



# AppViewX Application Upgrade Guide

---

Version: 2022.1.0 FP5

# Copyright AppViewX, Inc.

**Copyright © 2025 AppViewX, Inc. All Rights Reserved.**

This document may not be copied, disclosed, transferred, or modified without the prior written consent of AppViewX, Inc. While all content is believed to be correct at the time of publication, it is provided as general-purpose information. The content is subject to change without notice and is provided “as is” and with no expressed or implied warranties whatsoever, including, but not limited to, a warranty for accuracy made by AppViewX. The software described in this document is provided under written license only, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. Unauthorized use of software or its documentation can result in civil damages and criminal prosecution.

## **Trademarks**

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

## **Contact Information**

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: [info@appviewx.com](mailto:info@appviewx.com)

Web: [www.appviewx.com](http://www.appviewx.com)

# Contents

Preface.....	4
Revision History.....	4
About this Guide .....	4
Audience.....	4
Third-Party Software Acknowledgements.....	4
Text Conventions.....	4
<b>Chapter 1. Prerequisites.....</b>	<b>5</b>
<b>Chapter 2. Upgrading AppViewX to 2022.1.0 FP5.....</b>	<b>8</b>
<b>Chapter 3. Avoiding Upgrade Errors.....</b>	<b>15</b>
Elastic Restore.....	16
Enabling HSM.....	17
Configuring Fortanix.....	18
Configuring Utimaco.....	19
Verifying/Modifying HSM Configuration for Private Key Encryption.....	20
<b>Chapter 4. Troubleshooting for Setup Limitations.....</b>	<b>22</b>

# Preface

## Revision History

Revision	Description	Date
v1.0	Application Upgrade Guide for Release 2022.1.0 FP5	May 2025

## About this Guide

The document describes the steps to upgrade AppViewX to the latest version 2022.1.0 FP5

## Audience

This guide is intended for AppViewX's customers deploying its products on Windows-based machines.

## Third-Party Software Acknowledgements

This section serves as a placeholder to document the third-party components referenced in this guide, along with their associated trademark information.

For example,

- This document includes software details developed by VMware, Inc. ([www.vmware.com](http://www.vmware.com)).

## Text Conventions

The following text conventions are used in this document:

Convention	Description
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>codeblock</code>	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

# Chapter 1: Prerequisites

## General Prerequisites

1. If you are currently using CentOS operating system, refer to the [CentOS Migration Guide](#).
2. Nodes must have the following OS:
  - RHEL 8.7, 8.8, 8.10, 9.5
  - Ubuntu 20.04
3. Keep the following file locations ready -
  - old installer file location, for example - `/home/appviewx/FP2/appviewx_kubernetes`
  - installed location, for example - `/home/appviewx/appviewx_cluster`
4. Location to save the new installer file - `/home/appviewx/appviewx/Application_upgrade` (Assign the folder name as required).
5. To list the nodes in the cluster, execute the command below and save the output for further reference.

```
kubectl get nodes --show-labels
```



**Note:** If custom labels are detected add them to the `custom_changes.yaml` file. Refer to the chapter *Adding Custom Pod Configuration* of the section **Monitoring and Maintaining AppViewX** in the **Install, Upgrade, and Maintenance Guide**.

6. To get the status of HPA, execute the command below and save the output for further reference

```
kubectl get hpa
```

7. Keep a backup of the iControl jar files available at location - `/home/appviewx/appviewx/appviewx_dependencies/external_libs/iControl-13.1.0.jar` for iControl to be done after the upgrade.
8. Check for any other custom changes that may have been done specifically for the customer.
9. Check the enabled plugins in `appviewx.conf` file of the old installer (previous version), in case there are plugins that are not present but are required to be installed in the latest versions, please add them, example
  - `avx_pkiaas_cert_ocsp_generator`
  - `avx_pkiaas_cert_ocsp_server`
  - `avx_platform_hsm`

## Updating the Kernel version

Following the upgrade to **Kubernetes v1.32.2**, the `kubeadm init` setup is no longer compatible with **older Linux kernel versions**. This is primarily due to enhanced reliance on **cggroups** (control groups), a Linux

kernel feature that manages resource isolation and allocation. This incompatibility typically affects nodes running older operating system versions, particularly those in the **RHEL 8 series** (e.g., 8.5, 8.6, or even 8.10), depending on the specific kernel version present on the node.

Figure 1. Error log from kubernetes

```

[0m [small_resource.kube_master_initialize_node@] (remote-exec): [CHECKING Host Key: false]
[0m [small_resource.kube_master_initialize_node@] (remote-exec): Connected
[0m [small_resource.kube_master_initialize_node@] (remote-exec): [sudo] password for appviewx: 00d02 02:29:45.012073 1891563 common.go:181] your configuration file uses a deprecated API spec: "kubeadm.k8s.io/v1beta3" (kind: "Cluster
Configuration"): Please use 'kubeadm config migrate --old-config old.yaml --new-config new.yaml' which will write the new, similar spec using a newer API version.
[0m [small_resource.kube_master_initialize_node@] (remote-exec): [WARNING FileExisting-tc]: tc not found in system path
[0m [small_resource.kube_master_initialize_node@] (remote-exec): [WARNING SystemVerification]: cgroups v1 support is in maintenance mode, please migrate to cgroups v2
[0m [small_resource.kube_master_initialize_node@] (remote-exec): [ERROR SystemVerification]: kernel release 4.18-0-k25.1.1.el8.x86_64 is unsupported. Recommended LTS version from the 4.x series is 4.19. Any 5.x or 6.x versions are
also supported. For cgroups v2 support, the minimal version is 4.15 and the recommended version is 5.8.
[0m [small_resource.kube_master_initialize_node@] (remote-exec): [preflight] If you know what you are doing, you can make a check non-fatal with '--ignore-preflight-errors=...'
[0m [small_resource.kube_master_initialize_node@] (remote-exec): To see the stack trace of this error, execute with '--vv' or higher
[0m [small_resource.kube_master_initialize_node@] Still creating... [10s elapsed] [0m [0m
[0m [small_resource.kube_master_initialize_node@] Still creating... [20s elapsed] [0m [0m

