Sandbox

Sandbox, Install and onboard Apps, Pubishing, Updates

Sandbox

Each Frame Account has a Sandbox - a virtual machine provisioned specifically to allow you to manage the operating system and applications for the Frame account. The Sandbox image acts as a template for the rest of your workload VMs. For non-persistent Frame accounts, any changes made to the Sandbox image (e.g., updating Windows OS or Linux OS, installing or updating applications) will be served to your users as soon as you Publish.

GRAPHIC GOES HERE

For persistent desktop Frame accounts, any changes made to the Sandbox image (e.g., updating Windows OS or Linux OS, installing or updating applications) will be made available to new users after you Publish and the new users are assigned to their persistent desktop. Already assigned persistent desktops will not receive those Sandbox changes. Refer to Persistent Desktop Lifecycle for more details.

Access your Sandbox

The Sandbox is accessed from the Frame Dashboard menu (`Dashboard > Sandbox`). From this page you can power it on, start the Sandbox session, and make desired changes to your operating system and applications.

image.png

Once the Sandbox is powered on, you can start a session by clicking on the **Start Session** option. If the Sandbox is currently being used by an admin, the system will first prompt you to confirm that you wish to close the existing session.

image.png

Installing and Publishing

With your Sandbox in place, you can install apps and customize your experience. Then, once it's all configured, it's time to deploy or **Publish** the Sandbox as a disk image to your instances.

Sandbox Options

Power Off or Reboot

When the Sandbox is powered on, the admin can power off or reboot the Sandbox by clicking the power slider or select the reboot option

image.png

If an administrator chooses to reboot the Sandbox while another admin is accessing it, the system will prompt the admin to choose whether to **reboot** or **force reboot** the Sandbox. Choosing reboot will ensure the Sandbox is rebooted once the active Sandbox session is closed. The force reboot option will immediately close the active session and reboot the Sandbox.

Sandbox - Reboot Options

Change Instance Type

The Sandbox instance type is defined by the administrator during account creation, however, this can be changed (provided the Sandbox VM is powered off) at any time. Changing the Sandbox instance type can be helpful if you wish to:

- Test your applications and configuration on Sandbox VMs with a different instance type
- Install or update applications that require a specific instance type. For example, an admin may wish to install a CAD application that requires a GPU. It can be helpful to switch to a GPU-based instance type and then back to a CPU-only instance type for installation/update tasks that don't require a GPU.

For public cloud infrastructure, changing the instance type requires the new VM to power on after the existing Sandbox disk is attached to the new VM and the old VM is terminated.

Click **Change Instance Type**. A dialog will appear prompting you to select a new instance type for your Sandbox.

Sandbox - Change Instance Type

Increase Disk Size

If your users need a larger C:\ drive, you can increase the size of the Sandbox disk in increments of 1 GB. If you are using Azure, you will only be allowed to increase the disk size in discrete disk sizes.

Sandbox - Increase Disk Size

Increasing the size of the disk should be used with caution as this operation is irreversible.

Sandbox Session Settings

Frame admins can change the behavior of the session by overriding the default account-level session settings. To override the account settings, simply disable the **Use account settings** slider. You will then be allowed to edit the settings.

image.png

This is particularly important when Frame admins need ample time to install/configure applications, update their operating system/applications, or to test specific features. We recommend increasing the Sandbox Time Limits for this work to prevent your Sandbox session from ending prematurely.

As a best practice, specific timeout settings to consider increasing are:

- User Inactivity Timeout
- Idle Timeout

You may also want to review and enable features that allow you to do your work more efficiently, whether or not your users are allowed to use the same features in their Frame sessions:

- Clipboard Integration
- Download, Upload, and Print
- USB Redirection

Refer to Session Settings for details of each session setting parameter.

Cloning

The Sandbox disk image can be cloned (copied) to other Frame accounts, provided the source and destination Frame accounts share the same cloud account (public or AHV).

