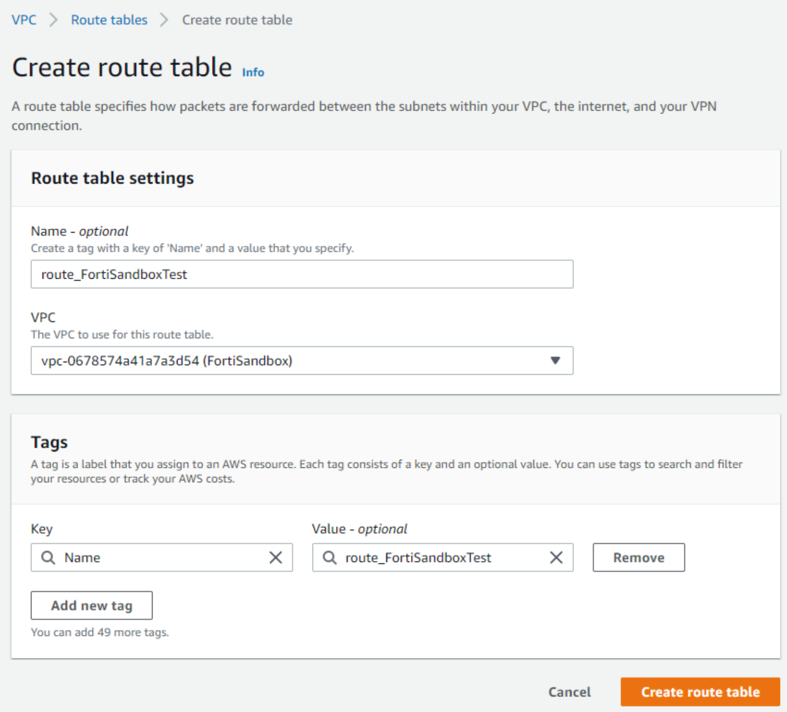
1. Under *Virtual Private Cloud* > *Route Tables*, click *Create Route Table*.



Route tables (4) Info

☐	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
☐	–	rtb-0016102f1235f46a5	–	–	Yes	vpc-0678574a41a7a3d54 | Fo...	272182568072
☐	eth0_route_easyVPC	rtb-00b7950d609df8d49	2 subnets	–	Yes	vpc-0d414f81a0e046ec7 | eas...	272182568072
☐	vmPeerVPC	rtb-0ef4cfd01a750f991	subnet-0d8e5cc0a4945...	–	Yes	vpc-0ac0a6038de45668f | vm...	272182568072
☐	fml_rt	rtb-0a886d2338331b41a	subnet-06882456da2c5...	–	No	vpc-0d414f81a0e046ec7 | eas...	272182568072

2. In the *Create Route Table* dialog box, enter the following information, then click *Create route table*.
   - 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.

Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
route_FortiSandboxTest

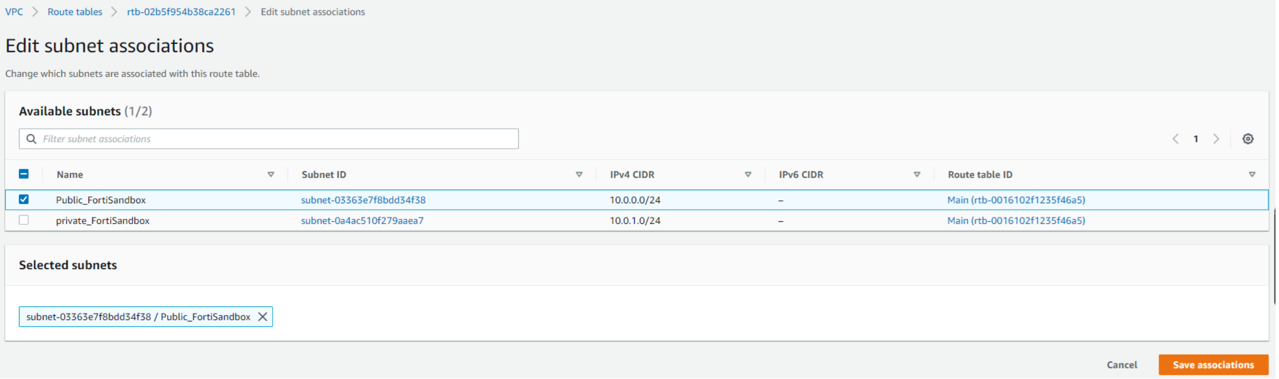
VPC
The VPC to use for this route table.
vpc-0678574a41a7a3d54 (FortiSandbox)

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	route_FortiSandboxTest

You can add 49 more tags.

3. Go to *Subnet Associations* > *Edit subnet associations*, select the management subnet you created, then click *Save associations.*.



VPC > Route tables > rtb-02b5f954b38ca2261 > Edit subnet associations
Filter subnet associations
1
Cancel
Save associations

Edit subnet associations

Change which subnets are associated with this route table.

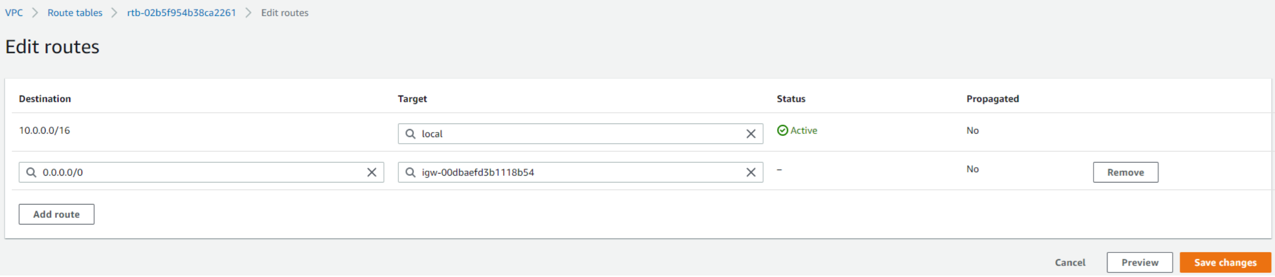
Available subnets (1/2)

▬	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	Public_FortiSandbox	subnet-03363e7f8bdd34f38	10.0.0.0/24	–	Main (rtb-0016102f1235f46a5)
☐	private_FortiSandbox	subnet-0a4ac510f279aaea7	10.0.1.0/24	–	Main (rtb-0016102f1235f46a5)

Selected subnets

subnet-03363e7f8bdd34f38 / Public_FortiSandbox

4. After the route table is created, you can add static route entries to define how the FortiSandbox instance to communicate with others. For example, to access FortiSandbox instance from the Internet:
   Go to *Routes* > *Add Route*, enter the following information, then click *Save changes*.
   - For *Destination*, enter `0.0.0.0/0`.
   - For *Target*, select the internet gateway for the management subnet you created.



VPC > Route tables > rtb-02b5f954b38ca2261 > Edit routes

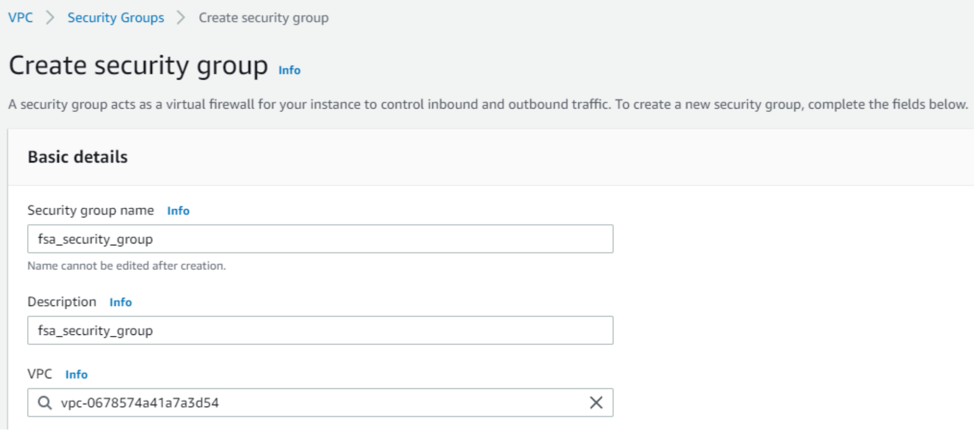
Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw-00dbaefd3b1118b54	-	No	Remove

Create a security group

It's important to limit only valid network traffic to and from FortiSandbox instance. To do that, you will need to create security groups and security rules for traffic.

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



VPC > Security Groups > Create security group

Create security group Info

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

Basic details

Security group name Info: fsa_security_group

Name cannot be edited after creation.

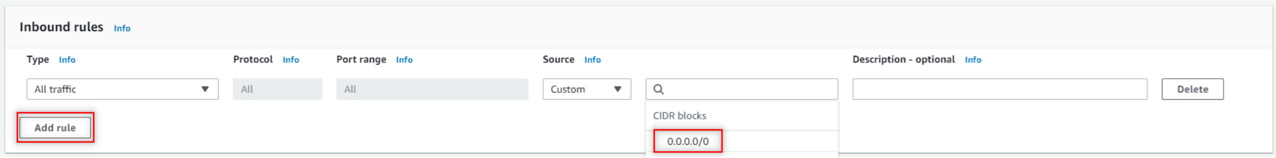
Description Info: fsa_security_group

VPC Info: vpc-0678574a41a7a3d54

3. Add the following Inbound rules:

Details	Value
Type	Custom TCP.
Protocol	TCP
Port Range	Allow the following ports to be accessible: • 443 (HTTPS) • 22 (if SSH access is needed)

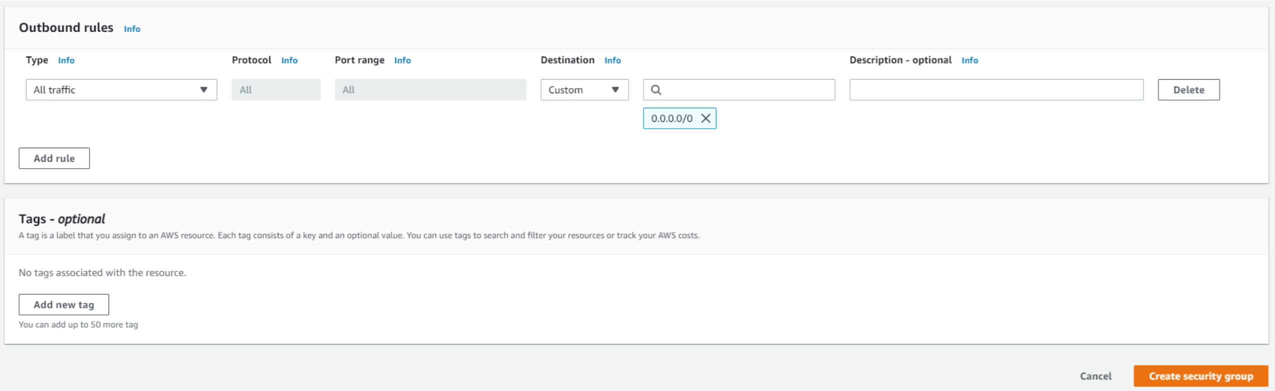
Details	Value
	• 514 (if Fortinet Fabric devices such as FortiGate and FortiMail need to submit jobs) • 9833 (for on-demand interactive scans) • 21 (FortiSandbox hardcoded port2 to communicate with custom VM clones via FTP) More rules can be added. For example, you can add a rule to allow access to FortiSandbox's MTA adapter. For more port information, see *Port Information* section of the *FortiSandbox Administration Guide*.
Source	Custom. For the *SourceIP*, enter a trusted IP range that can access the FortiSandbox instance.



Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
All traffic	All	All	Custom	CIDR blocks 0.0.0.0/0		Delete

4. Allow all traffic for outbound rules, then click *Create security group*.



Outbound rules Info

Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info	
All traffic	All	All	Custom	0.0.0.0/0		Delete

Tags - *optional*

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add up to 50 more tag

Generate AWS access key for FortiSandbox

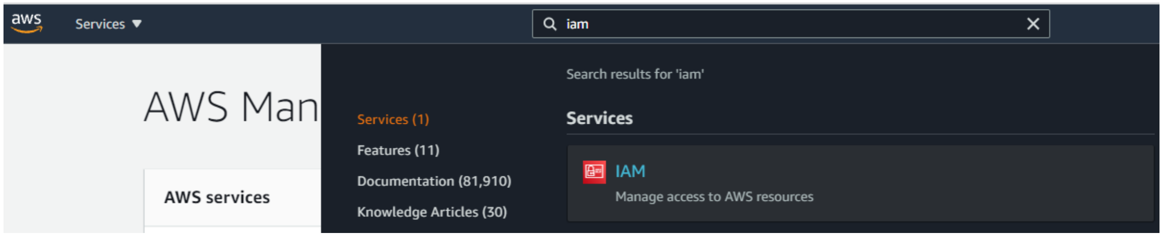
You will need to generate an access key from your AWS account to allow the FortiSandbox instance to access AWS resources.

To generate a AWS access key for FortiSandbox:

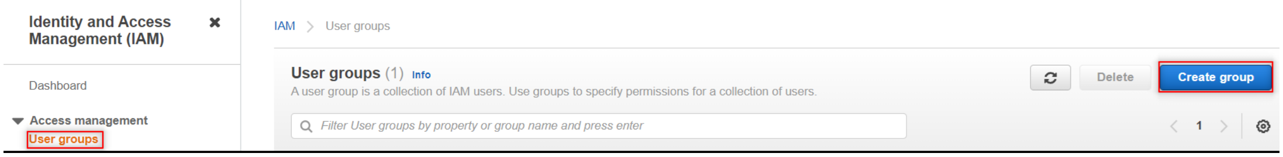
1. Create an IAM group
2. Attach policies
3. Create IAM users and an AWS API key

Create 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 *User Groups* > *Create Group*.


Identity and Access Management (IAM)
Dashboard
Access management
User groups
IAM > User groups
User groups (1) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Filter User groups by property or group name and press enter
1

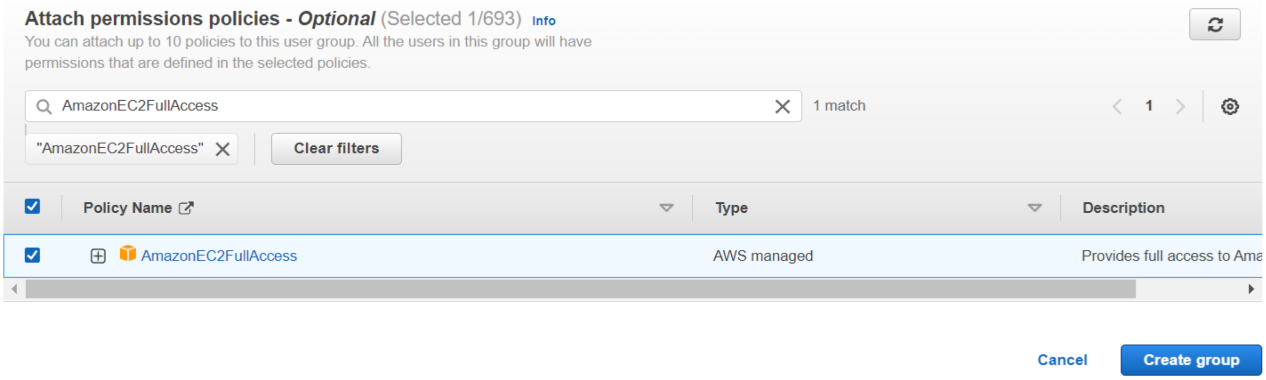
5. In the *User group name* field, enter a name, for example, *QA_FortiSandboxTest*.

