



# FortiSandbox PaaS - Deployment Guide

Version 23.4.4374

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



February 27, 2024

FortiSandbox PaaS 23.4.4374 Deployment Guide

34-4374-968246-20240227

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Requirements	5
Licensing	5
<b>Deploying FortiSandbox PaaS</b>	<b>6</b>
Verifying system status	9
Assigning sandboxing VM	9
Integrating Security Fabric	10
Setting up and making an API call	12
Establishing a connection to a region	13
FortiOS v7.0.3	13
FortiMail v7.0.3 and earlier	14
FortiClient EMS v7.0.3	14
Feature limitations	14
<b>Maintaining FortiSandbox PaaS</b>	<b>15</b>
Expanding VM capacity	15
Keeping firmware up-to-date	16
Renewing the contract	17
Adding an IAM user	18
Adding a secondary account	18
Subscribe to Service Status updates	20
<b>Appendix A - Supported regions</b>	<b>21</b>
<b>Appendix B - Port and access control information</b>	<b>22</b>
Default Ports	22
Access Control List	22

# Change Log

Date	Change Description
2023-11-10	Initial release.
2024-02-27	Updated <a href="#">Keeping firmware up-to-date on page 16</a> .

# Introduction

FortiSandbox PaaS is a cloud-based sandbox service based on FortiSandbox PaaS. The service subscription is available for purchase under FortiCloud.

For upgrade information, product integration and support, and resolved and known issues, see the [FortiSandbox Cloud Release Notes](#).

## Requirements

The following items are required before you can initialize FortiSandbox PaaS:

- **FortiCloud account:** Subscribe to a FortiCloud Premium account. A FortiCloud account is required to launch FortiSandbox PaaS Cloud.
- **FortiGate firmware:** For version 6.4, you must use 6.4.2 or higher. For version 6.2, you must use 6.2.5 or higher. For other models, contact [Customer Service & Support](#).
- **FortiMail firmware:** Version 6.4.3 or higher. For other models, contact [Customer Service & Support](#).
- **Internet access:** You must have Internet access to create a FortiSandbox PaaS instance.
- **Browser:** A device with a browser to access FortiSandbox PaaS.



After creating a new FortiCloud account, wait 30 minutes before proceeding.

---

## Licensing

FortiSandbox PaaS requires the following licenses:

- FortiCloud Premium license.
- FortiSandbox PaaS Entitlement: Purchase FortiSandbox PaaS Cloud licenses for full functionality.
- Security Fabric devices.
  - FortiGate license: You must have a FortiGate license. Register the FortiGate on the same account as the FortiCloud.
  - FortiMail license: You must have a FortiMail license. Register the FortiMail on the same account as the FortiCloud.

# Deploying FortiSandbox PaaS

This section explains how to deploy and manage FortiSandbox PaaS with FortiGate and FortiMail devices.

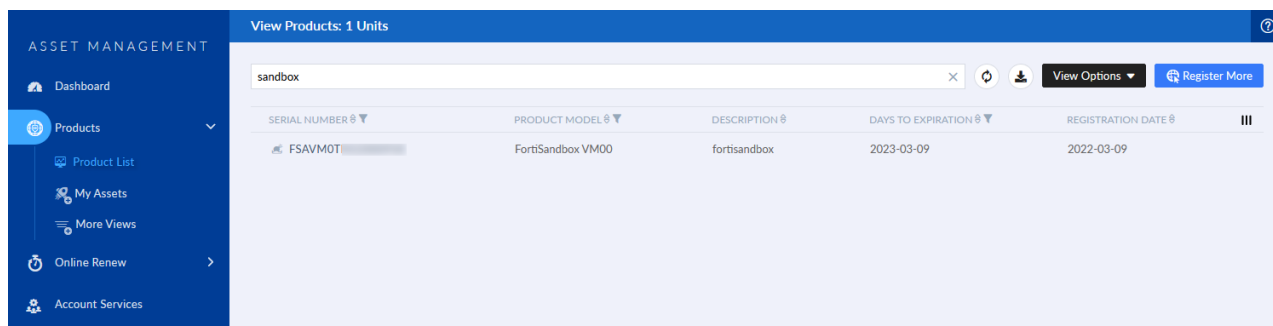
FortiSandbox PaaS supports TLS v1.2. Ensure your browser and firewall setting permits TLS v1.2.



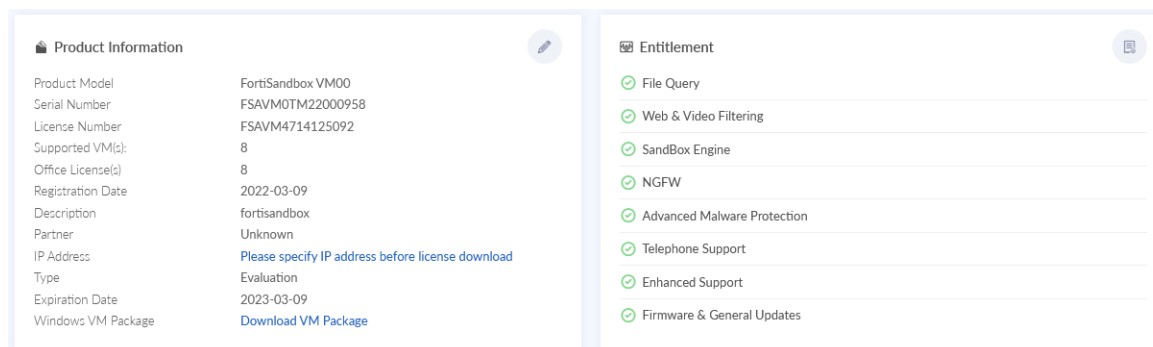
FortiSandbox PaaS Cloud can only communicate with FortiGate, FortiMail and FortiClient.