Refer to Cloning for details on how to clone a Sandbox (or a Sandbox backup) to one or more destination Sandboxes.

Backup and Restore

There are 3 different ways to perform a backup of your Sandbox image:

1. Publish: when you start a publish, your Sandbox disk will automatically be backed up.
2. Manual backup: you can manually backup your Sandbox disk at any time.
3. Automated backup: you can schedule a task to backup your Sandbox with a daily or hourly periodicity.

Refer to Backups for additional information on these three backup approaches and how to restore the Sandbox disk from a backup.

Reset Master Image

If you have used your own image (BYO Image) to create your Frame account, you will have the option to reset your Sandbox image back to a template image of your choice, as specified in your Cloud Account, under the Template Images tab. Reset Master Image will terminate your existing Sandbox VM and provision a new Sandbox VM with a same instance type using a copy of the default template image.

If you are using Application Launchpads, you must ensure that the onboarded applications are in the new Sandbox VM and/or manually remove the onboarded application entries from the Sandbox page to match what is in the Sandbox before publishing the Sandbox.

Sandbox - Reset Master Image

Once you have selected the template image that will be used, click **Reset** to proceed with the replacement of your Sandbox image.

Sandbox - Reset Master Image Confirmation

Updates

The **Updates** page of your Account Dashboard will display any needed OS or Frame-related updates for your Sandbox. More details can be found in the Updates section of our documentation.

Local Group Policies

In order for users to be able to use Frame, administrators must ensure that the following Windows Local Group Policy requirements are met.

Policy	Location	Required Value	Explanation
Interactive logon: Don't display last signed-in	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	Enabled	Auto-login is required for the Frame session to be able to start.

Policy	Location	Required Value	Explanation
Interactive logon: Message title for users attempting to log on	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	Not defined	Frame session will not start if the title is defined.
Interactive logon: Message text for users attempting to log on	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	Not defined	Frame session will not start if the message is defined.
Password protect the screen saver	User Configuration\Administrative Templates\Control Panel\Personalization	Disable	Frame session will not start or resume if the screen saver requires a password.

Frame-specific Local Windows Users

Frame adds two local Windows users to each Windows workload VM:

- `Frame` - a local Windows user that is included in the local Administrators group.
- `FrameUser` - a local Windows user used in non-domain-joined workload VMs when the Enterprise Profiles feature is enabled. This local Windows user does not have local Windows administrative privileges.

> Do not:Remove the `Frame` user from the local Windows Administrators group.
>
> - Modify the `Frame` user permissions in `Computer Configuration\\Preferences\\Control Panel Settings\\Local Users and Groups`.
> - Change the `Frame` user password.Remove the `FrameUser` user (if the Enterprise Profile feature is to be used in a non- domain-joined pool of workload VMs).
> - Change the `FrameUser` user password (if the Enterprise Profile feature is to be used in a non-domain-joined pool of workload VMs).
> - Modify the local user password policy or implement a stronger password policy.

Otherwise, you will not be able to access the workload VMs using Frame Remoting Protocol.

Changing these passwords on a workload VM can cause the Frame session to fail to start. If a password management solution such as Microsoft Local Administrator Password Solution (LAPS) is used, the two Frame-specific users must be excluded.

Frame-specific Local Linux User

Frame adds one local Linux users to each Linux workload VM:

- `frame` - a local Linux user.

The same warnings from the local Windows user `Frame` listed above apply for the local Linux user `frame`.

Local Frame User Password Policy

The `Frame` (Linux and Windows) and `FrameUser` (Windows only) password is rotated automatically by Frame for each Frame session. These passwords have the following characteristics:

- Randomly generated
- 25 characters long
- Contains 4 uppercase characters
- Contains 4 lowercase characters
- Contains 4 numeric digits
- Contains 8 special characters (`!`, `@`, `#`, `$`, `%`, `^`, `&`, `*`, `(`, `)`, `,`, `.`, `?`, `:`, `{`, `}`, `|`, `<`, `>`, `_`)

Install and Onboard Apps

In general, if you are planning to only deliver virtual desktops to your users, then onboarding applications is not required – simply install your desired applications to the Sandbox.

