



FortiSandbox - Cloud Deployment Guide

Version 23.1

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



May 08, 2023

FortiSandbox 23.1 Cloud Deployment Guide

34-223-807422-20230508

TABLE OF CONTENTS

Change Log	4
Introduction	5
Requirements	5
Licensing	5
Deploying FortiSandbox Cloud	6
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
Maintaining FortiSandbox Cloud	15
Expanding VM capacity	15
Keeping firmware up-to-date	16
Renewing the contract	16
Adding an IAM user	16
Adding a secondary account	19
Appendix A - Ingress and egress IP addresses	21

Change Log

Date	Change Description
2023-01-27	Initial release.
2023-04-26	Updated Integrating Security Fabric on page 10.
2023-05-08	Updated Licensing on page 5.

Introduction

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

Requirements

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

- **FortiCloud account:** Subscribe to a FortiCloud Premium account. A FortiCloud account is required to launch FortiSandbox 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 Cloud instance.
- **Browser:** A device with a browser to access FortiSandbox Cloud.



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

Licensing

FortiSandbox Cloud requires the following licenses:

- FortiCloud Premium license.
- FortiSandbox Cloud Entitlement: Purchase FortiSandbox 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 Cloud

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

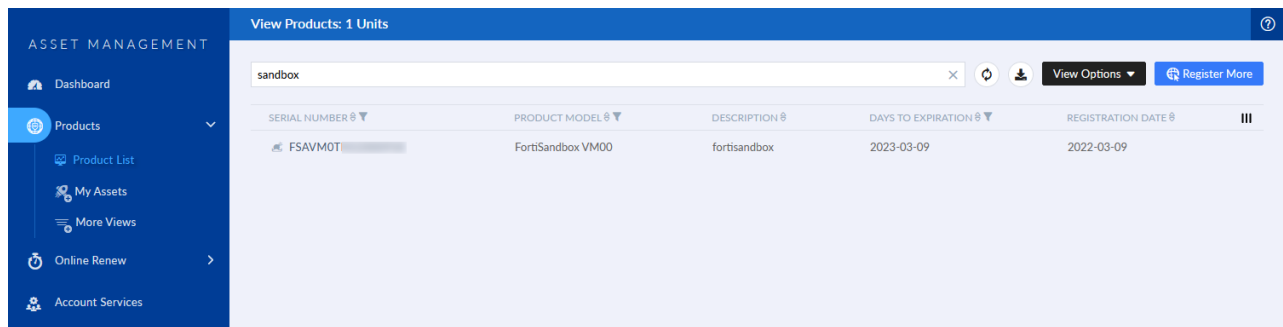
FortiSandbox Cloud supports TLS v1.2. Ensure your browser and firewall setting permits TLS v1.2.



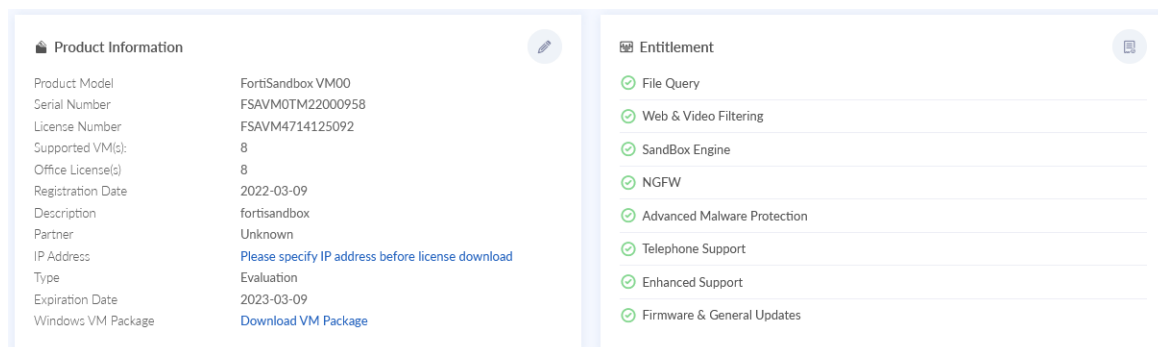
FortiSandbox Cloud can only communicate with FortiGate, FortiMail and FortiClient.