## To verify you have a product entitlement:

1. Log in to [FortiCloud](#). The Asset Management portal opens.
2. Go to *Products > Product List* and search for FortiSandbox PaaS.



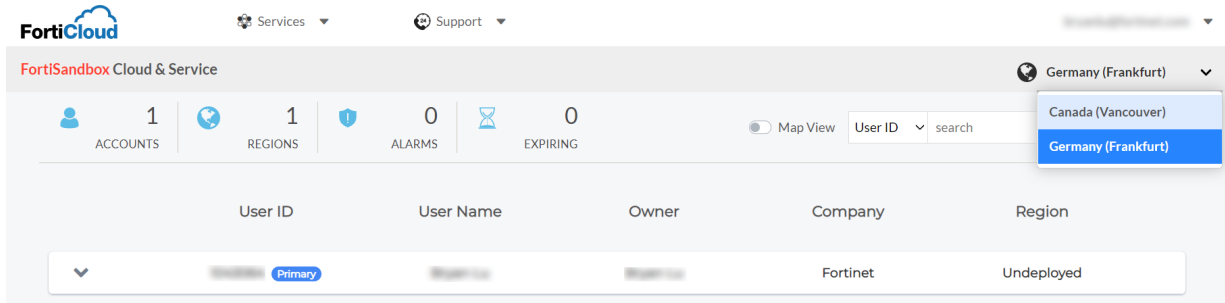
3. Click the Serial Number and check the *Product Entitlements* for FortiSandbox PaaS.



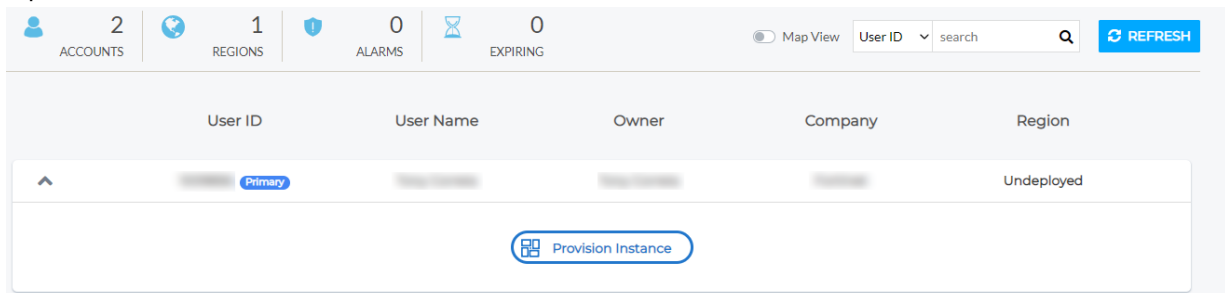
## To launch FortiSandbox PaaS:

1. In the Asset Portal, click *Services > Cloud Services > FortiSandbox Cloud*. The *FortiSandbox Cloud & Service* page opens. Alternatively, you can launch the instance from <https://fortisandboxcloud.com>.

2. Select the region and provision the instance.
  - a. Select the region from the dropdown menu.



- b. Select the account that contains the FortiSandbox Cloud entitlement and expand the instance. The *User ID* represents the dedicated instance.

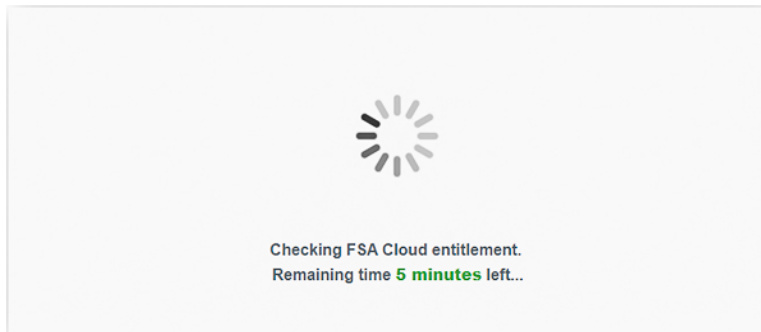


- c. Click *Provision Instance*. Allow a few minutes for the FortiSandbox PaaS Cloud instance to be provisioned.

3. Confirm the instance region as it cannot be moved to another region.

Once your cloud instance is deployed in the current region, it cannot be deployed in another region. Are you sure to provision instance? YES NO

FortiSandbox PaaS instance is provisioned in a few minutes.




If an entitlement is not set up correctly, the provisioning reports an error. For information, see [Requirements on page 5](#) and [Licensing on page 5](#)



Unable to provision the cloud instance.  
Entitlement is required to provision the instance. (code: -3015)

4. When provisioning is complete, the dedicated VM instance displays the resources and firmware information, click *Enter* to access the web GUI.


@qatest.com

### FortiSandbox Cloud & Service

Please choose your account

User ID	User Name	Owner	Company
10... (Primary)			Fortinet

CPU (4 VCPU) 0.3%

RAM (16.0 G) 17.7%

Disk (185.0 G) 3.1%

Stop Reboot Enter

Firmware Version: FSACLP-3.2-0-5108-...