```

## Cgroups Overview:

Control Groups (cgroups) are a kernel-level feature that enables the limitation, prioritization, and isolation of resource usage (CPU, memory, I/O, etc.) among process groups. Kubernetes leverages cgroups extensively for container orchestration.

## Determining the Cgroups Version in Use:

To identify the active cgroups version on a Linux system, run the following command:

```
stat -fc %T /sys/fs/cgroup
```

- If the output is `tmpfs`, the system is using **cgroups v1**.

```

appviewx@ [redacted] :~$ stat -fc %T /sys/fs/cgroup
tmpfs
appviewx@ [redacted] :~$ ^C
appviewx@ [redacted] :~$ █

```

- If the output is `cgroup2fs`, the system is using **cgroups v2**.

```

groups: cannot find name for group id 1145011047
appviewx@ [redacted] :~$ stat -fc %T /sys/fs/cgroup
cgroup2fs
appviewx@ [redacted] :~$ █

```

## Kernel Version Requirements Based on Cgroups Version

Cgroups Version	Minimum Kernel Version	Recommended Kernel Version
v1	4.19+	5.x or 6.x series
v2	4.15+	5.8 or later

To ensure compatibility with Kubernetes 1.32.2, it is recommended to validate and, if necessary, upgrade the Linux kernel version in accordance with the cgroups configuration of the host system.

To verify the kernel version, execute the command:

```
uname -r
```

```
appviewx@ [REDACTED] :~$ uname -r
5.4.0-153-generic
appviewx@ [REDACTED] :~$ █
```

### Solution provided:

Since the issue is not OS-specific, the prerequisite scripts now contain the generic checks during both the installation and application upgrade processes.

- If the system does not meet the minimum required kernel version, the installation will be blocked from proceeding.
- Additionally, if the system is using cgroups v1, a warning message will be displayed recommending an upgrade to cgroups v2 for improved compatibility and performance.

## Points to Remember when Upgrading to 2022.1.5

Know the following before proceeding with the upgrade.

1. If an external CA certificate is configured for kubernetes, the infra upgrade will overwrite the certificates.
2. A manual elastic restore must be performed post the upgrade. Post the application upgrade the back of the elastic search will be stored at the following location - `INSTALLER_PATH/appviewx_kubernetes/statistical_data_backup`. The steps for Elastic Restore are explained in the section [elastic restore](#)

## Chapter 2: Upgrading AppViewX to 2022.1.0 FP5

You can now upgrade to AppViewX version 2022.1.0 FP5 if you are currently using the following versions of AppViewX in RHEL (8.7, 8.8, 8.10, 9.5) or Ubuntu (20.04) OS:

- 2020.3.0 FP10-F11
- 2021.1.0 FP3
- 2022.1.0 FP1-FP4

1. Log in to the [release portal](#) and download the installer and addons file –
  - **appviewx\_kubernetes\_2022.1.5.tar.gz**
  - **appviewx\_kubernetes\_addons\_2022.1.5.tar.gz**
2. Create a new folder in the same location as the existing installer directory.

**Example:** `/home/appviewx/Application_upgrade/`

```
[~]$ pwd
/home/appviewx
[~]$ mkdir Application_upgrade
[~]$ cd Application_upgrade
[Application_upgrade]$ pwd
/home/appviewx/Application_upgrade
[Application_upgrade]$
```

3. Copy the installer file **appviewx\_kubernetes\_2022.1.5.tar.gz** into the new folder location `/home/appviewx/Application_upgrade/`.
4. Untar the installer file using the command below:

```
tar -xf appviewx_kubernetes_2022.1.5.tar.gz
```

After the command is executed, the **appviewx\_kubernetes** folder is created: `/home/appviewx/Application_upgrade/appviewx_kubernetes/`

5. Copy the **appviewx\_kubernetes\_addons\_2022.1.5.tar.gz** file to the **appviewx\_kubernetes** folder using the command:

```
mv appviewx_kubernetes_addons_2022.1.5.tar.gz appviewx_kubernetes/
```

6. Navigate to the **scripts** directory in the **appviewx\_kubernetes** folder (`/home/appviewx/Application_upgrade/appviewx_kubernetes`) using the command:

```
cd /home/appviewx/Application_upgrade/appviewx_kubernetes/scripts
```

The **scripts** folder contains the **appviewx.conf.template** file.