If you wish to make individual applications available to your users via an Application Launchpad, you will need to install and onboard each application. Onboarding an application for your users registers the application with the Frame control plane and prepares it to be shared as an individual application without the desktop being visible.

Once you have installed or updated your applications for either Desktop or Application Launchpad, you must publish your Sandbox to make the applications available to your users.

This guide will show Frame administrators the basics of installing, onboarding (if required), and deleting applications for their users.

AWS-specific best practice

When an Amazon Elastic Block Storage (EBS) volume is created for each AWS Elastic Cloud 2 (EC2) instance provisioned during the publishing process, Amazon does not copy all of the Simple Storage Service (S3) blocks of the underlying EBS snapshot into the EC2 instance's EBS volume. This allows the EBS volume to be used immediately. Any S3 blocks that are subsequently needed are then loaded into the EBS volume on-demand ("lazy loading"). This AWS-specific behavior can result in slower than expected application and file loading until the relevant S3 blocks are loaded into the EBS volume.

For customers providing virtual desktops using AWS infrastructure, Frame recommends administrators install and onboard applications in the Sandbox. The first time the EC2 instance is provisioned and powered on, Frame will start up all onboarded applications to force the applications' S3 blocks to be loaded into the EBS volume, in order to speed up application start up time.

Install and Onboard Applications

As a best practice, Frame recommends manually backing up your Sandbox before installing your applications. This backup allows you to quickly revert to a base OS image in the case of catastrophic image corruption. With Bring Your Own (BYO) image, you can reset the Sandbox

image to a previously registered template image using the Reset master image feature.

> The onboarding process only applies to executables (.exe files), scripts which launch executables, and shortcuts that point to executable files.

1. Go to the **Sandbox** page of your account's *Dashboard*. Click **Power On** to boot your Sandbox if needed . When the Sandbox is available, click **Start Session**.

   image.png
2. If your installer is available online, you can download it directly using the browser in your Sandbox (Chrome) – this will be the fastest method for large installers. If your installer is not available online, and you have it on your local machine, you can upload it to your Frame session from your local machine. Additionally, you can opt to connect your cloud storage account to your Frame account, which would enable you to see the files in a virtual drive in your Sandbox. You can connect your cloud storage accounts from the admin menu in the upper right corner (to the right of the Sandbox image) or from within your Sandbox session by clicking on the icons at the bottom right corner of your desktop session.

3. If you downloaded your installer using the browser in the Sandbox, simply launch the setup file from the "Downloads" folder. If you used a cloud storage account, navigate to "Computer" and open the appropriate drive (e.g., X: drive for Box). If you uploaded your installer from your local machine, you can access it by going into the "Uploads" folder.

> **Caution**
> Copy your setup file(s) from the original drive to the C: drive, and then run the installation of your app as you would on a PC from the local **C: drive**.

Tip

Looking to automate app onboarding?

If you're interested in scripting and automating app onboarding, see Onboard applications via CLI.

4. If you are planning to deliver your applications in an Application Launchpad, accept the Frame prompts to onboard your application. Frame automatically imports the application's icon during the onboarding process. Otherwise, you can click **Cancel**.

Sandbox Panel

> To manually onboard an application, simply right-click on the application in the program menu or directly on the application's .exe file in its install folder (e.g. in the "Program Files (x86)" or "Program Files" folder) and select "Onboard to Frame."

