Deployment Guide

FortiSandbox PaaS 5.0.4
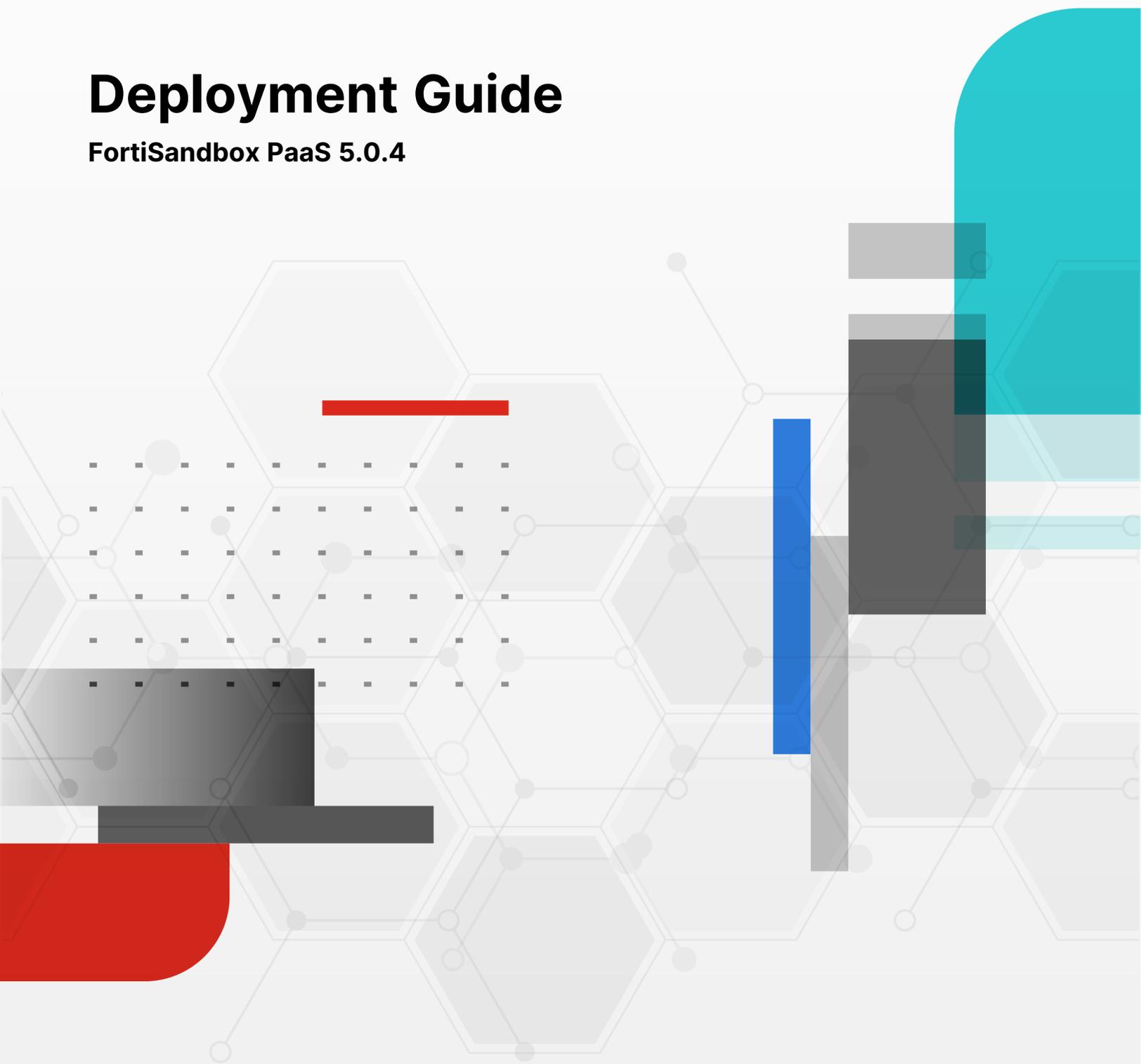
FORTINET DOCUMENT LIBRARY

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

TABLE OF CONTENTS

Change log

Date	Change Description
2025-08-25	Initial release.
2025-08-27	Updated Appendix A: Supported regions on page 22.