7. Update the [conf parameters in the appviewx.conf](#) file as mentioned in the Install and Upgrade Maintenance guide after copying the **appviewx.conf.template** file as **appviewx.conf**

To copy, use the command:

```
cp appviewx.conf.template appviewx.conf
```

OR

Skip the above step to use the conf merge feature as part of step 10b.



**Note:**

- For the complete list of the appviewx.conf file parameters refer the [Configuring the appviewx.conf File to Install Appviewx](#) section in the **Install and Upgrade Maintenance Guide**.

8. From the `/home/appviewx/ApplicationUpgrade/appviewx_kubernetes/scripts` directory execute the upgrade command below:

```
./upgrade.sh
```

9. Provide the input of the older installer directory and the directory where the application is currently installed.

```
[scripts]$ ./upgrade.sh
Enter the AppViewX old installer path: /home/appviewx/FP10/appviewx_kubernetes
Enter the AppViewX installed location: /home/appviewx/appviewx
```

After entering both inputs, the system checks for newly introduced conf file parameters.

10. You will now be prompted with the message about the presence of the conf file, answer Y/N as follows:
  - a. If the updated conf file is available in the installer folder, and you choose **Y**, the upgrade proceeds.

```
We found the appviewx.conf file so it will be used for the installation and conf file will not be merged from the existing cluster. Do you want
you proceed(Y/N): Y
EXISTING INSTALLATION PATH : /home/appviewx/appviewx/
/home/appviewx/Installer/appviewx_kubernetes/scripts
***** Fetching running db instance *****
mongodb-0
***** Fetching db list *****
DB list retrieved.
*****
admin appSession appviewx appviewxCA config connectedPlatform imageDetails local templateDB workFlowDB workFlowDBEngine
```

- b. If the updated conf file is available in the installer folder, and you choose **N**, the upgrade stops/exits.

```
We found the appviewx.conf file so it will be used for the installation and conf file will not be merged from the existing cluster. Do you want
you proceed(Y/N): N
Exiting..!
[appviewx@pe-lu-node27 scripts]$
```

To continue with the upgrade

- Edit the conf file and resume the upgrade.
- Delete the conf file from the installer location and resume the upgrade (the upgrade script will handle the merging of the new conf parameters).

11. Enter the appropriate value to alter the default value OR hit the enter key (*recommended*) to use the default value. An example is shown below.

```
Checking for newly introduced conf parameters...
=====
Please provide the appropriate input for SAAS_ENABLED
# Flag to check if saas enabled or on-prem
#####
# DO NOT CHANGE FOR ON-PREM #
#####
Default value for the parameter is : false

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value : █
```

- a. To enable msp, the default value is False. Hit the enter key to select the default value and continue.
- b. For the parameters HSM\_HOST and REDIS\_HOST enter the value as follows:

```
=====
Please provide the appropriate input for HSM_HOST
# Comma separated values of node hostnames in which HSM pods will be scheduled
# Note: Execute the command "hostname" in the node and add that output to this field
# IMPORTANT: (i) For single node AppViewX deployments add the IP address of the instance where AppViewX is installed.
# (ii) To ensure high availability in multiple DC deployments, It is recommended to add a minimum of one host per DC.
Default value for the parameter is : $(hostname)

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value : █
```

- i. If you have a single node, hit Enter for the default value or the IP address of the instance where AppViewX is installed.
  - ii. If you have a multi-node setup, you must enter one hostname per DC of the worker nodes.
- c. To configure the BACKUP\_CRONJOB\_SCHEDULE, enter the values in double quotes. For example, "0 4 \* \* \*" states that the cron job will run at 4:00 AM every day.
- d. To configure BACKUP\_CRONJOB\_RETENTION, enter an inter value. For example, 5, which means that the system will keep the last 5 backups and delete any older ones.
- e. To configure the SECONDARY\_DB\_BACKUP, set the value to true, if DB backup has to be taken from the secondary shared DB.
- f. To configure EXTERNAL\_GATEWAY\_HOST, enter one of the ingress host's hostname in which the external gateway is to be deployed.
- g. For SENTINAL\_DC enter the value as follows (only for 2-DC setup):
  - i. If it's not a 2-DC setup, enter any one of the DCs.
  - ii. If you have a multi-node 2-DC setup, enter the DC which has less number of redis instances than the other DCs.



**Note:** Ensure you read all the instructions specified in the conf parameters before entering the values.

12. The upgrade continues and the following operations are carried out during the process.

**a. Taking backups of mongo and vault**

```
Copied backup in installer node successfully. Location : /home/appviewx/hudson/appviewx_kubernetes/mongo_backup/mongo_backup_Thu_Jul_6_05_14_46_EDT_2023.tar.gz
Mongo backup has been completed.
/home/appviewx/hudson/appviewx_kubernetes/scripts
Vault Backup File: /home/appviewx/hudson/appviewx_kubernetes/vault_backup/vault_backup_Thu_Jul_6_05_14_56_EDT_2023
Vault backup has been completed.
Taking backup of /home/appviewx/appviewx/appviewx_dependencies/properties
/home/appviewx/hudson/appviewx_kubernetes/scripts
```


**b. Uninstalling the old version**

i. You will be prompted to enter the node password.

```
kubernetes setup is found. Uninstalling the existing setup
Please enter appviewx password of absecon:pe-iu-rhel-node07.lab.appviewx.net :
```

ii. After the uninstall is complete, you will be prompted to enter the password for the DC host.

```
Apply complete! Resources: 5 added, 0 changed, 0 destroyed.
Kube uninstall is successfull
Please wait while we extract the addons...
/home/appviewx/Application_upgrade/appviewx_kubernetes/scripts
Please enter appviewx password of .appviewx.net :
```