5. Test your application from within the Sandbox to make sure everything is functioning as expected (for instance, if you need to enter a license code/load a license file, do so now). If you onboarded the application, you can disconnect from your Sandbox session by selecting **Disconnect** from the gear menu. You will see your newly onboarded application as an application icon in your Dashboard next to your other onboarded apps. Set custom application properties by hovering over your icon and selecting the gear icon.
   Sandbox Panel

Delete Onboarded Applications

If you wish to remove a particular application from your users' Launchpad, you can do so easily from the account Dashboard by following the steps below:

1. Navigate to the Dashboard. On the *Sandbox* page of the *Dashboard*, look for the **Applications** section near your Sandbox. Hover over the application you would like to get rid of – you should see a gear icon and trash can icon, like this:
   Sandbox Panel
2. Click on the trash symbol to schedule the deletion of the application on the next publish. This means that your users will still see the application in their Application Launchpad until the next time you publish.

Uninstall an Application

If your application has been installed on the Sandbox and you want to ensure that your users are no longer able to access the application (especially if they are using a Desktop Launchpad), you must uninstall the application from your Sandbox.

1. To uninstall applications, launch your Sandbox, click on the Windows Start button and select "Installed apps"

   image.png

2. A new window will pop up, from there you can see a list of all installed Applications, and can select which one should be removed.

   Publish your Sandbox to ensure the application binaries are no longer in the production VMs.

> If your users are using an Application Launchpad and you did not delete the onboarded application in the Sandbox page before publishing, your users will see an error when they try to access the application from their Application Launchpad.

Publishing

Once you have installed one or more applications, tested them in the Sandbox, set up a Desktop Launchpad or Application Launchpad, and defined your production capacity, you're ready to publish. There are three types of publishing:

- **Publish**: A standard publish will always create the **max** number of instances specified in the account's Capacity settings for each configured Instance Pool before the existing instances are terminated.
- **Quick Publish**: Quick publish allows administrators to specify how many production instances (less than or equal to Default Capacity **max**) are created on publish and powered on for each Instance Pool before any existing instances are terminated. Frame will then continue to create the remaining new VMs for each Instance Pool up to the Max Instances setting. This results in a quicker publish; however, it can result in a temporary reduction in the number of instances for each Instance Pool.
- **Test Publish**: This feature allows you to test Launchpad functionality and Sandbox changes in your Frame account before committing your changes to your production environment.

> **Publishing requires capacity**
>
> Before publishing, you will need to set your production capacity. Setting your production capacity specifies the amount of VMs you would like to publish your Sandbox image to. If you are not familiar with this, you can read more about system capacity and elastic instance management in our documentation here.If there are no instance types with a max set to at least 1, **publishing will be disabled**.

Fundamentals

A **Publish** pushes any changes and configurations made to the Sandbox image to the production (or test) instances and, in turn, to the end users accessing your Frame-managed workload VMs.

image.png

Initiating a Publish

Once your Sandbox is configured as desired and you're ready to publish, follow the steps below:

1. Navigate to the **Sandbox** page of your account Dashboard and ensure your Sandbox is powered on.
2. Click **Publish** in the top right corner of the Sandbox panel. A confirmation dialog will appear.

   Are you sure you want to continue?

3. Click **Publish** to confirm. The Sandbox panel will update and show a status of `PUBLISHING`. Progress updates about the publish are displayed at the bottom of the Sandbox card.

   Sandbox in PUBLISHING status

4. The status will return to `STOPPED` once the publish is complete. You can also see the status of your publish by clicking on your tasks (next to the bell icon in the upper right corner of your console) or by navigating to the Notification Center page accessible from the sidebar of the Dashbaord.

That's it! Now that the publish is complete, all *production instances* have been updated with the latest image from the Sandbox.

Cancelling a Publish

Cancel Publish gives administrators the ability to cancel or abort an ongoing Publish or Test Publish task.

With this feature, administrators can cancel a Publish that has been accidentally initiated or a publish that is consuming more time than usual.

> You may cancel a publish up **until the time Frame Platform begins creating production or test instances** (depending on whether you invoked a Publish, Quick Publish, or a Test Publish, respectively).