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.



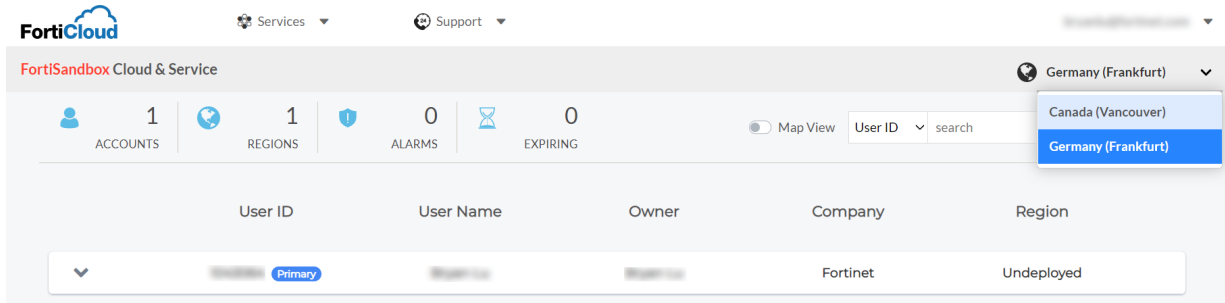
3. Click the Serial Number and check the *Product Entitlements* for FortiSandbox Cloud.



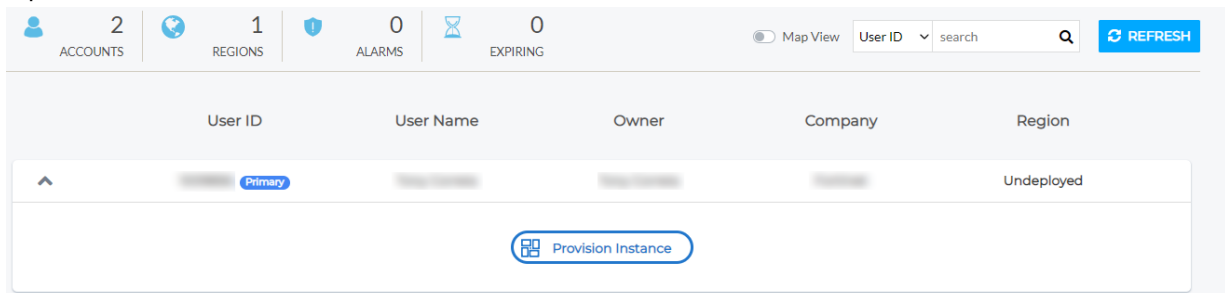
To launch FortiSandbox Cloud:

1. In the Asset Portal, click Services > Cloud Services > FortiSandbox Cloud. The *FortiSandbox Cloud & Service* page opens. Alternatively, you can launch the Cloud 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.

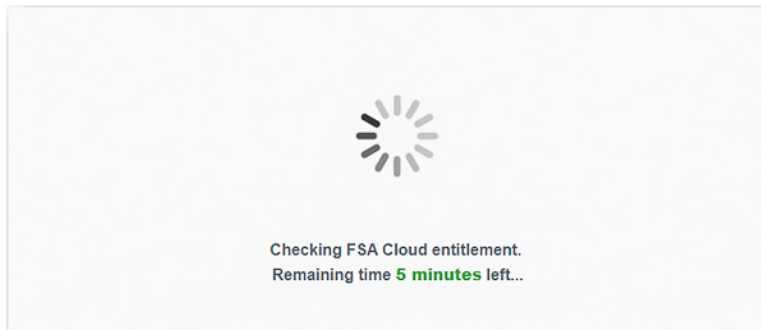


- c. Click *Provision Instance*. Allow a few minutes for the FortiSandbox Cloud instance to be provisioned.

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 Cloud 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%

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

Serial Number: FSA-...