Serial Number: FSA-...

Expiry Date: 2021-07-16

**REFRESH** Can't find your account? Try to refresh it.

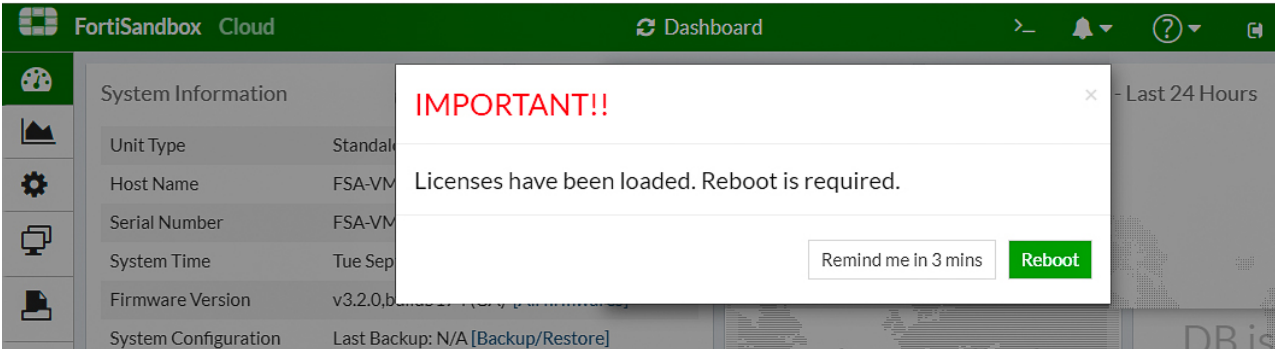


You can directly access FortiSandbox PaaS at <https://fortisandboxcloud.com> using your Fortinet support login credentials.

5. On the FortiSandbox PaaS VM instance, Go to the Dashboard and verify the following:

- A serial number has been assigned
- The licenses are valid

In some cases where the internal sync does not happen in time, you may find the licenses are invalid. FortiSandbox PaaS is designed to automatically resolve that. When the licenses are properly loaded, you must reboot the unit.



**FortiSandbox Cloud** Dashboard

System Information	
Unit Type	Standalone
Host Name	FSA-VM
Serial Number	FSA-VM
System Time	Tue Sep
Firmware Version	v3.2.0, build 271 (2021-07-16)
System Configuration	Last Backup: N/A [Backup/Restore]

**IMPORTANT!!**

Licenses have been loaded. Reboot is required.

Remind me in 3 mins **Reboot**



## Verifying system status

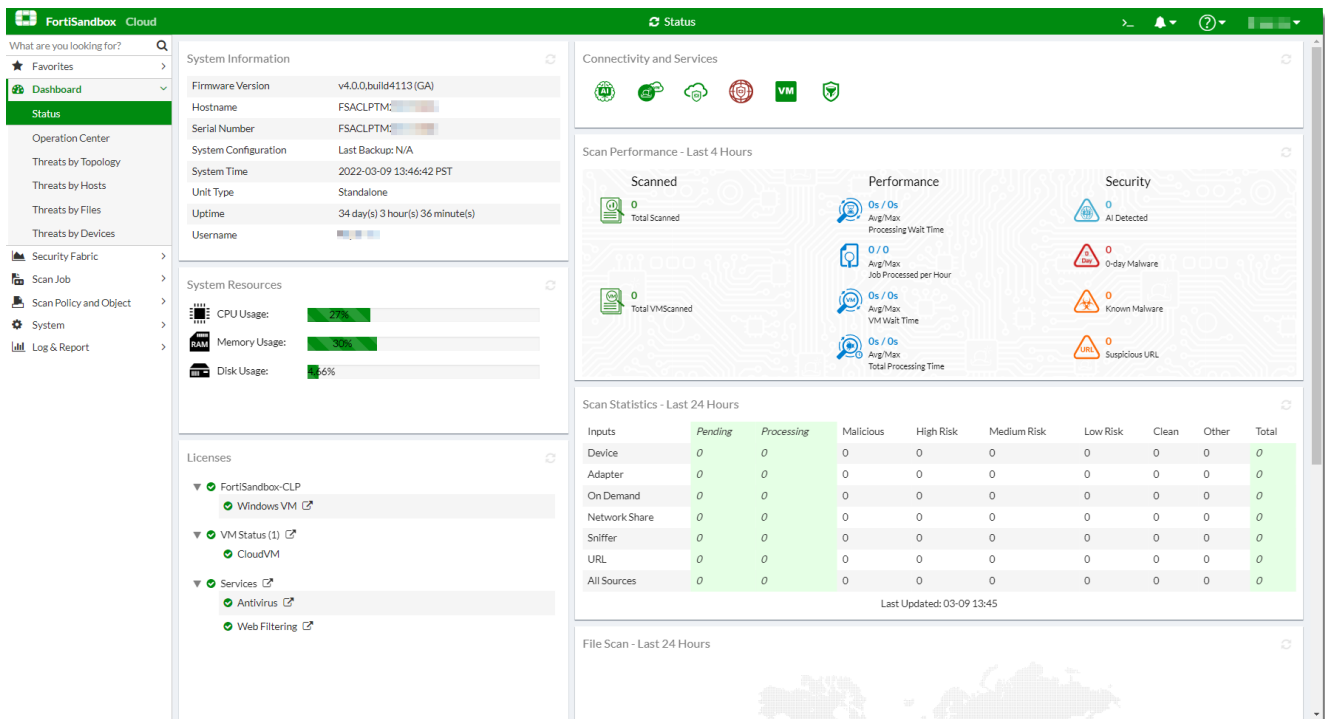
When you log in to FortiSandbox PaaS, *Dashboard > Status* is displayed.

