



**PROXEDO**

**API SECURITY**

# Proxedo API Security based on VM environment

Migration manual from 4.3.0 to 4.4.0

*Copyright (C) Balasys IT Ltd. 4.4.0, 2023-05-03*

Copyright © 2019 Balasys IT Ltd.. All rights reserved. This document is protected by copyright and is distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Balasys.

This documentation and the product it describes are considered protected by copyright according to the applicable laws.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com))

Linux™ is a registered trademark of Linus Torvalds.

Windows™ 10 is registered trademarks of Microsoft Corporation.

The Balasys™ name and the Balasys™ logo are registered trademarks of Balasys IT Ltd.

The Proxedo™ name and the Proxedo™ logo are registered trademarks of Balasys IT Ltd.

AMD Ryzen™ and AMD EPYC™ are registered trademarks of Advanced Micro Devices, Inc.

Intel® Core™ and Intel® Xeon™ are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

All other product names mentioned herein are the trademarks of their respective owners.

#### **DISCLAIMER**

Balasys is not responsible for any third-party websites mentioned in this document. Balasys does not endorse and is not responsible or liable for any content, advertising, products, or other material on or available from such sites or resources. Balasys will not be responsible or liable for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through any such sites or resources.

2023-05-03

# 1. Introduction

This guide describes the necessary steps and commands to upgrade PAS instance from version 4.3.0 to 4.4.0.

There are four main stages to describe the different phases and scenarios of the upgrade.

1. Creating a backup for safety
2. Upgrading a single node setup
3. Upgrading a multi node setup
4. Restoring the pre-upgrade state

## 2. Creating a backup for safety

Before starting the upgrade process, make sure there is a backup to which the current state of the actual PAS setup can be restored.

The following steps describe how to create a backup of an actual configuration manually.



All instructions need to be executed on the management node even in case of a multi node setup.



The password for the management component's admin user will be necessary to be able to backup the running configuration.



This upgrade includes an operating system upgrade. For this reason it is also recommended to create a backup of the state of the PAS nodes if that is possible. Since backing up nodes highly depends on their environment, it is excluded from this guide.

### 2.1. Bootstrap configuration

1. Log in to `pas` user by running `sudo -iu pas`.
2. Save the following configuration files on the node in a zip file:
  - `/opt/balasy/etc`
  - `/opt/balasy/.ssh` for a multi node setup
  - Parts of the automated core deployment tool:
    - `/opt/balasy/usr/share/automation/deploy-core.yml`
    - `/opt/balasy/usr/share/automation/host_vars`
    - `/opt/balasy/usr/share/automation/inventory.yml`
    - `/opt/balasy/usr/share/automation/roles/deploy-core/vars/main.yml`

Example command to compress bootstrap files in a single node setup

```
zip --recurse-paths bootstrap-config.zip --symlinks \
  /opt/balasy/etc/ \
  /opt/balasy/usr/share/automation/{deploy-core.yml,host_vars,inventory.yml} \
  /opt/balasy/usr/share/automation/roles/deploy-core/vars/main.yml
```

Example command to compress bootstrap files in a multi node setup

```
zip --recurse-paths bootstrap-config.zip --symlinks \
  /opt/balasy/.ssh/ \
  /opt/balasy/etc/ \
  /opt/balasy/usr/share/automation/{deploy-core.yml,host_vars,inventory.yml} \
  /opt/balasy/usr/share/automation/roles/deploy-core/vars/main.yml
```

## 2.2. Creating a backup of the running configuration

1. Log in to the Web UI as admin user and navigate to the *Configuration Backup* page from the top bar.
2. On the *Configuration Backup* page select *Running* from the *Export configuration* dropdown menu.