Expiry Date: 2021-07-16

Stop Reboot Enter

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

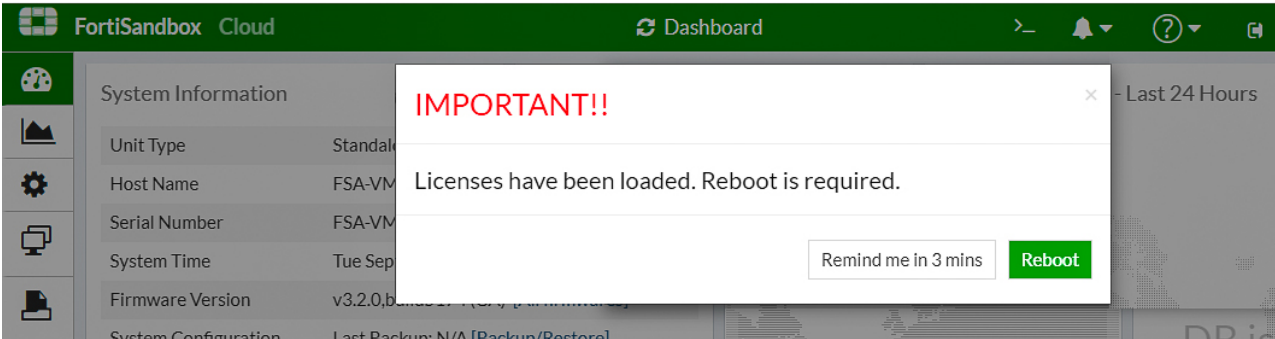


You can directly access FortiSandbox Cloud at <http://fortisandboxcloud.com> using your Fortinet support login credentials.

5. On the FortiSandbox 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 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

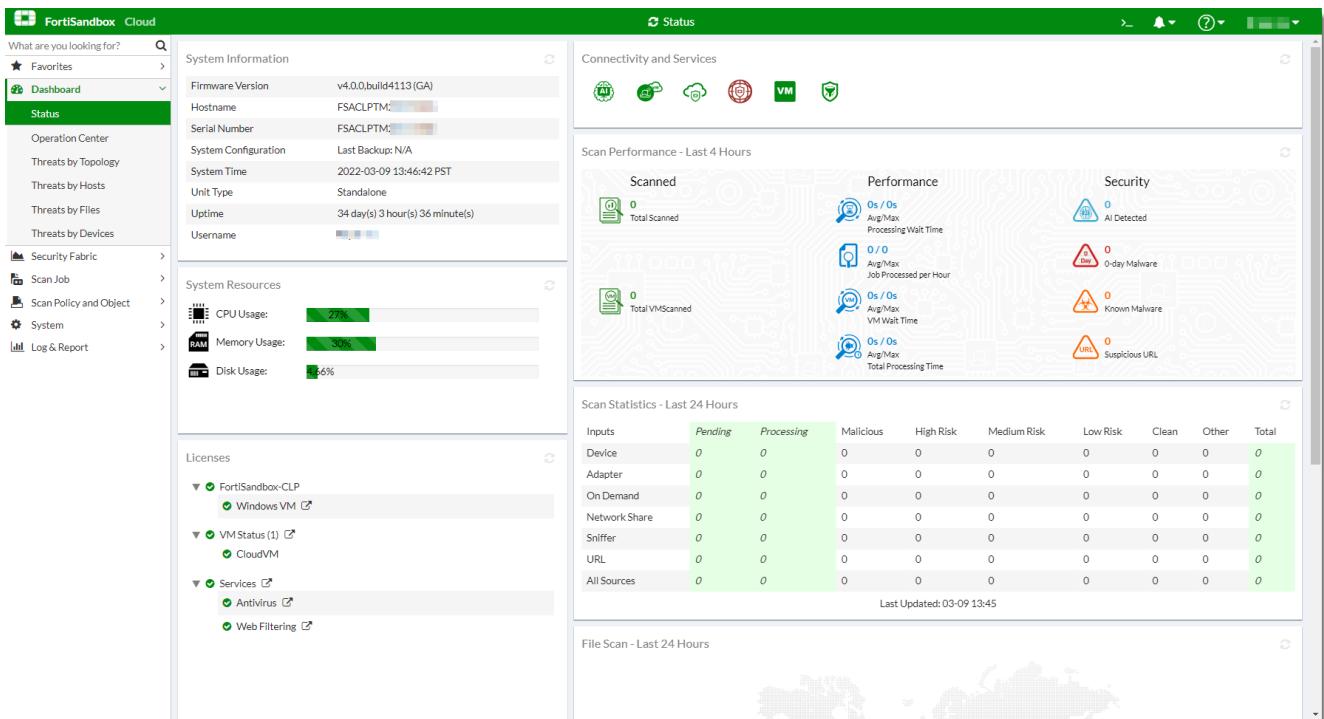
When you log in to FortiSandbox Cloud, *Dashboard > Status* is displayed.