 **Note:**

i. In case of upgrade failures, resume the upgrade by executing the command:

```
/upgrade.sh
```

ii. In case of Infra upgrade failure, the script will prompt a question to clean the setup as shown below. Enter 'Y' (yes) to proceed with the clean-up.

```
Warning: Quoted type constraints are deprecated
on ../yaml/appviewx_vault/consul/deploy/chart_deploy.tf line 14, in variable "appviewx_dependent_check":
14:     type = "list"
Terraform 0.11 and earlier required type constraints to be given in quotes,
but that form is now deprecated and will be removed in a future version of
Terraform. To silence this warning, remove the quotes around "list" and write
list(string) instead to explicitly indicate that the list elements are
strings.
(and 4 more similar warnings elsewhere)
Error: error executing "/tmp/terraform_1469185875.sh": Process exited with status 1
Failed during infra upgrade
Please provide the input if you want to clean the setup (default is N): Y/N y
Cleaning up the setup.
```

**c. Time Sync (NTP/Chrony)**

```
Apply complete! Resources: 4 added, 0 changed, 0 destroyed.
-----
Validating Single Node Setup
-----
Valid Username      : appviewx
Valid IP address    : 192.168.145.15
Hostname matches   : pe-1u-rhel-node07.lab.appviewx.net
Valid enabled plugins : Yes
Duplicate plugins   : No
Valid Datacenters   : absecon
Valid Ingress host  : 192.168.145.15
-----
Do you want to configure the NTP/Chrony?[Yes|No](Recommended 'Yes' and 'No' if already configured):
```

- For a single node - Enter **No** as we do not have to sync time.
- For multi-node - If time sync is already configured before the upgrade then enter **No**. If the time sync for nodes has to be configured then enter **Yes**.

#### d. Installing the new version and restoring the backups

```
2023-07-06T09:34:26.149+0000 18900 document(s) restored successfully. 0 document(s) failed to restore.
Restoring completed
Mongo has been restored successfully
Backup file path is /home/appviewx/hudson/appviewx_kubernetes/scripts/../../vault_backup/vault_backup_Thu_Jul_6_05_14_56_EDT_2023
Vault Restore Script begins
AVX Installation path: /home/appviewx/appviewx/
Success! Data written to: transit/keys/uEynbUXcwm/config
Success! Data deleted (if it existed) at: transit/keys/uEynbUXcwm
Success! Data written to: transit/restore/uEynbUXcwm
configmap/avx-common-config replaced
Restarting the pods for the namespace absecon...
```

```
Successfully Updated DB with hash
Successfully restarted the pods
None
configmap/avx-common-config patched
configmap/avx-common-config patched
configmap/avx-common-config patched
configmap/avx-common-config patched
configmap/avx-common-config patched
configmap/avx-common-config patched
configmap/avx-common-config patched
Vault has been restored successfully

Started Plugins installation..
Labelling the HSM nodes
```



**Note:** In the case of Mongo restore, if the restore operation is stuck or takes more time than usual, then stop the installation process and increase Mongo's **wiredTiger** cachesize of the **mongodb** or **mongo-shardeddb statefulset**. (The **mongodb** is for single node setup and **mongo-shardeddb statefulset** is for multi-node setup). Use the commands below.

Single Node:

```
kubectl edit statefulset mongodb -n avx
```

Multi node:

```
kubectl edit statefulset mongo-shardeddb -n avx
```

Navigate to **MONGO\_CACHE\_SIZE** key value of the **env** field and increase the cache size value by 1 to 2 GB

```
env:
- name: MONGO_CACHE_SIZE
  value: "0.25"
image: mongo:4.2.18
imagePullPolicy: Never
```

After making the required changes run command `./upgrade.sh` to resume the upgrade.

**e. Merging the common config map**

```
=====
Take a backup of following files and remove the files:
/home/appviewx/hudson/appviewx_kubernetes/scripts/./infra/.vault_key_for_reference
/home/appviewx/appviewx/./appviewx_configuration
Remote/External backup setup has not been done.
To configure fill in the values under 'Configure the SFTP Transfer for Mongo and Vault backup' section of appviewx.conf and trigger ./sftp_transfer.sh.
Ensure /home/appviewx/appviewx/backup-server-cert directory has appviewx ownership in all nodes before triggering the sftp_transfer.sh script
(Ignore if directory not present).

Take backups of keys under /home/appviewx/appviewx/backup-server-cert for decrypting the backups in future.

In order to ensure optimal performance and stability of your system, we highly recommend that you regularly check for any available hotfixes for this Feature Pack.
To do so, please log in to our Release Portal and navigate to the section Plugins (https://release.appviewx.com/#plugins). Here, you will find information on any available hotfixes and instructions on how to download and apply them.
Application Upgrade has been completed

Merging common config map...
Merging common config has been completed
```

- f. After the installation is complete, take a backup of the below files and copy it to a secure location. Then, remove it from the installer location. The files are
  - <installer location>/infra/.vault\_key\_for\_reference
  - <installer location>/appviewx\_configuration