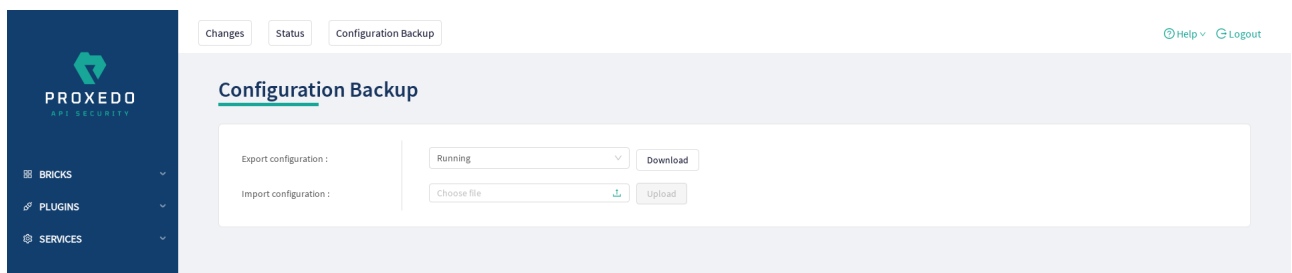


Figure 1. Backup and restore services with Proxedo API Security configuration

3. To export the running configuration, press the *Download* button. This will save the running configuration to a file named `running-config-backup.zip` in the working directory.



Save both files (`bootstrap-config.zip` and `running-config-backup.zip` displayed in the examples) to a backup server.

To restore the backup, follow the instructions in section [Restoring the pre-upgrade state](#).

## 3. General notifications

During the upgrade from PAS 4.3.0 to 4.4.0, an operating system upgrade is necessary from Ubuntu 18.04 to 22.04. Upgrading the host OS is not described in this guide. The rest of the instructions assume that they are carried out on an Ubuntu 22.04 machine and that the backup is available. They will not presume that the old running PAS is available, so that the upgrade can be carried out on the same machine if necessary.

In case of a multi node setup, both machines are assumed to be upgraded to Ubuntu 22.04.

## 4. Upgrading a single node setup

This section describes how to upgrade PAS in a single node setup. In case any problem occurs during the upgrade and the version 4.3.0 needs to be restored, follow the instructions in section [Restoring the pre-upgrade state](#).

## 4.1. Prerequisites

The following requirements need to be met before carrying out the upgrade process:

- The management machine is upgraded to Ubuntu 22.04
- Both the bootstrap and the running configuration are available on the new node
- The new Debian packages are downloaded and available for installation on the node:
  - proxedo-api-security\_4.4.0\_all.deb
  - proxedo-api-security-mgmt\_4.4.0\_all.deb
  - proxedo-api-security-storage\_4.4.0\_all.deb

## 4.2. Upgrade steps

1. Install the new Proxedo API Security packages as `root` user.
  - Use the simplified installer windows for a directed and easier way of installing the PAS packages.
  - Follow the installer's instructions to configure a new PAS instance. For detailed instructions, refer to section *Standalone setup* in *Proxedo API Security based on VM environment: Administration Guide*.
2. Log in to `pas` user by executing `sudo -iu pas`. Carry out the following operations as `pas` user.
3. Run the update command for each component:
  - `pas-update` for core
  - `pas-mgmt-update` for management
  - `pas-storage-update` for storage
4. Run the `checkconfig` command for each component for which it is available:
  - `pas-mgmt-checkconfig` for management
  - `pas-storage-checkconfig` for storage
5. Copy the license file to `/opt/balasy/etc/pas/license.txt`.
6. Start all the components by running `systemctl start proxedo-api-security-mgmt proxedo-api-security`
7. Run `pas-mgmt-upgrade-config convert-config --config running-config-backup.zip` in the directory where the backup of the running configuration is stored. It will convert the old running configuration to be compatible with the new version. The new configuration will be saved as `running-config-backup.upgraded-to-4.4.0.zip`.
8. Run `pas-mgmt-upgrade-config post-upgrade --config running-config-backup.upgraded-to-4.4.0.zip --config-apply-timeout 20` in the same directory where the configuration conversion step was performed. Follow the instructions of the script to complete.