In the Dashboard, verify the following:

- The *Windows VM* and servers (*FDN Download Server*, *Community Cloud Server*, and *Web Filtering Server*) connectivity display a green icon to show they are up.
- The *Antivirus DB* and *Web Filtering* contracts display a green icon to show they are valid.
- The *Sandbox Cloud Contract* is valid and shows at least one (1) count.
- The *System Resources* and *Disk Monitor* widgets show normal usage.

Other than the *MacOS VM* and *Industry Security Signature* contracts, verify that all contracts and services are valid as they are included in the FortiSandbox PaaS entitlementment.

*MacOS VM* and *Industry Security Signature* contracts are not currently supported so they show *No Contract*.

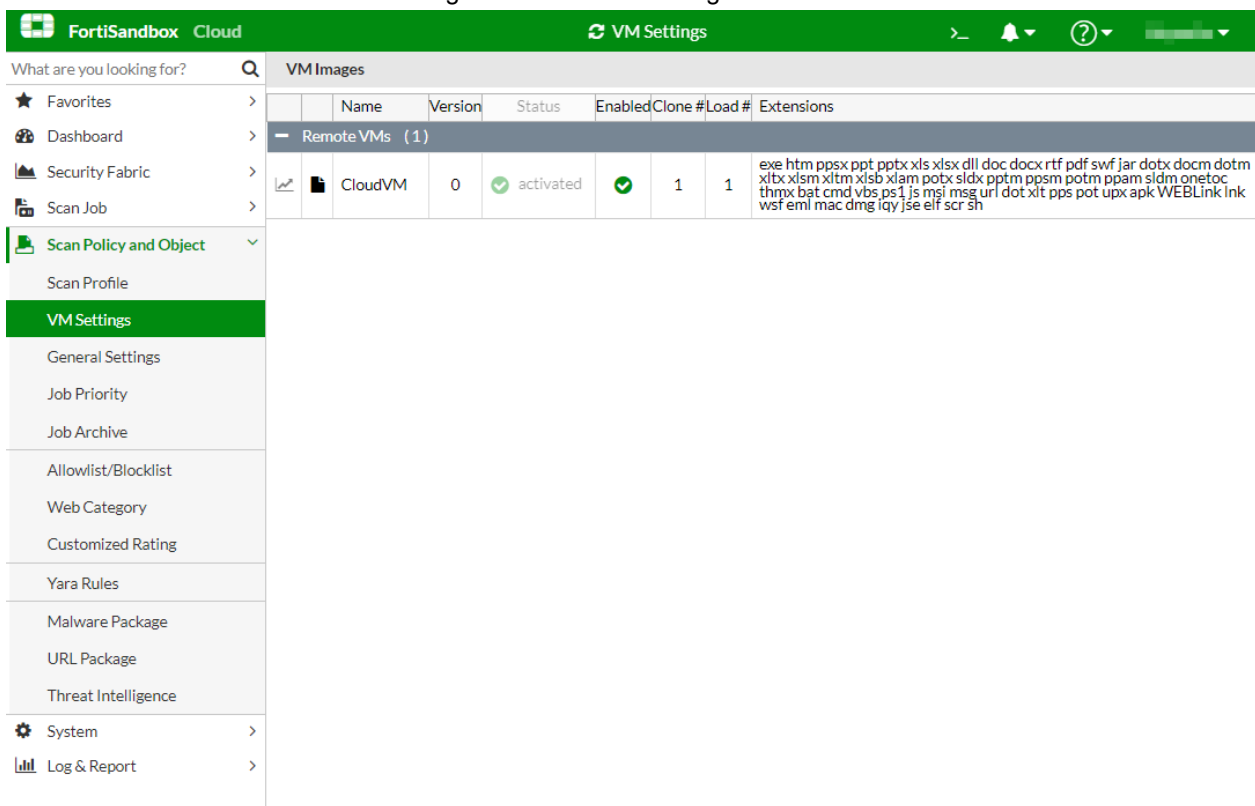


## Assigning sandboxing VM

For new setups, the sandboxing VM clones are not assigned by default since there are different types of VM. Assign a clone number to use the dynamic analysis feature.

**To assign a clone number:**

1. In FortiSandbox PaaS, go to *Virtual Machine > VM Settings*.
2. Double-click the VM's *Clone #* and change the number to 1 or higher.



## Integrating Security Fabric

FortiSandbox PaaS uses port TCP/514 for client connectivity (FortiGate and FortiMail). Ensure any firewall in between allows for that.

For devices connected to Security Fabric, ensure they are configured properly. Do all related configuration from either the root Fabric or FortiManager.

**To integrate with Security Fabric in FortiGate:**

1. Go to *Security Fabric > Fabric Connectors* and double-click the *Cloud Sandbox* card.
2. Set *Status* to *Enable*.

### 3. For *Type*, select *FortiSandbox Cloud*.



If the FortiSandbox PaaS option is grayed out or not visible, enter the following in the CLI:

```
config system global
    set gui-fortigate-cloud-sandbox enable
end
```

### 4. Click *OK*.

#### To integrate with Security Fabric in the CLI:

```
config system fortisandbox
    set status enable
    set forticloud enable
    set server <string>
end
```

If the FortiGate does not detect the proper entitlement, a warning is displayed and the CLI configuration will not save.