Attach 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*.



Attach permissions policies - *Optional* (Selected 1/693)

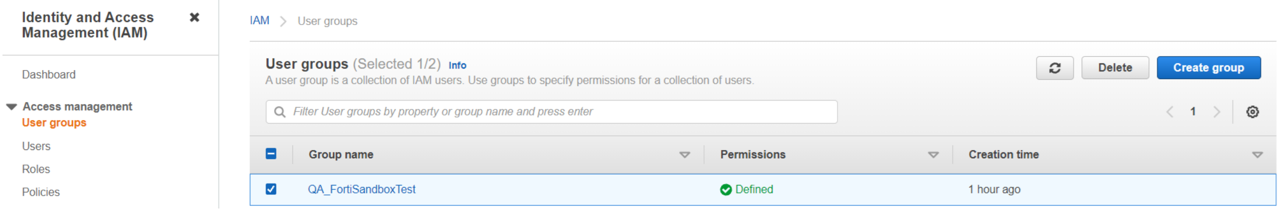
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

AmazonEC2FullAccess

"AmazonEC2FullAccess"

☑	Policy Name	Type	Description
☑	AmazonEC2FullAccess	AWS managed	Provides full access to Ama

3. Repeat this for all policies.
4. Click *Create Group*.
5. Check the group you created (*QA_FortiSandbox*) to review the group summary.



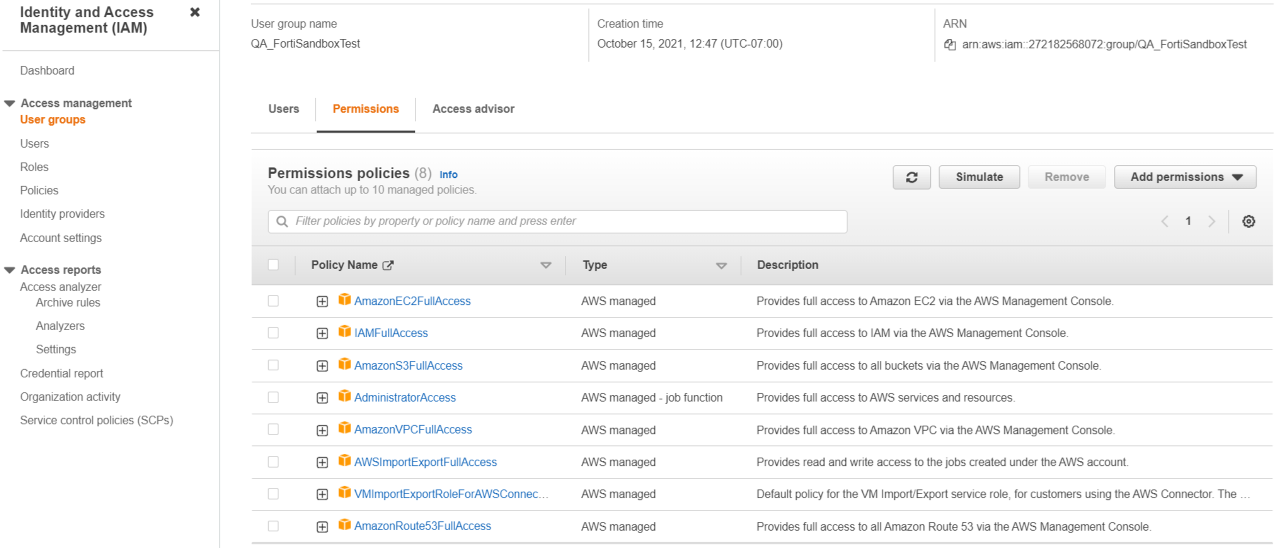
User groups (Selected 1/2)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

☐	Group name	Permissions	Creation time
☑	QA_FortiSandboxTest	✓ Defined	1 hour ago

6. In the *Permissions* tab, review the attached policies.



User group name: QA_FortiSandboxTest

Creation time: October 15, 2021, 12:47 (UTC-07:00)

ARN: arn:aws:iam::272182568072:group/QA_FortiSandboxTest

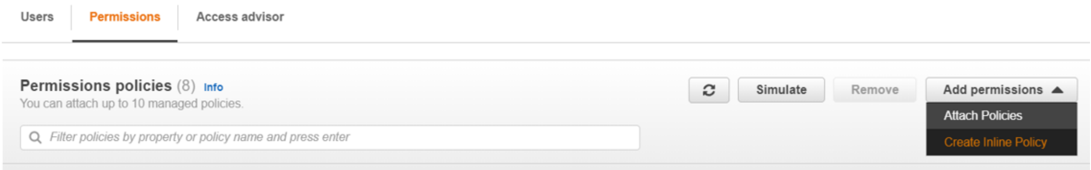
Permissions policies (8)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

☐	Policy Name	Type	Description
☐	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Management Console.
☐	IAMFullAccess	AWS managed	Provides full access to IAM via the AWS Management Console.
☐	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Management Console.
☐	AdministratorAccess	AWS managed - job function	Provides full access to AWS services and resources.
☐	AmazonVPCFullAccess	AWS managed	Provides full access to Amazon VPC via the AWS Management Console.
☐	AWSImportExportFullAccess	AWS managed	Provides read and write access to the jobs created under the AWS account.
☐	VMImportExportRoleForAWSConnec...	AWS managed	Default policy for the VM Import/Export service role, for customers using the AWS Connector. The ...
☐	AmazonRoute53FullAccess	AWS managed	Provides full access to all Amazon Route 53 via the AWS Management Console.

7. Click *Add permissions* > *Create Inline Policies*. Select *Custom Policy* and use the policy editor to customize your own set of permissions.

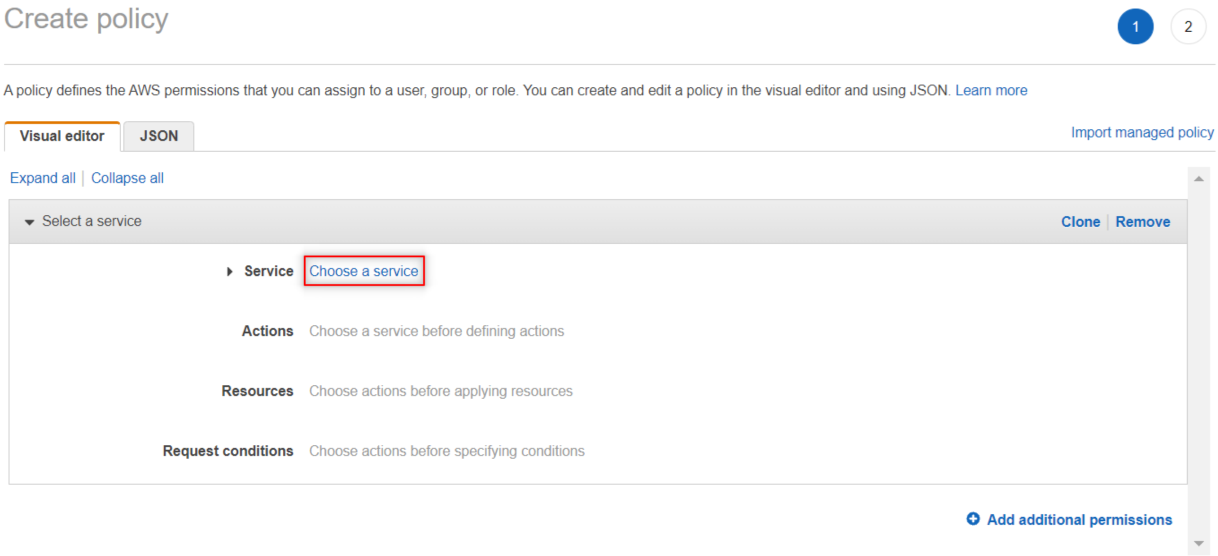


Permissions policies (8)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

8. You can use the AWS Visual editor or a JSON editor to create policies. If the validation is successful, click *Review Policy*.
   - **To create the policy by using AWS Visual editor:**



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

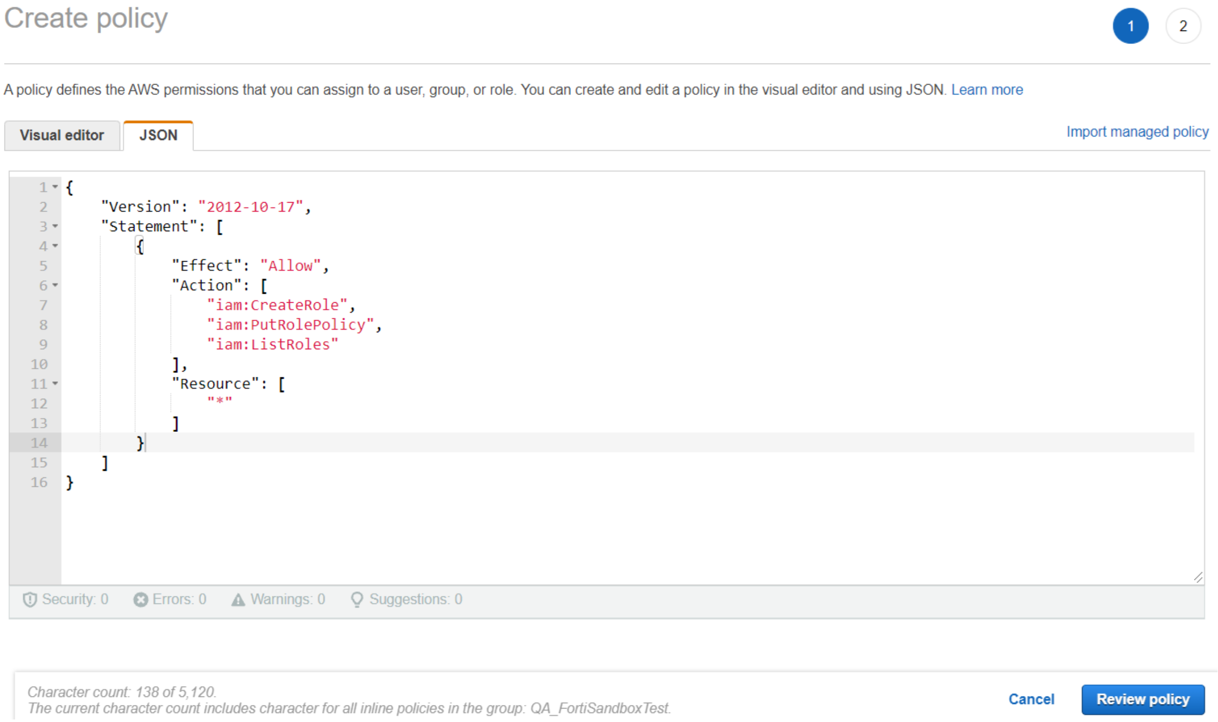
Service: Choose a service

Actions: Choose a service before defining actions

Resources: Choose actions before applying resources

Request conditions: Choose actions before specifying conditions

   - **To create the policy in JSON format:**



Create policy

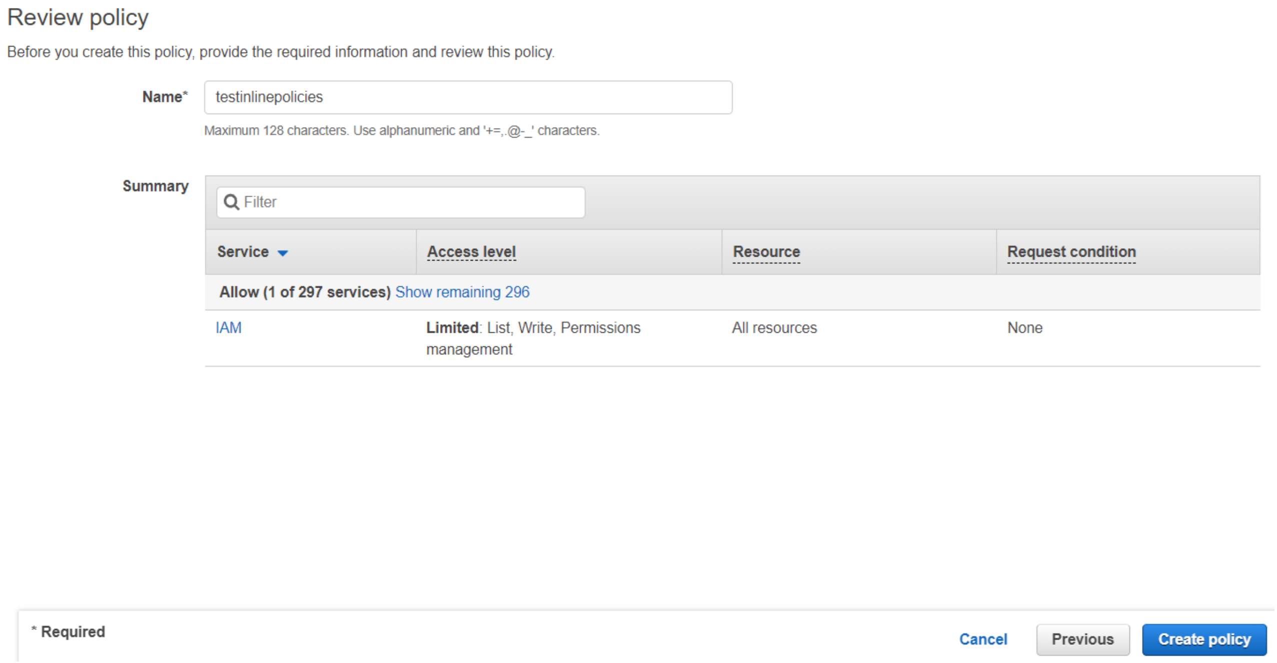
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:ListRoles"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Character count: 138 of 5,120.
The current character count includes character for all inline policies in the group: QA_FortiSandboxTest.

9. Under *Review policy*, enter a policy *Name* and then click *Create policy*.



Review policy

Before you create this policy, provide the required information and review this policy.