Introduction

FortiSandbox PaaS is a cloud-based sandbox service. 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**: A FortiCloud account is required to launch FortiSandbox PaaS Cloud.
- **Internet access**: You must have internet access to create a FortiSandbox PaaS instance.
- **Browser**: A device with a browser to access FortiSandbox PaaS.

> Once you create a new FortiCloud account, please wait 30 minutes before proceeding to deploy FortiSandbox PaaS.

Licensing

FortiSandbox PaaS requires the following licenses:

- FortiSandbox PaaS Entitlement: Purchase FortiSandbox PaaS Cloud licenses for full functionality.
  The Cloud VM for FortiSandbox PaaS supports scanning files for Windows, Microsoft Office, Linux, MAC and Android.
- 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.

Provision FortiSandbox PaaS

To verify you have a product entitlement:

1. Log into FortiCloud.
2. Go to *Services > Assets & Accounts > Account Management > Account Services* and verify the subscription for FortiSandbox PaaS.
3. To verify the entitlements for *FortiSandbox PaaS* click the serial number.

To launch FortiSandbox PaaS:

1. In the Asset Portal, go to *Services > Cloud Services > FortiSandbox Cloud*. The *FortiSandbox Cloud & Service* page opens. Alternatively, you can provision the PaaS instance from FortiSandbox Cloud Portal https://fortisandboxcloud.com.
2. Select the region and provision the instance.
   a. Select the account that purchased the FortiSandbox PaaS services and expand the instance. The *Account ID* represents the dedicated instance.
   b. Select the region from the dropdown menu.
   c. Click *Submit* to provision the instance. Allow a few minutes for the FortiSandbox PaaS Cloud instance to be provisioned.
   If an entitlement is not set up correctly, the provisioning will report an error. For information, see the Ordering Guide.
3. When provisioning is complete, the dedicated PaaS instance displays the resources and firmware information.
4. Click *Detail*. The *License Detail* information is displayed.
5. Click *Enter* to access the web GUI.

Verifying system status

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

Verify the following in the PaaS Dashboard:

- A *Serial Number* has been assigned.
- The *Licenses* are valid.
- The *System Resources* and *Disk Monitor* widgets show normal usage.
- The *Connectivity and Services* .

Assigning sandboxing VM clones

For new setups, the sandboxing VM clones are not assigned by default.

To assign a clone number:

1. Go to *Scan Policy and Object > VM Settings*.
2. Double-click the *Clone* # to modify it. Click the Green Arrow icon to update and then click *Apply*.

Integrating Security Fabric

FortiSandbox PaaS uses a Fortinet proprietary traffic protocol (based on OFTP) to communicate with connected Security Fabric devices via TCP port 514. FortiSandbox PaaS uses port TCP/4443 for FortiGate Inline Block (HTTP/2). The traffic data is encrypted over TLS. Ensure any firewall between FortiSandbox PaaS and the fabric devices allows them to communicate.

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

FortiGate

To integrate with the Security Fabric in FortiGate:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *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*.

> Steps 5 and 6 are required if the FortiGate is running FOS 7.6.3 or later. Otherwise, proceed directly to step 7.

5. In the pane that opens, verify FortiSandbox's serial number, then click *Accept*.

6. Click *OK* in the confirmation dialog to open a window to authorize the FortiGate on the FortiSandbox.

   a. A login screen opens in a new browser window.

   b. Enter the username and password, then click *Login*.

7. In FortiSandbox PaaS, go to *Security Fabric > Device*, click the *Authorize* icon on the FortiGate so that it can establish Fabric connectivity. Verify that the *Status* is updated.

8. In FortiGate, verify the *Connection status* is *Authorized*.

To integrate with Security Fabric in the FortiGate CLI

For information, see *Configuring sandboxing* in the *FortiGate / FortiOS Administration Guide*.