**13. Check the upgraded version and the pods running status.**

- a. To check the upgraded version, run the following:

```
kubectl get no
```

```
[ ~]$ kubectl get nodes
NAME                                STATUS    ROLES    AGE     VERSION
.appviewx.net                       Ready    control-plane  19h    v1.29.1
```

b. To check the pods running status, run the following:

```
kubectl get po -A

[ ~]$ kubectl get po -A
NAMESPACE      NAME                                                    READY   STATUS    RESTARTS   AGE
absecon        avx-commons-54885b9d88-vhxdc                          3/3     Running   0           12m
absecon        avx-config-server-6bb868f559-pkc2f                    3/3     Running   0           11m
absecon        avx-platform-core-c4dc4976-296dd                      3/3     Running   0           10m
absecon        avx-platform-logforwarding-5cff778655-txvvg           3/3     Running   0           12m
absecon        avx-platform-queue-bbdfd565c-jljvv                   3/3     Running   0           11m
absecon        avx-platform-report-generator-b7ff97c5d-wlwb8         2/2     Running   0           12m
absecon        avx-subsystems-6f584c6656-n5bsq                       3/3     Running   0           5m
absecon        avx-subsystems-6f584c6656-vgj5n                       3/3     Running   0           5m
absecon        avx-subsystems-sync-678d54df58-tjkwk                  3/3     Running   0           12m
absecon        avx-vendor-cert-network-discovery-74bdfcd76d-wpfhg    3/3     Running   0           12m
absecon        avx-vendors-7f6644d889-q5qtl                          3/3     Running   0           12m
absecon        avx-visual-page-builder-65f8c55b4f-mwzrq              2/2     Running   0           12m
avx-jobs       mongoutil-mongooseed-xwcqt                             0/1     Completed 0           20m
avx            avx-config-server-23.1.0.0-db-migration-x66h4         0/1     Completed 0           12m
avx            avx-crontab-5b576c4b59-tq9wc                          3/3     Running   0           12m
avx            avx-platform-core-23.1.0.0-db-migration-d48wf         0/1     Completed 0           12m
avx            avx-platform-gateway-6b6947746b-s8t66                 2/2     Running   0           3m16s
avx            avx-platform-queue-23.1.0.0-db-migration-kxs46        0/1     Completed 0           12m
avx            avx-platform-web-8496bdc97f-x4g24                     2/2     Running   0           11m
avx            avx-subsystems-23.1.0.0-db-migration-8hfpt            0/1     Completed 0           12m
avx            crypt-migration-job-hhzhg                              0/1     Completed 0           4m39s
avx            logs-daemon-bs9pw                                       2/2     Running   0           18m
avx            mongodb-0                                               2/2     Running   0           22m
avx            prune-pod-mg4kx                                         2/2     Running   0           12m
avx            redis-0                                                  4/4     Running   0           22m
avx            vault-0                                                  2/2     Running   0           19m
default       cryptutilencrypt-8t7mx                                 0/1     Completed 0           15m
istio-operator istio-operator-5b6f47d749-twmmb                       1/1     Running   0           24m
istio-system  istio-ingressgateway-5d7cb55c7f-sct97                 1/1     Running   0           24m
istio-system  istiod-74d6fc9995-wdr6l                               1/1     Running   0           24m
```

# Chapter 3: Avoiding Upgrade Errors

The following actions must be taken to avoid any post-upgrade errors, if they are applicable in your respective setup:

## 1. Loss of Mongo replica set priority configurations

During application upgrade, mongodb is freshly set up with the latest upgraded versions. The existing replicaset configurations such as replicaset priorities will not be taken ahead and hence have to be re-configured. High latency customers must perform the following step:

- a. Configure the parameters `OPTIMISE_ROUTING_FOR_LATENCY` and `PREFERRED_DEFAULT_DC` in the `appviewx.conf`
- b. Re-trigger the `plugins_install.sh` to change the configurations.

## 2. Custom changes

If the `custom_changes.yaml`, `custom_vm_args.conf` are present and updated in the custom changes, then the custom changes will be persistent. Any of the custom changes that may have been done specifically for the customer as noted in the prerequisites will not be present if the above mentioned files are not updated with this configuration.

## 3. External web cert is not upgraded

To update the external CA web certificate, execute the command below:

```
./appviewx.sh --update-web-cert
```

The following prompts will be displayed:

- Enter the absolute path of external cert file:
- Enter the absolute path of external key file:

Enter both the values to proceed. Once the cert upgrade is completed, restart the gateway and web.

4. Download the `icontrol.jar`, `axis.jar`, and `javax.xml.soap-api-1.4.0.jar` files and copy them to the `external_libs` directory. For details, refer to the section [iControl F5 Integration](#) of the *AppViewX Install, Upgrade and Maintenance Guide*.

## 5. Setting the `ELASTIC_ENABLE` as True in the Statistics Configuration

There are two ways to do it, choose from either the command prompt (a) or from the management console UI (b).