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 entitlement.

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

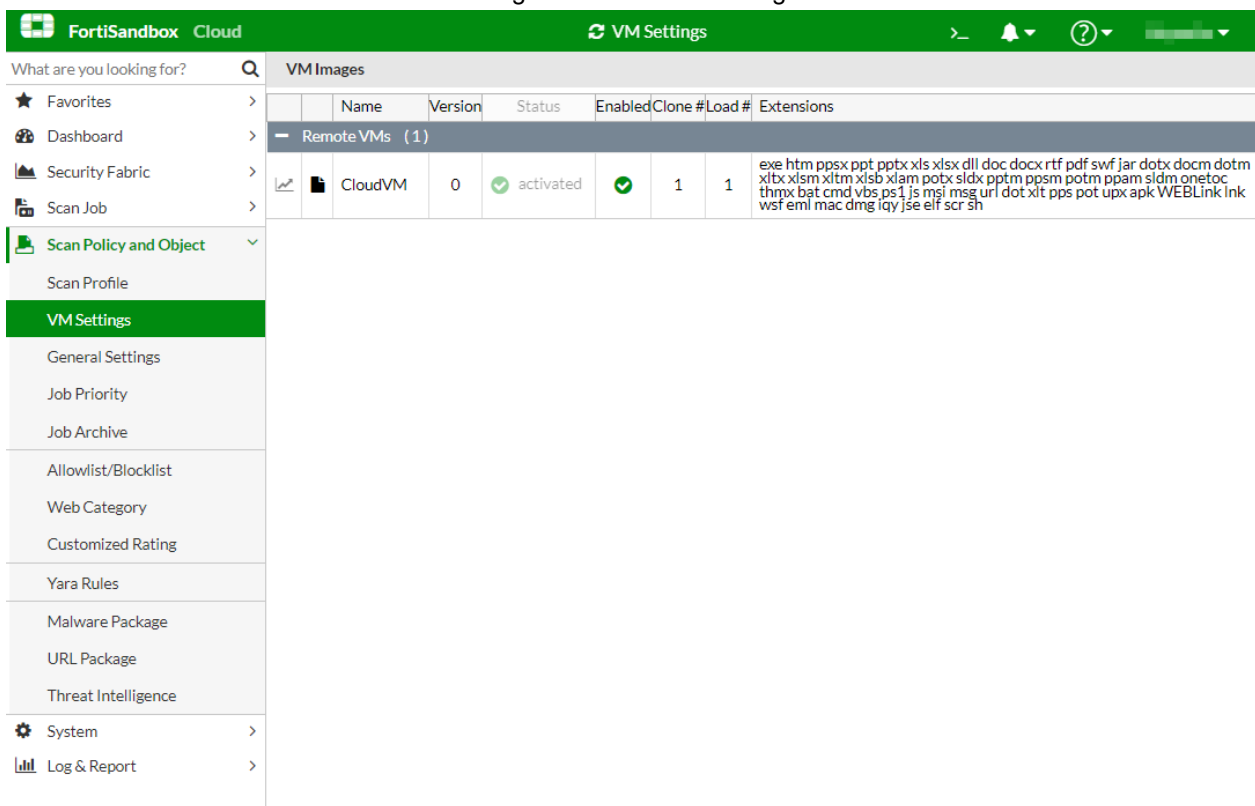


Assigning sandboxing VM

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



Integrating Security Fabric

FortiSandbox Cloud 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 Cloud 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 Cloud 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 the customer selected to deploy their FortiSandbox Cloud 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 type*, click *Enhanced Cloud*.
3. In FortiSandbox Cloud, 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 Cloud. On the client software, use the token to authorize and make the API call to establish the session.