FortiMail

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 #
```

FortiClient

To integrate with the Security Fabric in FortiClient:

1. In the FortiClient Console, go to *Sandbox Detection*.
2. Enter the domain in the *IP* field. For example: *856651.eu-central-1.fortisandboxcloud.com*
3. In FortiSandbox PaaS, go to *Security Fabric > FortiClient*, click the *Authorize* icon on the FortiClient so that it can establish Fabric connectivity. Verify that the *Status* is updated.

To integrate with the Security Fabric in FortiClient EMS

1. In the EMS Console, go to *Endpoint Profiles > Sandbox > Edit the profile for FortiSandbox PaaS > Enable Sandbox Detection*.
2. In the *IP address/Hostname* field, enter the FortiSandbox PaaS FQDN. For example: *us-west-1.fortisandboxcloud.com*
3. In the *Account ID* field, enter the Account ID.
4. In FortiSandbox PaaS, go to *Security Fabric > Device*, click the *Authorize* icon on the EMS so that it can establish Fabric connectivity with all FortiClient Endpoints automatically.
5. In the FortiClient Endpoints, go to *Sandbox Detection*, verify the IP field is overridden by EMS and that it is connected to the FortiSandbox PaaS.
6. In FortiSandbox PaaS, go to *Security Fabric > FortiClient*, verify the *Status*.

Setting up and making an API call

To set up and establish a session to your FortiSandbox PaaS instance, generate a token first. 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, open the CLI console by clicking the CLI icon at the top-right of the page.
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>.<region>.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 API document.

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

Establishing a connection to a region

FortiSandbox PaaS 5.0.4 supports the EMEA region. When EMEA is selected, FortiOS v7.0.4 and later 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 later

For FortiMail 7.0.3 and later, 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`.
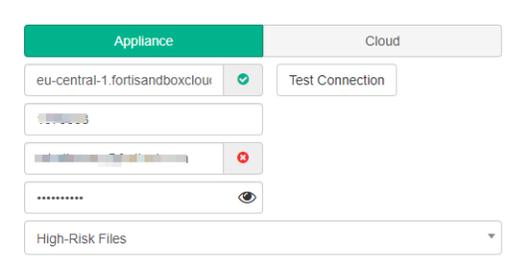
Feature limitations

The view a table compares the available features in FortiSandbox with those available in FortiSandbox PaaS, go to Appendix F: FortiSandbox PaaS supported features in the *FortiSandbox PaaS Administration Guide*.

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 on page 13