If the FortiSandbox PaaS is running version 4.0.0 and later, the FortiGate will automatically connect to fortisandboxcloud.com, and then discover the specific region and server to connect to based on which region you selected to deploy your FortiSandbox PaaS instance. The FortiGate must have a FortiCloud premium account license and a FortiSandbox Cloud VM license for this functionality.

#### To integrate with Security Fabric in FortiMail:

1. In FortiMail, go to *System > FortiSandbox*.
2. For *FortiSandbox PaaS type*, click *Enhanced Cloud*.
3. In FortiSandbox PaaS, go to *Security Fabric > Device*, click the *Authorize* icon on the FortiMail so that it can establish Fabric connectivity. Verify that the *Status* is updated.



Specific firmware versions of FortiMail models support the above Security Fabric connectivity. See [Requirements on page 5](#).

#### To troubleshoot the connection on FortiMail:

Run the following CLI command:

```
diagnose debug application sandboxclid <ID>
```

#### Example:

In the example below, the connection failed due to a firewall policy on the client side to block connectivity to port 514.

```
insidemail02 # diagnose debug application sandboxclid 65
System Time: 2023-04-12 09:02:43 JST (Uptime: 5d 8h 48m)

insidemail02 # diagnose debug application sandboxclid display
System Time: 2023-04-12 09:03:07 JST (Uptime: 5d 8h 48m)
sandboxclid:2023-04-12T09:03:00:SandboxJob.cpp:145:process():use configured FortiSandbox
server
sandboxclid:2023-04-12T09:03:00:Connection.cpp:31:___s2ip():'fortisandboxcloud.com' is not an
IP, try to resolve it
sandboxclid:2023-04-12T09:03:00:Connection.cpp:321:ConnectionSecure__():remote address is
```

```
fortisandbox cloud, user_id=1423794
sandboxclid:2023-04-12T09:03:00:Connection.cpp:31: __s2ip(): 'fortisandboxcloud.com' is not an
IP, try to resolve it
sandboxclid:2023-04-12T09:03:00:Connection.cpp:167:Connect(): connecting to 66.35.19.98
sandboxclid:2023-04-12T09:04:02:Connection.cpp:171:Connect(): connect() failed, errno = 115
sandboxclid:2023-04-12T09:04:02:Session.cpp:248:ConnectImpl(): FortiSandbox server is not
available at the moment. Connection block time: 1 seconds
sandboxclid:2023-04-12T09:04:02:Session.cpp:101:Connect0(): connection broken
sandboxclid:2023-04-12T09:04:10:Connection.cpp:31: __s2ip(): 'fortisandboxcloud.com' is not an
IP, try to resolve it
sandboxclid:2023-04-12T09:04:10:Connection.cpp:321:ConnectionSecure__(): remote address is
fortisandbox cloud, user_id=1423794
sandboxclid:2023-04-12T09:04:10:Connection.cpp:31: __s2ip(): 'fortisandboxcloud.com' is not an
IP, try to resolve it
sandboxclid:2023-04-12T09:04:10:Connection.cpp:167:Connect(): connecting to 66.35.19.98
sandboxclid:2023-04-12T09:04:15:Connection.cpp:31: __s2ip(): 'fortisandboxcloud.com' is not an
IP, try to resolve it
sandboxclid:2023-04-12T09:04:15:Connection.cpp:321:ConnectionSecure__(): remote address is
fortisandbox cloud, user_id=1423794
sandboxclid:2023-04-12T09:04:15:Connection.cpp:31: __s2ip(): 'fortisandboxcloud.com' is not an
IP, try to resolve it
sandboxclid:2023-04-12T09:04:15:Connection.cpp:167:Connect(): connecting to 66.35.19.98
sandboxclid:2023-04-12T09:04:20:Connection.cpp:31: __s2ip(): 'fortisandboxcloud.com' is not an
IP, try to resolve it
sandboxclid:2023-04-12T09:04:20:Connection.cpp:321:ConnectionSecure__(): remote address is
fortisandbox cloud, user_id=1423794
sandboxclid:2023-04-12T09:04:20:Connection.cpp:31: __s2ip(): 'fortisandboxcloud.com' is not an
IP, try to resolve it
sandboxclid:2023-04-12T09:04:20:Connection.cpp:167:Connect(): connecting to 66.35.19.98
sandboxclid:2023-04-12T09:05:11:Connection.cpp:171:Connect(): connect() failed, errno = 115
sandboxclid:2023-04-12T09:05:11:Session.cpp:248:ConnectImpl(): FortiSandbox server is not
available at the moment. Connection block time: 1 seconds
sandboxclid:2023-04-12T09:05:11:Session.cpp:101:Connect0(): connection broken
sandboxclid:2023-04-12T09:05:11:Session.cpp:72:Connect0(): connection is blocked for 1
seconds

^C
insidemail02 # execute telnettest fortisandboxcloud.com:514
Connection timed out in 30 seconds.

Connection status to fortisandboxcloud.com port 514:
Connecting to remote host failed.

insidemail02 #
```

## Setting up and making an API call

To set up and establish a session to your VM instance, first generate a token in FortiSandbox PaaS. On the client software, use the token to authorize and make the API call to establish the session.