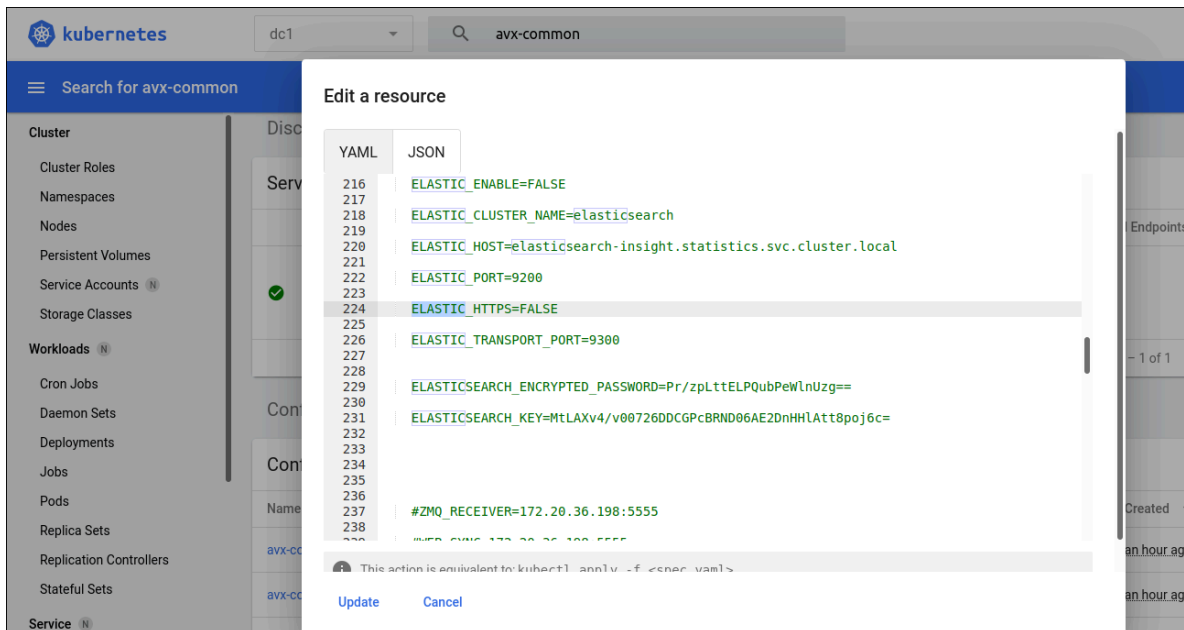
- a. Execute the command

```
kubect! edit configmaps -n <Datacenter1>
```

Search for the keyword as Elastic and set ELASTIC\_ENABLE as True and below params should have default values as below

```
ELASTIC_ENABLE=TRUE
ELASTIC_CLUSTER_NAME=elasticsearch
ELASTIC_HOST=elasticsearch-insight.statistics.svc.cluster.local
ELASTIC_PORT=9200
ELASTIC_HTTPS=FALSE
ELASTIC_TRANSPORT_PORT=9300
```

- b. Login to management console >> Search for the namespace with the configured DC >> Search for avx-common-config in config maps >> Click on Edit and search for Elastic >> Set as True and give as update as shown below.



- Elastic Restore
- Enabling HSM

## Elastic Restore

The script **elastic\_restore.py** is used for restore. To manually perform the elastic restore,

1. Navigate to the scripts directory.
2. Run the elastic\_restore.py script to restore the backup.

```
/home/appviewx/appviewx/appviewx_dependency/appviewx_addons/Python_Linux/bin/python elastic_restore.py elasticsearch_insight
```

- Script will ask for the backup tar which was created manually. Provide the absolute path of the backup tar.

```

[appviewx@pe-lu-node23 scripts]$ ./appviewx/appviewx_dependencies/appviewx_addons/Python/bin/python elastic_restore.py elasticsearch_insight
Please provide absolute path of statistical backup data tar: /home/appviewx/ApplicationUpgrade/appviewx_kubernetes/statistical_data_backup/elasticsearch_insight_backup_2023mar27_060346.tar.gz
kubectl exec -it elasticsearch-insight-0 -n statistics -- curl -XGET -u elastic:QPG7uXGGCHmmuXC localhost:9200/_snapshot/elasticbackup/_all?pretty
Defaulted container "elasticsearch-insight" out of: elasticsearch-insight, initialcontainer (init)

List of available snapshots:
1 : snapshot_2023mar24_075630
2 : snapshot_2023mar24_085927
3 : snapshot_2023mar27_055337
4 : snapshot_2023mar27_055540
5 : snapshot_2023mar27_060345
6 : snapshot_2023mar27_071346
7 : snapshot_2023mar27_075037
Enter the snapshot you want to restore :snapshot_2023mar24_075630
Defaulted container "elasticsearch-insight" out of: elasticsearch-insight, initialcontainer (init)

Current Indices in the cluster:
green open .security-7 wftbKwlvQveKzFbcIfGbpw 1 0 9 0 36.1kb 36.1kb
Defaulted container "elasticsearch-insight" out of: elasticsearch-insight, initialcontainer (init)

Indices in the snapshot:
- .security-7
- .ds-ilm-history-5-2023.03.24-000001
- .ds-.logs-deprecation.elasticsearch-default-2023.03.24-000001
*****Note*****
Open indices will be closed before restore can proceed
Enter the indices from above list that you want to restore(commas[,]separated) OR give all to restore all indices [Except security index]: .security-7,.ds-ilm-history-5-2023.03.24-000001,.ds-.logs-deprecation.elasticsearch-default-2023.03.24-000001
Defaulted container "elasticsearch-insight" out of: elasticsearch-insight, initialcontainer (init)

{"acknowledged":true,"shards_acknowledged":true,"indices":{".security-7":{"closed":true}}}
Defaulted container "elasticsearch-insight" out of: elasticsearch-insight, initialcontainer (init)

{"acknowledged":true,"shards_acknowledged":true,"indices":{".ds-ilm-history-5-2023.03.24-000001":{"closed":true}}}

```

- Script will list all the available snapshots that has date and time in the naming. Select the backup which you want to restore.
- Provide the details of the indices you want to restore (follow the screenshot above).

