Trellix Intelligent Sandbox 5.2.x Migration Guide
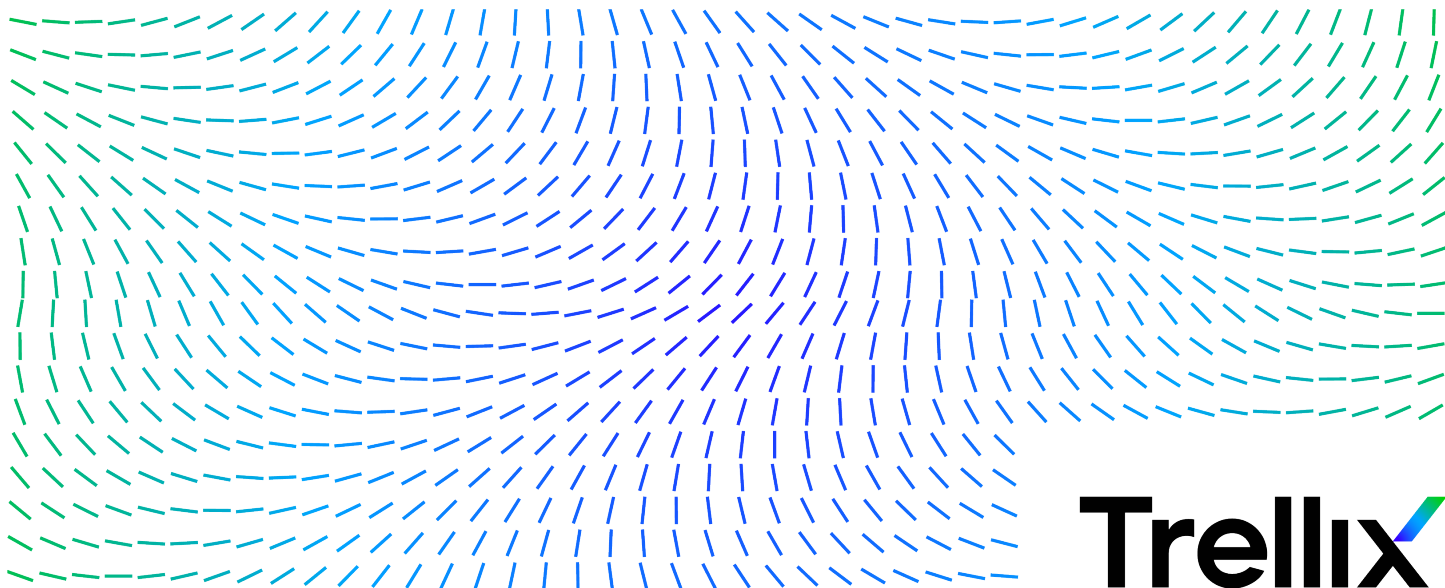
Contents

Migration overview

With every new release, **Trellix Intelligent Sandbox** is optimized for improved performance and enhanced security through kernel and RPM file changes. This migration guide helps you migrate your **Intelligent Sandbox** software, both physical and virtual, to **5.2**.

During migration, the operating system of your appliance is updated with the **Intelligent Sandbox** software. The migration process includes the following:

- All your data and configurations are backed up
- Operating system installation
- Data restoration
- Installation of the **Intelligent Sandbox 5.2** software.

Whereas, during an upgrade, only your **Intelligent Sandbox** software is updated.

Who is this document for?

If you are currently using version 4.10, 4.12, 4.14, or 5.0, use this document to migrate to **Intelligent Sandbox 5.2**.0.

For more information, see Migration criteria.

ⓘ **Attention**

Intelligent Sandbox 5.2 is not available for Microsoft Azure.

What are backed up during the migration process?

During migration, all data present in your existing **Trellix Intelligent Sandbox Appliance** is backed-up. After data back up, the installer automatically installs the operating system, restores the backed-up data, and installs the latest **Intelligent Sandbox** software.

The following are backed up:

- All databases
- Blacklist and whitelist database
- **McAfee ePO** Host Operating System information
- All configurations and certificates
- Results of all previously analyzed samples.
- All Virtual Machine Images present in your **Trellix Intelligent Sandbox Appliance**.
- All sample pending for analysis.
- All logs.

Migration criteria

To successfully migrate your physical or virtual appliance to **Intelligent Sandbox 5.2**.0, it is important that you review the migration criteria.

✎ **Note**

> If you migrate using the migration package, all your data and configurations are backed up and then restored.