**To generate a token in FortiSandbox PaaS:**

1. In FortiSandbox PaaS, click the CLI icon at the top right to open the CLI console.
2. In the CLI console, run the following CLI command to generate a new token.  
login-token -g

**To authorize and make the API call on the client software:**

1. On your client software, make the following API call to:

```
https://<account-id>.fortisandboxcloud.com/jsonrpc

{
  "method": "get",
  "params": [
    {
      "url": "/sys/login/token",
      "token": "<token>"
    }
  ],
  "session": "",
  "id": 53,
  "ver": "2.5"
}
```

Field	Description
id	The user-id on the portal or one used in the URL in your FortiSandbox PaaS instance.
token	The token you just generated.

When the session is established, all API calls are similar to the FortiSandbox PaaS API documentation.

We recommend renewing your token on a regular basis to keep access to your VM instance secure.

## Establishing a connection to a region

FortiSandbox PaaS 23.4.4374 supports the EMEA region. When EMEA is selected, FortiOS v7.0.4 will automatically re-establish the connection to the location where the FortiSandbox PaaS is provisioned.

### FortiOS v7.0.3

For FortiOS v7.0.3 and earlier, we recommend making the following configurations using the CLI:

```
config system fortisandbox
  set status enable
  set forticloud enable
  set server ""<your Instance ID>.eu-central-1.fortisandboxcloud.com"
  set email "<your email>"
end
```

---

FortiMail and FortiClient connectivity to the EMEA region are not currently supported since the server cannot be overridden.

---

## FortiMail v7.0.3 and earlier

For FortiMail 7.0.3 and earlier, the network traffic is directed to *fortisandboxcloud.com* that is mainly hosted in Canada . The traffic is then forwarded to the EMEA location.

## FortiClient EMS v7.0.3

For FortiClient EMS 7.0.3, configure the server to `eu-central-1.fortisandboxcloud.com`.

## Feature limitations

The following is a list of features in FortiSandbox that are not available in FortiSandbox PaaS.

GUI	Custom VM modification within FortiSandbox PaaS.
<b>Fabric integration</b>	<ul style="list-style-type: none"> <li>• Multiple ICAP adapter profile for multi-tenancy support.</li> <li>• Multiple ICAP Adapter Profile.</li> <li>• <i>Hold</i>" option to ICAP adapter deployment.</li> <li>• Sending TCP RST on <i>Sniffer</i> mode deployment.</li> </ul>
<b>Scan</b>	<ul style="list-style-type: none"> <li>• <i>Configurable Internet Browser</i> on <i>Dynamic Scan</i>.</li> <li>• Hot-standby VMs on AWS and Azure cloud deployment for improving performance.</li> <li>• Email relay with MTA adapter.</li> </ul>
<b>System &amp; Security</b>	<ul style="list-style-type: none"> <li>• System time discrepancy on HA-Cluster deployment and logged a Warning event.</li> <li>• Custom Linux VM support on public cloud.</li> </ul>

# Maintaining FortiSandbox PaaS

You are responsible for maintaining the FortiSandbox PaaS firmware, VM capacity, and users. Fortinet maintains the contracts, services, and infrastructure.

## Expanding VM capacity

VMs can be easily expanded to hold more files for sandboxing. The limit is 200 VMs. The current VM count is displayed in the *Dashboard > Sandbox Cloud Contract*.

You can purchase additional VMs and add them to your existing deployment.

When adding VMs, you must change the *Clone #* to 1 or higher. For details, see [Assigning sandboxing VM on page 9](#).

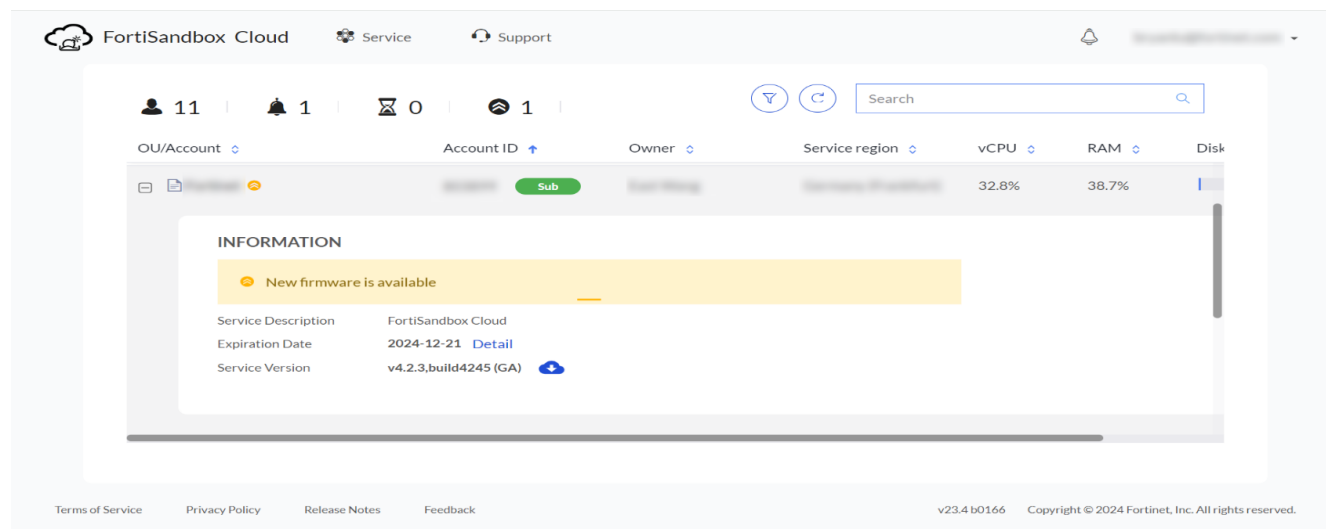
The screenshot displays the FortiSandbox Cloud interface. On the left is a navigation menu with options: Dashboard, FortiView, System, Virtual Machine, Scan Policy, Scan Input, File Detection, URL Detection, and Log & Report. The main panel is titled 'System Information' and contains a table of system details and contracts.