- Keeping firmware up-to-date on page 13
- Renewing the contract on page 14
- Adding an IAM user on page 15
- Subscribe to service status updates on page 17

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 > Connectivity and Services*.

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 clones on page 7.

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.
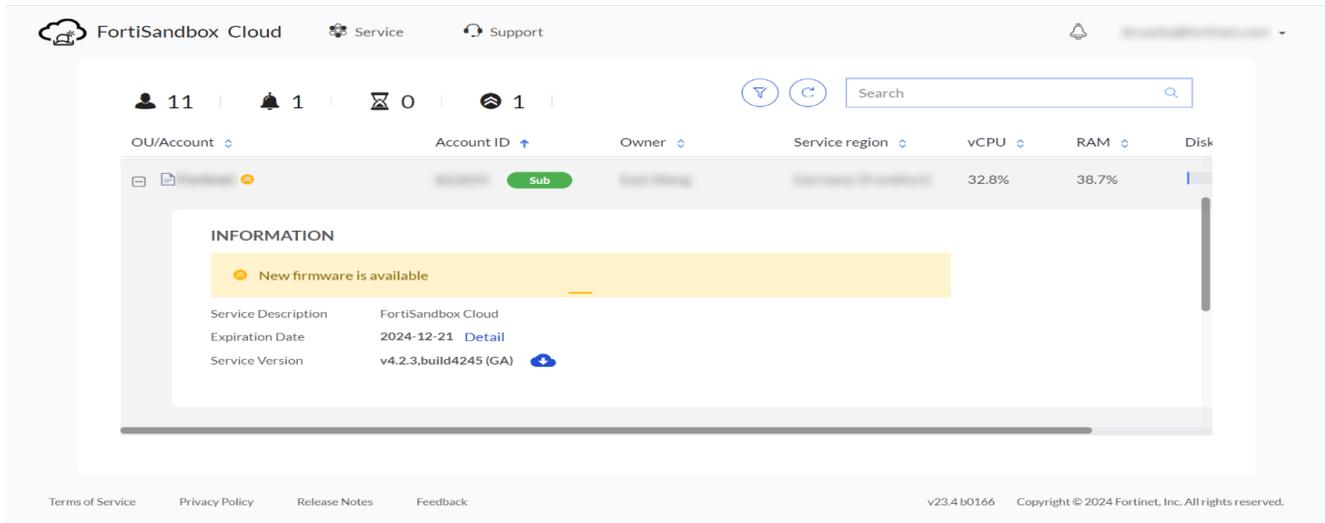
To upgrade the firmware:

1. Go to *Dashboard > Status*.
2. Click the *System Information* widget.
3. From the menu, select *Update Firmware*.
4. The firmware upgrade page provides the following options:
   - Manually upload a firmware image.
   - Download and install the latest available firmware.
   - Create a backup of the current configuration before upgrading.

Always back up your configuration before performing a firmware upgrade.

Renewing the contract

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

Click the *Detail* link beside the *Expiration Date* to check the expired *License Detail*. Entitlements and the sandboxing services are 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 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:

IAM Profile	FortiSandbox PaaS access
Admin	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.
Read-Write	The IAM Read-Write permission is mapped to the FortiSandbox PaaS Device Admin profile.
Read-Only	The *Read-Only* Admin profile is mapped to the IAM Read-Only access type. This FortiSandbox PaaS profile is configurable.

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.
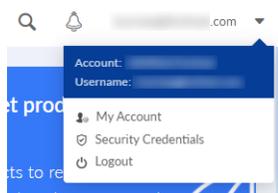
3. Click *Manage User*.

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

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.

6. Log into FortiSandbox Cloud Portal (https://fortisandboxcloud.com), you will see an account listed as a sub-user.

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.

Setting up multiple PaaS

Setup Organizational Units (OU)

When you create an Organization, your account becomes the Root Account for the organization. Users with the proper permissions can add Organizational Units (OU) and invite members to join the organization.

> The Organization Portal must first be enabled by the Master User. See Enabling Organizations in the *Identity & Access Management (IAM) Guide*.