## 5. Upgrading a multi node setup

This section describes how to upgrade PAS in a multi node setup. In case any problem occurs during the upgrade and the version 4.3.0 needs to be restored, follow the instructions in section [Restoring the pre-upgrade state](#).

### 5.1. Prerequisites

The following requirements need to be met before carrying out the upgrade process:

- Both the management and the core machines are upgraded to Ubuntu 22.04

- Both the bootstrap and running configuration are available on the new management node
- The new Debian packages are downloaded and available for installation on the management node:
  - proxedo-api-security\_4.4.0\_all.deb
  - proxedo-api-security-mgmt\_4.4.0\_all.deb
  - proxedo-api-security-storage\_4.4.0\_all.deb

## 5.2. Upgrade steps

Execute all steps on the management node.

1. Install the new Proxedo API Security packages locally as `root` user.



The simplified installer is designed to help single node installation. Ignore all questions asked by the installer during the upgrade and select "No" where possible. Ignore any questions asked twice and any error prompts.

2. Log in to `pas` user by executing `sudo -iu pas`. Carry out the following operations as `pas` user.
3. Restore the bootstrap configuration created from the old version by running `unzip -u -o /path/to/bootstrap-config.zip -d /.`

*Example bootstrap configuration restore command and output*

```
$ unzip -u -o /path/to/bootstrap-config.zip -d /
Archive:  bootstrap-config.zip
  creating: /opt/balasy/etc/
  creating: /opt/balasy/etc/ha/
 inflating: /opt/balasy/etc/ha/config.yml
  creating: /opt/balasy/etc/mgmt/
 extracting: /opt/balasy/etc/mgmt/users.htpass
 inflating: /opt/balasy/etc/mgmt/config.yml
  creating: /opt/balasy/etc/storage/
[...]
```

4. Update the `DOCKER_IMAGE_TAG` variable to 4.4.0 in all `docker-compose.conf` files:
  - `/opt/balasy/etc/infrastructure/pas/docker-compose.conf` for core
  - `/opt/balasy/etc/infrastructure/mgmt/docker-compose.conf` for management
  - `/opt/balasy/etc/infrastructure/storage/docker-compose.conf` for storage
5. Run `pas-mgmt-upgrade-config convert-config --config running-config-backup.zip` in the directory where the running configuration is available. It will convert the old running configuration to be compatible with the new version. The new configuration will be saved as `running-config-backup.upgraded-to-4.4.0.zip`.
6. Update the configuration of the automated deployment tool.
  - a. At `/opt/balasy/etc/automation/common_vars.yml`
    - Update the `storage_deb_path` to the new `.deb` file.
    - Update the `core_deb_path` to the new `.deb` file.
    - Update the `common.docker.PAS_IMAGE_TAG` to 4.4.0.

Example extract of values for the updated attributes

```
storage_deb_path: /tmp/proxedo-api-security-storage_4.4.0_all.deb
core_deb_path: /tmp/proxedo-api-security_4.4.0_all.deb
common:
  docker:
    PAS_IMAGE_TAG: 4.4.0
```

7. Run the update command for each component:
  - `pas-update` for core if core is also run on the management node
  - `pas-mgmt-update` for management
  - `pas-storage-update` for storage
8. Run the `checkconfig` command for each component for which it is available:
  - `pas-mgmt-checkconfig` for management
  - `pas-storage-checkconfig` for storage
9. Copy the license file to `/opt/balasy/etc/pas/license.txt`.
10. Start the *local* PAS management and storage components.
11. If HA is required, also start the *local* HA and core components.
12. Make sure the automated core deployment tool has access to a user on the remote VM. For details how to set that up, please refer to section *Configuring multi-node setup in Proxedo API Security based on VM environment: Administration Guide*.
13. Start the *remote* core and storage components by running `pas-mgmt-deploy-core --deploy-core`.
14. Run `pas-mgmt-upgrade-config post-upgrade --config running-config-backup.upgraded-to-4.4.0.zip --config-apply-timeout 20` in the same directory where the conversion of configuration was performed. Follow the instructions of the script to complete.
15. If HA is required, also start the *remote* HA component by running `pas-mgmt-deploy-core --deploy-ha`.