To generate a token in FortiSandbox Cloud:

1. In FortiSandbox Cloud, 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 Cloud VM instance.
token	The token you just generated.

When the session is established, all API calls are similar to the FortiSandbox 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 23.1 supports the EMEA region. When EMEA is selected, FortiOS v7.0.4 will automatically re-establish the connection to the location where the FortiSandbox Cloud 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
```

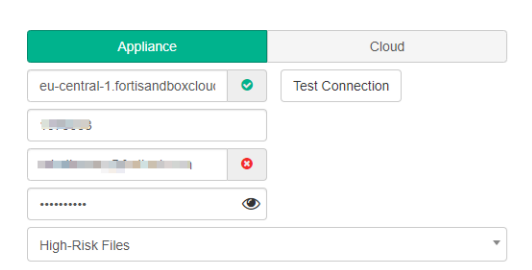
FortiMail and FortiClient connectivity to the EMEA region are not currently supported since the server cannot be overridden.

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`.



The screenshot shows the FortiClient EMS configuration interface with the 'Appliance' tab selected. The 'Cloud' tab is also visible. The 'Appliance' section contains the following fields:

- Server: `eu-central-1.fortisandboxcloud.com` with a green checkmark icon.
- Test Connection: A button.
- Port: A text field with a red 'x' icon.
- Username: A text field with a red 'x' icon.
- Password: A text field with a red 'x' icon and an eye icon.
- High-Risk Files: A dropdown menu.

Maintaining FortiSandbox Cloud

You are responsible for maintaining the FortiSandbox Cloud 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 Cloud 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 web 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 content area 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 updated firmware, the Dashboard displays a notification and a download link. Your maintenance schedule should include upgrading the firmware.



Renewing the contract

The contract must be renewed annually. FortiSandbox Cloud 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.



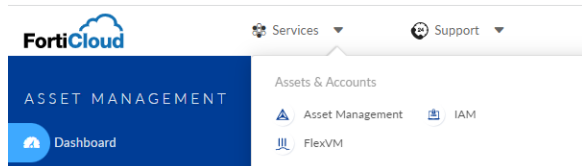
An expired instance is preserved for 30 days.

Adding an IAM user

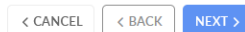
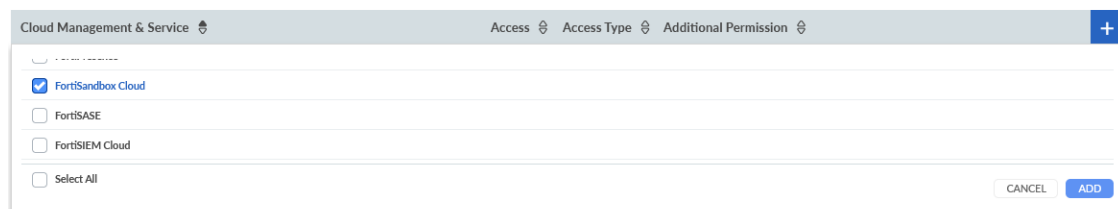
Identity and Access Management (IAM) is a service to manage user access and permissions to FortiCloud portals and assets. For more information about IAM users, see [Identity & Access Management \(IAM\)](#).

To add an IAM user:

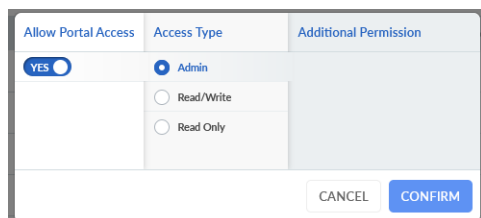
1. Log in to [FortiCloud](#). The Asset Management portal opens.
2. In the banner, click *Services > Asset & Accounts > IAM*. The *IAM Users* page opens.



3. Click *Add IAM User*. The *User Details* page opens.
4. Enter the IAM User information, and click *Next*. For more information, see [Adding IAM users](#).
5. Configure the IAM User Asset and Portal permissions. For more information, see [Adding IAM users](#).
6. In the *Cloud Management & Service Section*, click the Add symbol (+).
7. Search for and select *FortiSandbox Cloud* and click *Add*. FortiSandbox Cloud is added.



8. Click the *Edit* icon. The *Allow Portal Access* dialog opens.
9. Enable the toggle and set the *Access Type* to either *Admin*, *Read/Write*, or *Read Only* and click *Next*. The *Confirmation* page opens.