Name* testinlinepolicies

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

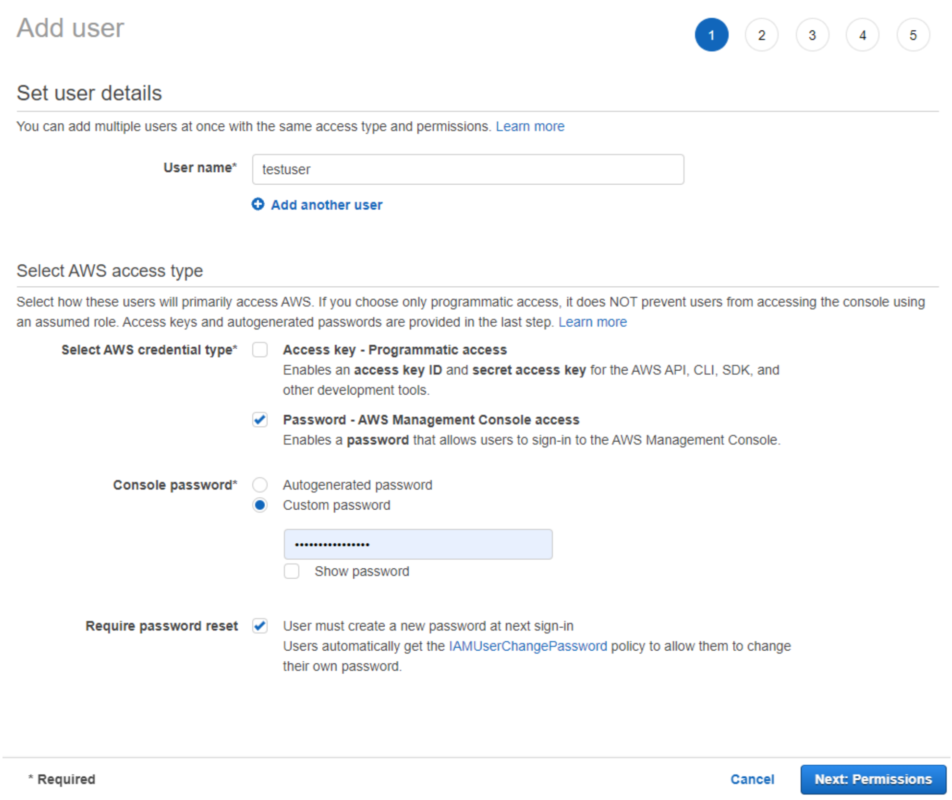
Service	Access level	Resource	Request condition
Allow (1 of 297 services) Show remaining 296			
IAM	Limited: List, Write, Permissions management	All resources	None

10. Under *Permissions policies*, review the policies you created.

Create IAM users and an AWS API key

To create an IAM user:

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



Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* testuser

Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

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

Console password*
- ○ Autogenerated password
- ● Custom password

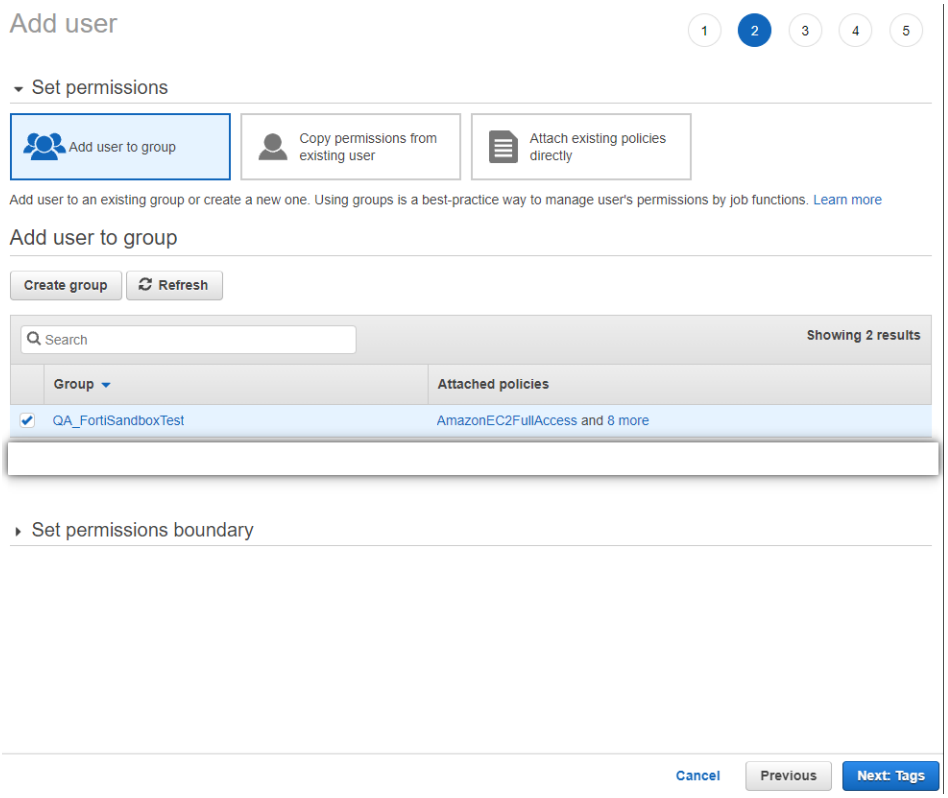
••••••••••••••••

□ 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

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



Add user

1 2 3 4 5

Set permissions

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

Add user to group

Create group
Refresh
Search

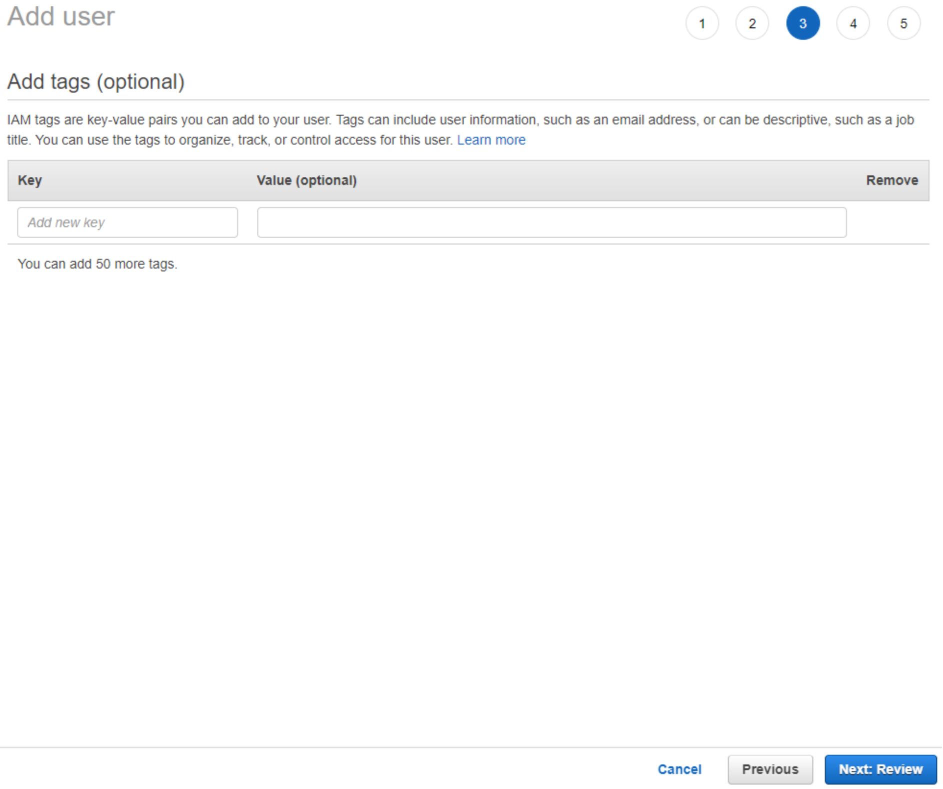
Showing 2 results

	Group	Attached policies
☑	QA_FortiSandboxTest	AmazonEC2FullAccess and 8 more

Set permissions boundary

Cancel
Previous
Next: Tags

4. (Optional) Add any tags that you need. If you do not require any tags, click *Next: Review*.



Add user

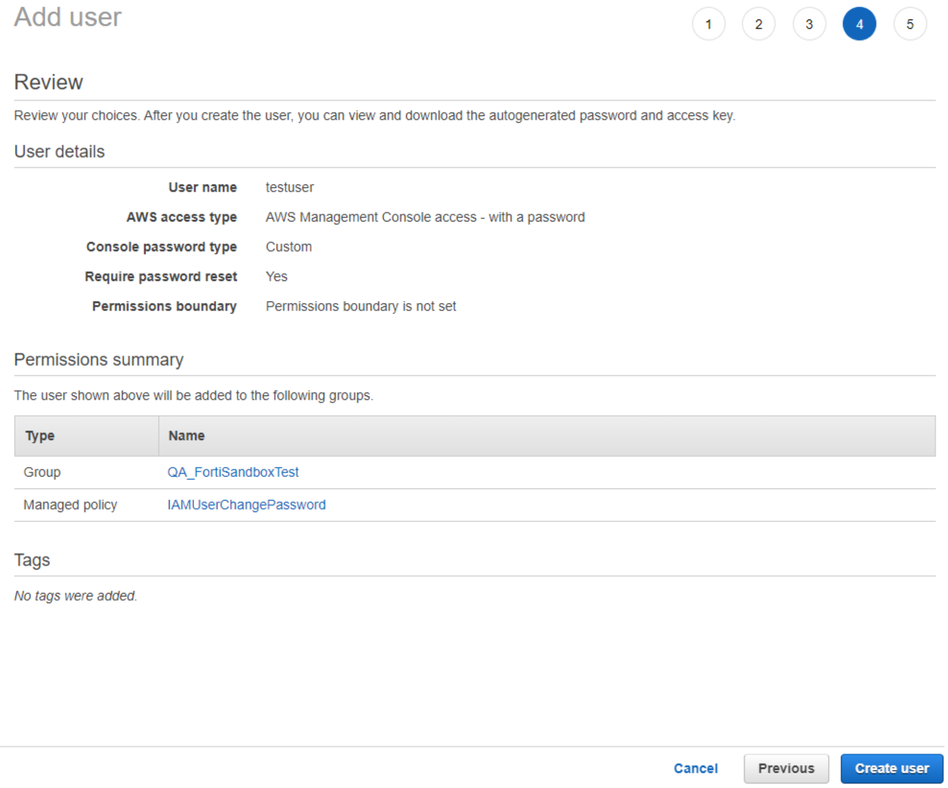
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

5. Under *Review*, review the user details, then click *Create user*.



Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	testuser
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

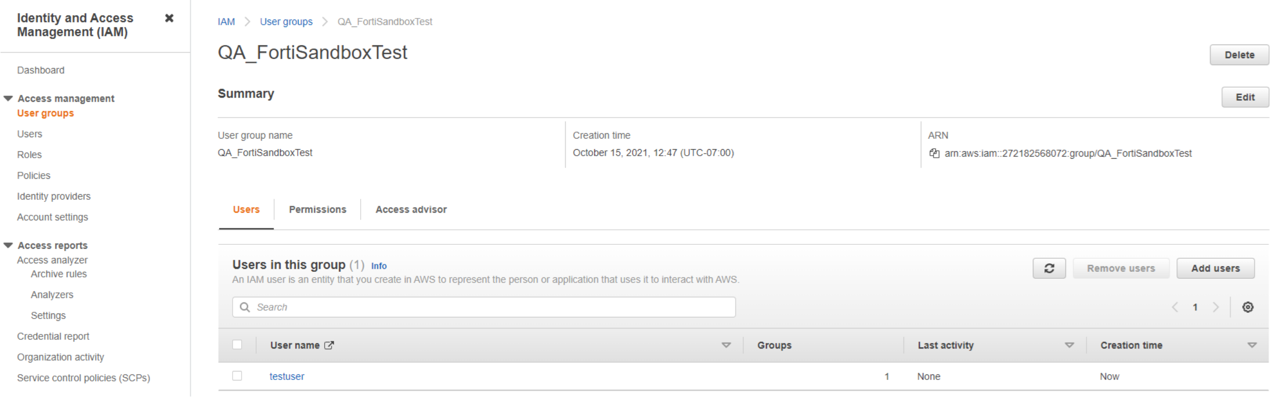
Type	Name
Group	QA_FortiSandboxTest
Managed policy	IAMUserChangePassword

Tags

No tags were added.

6. Click *Close*.

7. Click *User groups* to view the user you created.



QA_FortiSandboxTest

Summary

User group name	Creation time	ARN
QA_FortiSandboxTest	October 15, 2021, 12:47 (UTC-07:00)	arn:aws:iam::272182568072:group/QA_FortiSandboxTest

Users in this group (1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

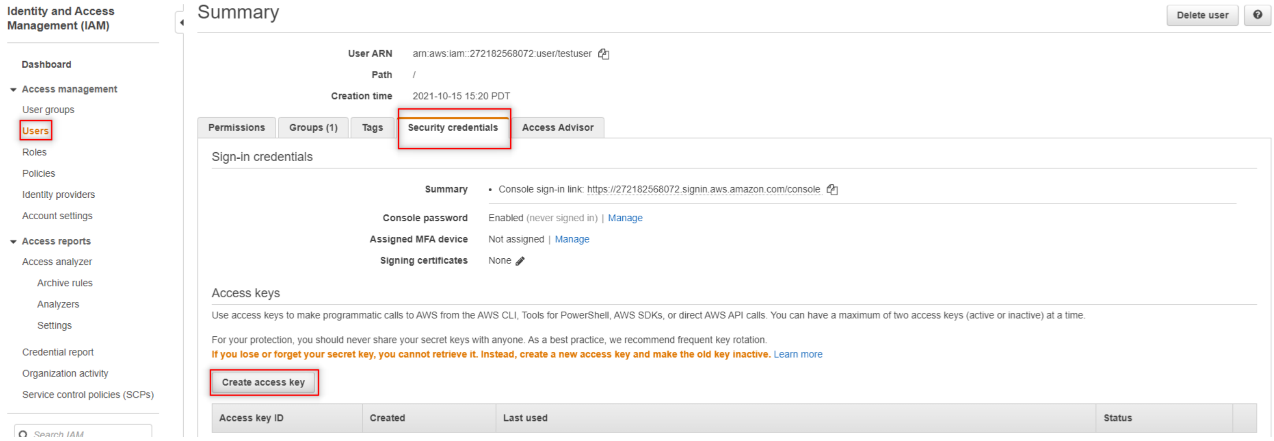
User name	Groups	Last activity	Creation time
testuser	1	None	Now

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

Create an AWS API Key

To create an AWS API key:

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



Summary

User ARN arn:aws:iam::272182568072:user/testuser
Path /
Creation time 2021-10-15 15:20 PDT

Sign-in credentials

Summary • Console sign-in link: https://272182568072.signin.aws.amazon.com/console
Console password Enabled (never signed in) | Manage
Assigned MFA device Not assigned | Manage
Signing certificates None

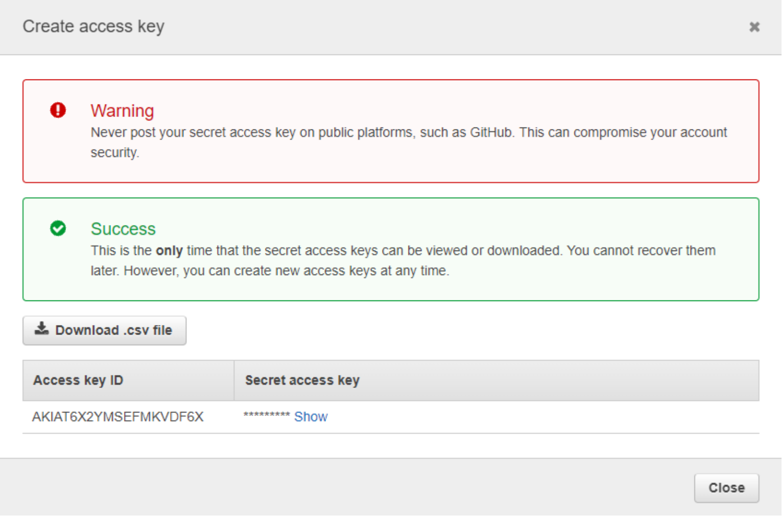
Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.
If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. Learn more

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*.



Create access key

Warning
Never post your secret access key on public platforms, such as GitHub. This can compromise your account security.