System Information	
Host Name	FSA-VM0000000000 [Change]
Serial Number	FSACLPTM20090128
System Time	Fri Jul 24 17:35:24 2020 PDT [Change]
Firmware Version	v3.2.0,build5131 (GA) [All firmwares]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 0 hour(s) 1 minute(s)
Windows VM	✓
FDN Download Server	✓
Community Cloud Server	✓
Web Filtering Server	✓
Antivirus DB Contract	✓ 2021-07-20
Web Filtering Contract	✓ 2021-07-20
MacOS VM Contract	✗ No Contract
Industry Security Signature Contract	✗ No Contract
Sandbox Cloud Contract	✓ 2021-07-17, 11 available (Up to 11)

## Keeping firmware up-to-date

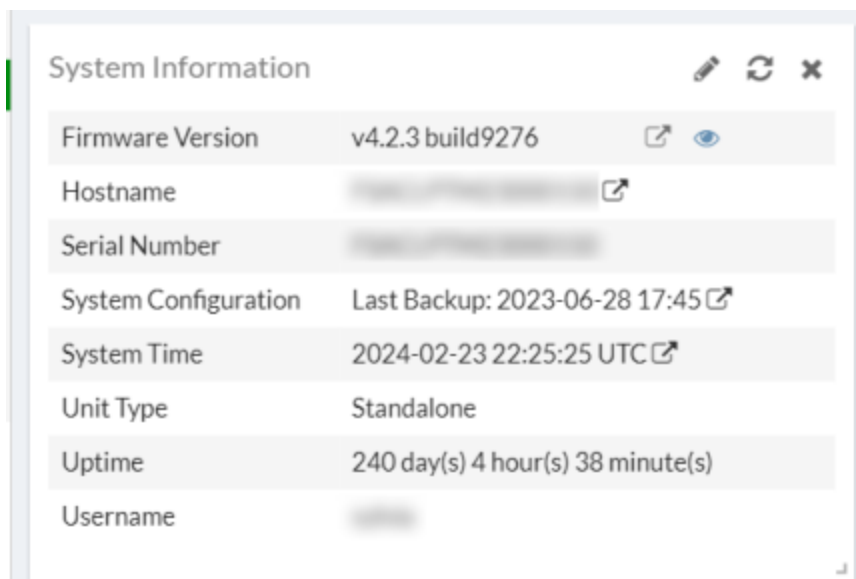
Firmware updates include new features and bug fixes. If there is an updated firmware, the *Dashboard* in the portal displays a notification and a download link. Your maintenance schedule should include upgrading the firmware.

You can download the firmware from the portal to your local PC.



### To upgrade the firmware:

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





3. Choose one of the following options:

**Upload Firmware**
Choose this option if you have downloaded the image via the Portal.

**Download & Upgrade**
Choose this option to allow the system to upgrade on its own.

FortiSandbox Firmware Information:

Current Version

FortiSandbox v4.2.3.build

New firmware update is available

Upload Firmware

Upgrade firmware manually with a file from local host

Upload Firmware

Available Firmware

Recommended

All Available

FortiSandbox V4.4.0 Build 4367

View Release Notes

Note: Upgrading firmware will cause system to reboot.

Note: Please read the release notes of new version to see if you can upgrade directly to it.

Backup Configuration

Download & Upgrade

## Renewing the contract

The contract must be renewed annually. FortiSandbox PaaS notifies you to renew the contract before it expires.

If the contract expires, the banner displays a red *EXPIRED* notification. You can still access the instance for reports and existing data. Entitlements and the sandboxing service is not available until you renew the contract. If you renew the contract after the expiry date, it may take a day for the license to be applied.

User ID

User Name

Owner

Company

EXPIRED

(Primary)

Fortinet

CPUs (4 VCPU) 0.4%

RAM (16.0 G) 9.9%

Disk (185.0 G) 4.1%

Firmware Version: FSACLP-3.2-0-5108-Interim-200709

Serial Number: FSA-CLP-3.2-0-5108-Interim-200709

Expiry Date: 2020-06-04

Stop

Reboot

SSH

Enter



An expired instance is preserved for 30 days.

## Adding an IAM user

Identity and Access Management (IAM) is a service to manage user access and permissions to FortiCloud portals and assets. For more information about creating IAM users, see [Adding IAM users](#) in the *Identity & Access Management (IAM) Administration Guide* of FortiCloud.

IAM provides three types of access: *Admin*, *Read-Write* and *Read-Only*.

In FortiSandbox PaaS:

- The IAM Admin profile is mapped to the hidden FortiSandbox PaaS Admin profile. This profile grants full access to all the features of the FortiSandbox PaaS.
- There is no Admin profile for the IAM Read-Write access type. This is by-design.
- The Read-Only Admin profile is mapped to the IAM Read-Only access type. This FortiSandbox PaaS profile is configurable. For example, you want to deny IAM users Administrative access but grant access to On-Demand File submission.