## 6. Restoring the pre-upgrade state

### 6.1. Cleaning up to pre-upgrade state

1. Stop all PAS services on *all nodes*.
  - `systemctl stop proxedo-api-security` for core
  - `systemctl stop proxedo-api-security-mgmt` for management
  - `systemctl stop proxedo-api-security-storage` for storage
2. Remove PAS packages as `root` user on *all nodes*. Remove packages only from those nodes where they are installed.
  - `apt remove --purge proxedo-api-security` for core
  - `apt remove --purge proxedo-api-security-mgmt` on management
  - `apt remove --purge proxedo-api-security-storage` on storage
3. Remove the `pas` user by running `userdel --force --remove pas`.

## 6.2. Restoring the configuration to pre-upgrade state



This upgrade includes an operating system upgrade. If PAS 4.4.0 is installed on the same node, and therefore the new supported version of Ubuntu is installed, the backup should start with restoring the node to the old operating system.

All instructions need to be executed on the management node.

1. Install PAS version 4.3.0 packages.
2. Log in to `pas` user by running `sudo -iu pas`.
3. Copy the files saved during the backup to the `pas` user's home directory.

### 6.2.1. Bootstrap configuration



It is important to run all commands as `pas` user to prevent from accidentally overwriting system files.

1. Unzip the saved bootstrap configuration files in the `/opt/balasy` directory as `pas` user by running `unzip -u -o bootstrap-config.zip -d /`.

*Example bootstrap configuration restore command and output*

```
$ unzip -u -o bootstrap-config.zip -d /
Archive:  bootstrap-config.zip
  creating: /opt/balasy/etc/
  creating: /opt/balasy/etc/ha/
 inflating: /opt/balasy/etc/ha/config.yml
  creating: /opt/balasy/etc/mgmt/
 extracting: /opt/balasy/etc/mgmt/users.htpass
 inflating: /opt/balasy/etc/mgmt/config.yml
  creating: /opt/balasy/etc/storage/
[...]
```

2. Start all PAS services including the HA component if previously an HA setup was run.
3. If a multi node setup is being restored, also deploy the remote node by running the remote deployment command.

```
pas-mgmt-deploy-core --deploy-core
```

4. If an HA setup is run, also start the HA service on the remote node.

```
pas-mgmt-deploy-core --deploy-ha
```

### 6.2.2. Restoring the running configuration

1. Log in to the Web UI as the administrator user and navigate to the *Configuration Backup* page from the top bar.



- To import the running configuration, on the *Configuration Backup* page choose a configuration file from the computer and press *Upload* to upload the configuration.

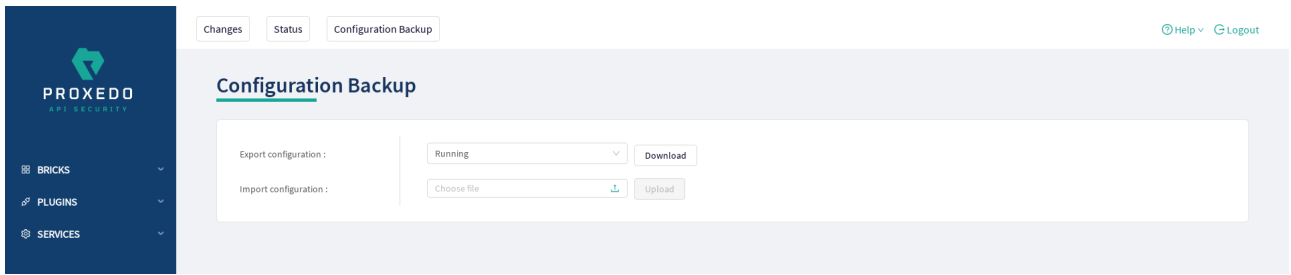


Figure 2. Backup and restore services with Proxedo API Security configuration

- Apply the configuration.