Success
This is the **only** time that the secret access keys can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

Access key ID	Secret access key
AKIAT6X2YMSEFMKVDF6X	********* Show

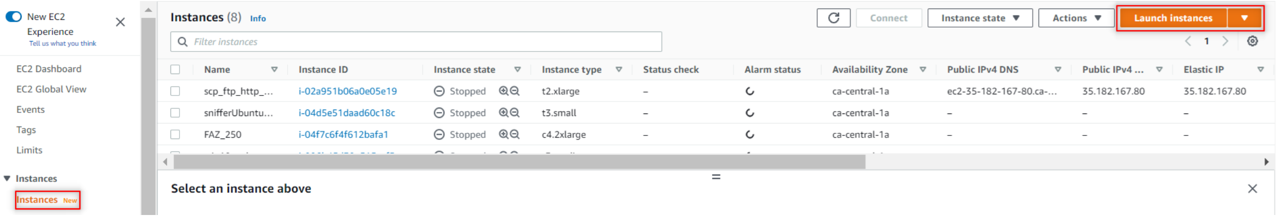
3. Click *Close*.

Deploy FortiSandbox on AWS (BYOL/On-Demand)

You can create your FortiSandbox instance on AWS in On-Demand mode or BYOL mode. For BYOL mode, a FSA VM00 license file should be purchased and uploaded.

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

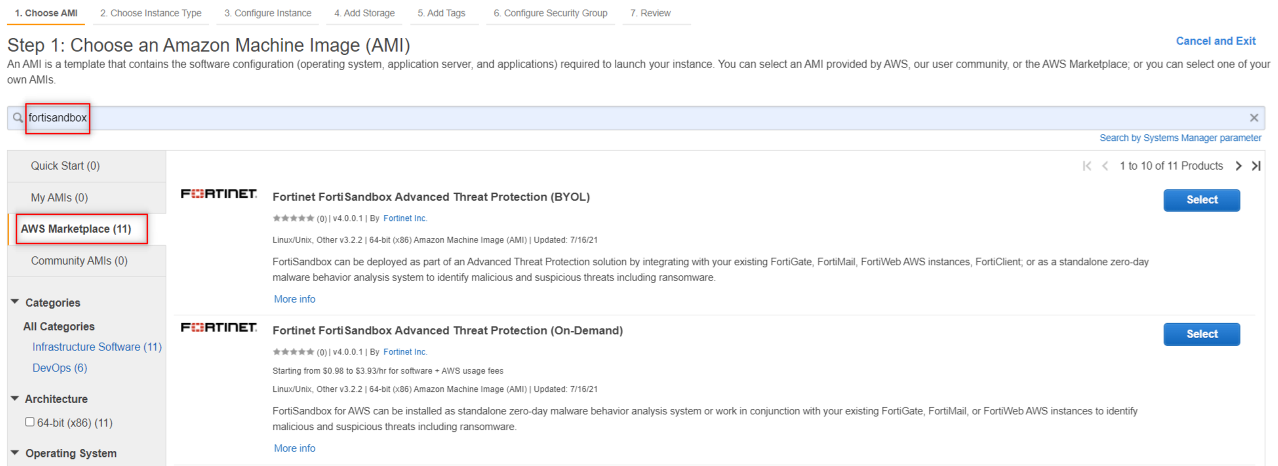
1. Go to *EC2* > *Instances* and click *Launch Instance*.



	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
□	scp_ftp_http_...	i-02a951b06a0e05e19	Stopped	t2.xlarge	–		ca-central-1a	ec2-35-182-167-80.ca-...	35.182.167.80	35.182.167.80
□	snifferUbuntu...	i-04d5e51daad60c18c	Stopped	t3.small	–		ca-central-1a	–	–	–
□	FAZ_250	i-04f7c6f4f612bafa1	Stopped	c4.2xlarge	–		ca-central-1a	–	–	–

Select an instance above

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



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Fortinet FortiSandbox Advanced Threat Protection (BYOL)

★★★★★ (0) | v4.0.0.1 | By Fortinet Inc.

Linux/Unix, Other v3.2.2 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 7/16/21

FortiSandbox can be deployed as part of an Advanced Threat Protection solution by integrating with your existing FortiGate, FortiMail, FortiWeb AWS instances, FortiClient; or as a standalone zero-day malware behavior analysis system to identify malicious and suspicious threats including ransomware.

Fortinet FortiSandbox Advanced Threat Protection (On-Demand)

★★★★★ (0) | v4.0.0.1 | By Fortinet Inc.

Starting from $0.98 to $3.93/hr for software + AWS usage fees

Linux/Unix, Other v3.2.2 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 7/16/21

FortiSandbox for AWS can be installed as standalone zero-day malware behavior analysis system or work in conjunction with your existing FortiGate, FortiMail, or FortiWeb AWS instances to identify malicious and suspicious threats including ransomware.

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

Technical Specification	Details		
	On-Premise (Private) Cloud	Public Cloud - BYOL	Public Cloud - PYAG
Hypervisor Support	VMware ESXi Microsoft Hyper-V Windows server 2016 and 2019	AWS Azure	
HA Support	FortiSandbox 3.2 or later		

Technical Specification	Details		
	On-Premise (Private) Cloud	Public Cloud - BYOL	Public Cloud - PYAG
Virtual CPUs (min / max)	4/Unlimited Fortinet recommends four virtual CPUs plus the number of VM clones.	4/16 Fortinet recommends following virtual CPUs based on the number of VM Clones: 0-4 clones - 4 cores, 5-32 clones - 8 cores, 33-100 clones - 16 cores, 101+ clones - 16 cores or higher. Pick up the appropriate Instance Type.	
Virtual Memory (min / max)	16 GB / 32 GB Fortinet recommends following virtual memory based n the number of VM Clones: 0-4 clones - 24 GB 5-8 clones - 32 GB	8 GB / 64 GB Recommended: Following virtual memory based on the number of VM Clones: 0-4 clones - 8 GB, 5-32 clones - 16 GB, 33-100 clones - 32 GB, 101+ clones - 64 GB. Pick the appropriate Instance Type.	
Virtual Storage (min / max)	200 GB / 16 TB Fortinet recommends at least 500 GB for a production environment.		
Virtual Network Interfaces	Recommended: 4 and above	Recommended: 2 and above	
VM Clones Support (Min/Max)	0[1]/ 8 (Local VMs) and 200 (Cloud VMs)	0[1] / 216[2]	0[1] / 128[3]

[1] For HA-Cluster deployment setup configured as Primary node acting as a dispatcher.

[2] Can enable any of the Custom VM or Cloud VM types up to the total seat count which is based on a combination of Windows licenses (max of 8), BYOL (8) and Cloud VMs (max of 200).

[3] Total seat count is based on the number of cores multiplied by 4. Maximum VMs is 128 since the highest available vCPU on PAYG is 32. CloudVMs can also be added on top and registered, however, this is not advised due to product serial number changes after shutdown.

4. Click *Next: Configure Instance Details*.

Configure 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

Details	Values
Subnet	Select the management interface 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 management interface subnet you created; Auto-Assign (or any IP in that subnet)
eth1	Select the local VM clone communication subnet you created, Auto-Assign (or any IP in that subnet) If you do not use a local VM clone, you don't need to add eth1. You can add it later if needed when the instance is not running.

Add storage

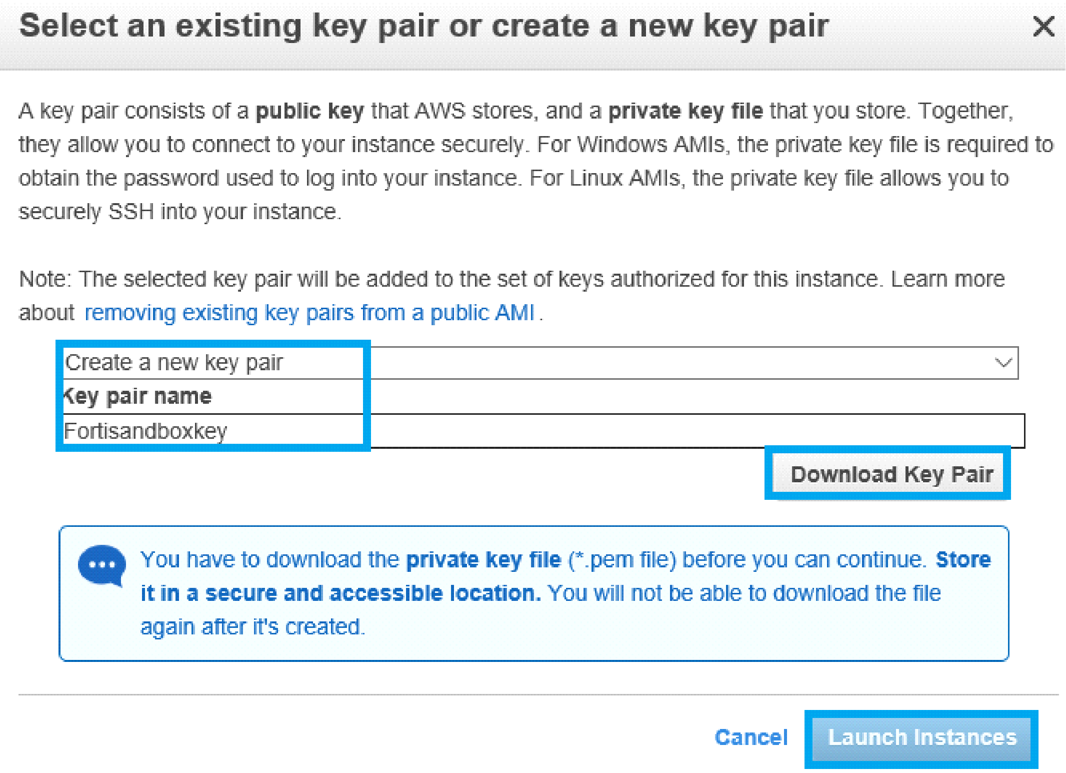
After configuring the Instance Details, click *Next, Add Storage*. Fortinet recommends 500GB to 16TB for storage size, depending on number of historical jobs user wants to keep in the system.

Adding tags

Do not configure anything on this page. Click *Next, Configure Security Group*. Choose the security group you created.

Launch the instance

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 to a safe place. The key files are needed to access FortiSandbox instance through SSH connection.



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 .

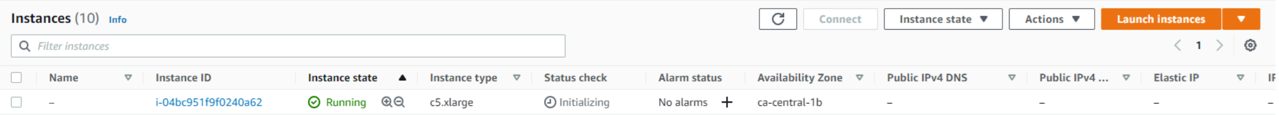
Create a new key pair

Key pair name

Fortisandboxkey

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.

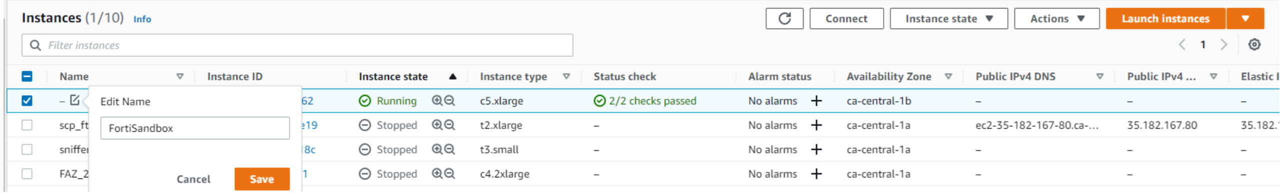
4. Click *Launch Instances*.
   After launching the instance, the next page shows that the FortiSandbox instance is running.
5. Click View Instances to view the instance state. Allow several minutes for *Status Checks* to change from *Initializing* to *2/2* checks.



Instances (10)

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IF
☐	–	i-04bc951f9f0240a62	Running	c5.xlarge	Initializing	No alarms +	ca-central-1b	–	–	–	–

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



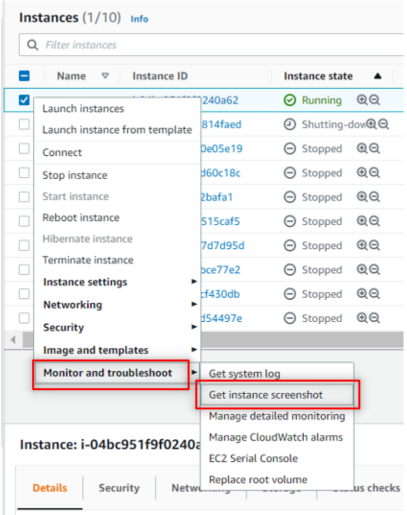
Instances (1/10)

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic I
☑	–	62	Running	c5.xlarge	2/2 checks passed	No alarms +	ca-central-1b	–	–	–
☐	scp_ft	19	Stopped	t2.xlarge	–	No alarms +	ca-central-1a	ec2-35-182-167-80.ca-...	35.182.167.80	35.182.
☐	sniffer	8c	Stopped	t3.small	–	No alarms +	ca-central-1a	–	–	–
☐	FAZ_2	1	Stopped	c4.2xlarge	–	No alarms +	ca-central-1a	–	–	–

Edit Name

FortiSandbox

7. Select the created instance. Right-click the instance and select *Monitor and troubleshoot > Get Instance Screenshot* to view the status of the launched instance.



Name	Instance ID	Instance state
	240a62	Running
	814faed	Shutting-dow
	0e05e19	Stopped
	d60c18c	Stopped
	2bafa1	Stopped
	515caf5	Stopped
	7d7d95d	Stopped
	bce77e2	Stopped
	cf430db	Stopped
	d54497e	Stopped

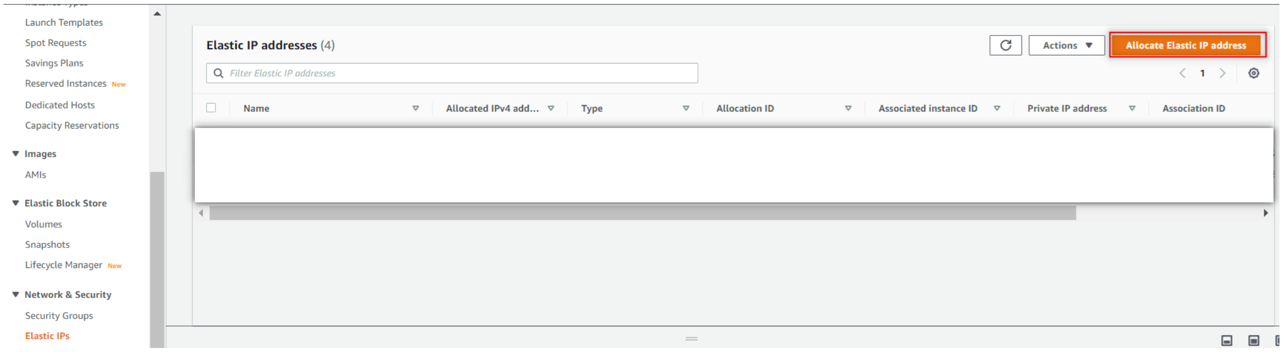
Instance: i-04bc951f9f0240a

Configure FortiSandbox instance network settings

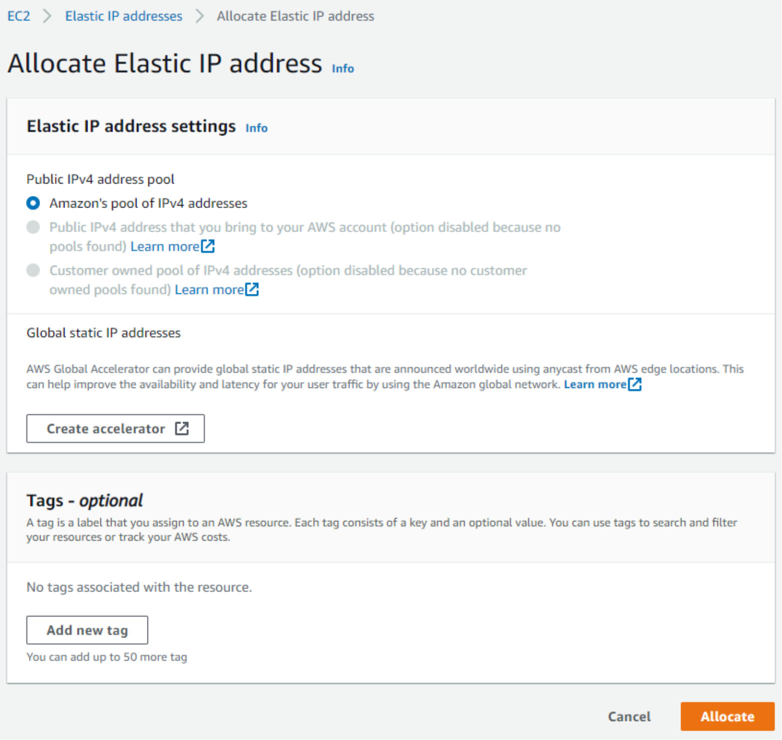
Create and assigning an Elastic IP to the instance

To access the FortiSandbox instance from the Internet, you will need to create an Elastic P (EIP) for your Virtual Private Cloud.