## Enabling HSM



**Note:** Refer this section only if you have upgraded from AppViewX v2020.3.0.

### Prerequisites

- To configure Fortanix and Utimaco, the **.so** file and **config** file must be present in the current Appviewx version.
  - The **.so** file is essential for communicating with the HSM using the PKCS11 interface.
  - The **config** file facilitates communication between the HSM and Appviewx.

After the successful upgrade, proceed with the steps below to enable HSM.

- Ensure the HSM pod is operational and running in the required datacenters and that the HSM node is specified in the appviewx.conf file, execute the following command:

```
kubectl get pods -A -o wide |grep hsm
```

- From the command line interface, navigate to the properties folder path `{APPVIEWX_INSTALLATION_PATH}/appviewx_dependencies/properties`

### For Fortanix

- a. Open the HSM file using the following command:

```
vi hsm
```

- b. Check and confirm if the HSM file has the following lines. If not, uncomment the following lines:

```
export FORTANIX_PKCS11_CONFIG_PATH= /appviewx/dependencies/hsm/fortanix/pkcs11.conf
```

```
echo "FORTANIX Config Path : $FORTANIX_PKCS11_CONFIG_PATH"
```

- c. If the file is edited, restart the **avx-platform-hsm** pod, using the following commands:

```
kubectl get pods -n <namespace>
```

```
kubectl delete pods -n <namespace> <PodName> --force
```

### For Utimaco

- a. Open the HSM file using the following command:

```
vi hsm
```

- b. Check and confirm if the HSM file has the following lines. If not, uncomment the following lines:

```
export CS_PKCS11_R2_CFG=/appviewx/dependencies/hsm/utimaco/cs_pkcs11_R2.cfg
```

```
echo "UTIMACO Config Path : $CS_PKCS11_R2_CFG"
```

- c. If the file is edited, restart the **avx-platform-hsm** pod, using the following commands:

```
kubectl get pods -n <namespace>
```

```
kubectl delete pods -n <namespace> <PodName> --force
```

3. Once the HSM pod is back to running state, login to AppViewX and navigate to **Platform > Vault & Security > HSM**.

4. Access the required HSM.

- [Configuring Fortanix](#)
- [Configuring Utimaco](#)
- [Verifying/Modifying HSM Configuration for Private Key Encryption](#)

## Configuring Fortanix

1. If the added HSM is Fortanix, upload the **.so** file and **config** file as follows:

To upload the **.so** file,

- a. Click **Browse**.
- b. Navigate to the location of the .so file.
- c. Select the .so file and click **Open**.

To upload the **.cfg** (config) file,

- a. Click **Browse**.
- b. Navigate to the location of the .cfg file.
- c. Select the .cfg file and click **Open**.

2. Choose the respective datacenter.
3. Update each HSM available in the inventory one by one, ensuring that the HSM is moved to the **Available** status.

## Configuring Utimaco

1. If the added HSM is Utimaco, upload the **.so** file and **config** file as follows:

To upload the **.so** file,

- a. Click **Browse**.
- b. Navigate to the location of the .so file.
- c. Select the .so file and click **Open**.

To upload the **.cfg** (config) file,

- a. Click **Browse**.
- b. Navigate to the location of the .cfg file.
- c. Select the .cfg file and click **Open**.

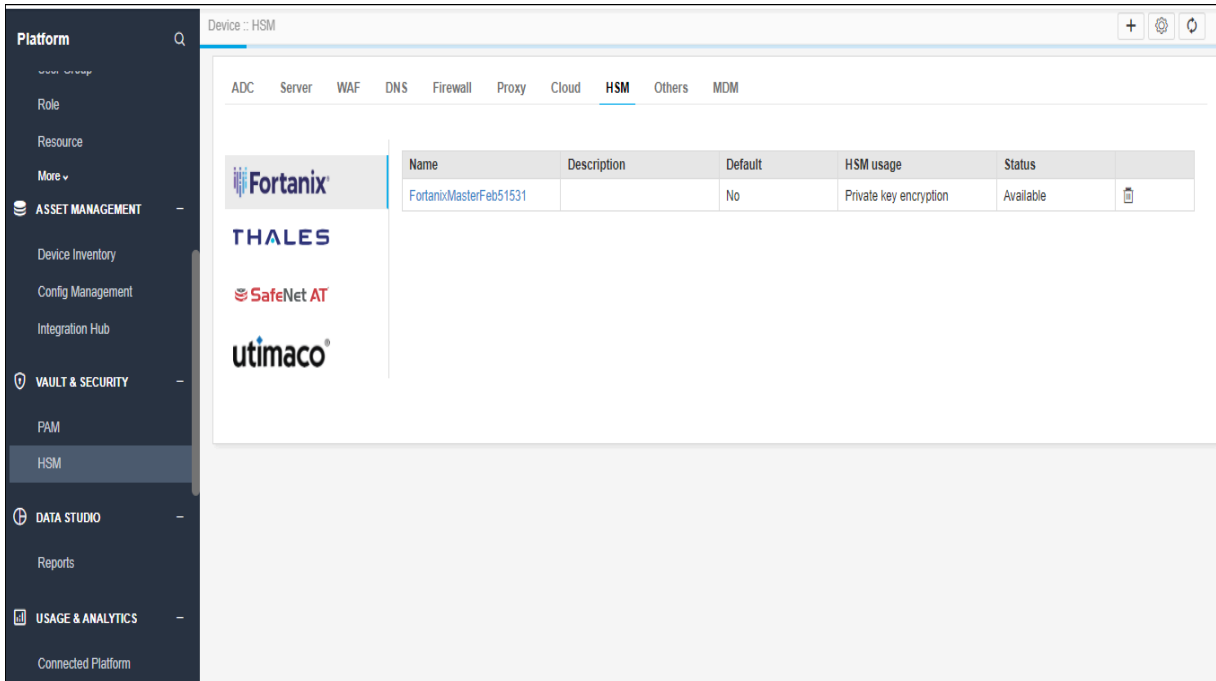
2. Choose the respective datacenter.
3. Update each HSM available in the inventory one by one, ensuring that the HSM is moved to the **Available** status.