Appliance	Upgrade path
• Advanced Threat Defense 5.0.x • Virtual Advanced Threat Defense 5.0.x (ESXi & HyperV)	5.0 » 5.2
• Advanced Threat Defense 4.14.x • Virtual Advanced Threat Defense 4.14.x (ESXi & HyperV)	4.14.x » 5.0 » 5.2
• Advanced Threat Defense 4.12.x • Virtual Advanced Threat Defense 4.12.x (ESXi & HyperV)	4.12.x » 5.0 » 5.2
• Advanced Threat Defense 4.10.x • Virtual Advanced Threat Defense 4.10.x (ESXi & HyperV)	4.10.x » 4.14.x » 5.0 » 5.2

Migration packages

Depending on the current version of **Intelligent Sandbox** on your appliance ensure that you download the right installation package.

The migration package is available for download from the McAfee download site.

1. Log on to https://secure.mcafee.com/apps/downloads/my-products/login.aspx?region=us with your grant number.
2. Download the correct migration package:

Appliance	Package name
Trellix Intelligent Sandbox physical (**ATD-3000/3100/3200** or **ATD-6000/6100/6200**) or virtual appliance	**migration-5.2.X.X.XXXXX.msu**

.

Migration process

We have created a migration package that allows you to migrate your physical or virtual appliance to **Intelligent Sandbox 5.2**. The package takes care of:

- Backing up your data and configurations
- Installing the OS
- Restoring the backed up data
- Installing the latest **Intelligent Sandbox** software.

🖉 **Note**

The migration takes minimum of 60-90 minutes to finish. However, depending on the number of records in your database and the total number of VMs to be created, it might take longer to finish. You can monitor the migration state using the RMM console for appliances or by logging into ESXi.

Precautions

This section describes the precautions to be considered during **Intelligent Sandbox** migration. Make sure that you adhere to these precautions to avoid migration failures.

- While using migration package, make sure that no USB storage device with a valid **Intelligent Sandbox** installer is connected to the **Intelligent Sandbox** Appliance. During pre-migration checks, if such a USB device is detected, you are prompted to remove it, and the migration will not continue.
- The migration requires several sanity checks with other steps, such as system backup, operating system installation, and restoration. We recommend that you perform the migration during downtime.

  ⊘ **Warning**

  Make sure that **Intelligent Sandbox** does not receive files for analysis during migration, through manual or managed product submissions. During migration, analysis and submissions could fail or timeout.

- During the migration process, do not address any prompts. The migration package is equipped to automatically address these prompts.
- Avoid force reboot of the system when the migration is in progress.

Migrate to Intelligent Sandbox 5.2.0

You can directly migrate to **Intelligent Sandbox 5.2**.0 using the migration package.

Task

1. **Download the migration package from the download site and upload it through SFTP using atdadmin account to your Intelligent Sandbox appliance.**
2. **Log on to your Intelligent Sandbox console, then navigate to Manage → Image & Software → Software.**
3. **In System Software, select the migration package from the drop-down list, then click Install.**

> 💡 **Tip**
>
> You need not select **Reset Database**, as this option is ignored during the migration process.

Monitor the migration progress and pre-check status from your Remote Monitoring and Management (RMM) or **Intelligent Sandbox** Serial Port.

Results

Your migration has now begun.

- The migration process begins with pre-checks. The time required to complete the pre-checks depends on your disk space and the number of records in your database.
- After the pre-checks are complete, the appliance reboots. The appliance reboots thrice during the entire course of the migration.
- Then, your data and configurations are backed up followed by the installation of the:
  - Operating system
  - **Intelligent Sandbox 5.2**.0 software
- After the migration is complete, you will see the logon screen.
  - Use your existing user name and password to log on to **Intelligent Sandbox**.
  - Verify the software version and VM creation status.

> 📝 **Note**
>
> You need to apply language pack after migration.

Migrate using the command line interface

You can also run the migration from the command line interface (CLI).

Task

1. **Download the migration package from the download site and upload it through SFTP using atdadmin account to your Intelligent Sandbox appliance.**
2. **Log on to the Intelligent Sandbox CLI as `cliadmin`.**
3. **Enter the following command, then press Enter:**

```
install msu <migration package.msu> 0
```

Replace `<migration package.msu>` with the file name of the migration package.

Migrate the nodes in cluster

On an **Intelligent Sandbox** cluster setup, if you choose to migrate to **Intelligent Sandbox 5.2**.0, ensure that you migrate all the nodes in the cluster.

Task

1. **In a typical load-balancing scenario, first migrate the backup node.**
   Post migration, the node remains a part of the cluster, however due to version mismatch incoming samples are not submitted to this node. The samples are distributed only between Primary and Secondary nodes. The status column of Backup node in the Load-balancing page displays the following message: **Node is on different software version**.
2. **Migrate 50 percent of the secondary nodes.**

   🖉 **Note**

   Migrate the Primary node only after you have migrated 50 percent of the secondary nodes.

3. **Migrate the Primary node.**
   Since the Primary node remains down during migration, Backup node takes over the Active role and distributes the incoming samples between Backup node (Active) and the migrated secondary nodes. Even after the Primary node is migrated, the Backup node continues to be in Active role.
4. **Migrate the remaining secondary nodes.**