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



2. Click *Allocate* to get the new EIP Address.



Allocate Elastic IP address Info

Elastic IP address settings Info

Public IPv4 address pool

● Amazon's pool of IPv4 addresses

○ Public IPv4 address that you bring to your AWS account (option disabled because no pools found) Learn more

○ Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) Learn more

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

Tags - *optional*

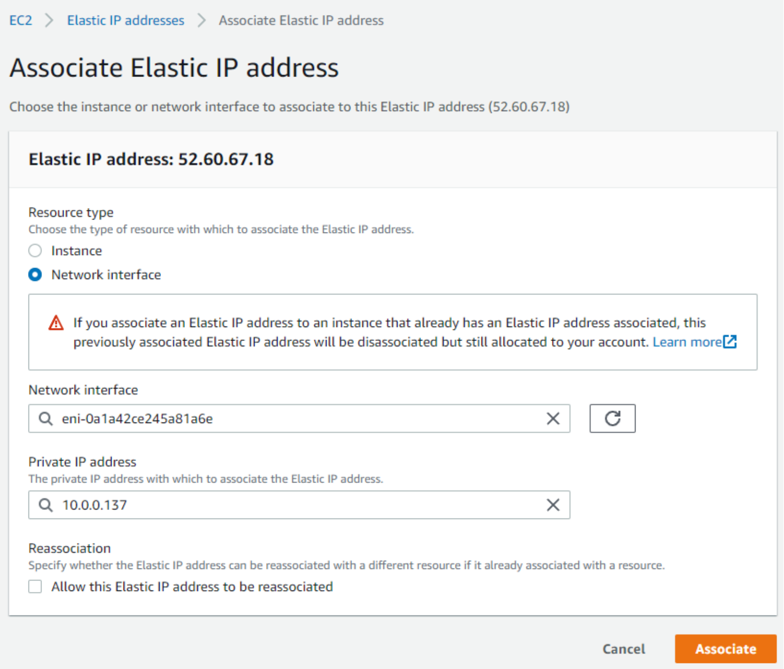
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add up to 50 more tag

3. Select the Elastic IP address you just created and click *Actions* to associate the EIP to FortiSandbox port1.
4. 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 (52.60.67.18)

Elastic IP address: 52.60.67.18

Resource type
Choose the type of resource with which to associate the Elastic IP address.
○ Instance
● Network interface

⚠ If you associate an Elastic IP address to an instance that already has an Elastic IP address associated, this previously associated Elastic IP address will be disassociated but still allocated to your account. Learn more

Network interface
eni-0a1a42ce245a81a6e

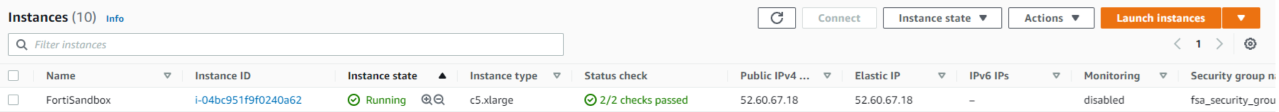
Private IP address
The private IP address with which to associate the Elastic IP address.
10.0.0.137

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

5. Click *Associate*.

Access FortiSandbox Web UI the first time

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



Instances (10) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring	Security group n
□	FortiSandbox	i-04bc951f9f0240a62	Running	c5.xlarge	2/2 checks passed	52.60.67.18	52.60.67.18	–	disabled	fsa_security_grou

2. Paste the copied IP address into a browser 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.

Configure the DNS

1. Go to *Network* > *System DNS*.
2. Configure the primary and secondary DNS server addresses of your organization such as the following:

Detail	Value
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4

3. Click *OK*.

Access FortiSandbox CLI

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

If you do not choose the *Without Key Pair* option, log in using the *admin* as the username, and 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. For information about opening CLI console through web UI, see the *Port Information* section of the *FortiSandbox Administration Guide*.

Prepare FortiSandbox for scanning contents

Upload firmware license to FortiSandbox instance

If the deployment mode is *On-Demand*, a firmware license file is not required. If the mode is *BYOL*, download a firmware license from the Customer Support website and then upload it to FortiSandbox.

To upload the license:

- Go to *Dashboard* > *Status* > *Licenses* widget.
- Click the *Upload License* the button next to FortiSandbox-AWS and upload the license.

Upload the rating and tracer engine

A copy of the rating and tracer engines are required for your instance to be fully functional. The instance can automatically download and install the engines if it is connected to FDN. You can also upload the engines manually. These engines can be downloaded from the Customer Support web site. For more information, see the *Tracer and Rating Engines* section of the *FortiSandbox Release Notes*.

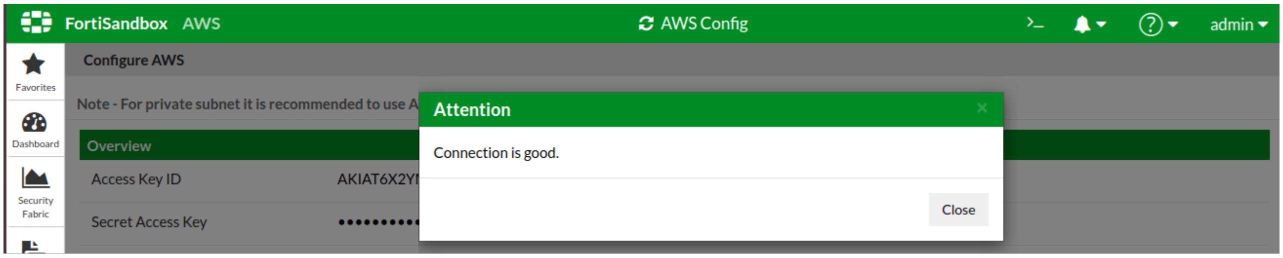
To manually upload the rating and tracer engine:

1. In FortiSandbox, go to *System* > *FortiGuard*.
2. Beside *Upload Package File*, click *Choose* file and locate the rating or tracer engine to be uploaded.

Import AWS settings into FortiSandbox

1. Go to *System* > *AWS Config* page, click *Configuration Wizard*, and enter the Access Key ID and Secret Access Key information created in Create an IAM group on page 12.
2. Select *Local VM Instance Type* and then select *t2-medium*.
3. Click *Next*.
4. For *VPC ID*, select the VPC you created.
5. For *Private Subnet*, select the subnet created for the local Windows or Linux VM communication (port2) if one exists. Otherwise, select the management subnet.
6. For *Security Groups*, select the security group for the Private Subnet you selected in step 5.
7. Click *Save*.
8. Click *Connection Test*.

9. When you get a confirmation that the connection is good, click *Close*.



Connection is good.

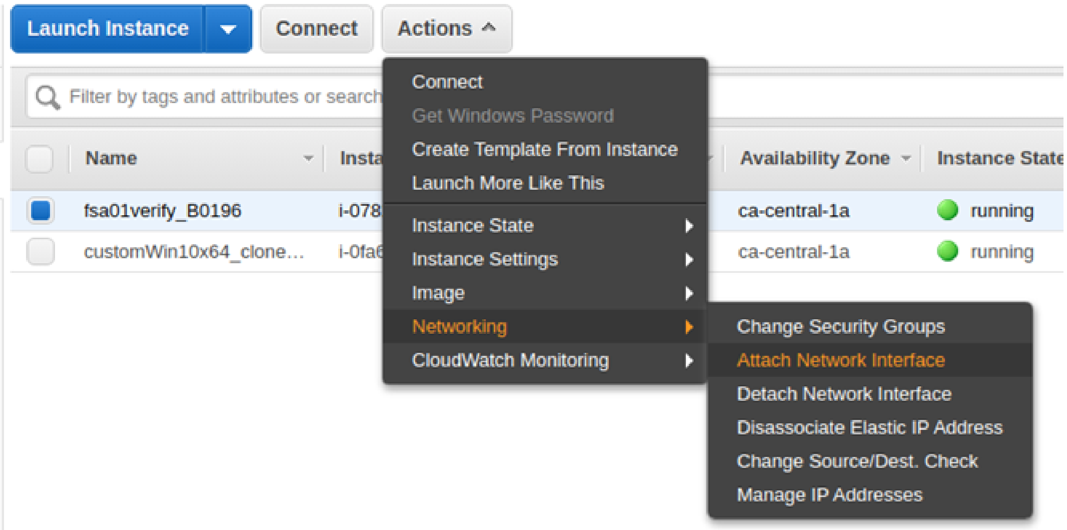
Set up a local custom Windows VM

Create custom VM for AWS

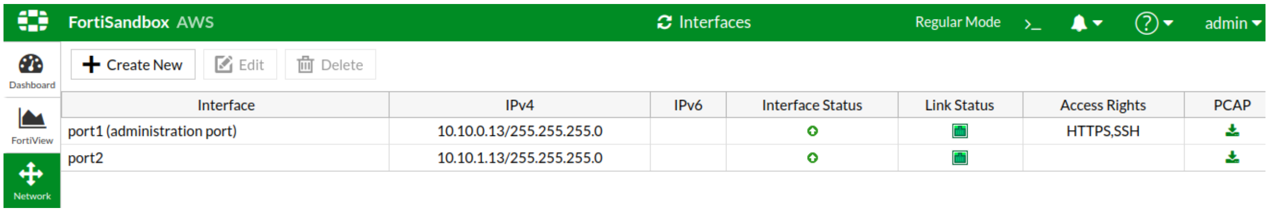
To create a custom Windows VM for AWS, follow steps in Custom VM Guide which can be found in the Fortinet Developer Network or is available on request from Customer Support.

Prepare the network interface for custom VM clones

The FortiSandbox instance uses port2 to communicate with local Windows or Linux clones. If you did not create an *eth1* in *Deploy FortiSandbox on AWS (BYOL/On-Demand)* > *Configure the instance*, you should create a new network interface under a local VM clone communication subnet and assign a private IP of this subnet to it.



After the interface is created, reboot the instance and go to *System* > *Interface* to verify the network interface is attached.



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		●	🟩		⭳

Create a NAT gateway

To create a NAT Gateway:

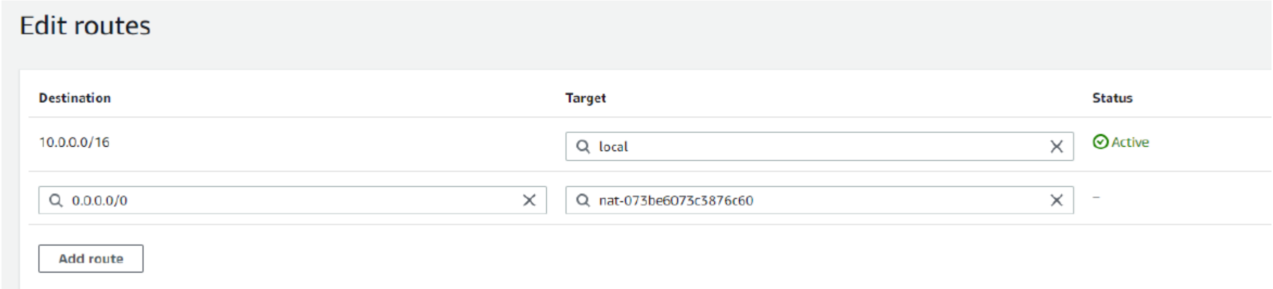
1. Go to *Virtual Private Cloud* > *NAT Gateways* and click *Create NAT gateway*.
2. Entre the following information, and click *Create NAT gateway*.

Name	Optional.
Subnet	Choose your management interface subnet (the one port1 is in).
Connectivity type	Choose *Public*.
Elastic IP allocation ID	Click *Allocate Elastic IP* and leave the optional bar empty as default.

Update the route table

1. Go to *Virtual Private Cloud* > *Route Table* and choose the Route Table associated to the subnet of FortiSandbox port2.
2. Go to *Routes* > *Edit routes* > *Add route* and enter the following information:

Destination	Enter `0.0.0.0/0`.
Target	Select the NAT gateway you created in the previous step.



Edit routes

Destination	Target	Status
10.0.0.0/16	local	Active
0.0.0.0/0	nat-073be6073c3876c60	-

3. Click *Save*.

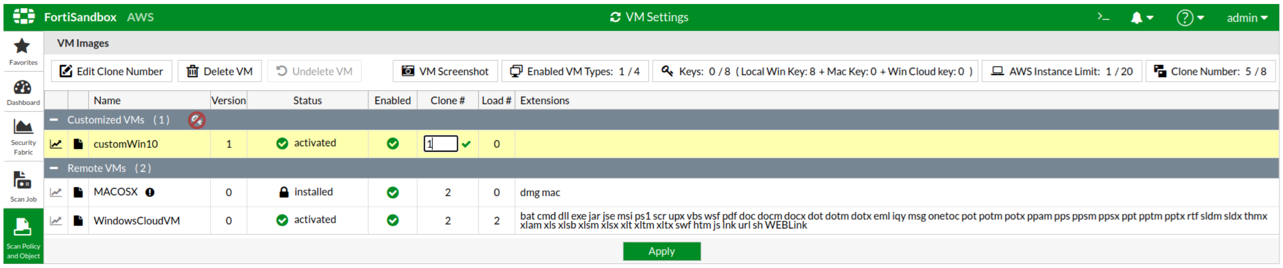
Install the custom VM using the CLI

After the custom VM image is created offline, it should be installed to AWS with the CLI. For details of using FortiSandbox CLI, see Access FortiSandbox CLI.

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

To install and enable 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 *Scan Policy and Object* > *VM Settings* and change *Clone #* to 1 or higher.