Create Organizational Units (OU) and subOU

Organizational Units (OU) are folders for organizing your accounts. You can create a maximum of three levels of OUs to build the structure of your organization. Users with the proper permissions can move Member Accounts between OUs, remove accounts from the organization, edit the organization details, move the OU, or delete it.

To create organizational units:

1. In the Organization Portal (https://support.fortinet.com/organizations/), click *Create Organization*. See Creating an organization
2. Create Organizational Units (OU) and SubOU. See Adding and deleting OUs
3. Create Member Accounts under different Organizational Units (OU). See Creating new Member Accounts.

Invitations

Invitation tokens are a secure method of inviting Member Accounts to join your organization. The Root Account for the organization can generate a token and then distribute it via SMS, Teams, or Slack. After a Member Account replies to the invitation, the root account can verify the invitation and accept or decline the response.

Creating invitation tokens

1. Log into the Organization Portal (https://support.fortinet.com/organizations/) as Root Account (e.g. Fortinet Email LDAP account) to create invitation token for each SubOU. See Creating invitation tokens.

> 💡 We recommend generating a separate token for each SubOU.

2. After the invitation tokens are created, click *Download* to save it to your computer as an Excel file.
3. Send the invitation token and the link to the Organization Portal (https://support.fortinet.com/organizations/) to the Member Account master users. You can share the Organization Portal link by copying the URL from your browser.

To approve the invitation:

1. After receiving the valid invitation token, the Member Account user goes to the Organization Portal (https://support.fortinet.com/organizations/), and clicks *Join Organization* with the invitation token. See Joining an organization.
2. The Root Account approves the invitation after the member account user joins the organization. See Invitation Approval.

# Organization user management

Advanced management features are available when using organizations. An Organization and Organizational Units can be created in the Organization portal and are used to enhance your company's security.