## Adding a secondary account

You can create a secondary account for FortiSandbox PaaS. A secondary account allows the Fortinet support team to troubleshoot the FortiSandbox PaaS deployment.

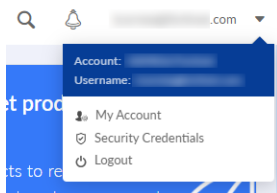


You can also create secondary accounts for additional users.

---

### To add a secondary account:

1. Log in to [FortiCloud](#).
2. In the banner, click the Account menu and click *My Account*. The *Account* page opens.



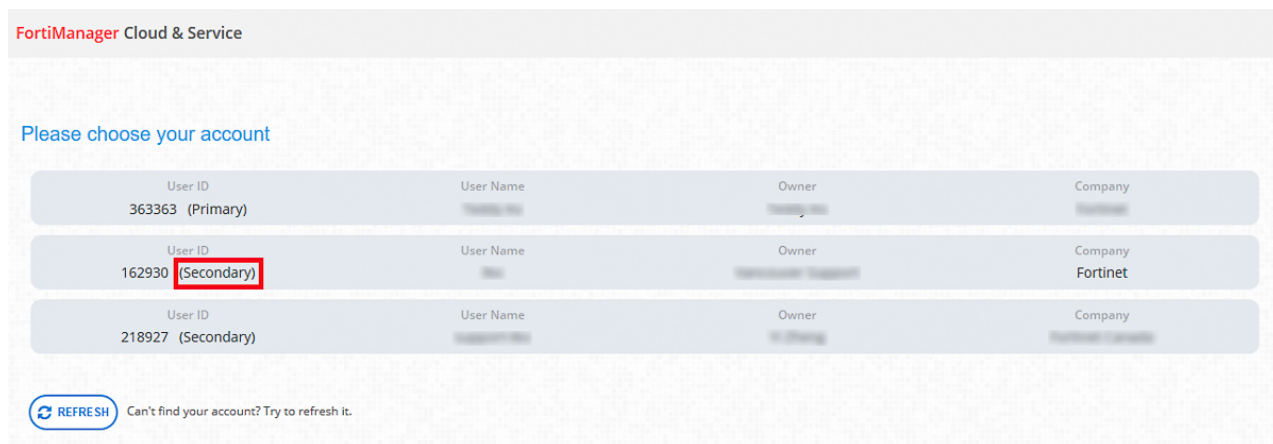
3. Click *Manage User*.

- Click the new user icon to add a new user.

- When creating an account for the Fortinet support team, specify an email for the secondary account, and select *Full Access* or *Limit Access*.

A user with full access has the same access level as a primary account user. A user with limited access can only manage the assigned product serial number and will be unable to receive renewal notices or create additional secondary account users.

- Log in to the personal FortiCare portal. In the FortiSandbox Cloud section, you will see an account listed as a secondary member.



## Subscribe to Service Status updates

Go to the FortiSandbox Cloud Service Status (<https://status.fortisandboxcloud.forticloud.com>) page to:

- View up-time in the last 10 weeks.
- Check any recent incidents.
- Subscribe via email, atom and Slack for any scheduled updates.

Click *Subscribe to Updates* to get email notifications whenever FortiSandbox Cloud Service Status creates, updates or resolves an incident.

## Appendix A - Supported regions

The following provides a list of ingress and egress IP addresses for FortiSandbox PaaS. You can use this list in access control lists to allow access to internal applications from FortiSandbox PaaS only.

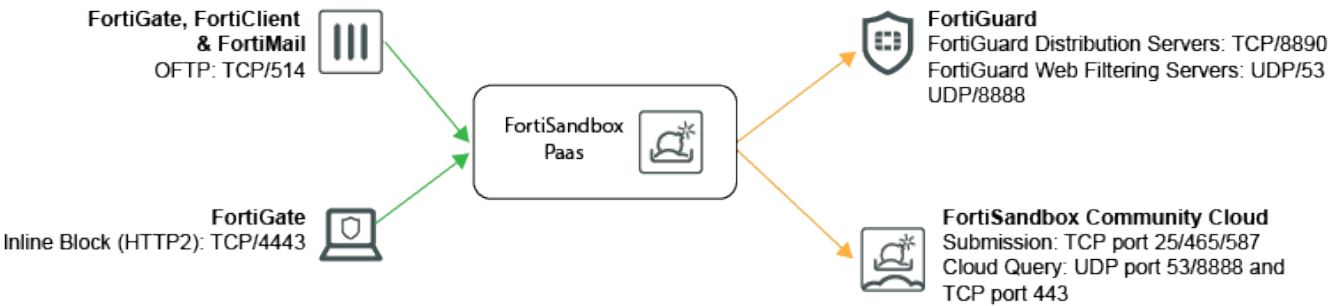
Region	Data center	Security ingress	Security egress
North America	Burnaby, Canada	66.35.19.98	173.243.137.20 - 29
Europe	Frankfurt, Germany	154.52.2.163	194.69.174.8
North America	San Jose, United States	38.21.192.35	208.184.237.20

# Appendix B - Port and access control information

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

## Default Ports

The following table provides information about ports by configuration.



## Access Control List

All access to FortiGuard and FortiSandbox services are pre-configured within FortiCloud.



**FORTINET®**



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.