Enabled VM Types: 1 / 4

Keys: 0 / 8 (Local Win Key: 8 + Mac Key: 0 + Win Cloud key: 0)

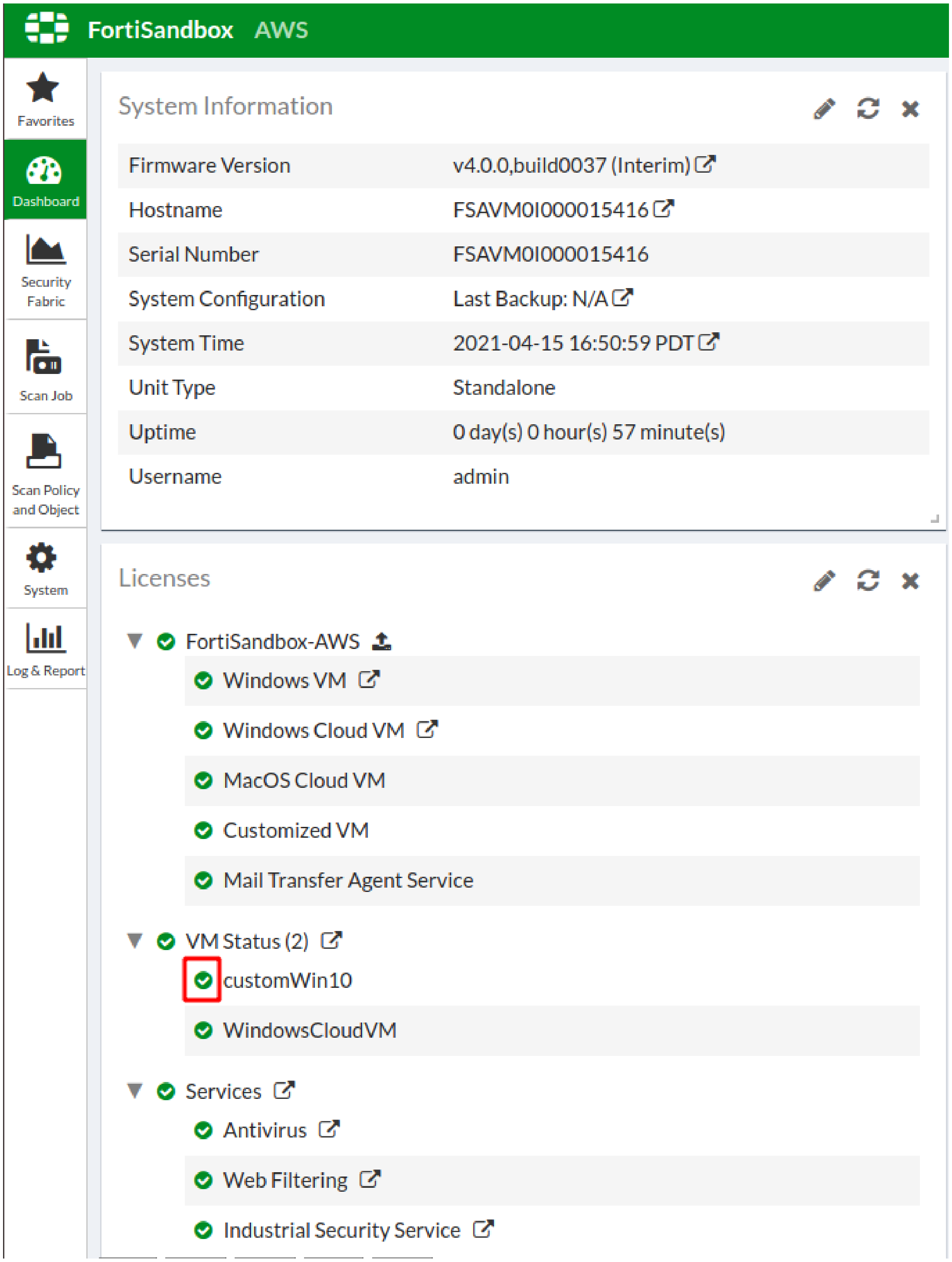
AWS Instance Limit: 1 / 20

Clone Number: 5 / 8

Name	Version	Status	Enabled	Clone #	Load #	Extensions
Customized VMs (1)						
customWin10	1	activated	✓	1	0	
Remote VMs (2)						
MACOSX	0	installed	✓	2	0	dmg mac
WindowsCloudVM	0	activated	✓	2	2	bat cmd dll exe jar jse msi ps1 scr upx vbs wsf pdf doc docm docx dot dotm dotx eml iqy msg onetoc pot potm potx ppam pps ppsm ppsx ppt pptm pptx rtf sldm sldx thmx xlam xls xlsb xlsm xlsx xlt xltm xltx swf htm js lnk url sh WEBLink

4. In a new CLI window, execute `diagnose-debug vminit` command.

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



System Information

Firmware Version	v4.0.0,build0037 (Interim)
Hostname	FSAVM01000015416
Serial Number	FSAVM01000015416
System Configuration	Last Backup: N/A
System Time	2021-04-15 16:50:59 PDT
Unit Type	Standalone
Uptime	0 day(s) 0 hour(s) 57 minute(s)
Username	admin

Licenses

- ✓ FortiSandbox-AWS
  - ✓ Windows VM
  - ✓ Windows Cloud VM
  - ✓ MacOS Cloud VM
  - ✓ Customized VM
  - ✓ Mail Transfer Agent Service
- ✓ VM Status (2)
  - ✓ customWin10
  - ✓ WindowsCloudVM
- ✓ Services
  - ✓ Antivirus
  - ✓ Web Filtering
  - ✓ Industrial Security Service

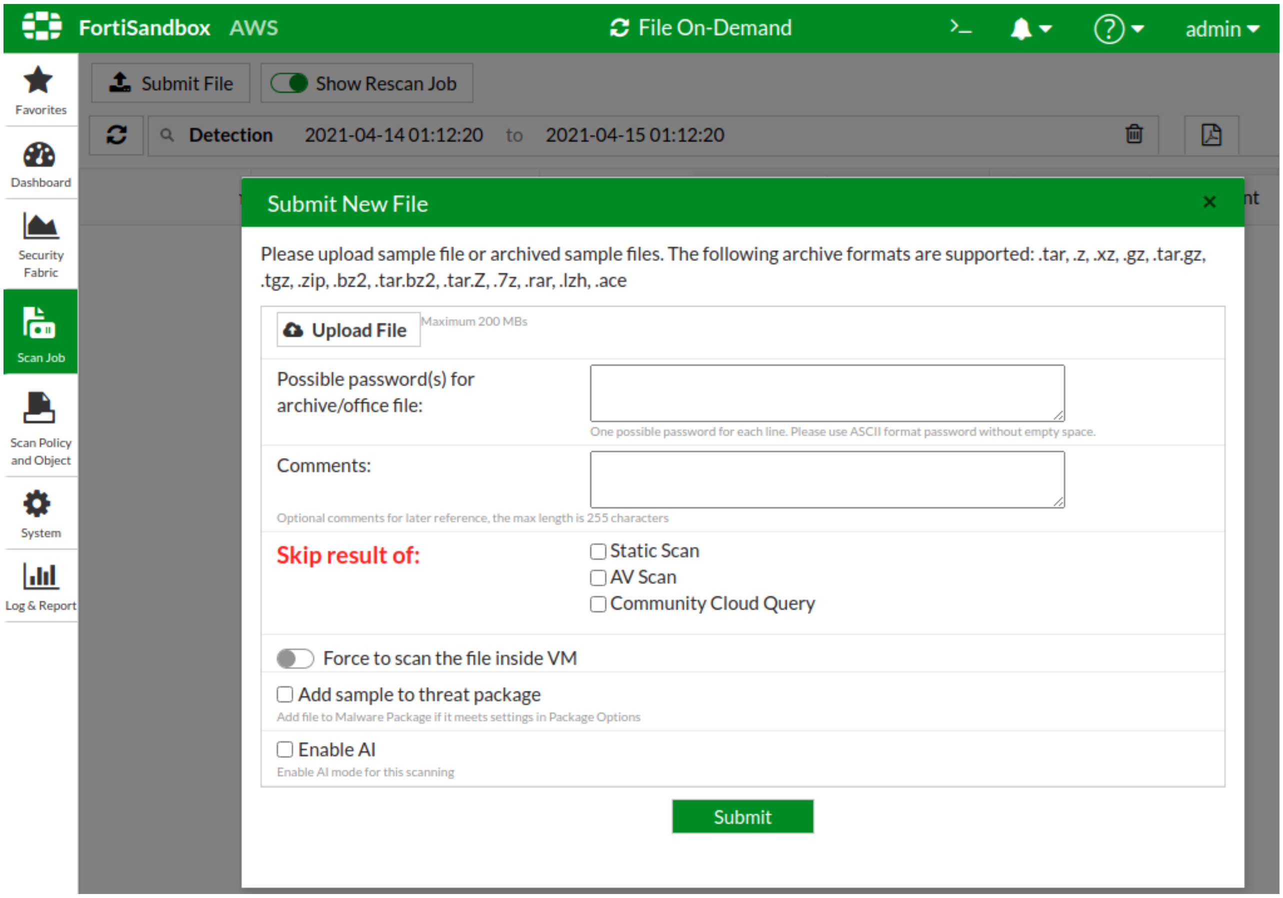
6. To associate file extensions to the custom VM, go to *Scan Policy and Object> Scan Profile* to the *VM Association* tab.

Test FortiSandbox instance with a file scan

To verify the configuration is successful, perform an on-demand file scan with a Windows VM clone.

To test FortiSandbox instance with a file scan:

1. Go to *Scan Job > File On-Demand > Submit File*.
2. Click *Choose File* and upload the sample file. You can force the file to be scanned inside a VM.
3. Click *Submit*.
   If the uploaded file is not malicious or suspicious, the rating is *Clean*.



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

Maximum 200 MBs

Possible password(s) for archive/office file:

One possible password for each line. Please use ASCII format password without empty space.

Comments:

Optional comments for later reference, the max length is 255 characters

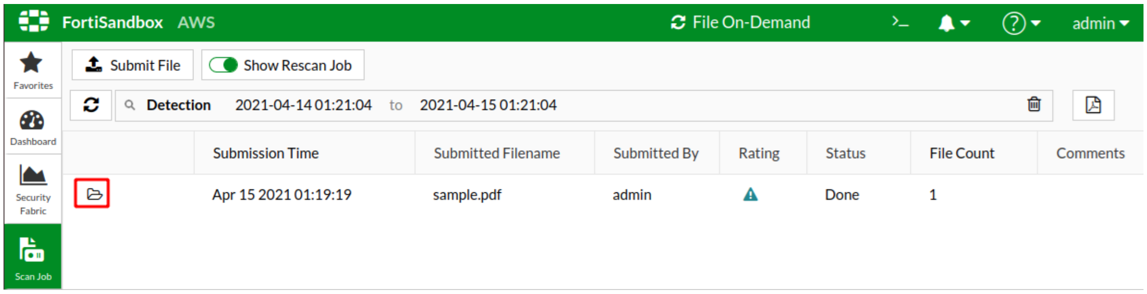
Skip result of:
☐ Static Scan
☐ AV Scan
☐ Community Cloud Query

○ Force to scan the file inside VM

☐ Add sample to threat package
Add file to Malware Package if it meets settings in Package Options

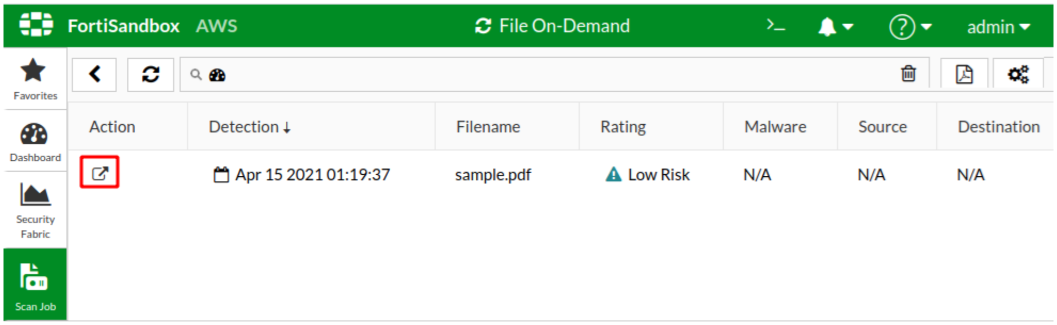
☐ Enable AI
Enable AI mode for this scanning

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



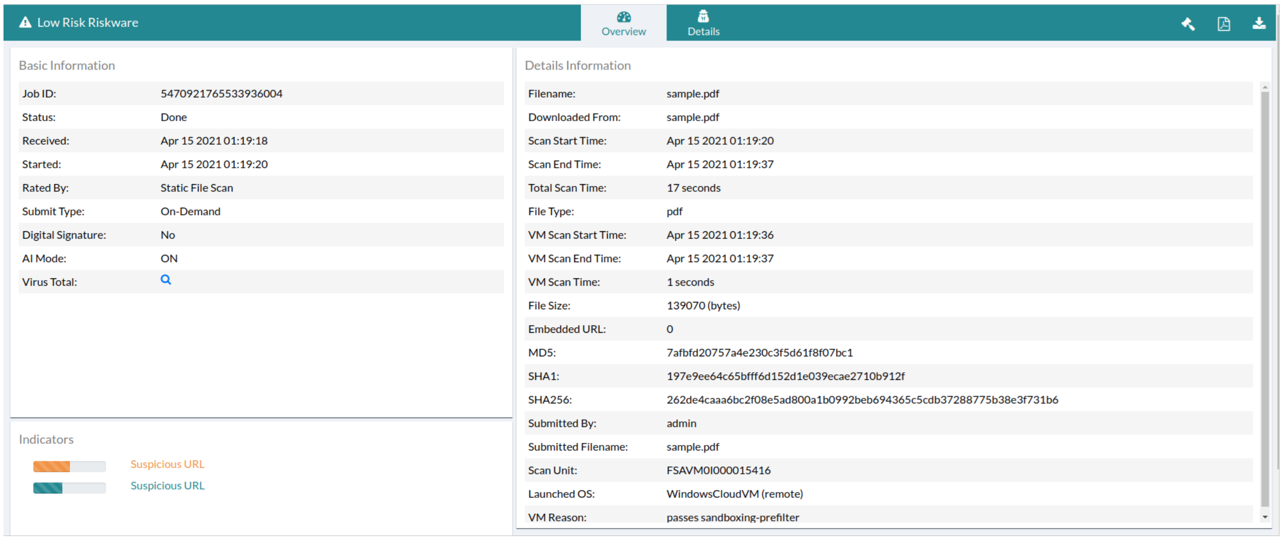
	Submission Time	Submitted Filename	Submitted By	Rating	Status	File Count	Comments
🗁	Apr 15 2021 01:19:19	sample.pdf	admin	▲	Done	1	

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



Action	Detection ↓	Filename	Rating	Malware	Source	Destination
	Apr 15 2021 01:19:37	sample.pdf	Low Risk	N/A	N/A	N/A

6. Check the file details that is displayed.



Basic Information

Job ID:	5470921765533936004
Status:	Done
Received:	Apr 15 2021 01:19:18
Started:	Apr 15 2021 01:19:20
Rated By:	Static File Scan
Submit Type:	On-Demand
Digital Signature:	No
AI Mode:	ON
Virus Total:	