IAM users, user groups, and so on can be created and associated with Organizational Units and OU accounts with the proper permissions. If you are using OUs to organize your company, you will need to create permission profiles that reflect this hierarchy so that the necessary users, user groups, and roles can be assigned. For more information, see Organization user management.

After the Master User creates the organization, they can create an IAM user with the same level of permissions. The IAM user can be used to create other IAM users and delegate their permissions. For more information, see the Identity & Access Management (IAM) Administration Guide and User permissions.

To create an IAM permission profile:

1. Create a permission profile. See Permission profiles within Organizations.
2. Make sure to select *Organization* as the profile type. **Once the permission profile is saved, the type cannot be edited**.
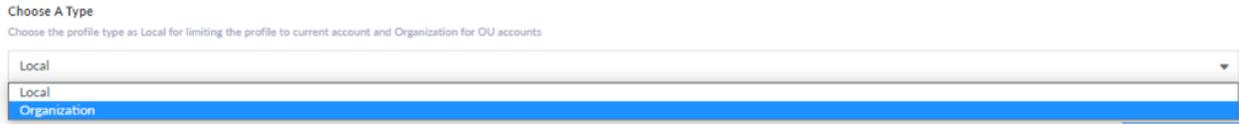
3. Click *Add Portal*. Add the following portals with a minimum of *Read-Only* the access type. Admin access of FortiSandbox PaaS Cloud Portal is required for provision FSA PaaS.
   - Asset Management
   - FortiCare
   - IAM
   - FortiSandbox Cloud
4. Repeat the steps above to create different IAM permission profiles for different OU scopes or member account users.

To create an IAM user group

1. Create an IAM user group. See Adding an IAM user group.
2. Ensure the IAM user group type is associated with OU.
   a. From the *Type* dropdown, select *Organization*.
   b. From the *Permission Scope* dropdown, select an OU created in the previous step.
   c. From the *Permission Profile* dropdown, select the permission profile created in the previous step for the selected OU.
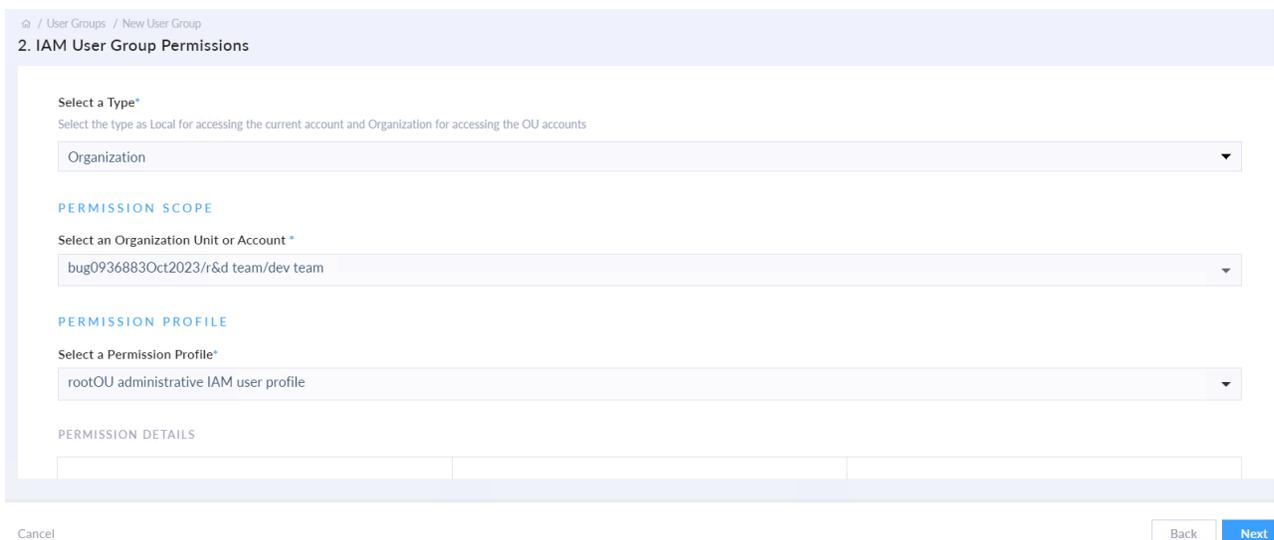
3. Skip add IAM user. Repeat the steps above to create different IAM user groups for different OU scopes or member account users.

To create an IAM user:

1. Add a new IAM user. See Creating users, user groups, and roles within Organizations.
2. Ensure the IAM user type is associated with an OU.
   a. From the *Type* dropdown, select *Organization*.
   b. From the *Permission Scope* dropdown, select an OU created in previous step.