From Sandbox

To cancel an ongoing Publish from the Sandbox, once your Sandbox is in the Publishing state, go to the Sandbox page and under the kebab menu, the **Cancel Publish** option can be selected:

Dashboard > Sandbox - Cancel Publish

From Notification Center

To cancel an ongoing Publish or Test Publish from Notification Center, once your Sandbox is in the Publishing state, follow the steps:

1. Navigate to the Notification Center page of your account Dashboard.
2. On the Task tag, click on the ellipsis listed next to the Publishing Sandbox to Production task and choose **Cancel**.

3. Choose “Yes” on the next screen.

4. A notification will appear on the upper right-hand side stating the task was canceled.

Troubleshooting

If the publishing Sandbox to production task status is not updating, reload or refresh the page in your browser for the current status.

Advanced Publishing

In general, we strongly recommended that customers publish during off-peak hours whenever possible.

Publish

By default, running a regular Publish will create new VMs based on the Max Instances specified within Capacity for each configured Instance Pool. Once all new VMs are created, existing VMs will be terminated and new user sessions will start utilizing the new VMs. For public cloud Accounts, newly created VMs are powered on and ready for use immediately after creation. For AHV Accounts, newly created VMs remain powered off and unavailable for hosting sessions until existing VMs are completely terminated.

Quick Publish

When Quick Publish is enabled (default for AHV Accounts), Frame will create new VMs within each Instance Pool up to the specified amount (10, by default) **before any existing instances are terminated**. Once the specified amount of new VMs are created for a given Instance Pool, they will be powered on and immediately made available for new sessions and Quick Publish will be considered complete. Once the Quick Publish process is complete, all other existing VMs will then be terminated and will no longer be available for hosting user sessions. Frame will then continue to create the remaining new VMs for each Instance Pool up to the Max Instances setting.

Because Quick Publish temporarily reduces the effective max instance capacity, **it is generally not recommended for public cloud Accounts**.

For AHV Accounts, enabling Quick Publish is generally recommended as it eliminates downtime during a publish by making a smaller pool of new VMs immediately available for user sessions while the larger pool of new VMs are created and powered on. It is recommended that Quick Publish is configured to equal the maximum expected number of new user sessions per hour during off-peak hours of your largest Instance Pool (if this number is not known, start with a value equal to 10% of your Max Instances setting). Customers should ensure that their AHV Cluster is properly sized to support the additional number of powered-on VMs created during the Quick Publish process.

> **Reminder**
> **By default, all AHV-based accounts use the quick publish function**. The default number of production instances created on publish is 10. If you wish to override this number, follow the instructions below.

1. From your account Dashboard, navigate to the **Settings** page. Under the *General* tab, **enable quick publish** as shown below.

2. Once enabled, you have the option to set the number of production instances you would like to be created on each publish. Smaller batches are faster, we recommend 5-10.

Click the **Save button** in the upper right corner of your Dashboard to apply your changes.

> If the min value in your capacity settings is set to less than the quick publish value specified, the quick value publish settings are ignored and a regular publish is performed.

That's it! You have successfully enabled quick publish for your Frame account. Any publish operations initiated from this point forward will be Quick Publishes.

Test Publish

Test Publishing gives administrators the ability to test their updated Sandbox image in a “Test Instance Pool” which is **separate from their production instances**. This gives administrators the option to alter the instances in an isolated environment, completely identical to production, without concern of interrupting access to the normal production instances. Test publishes can easily be rolled back via the restoration of a backup, or promoted to the active published configuration, depending on the results.

Before a test publish, you will need to set your test capacity. Setting your test capacity specifies the amount of VMs you would like to publish your Sandbox image to. If you are not familiar with this, you can read more about system capacity and elastic instance management in our documentation here.

1. In your Frame Account Dashboard under the **Settings** tab, **Enable Test Publish**. Click the **Save** button to apply the change.