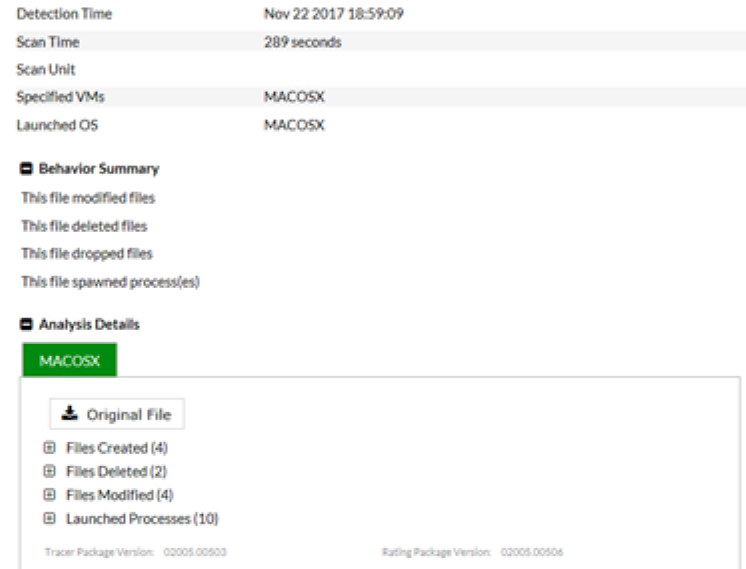
Indicators

Suspicious URL

Suspicious URL

Details Information

Filename:	sample.pdf
Downloaded From:	sample.pdf
Scan Start Time:	Apr 15 2021 01:19:20
Scan End Time:	Apr 15 2021 01:19:37
Total Scan Time:	17 seconds
File Type:	pdf
VM Scan Start Time:	Apr 15 2021 01:19:36
VM Scan End Time:	Apr 15 2021 01:19:37
VM Scan Time:	1 seconds
File Size:	139070 (bytes)
Embedded URL:	0
MD5:	7afbfd20757a4e230c3f5d61f8f07bc1
SHA1:	197e9ee64c65bfff6d152d1e039ecae2710b912f
SHA256:	262de4caaa6bc2f08e5ad800a1b0992beb694365c5cdb37288775b38e3f731b6
Submitted By:	admin
Submitted Filename:	sample.pdf
Scan Unit:	FSAVM0I000015416
Launched OS:	WindowsCloudVM (remote)
VM Reason:	passes sandboxing-prefilter



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

⊞ Files Created (4)

⊞ Files Deleted (2)

⊞ Files Modified (4)

⊞ Launched Processes (10)

Tracer Package Version: 02005.00503

Rating Package Version: 02005.00506

Optional: Using HA-Cluster

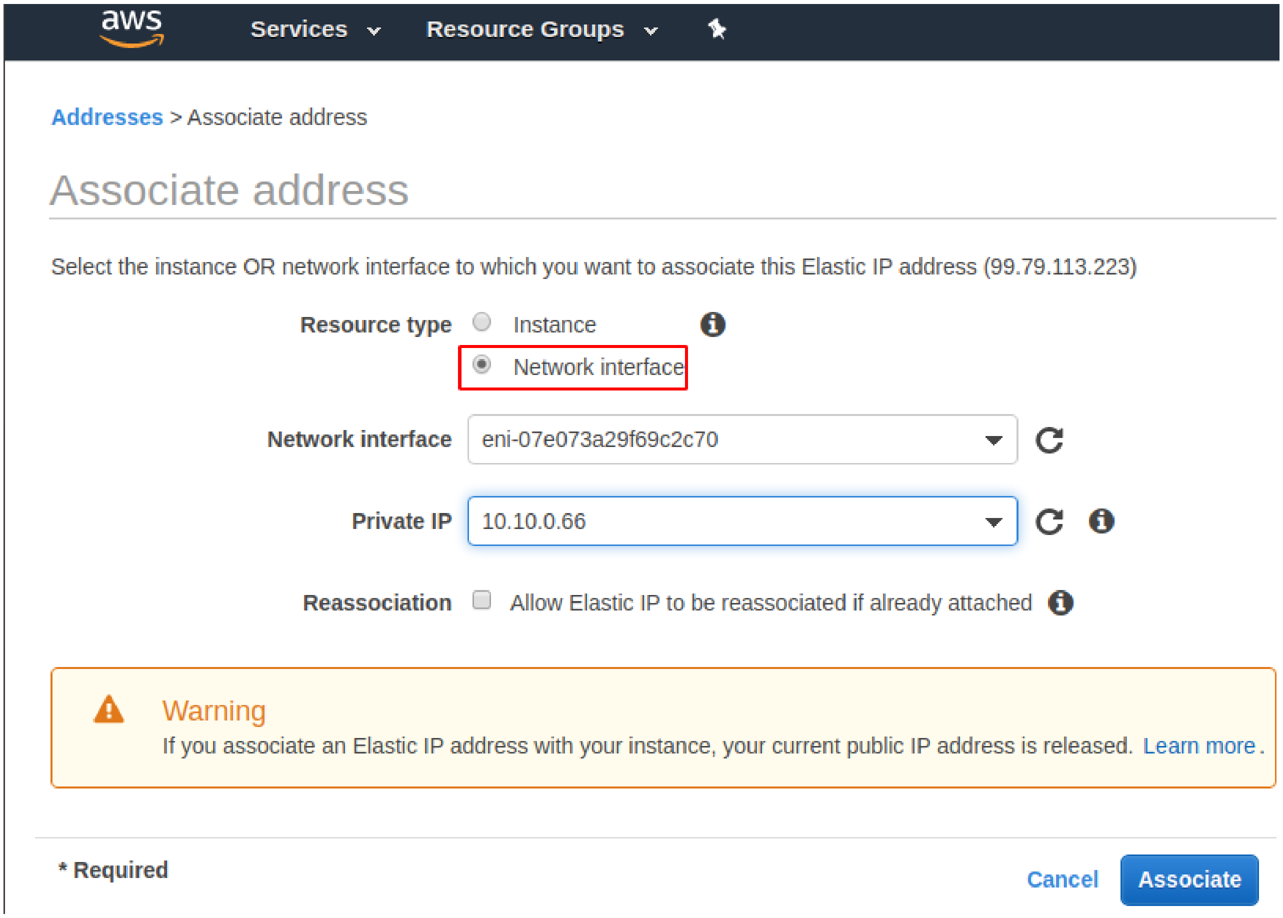
You can set up multiple FortiSandbox instances in a load-balancing HA (high availability) cluster.

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 instance and then launch the worker 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 local local Windows clone communication for custom VM.
   b. Create cluster inter-communication 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 inter-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 reassociated if already attached

Warning
If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more.

* Required

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-worker -a -sPrimary_Port3_private_IP -p123`
3. Configure the first worker node:
   - `hc-settings -sc -tR -nMyRWorker1 -cClusterName -p123 -iport3`
   - `hc-worker -a -sPrimary_Port3_private_IP -p123`
4. If necessary, configure consecutive worker nodes:
   - `hc-settings -sc -tR -nMyRWorker2 -cClusterName -p123 -iport3`
   - `hc-worker -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 *Scan Policy and Object* > *VM Settings* 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.

Appendix A - Reduce scan time in custom Windows VM

When a file is sent to local Windows clone for dynamic scan, it takes time to boot up the clone from power-off state. You can keep the custom VM clones running to reduce scan time.

To reduce the scan time in a custom Windows VM:

1. Go to *System* > *AWS Config* and enable *Allow Hot-Standby VM*. After *Allow Hot-Standby VM* is enabled, FortiSandbox will perform `vminit` again to apply changes to existing custom VM clones or prepare new clone(s).

Allow Hot-Standby VM ☑ Enabled Apply

2. After the clone initiation is done, go to the *AWS EC2* console to check that the clone(s) keep running with /without a scan job. Allow 2-3 minutes for a custom VM clone to restore status after a scan job done. Aftwerwards, the clone will keep running and standby for the next scan job to reduce VM scan time.

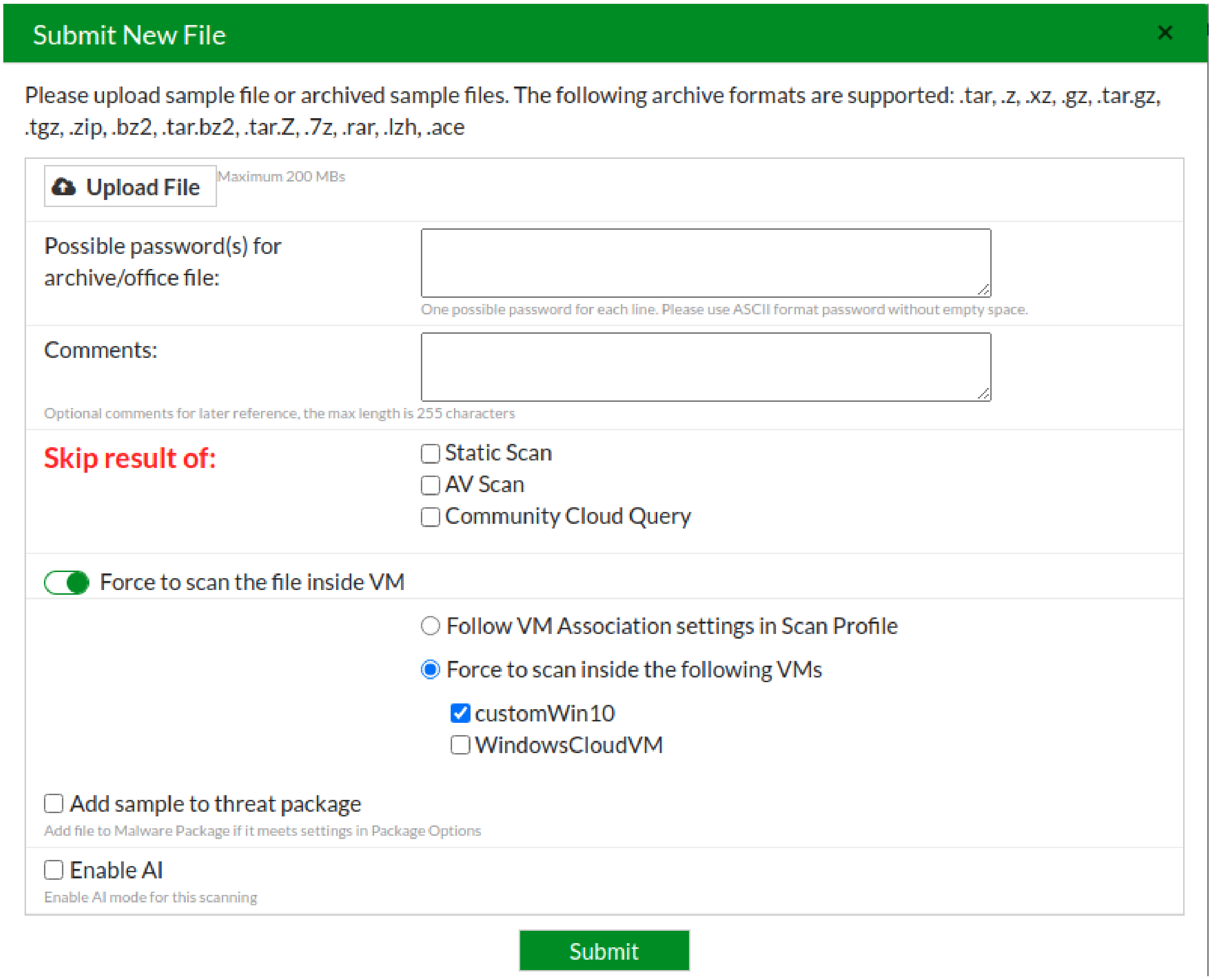
For this feature to work better we recommend enabling more clones than the maximum concurrent dynamic scan jobs, so when a new dynamic scan job is started, there are stand-by clones available immediately.

Appendix B - How to interact with a custom VM clone during scan

When a Windows clone is scanning a file, it's helpful to access it and monitor the scan process.

To interact with a custom clone during a scan:

1. Go to *Scan Job > 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

Upload File Maximum 200 MBs

Possible password(s) for archive/office file:

One possible password for each line. Please use ASCII format password without empty space.

Comments:

Optional comments for later reference, the max length is 255 characters

Skip result of:
- □ Static Scan
- □ AV Scan
- □ Community Cloud Query

● Force to scan the file inside VM

- ○ Follow VM Association settings in Scan Profile
- ● Force to scan inside the following VMs
  - ☑ customWin10
  - □ WindowsCloudVM

□ Add sample to threat package

Add file to Malware Package if it meets settings in Package Options

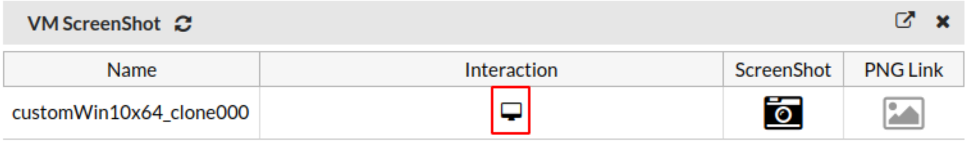
□ Enable AI

Enable AI mode for this scanning

Submit

4. Click *Submit*.
5. Go to *Scan Policy and Object> VM Settings* and click *VM Screenshot*.

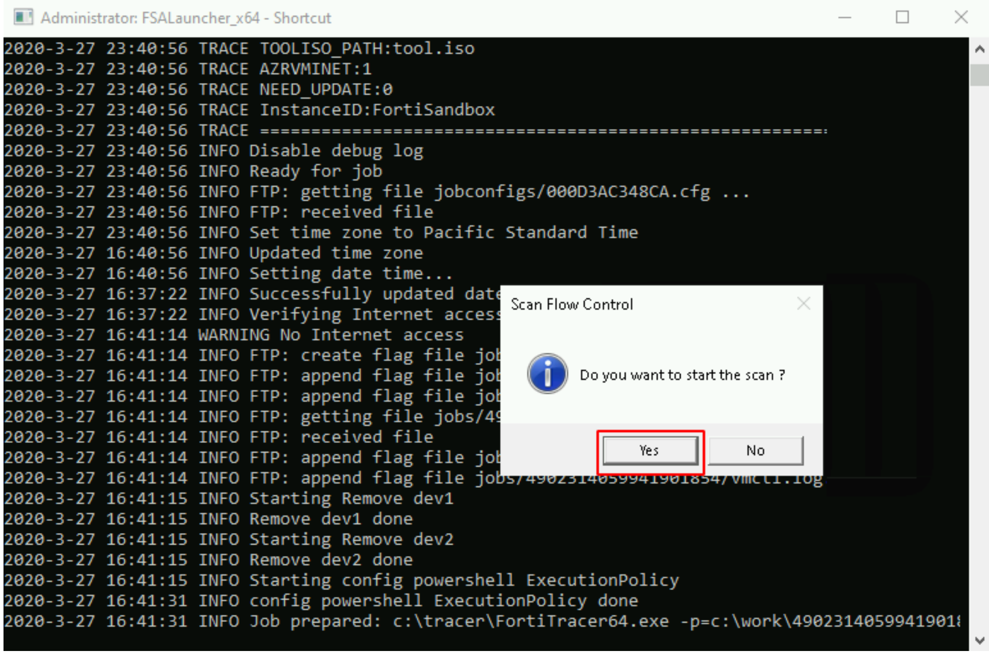
6. When the icon in the *Interaction* column is enabled, click the icon to establish an RDP tunnel.