   c. From the *Permission Profile* dropdown, select the permission profile created in previous step for the selected OU.
3. From the *Permission Scope* dropdown, select the permission to associate with an OU or a member account.
4. From the *Permissions Profile* dropdown, select the profile created for the selected OU or member account.
5. Associate the IAM user to the IAM user group.
6. Repeat the steps above to create different IAM users for different OU scopes or member account users.

Setup FSA PaaS

Users can access FortiCloud using IAM user accounts or an OU account when logging in with their IAM user credentials. Once the login credentials have been verified, users can then choose to proceed with an Organizational Unit (OU) account. OU access is dependent on the permission profile assigned to your login credentials. Available OUs and member accounts will turn blue when hovered over and display the *Select* button.

OU account login

1. OU member account user log into the FortiSandbox PaaS Cloud portal (https://fortisandboxcloud.com/) with the invitation token. See Logging into an OU account
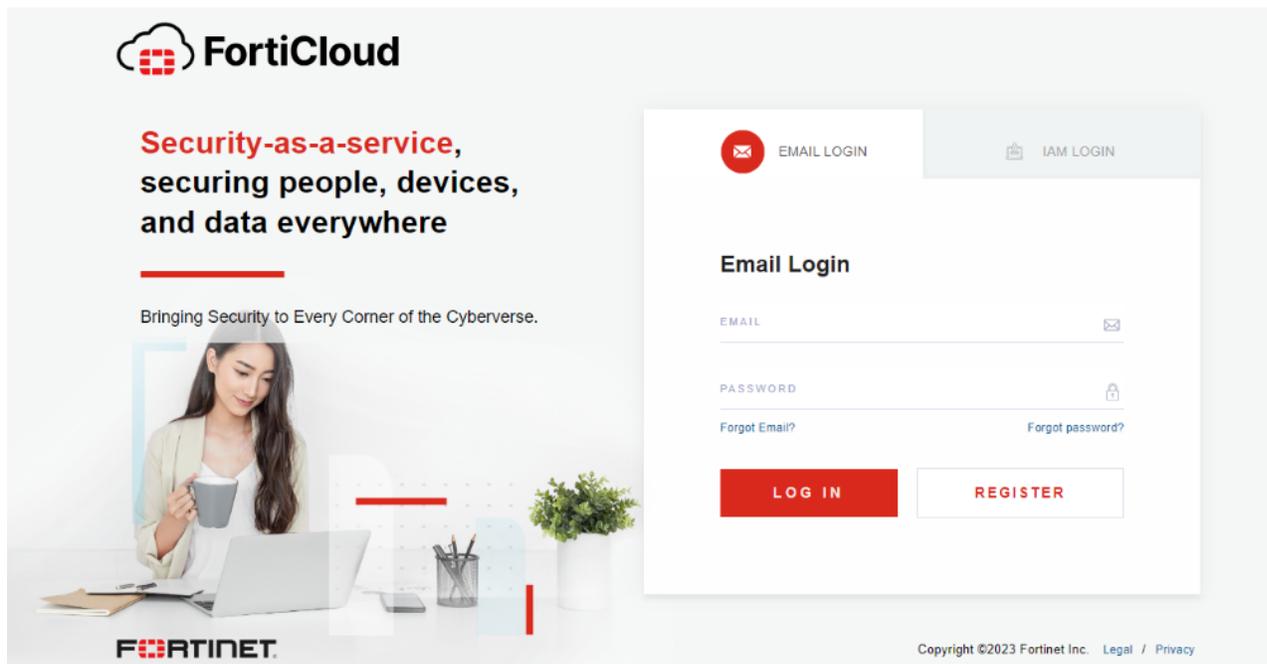
2. Select the Organization scope and then select the assigned OU or account for having access.

IAM OU account login

1. IAM user logs into the FortiSandbox PaaS Cloud portal (https://fortisandboxcloud.com/) via IAM login.
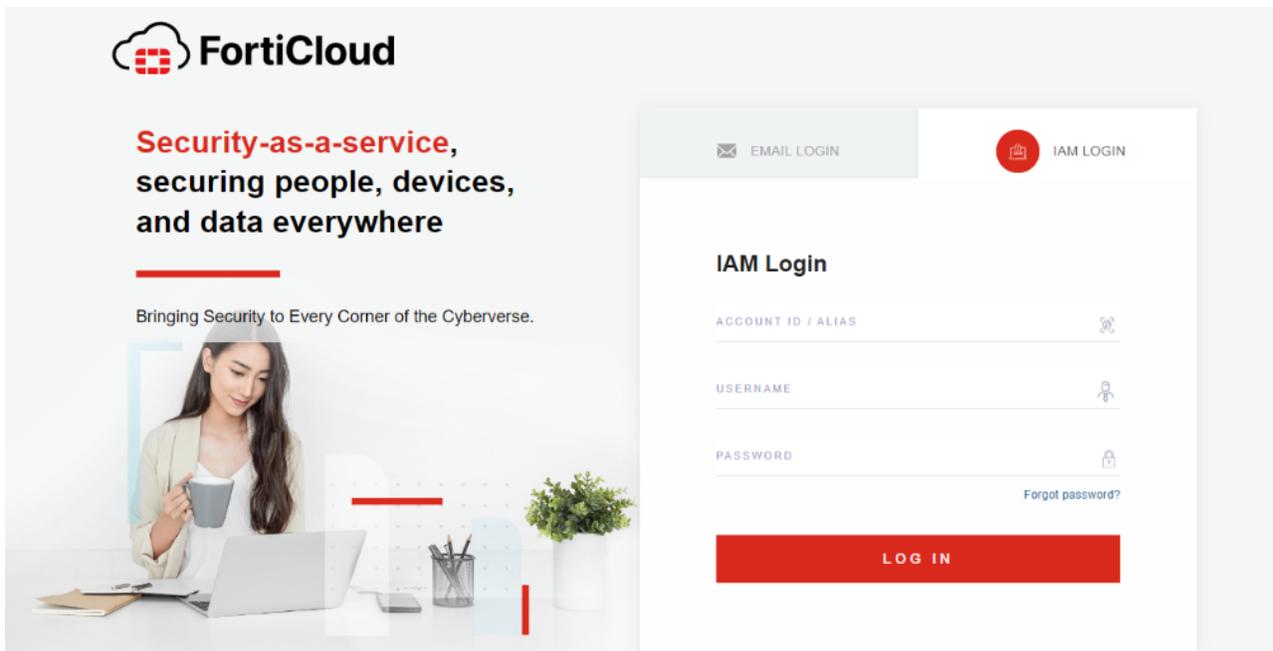
2. The Root Account manages the Account ID/Alias. the Root account ID is the Account ID for IAM users by default.
3. Select the Organization scope and then select the assigned OU or account for having access.

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	160.223.172.27	160.223.172.30 – 31
Europe	Madrid, Spain	141.109.169.0/28	141.109.169.0/28
North America	Dallas, United States	209.40.117.9	209.40.117.2 - 209.40.117.3

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.

For a comprehensive list of default ports by interface, as well as the endpoints that FortiSandbox PaaS must be able to reach, see the Port and access control information topic in the *FortiSandbox Getting Started Guide*.

Default Ports

The following topology provides information about ports by configuration.
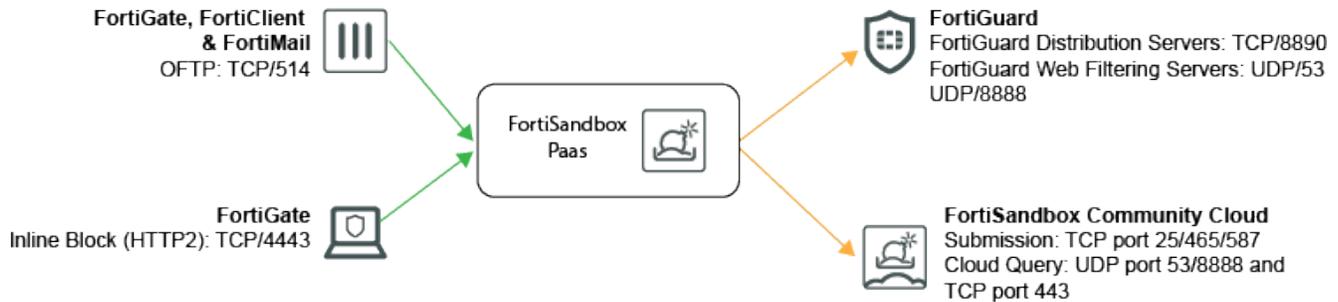
Access Control List

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

FORTINET

www.fortinet.com