10. Click *Confirm*.
11. Click *Download CSV* to download the IAM User's credentials as an Excel file. Send these credentials to the new

IAM User.

Add IAM User
1 user add-user
2 sidenav permissions
3 user confirmation
4 common complete
?

4. Successful User Registration : FStein
BACK TO IAM USER LIST
ADD ANOTHER IAM USER

IAM User Group
None

Effective Asset Permissions
My Assets

Effective Portal Permissions

Portals	Access	Access Type	Additional Permission
IAM	❌	Denied	-
Organization	❌	Denied	-
Cloud Management & Service			
FortiSandbox Cloud	✅	Read/Write	-

DOWNLOAD CSV

When the user logs in to FortiCloud, they can click *Sign in as IAM user* and use either the *Account ID/Alias* or *Username* to log in.

FortiCloud

Account ID / Alias:
Account

Username:
Username

Password:

ⓘ All fields are Case-Sensitive

LOGIN

Sign in using email | Forgot password?

Learn more about FortiCloud Privacy Terms

Adding a secondary account

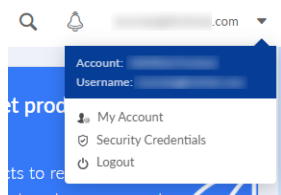
You can create a secondary account for FortiSandbox Cloud. A secondary account allows the Fortinet support team to troubleshoot the FortiSandbox Cloud deployment.



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*.
4. Click the new user icon to add a new user.

Name	Email (Account ID)	Description	Action

5. 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.

Account

- Account Profile
- Change Account ID (Email)
- Manage User

Add User

User Information

User Name:*

Telephone:*

Email (Account ID):*

Confirm Email (Account ID):*

Description:

Permissions

☒ Customer Service
 ☒ RMA/DOA
 ☒ Technical Assistance
 ☐ Notify the master account of ticket updates
 ☒ Send renewal notices
 ☒ Can create user

☒ Full Access
 ☐ Limit Access

You are about to create a sub-account for Fortinet, Inc. By doing so, you agree to share visibility for this account, including ticket history and asset management, as per the settings that you have defined. You agree to assure that sharing visibility does not breach any confidentiality obligations or applicable data protection legislation.

Note: If you have another account same email address, those accounts will be consolidated into one login account. Your original connection between email and accounts (master account or sub account) will be kept, you will use one login user ID/ password to access those accounts.

Save

Cancel

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

FortiManager Cloud & Service

Please choose your account

User ID	User Name	Owner	Company
363363 (Primary)	Travis H.	Travis H.	Fortinet
162930 (Secondary)	Travis H.	Travis H.	Fortinet
218927 (Secondary)	Travis H.	Travis H.	Fortinet

REFRESH

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

Appendix A - Ingress and egress IP addresses

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

Data center	Security ingress	Security egress
Burnaby	66.35.19.98	173.243.137.20 - 29
Frankfurt	154.52.2.163	194.69.174.8
San Jose	38.21.192.35	208.184.237.20



FORTINET®



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.