VM ScreenShot

Name	Interaction	ScreenShot	PNG Link
customWin10x64_clone000	🖥	📷	🖼

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



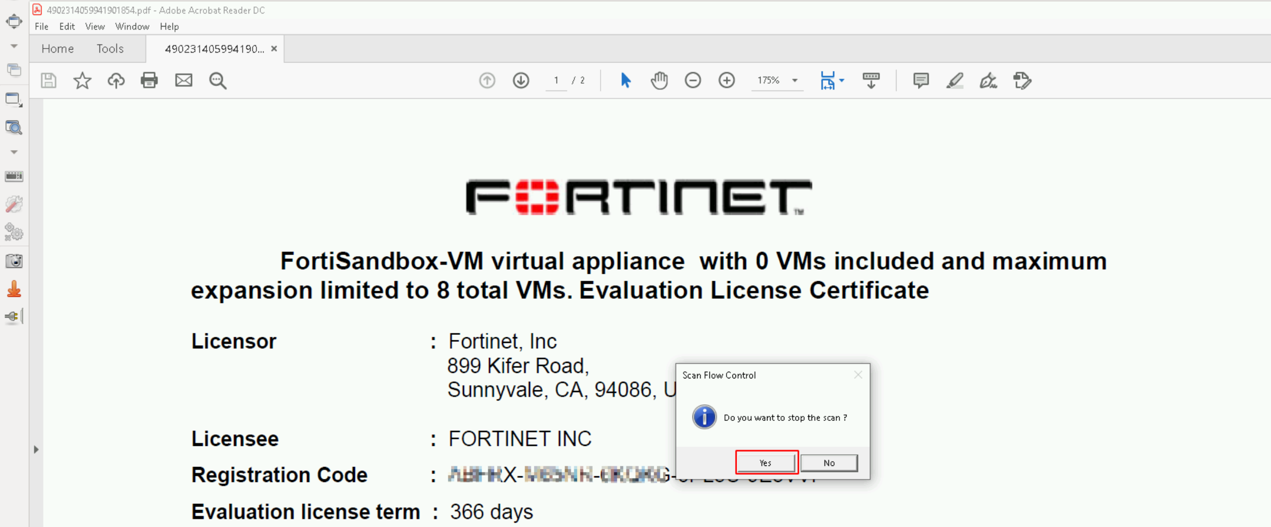
Administrator: FSALauncher_x64 - Shortcut

```
2020-3-27 23:40:56 TRACE TOOLISO_PATH:tool.iso
2020-3-27 23:40:56 TRACE AZRVMINET:1
2020-3-27 23:40:56 TRACE NEED_UPDATE:0
2020-3-27 23:40:56 TRACE InstanceID:FortiSandbox
2020-3-27 23:40:56 TRACE ========================================================
2020-3-27 23:40:56 INFO Disable debug log
2020-3-27 23:40:56 INFO Ready for job
2020-3-27 23:40:56 INFO FTP: getting file jobconfigs/000D3AC348CA.cfg ...
2020-3-27 23:40:56 INFO FTP: received file
2020-3-27 23:40:56 INFO Set time zone to Pacific Standard Time
2020-3-27 16:40:56 INFO Updated time zone
2020-3-27 16:40:56 INFO Setting date time...
2020-3-27 16:37:22 INFO Successfully updated date
2020-3-27 16:37:22 INFO Verifying Internet access
2020-3-27 16:41:14 WARNING No Internet access
2020-3-27 16:41:14 INFO FTP: create flag file job
2020-3-27 16:41:14 INFO FTP: append flag file job
2020-3-27 16:41:14 INFO FTP: append flag file job
2020-3-27 16:41:14 INFO FTP: getting file jobs/49
2020-3-27 16:41:14 INFO FTP: received file
2020-3-27 16:41:14 INFO FTP: append flag file job
2020-3-27 16:41:14 INFO FTP: append flag file jobs/4902314059941901854/vmctl.log
2020-3-27 16:41:15 INFO Starting Remove dev1
2020-3-27 16:41:15 INFO Remove dev1 done
2020-3-27 16:41:15 INFO Starting Remove dev2
2020-3-27 16:41:15 INFO Remove dev2 done
2020-3-27 16:41:15 INFO Starting config powershell ExecutionPolicy
2020-3-27 16:41:31 INFO config powershell ExecutionPolicy done
2020-3-27 16:41:31 INFO Job prepared: c:\tracer\FortiTracer64.exe -p=c:\work\4902314059941901
```

Scan Flow Control

Do you want to start the scan ?

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



4902314059941901854.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools 490231405994190...
1 / 2
175%

FORTINET

FortiSandbox-VM virtual appliance with 0 VMs included and maximum expansion limited to 8 total VMs. Evaluation License Certificate

Licensor : Fortinet, Inc
899 Kifer Road,
Sunnyvale, CA, 94086, U

Licensee : FORTINET INC

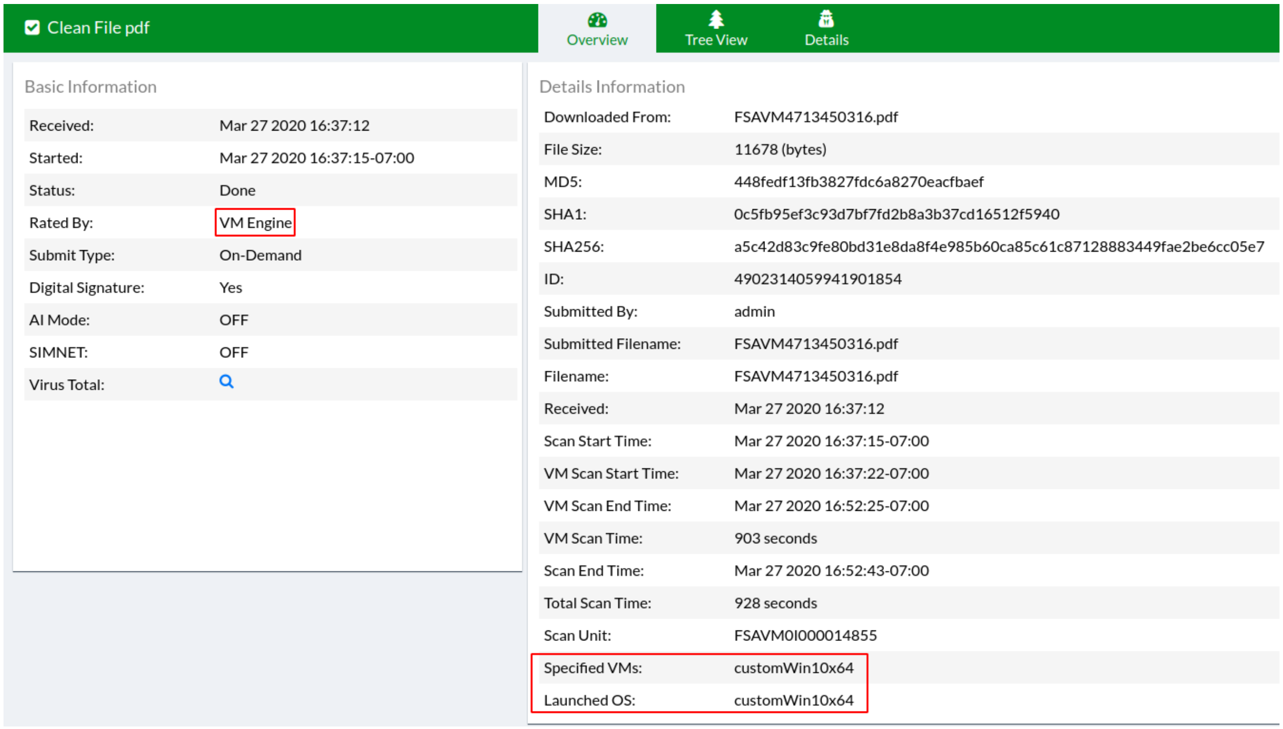
Registration Code : [redacted]

Evaluation license term : 366 days

Scan Flow Control

Do you want to stop the scan ?

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



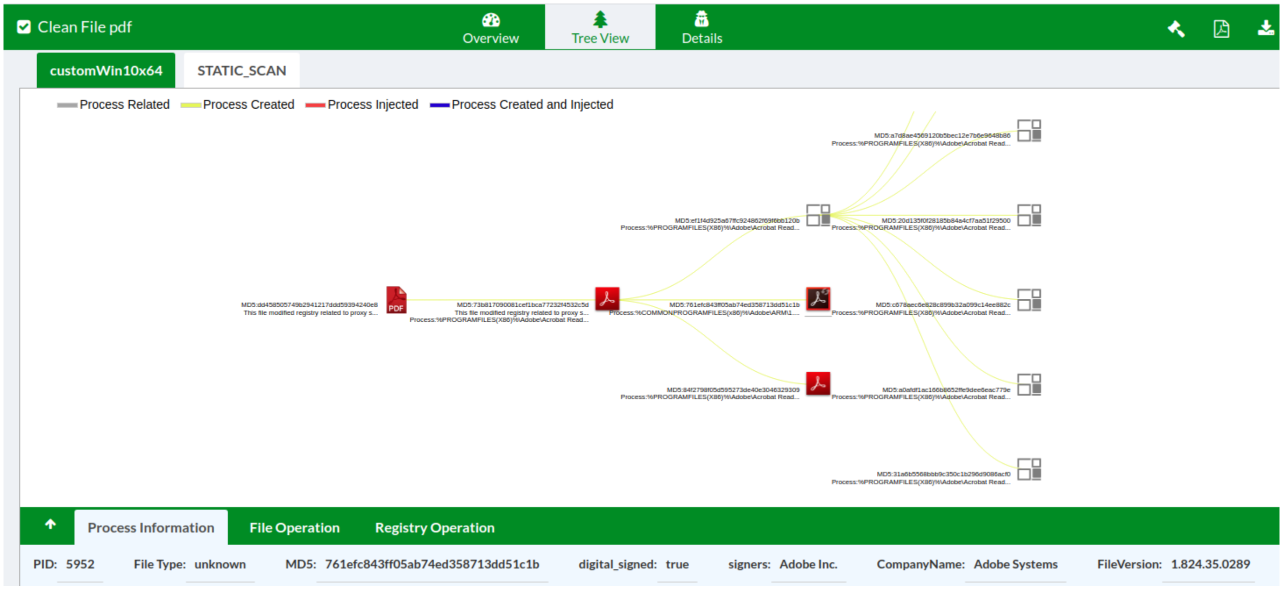
☑ Clean File pdf

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:	🔍

Details Information

Downloaded From:	FSAVM4713450316.pdf
File Size:	11678 (bytes)
MD5:	448fedf13fb3827fdc6a8270eacfbaef
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:	FSAVM0I000014855
Specified VMs:	customWin10x64
Launched OS:	customWin10x64

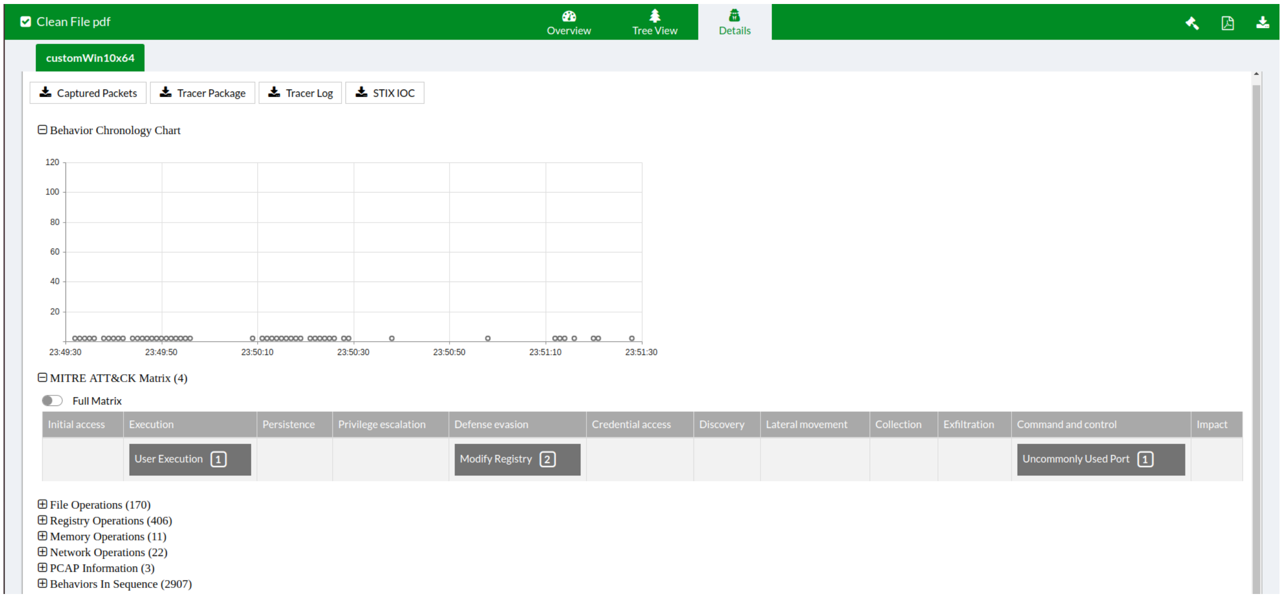


Overview
Tree View
Details
customWin10x64
STATIC_SCAN
Process Related
Process Created
Process Injected
Process Created and Injected
MD5:dd458505749b2941217ddd59394240e8
This file modified registry related to proxy s...
MD5:73b817090081cef1bca77232f4532c5d
This file modified registry related to proxy s...
Process:%PROGRAMFILES(X86)%\Adobe\Acrobat Read...
MD5:ef1f4d925a67ffc924862f69f6bb120b
Process:%PROGRAMFILES(X86)%\Adobe\Acrobat Read...
MD5:761efc843ff05ab74ed358713dd51c1b
Process:%COMMONPROGRAMFILES(x86)%\Adobe\ARM\1....
MD5:84f2798f05d595273de40e3046329309
Process:%PROGRAMFILES(X86)%\Adobe\Acrobat Read...
MD5:a7d8ae4569120b5bec12e7b6e9648b86
Process:%PROGRAMFILES(X86)%\Adobe\Acrobat Read...
MD5:20d135f0f28185b84a4cf7aa51f29500
Process:%PROGRAMFILES(X86)%\Adobe\Acrobat Read...
MD5:c678aec6e828c899b32a099c14ee882c
Process:%PROGRAMFILES(X86)%\Adobe\Acrobat Read...
MD5:a0afdf1ac166b8652ffe9dee6eac779e
Process:%PROGRAMFILES(X86)%\Adobe\Acrobat Read...
MD5:31a6b5568bbb9c350c1b296d9086acf0
Process:%PROGRAMFILES(X86)%\Adobe\Acrobat Read...

☑ Clean File pdf

Process Information | File Operation | Registry Operation

PID: 5952	File Type: unknown	MD5: 761efc843ff05ab74ed358713dd51c1b	digital_signed: true	signers: Adobe Inc.	CompanyName: Adobe Systems	FileVersion: 1.824.35.0289



⊟ Behavior Chronology Chart

⊟ MITRE ATT&CK Matrix (4)

○ Full Matrix

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control	Impact
	User Execution 1			Modify Registry 2						Uncommonly Used Port 1	

⊞ File Operations (170)
⊞ Registry Operations (406)
⊞ Memory Operations (11)
⊞ Network Operations (22)
⊞ PCAP Information (3)
⊞ Behaviors In Sequence (2907)

Change Log

Date	Change Description
2022-04-12	Initial release.
2022-10-05	Updated Prepare the AWS environment on page 5,Deploy FortiSandbox on AWS (BYOL/On-Demand) on page 20, Prepare FortiSandbox for scanning contents on page 28 as well as other improvements.
2022-10-05	Updated Prepare the AWS environment on page 5.

www.fortinet.com