If you have previously configured Thales GPN, Thales DPoD, and Thales TCT in the AppViewX v2020.3.0 and have performed the Application Upgrade, then freshly configure the same in the upgraded version. Refer the links below for the configuration:

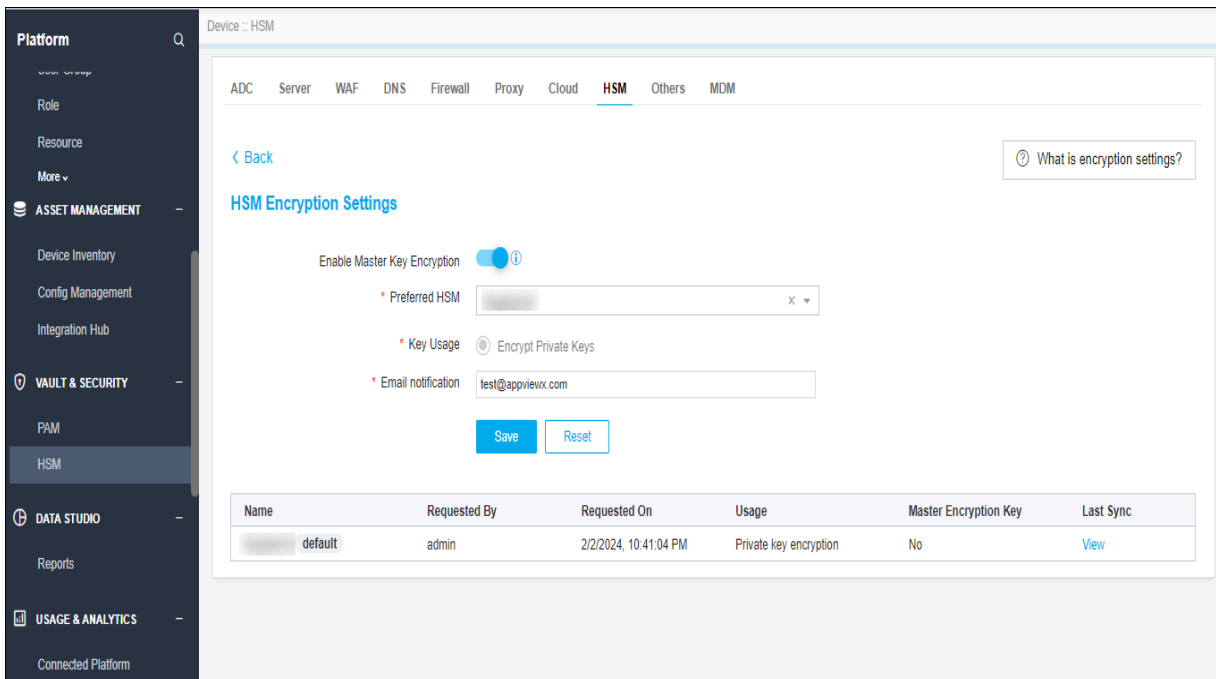
- [Thales GPN](#)
- [Thales DPoD](#)
- [Thales TCT](#)

## Verifying/Modifying HSM Configuration for Private Key Encryption

1. On the top-right corner of the HSM inventory page, click the master encryption settings icon.



2. If the already added HSM has implementation type **private key generation** or **Both** and Set as “default” in 2020.3.0 Appviewx version then that HSM will be available in the Master encryption settings page as default HSM.



3. To receive emails for default HSM health status, configure the email address in the settings page.



**Note:** For email use case SMTP settings should be available in **Platform > System Administration > SMTP**.

4. To change the new default HSM, add the new HSM with HSM usage as **Master key encryption** or **both**.
5. Once the HSM is moved to **Available** status it will be present in the **Preferred HSM** dropdown field of the master key encryption settings page.
6. Choose the new HSM and click **Save**.

# Chapter 4: Troubleshooting for Setup Limitations

## Error while installing the AppViewX plugins

If an error occurs during the installation of AppViewX plugins, it is likely due to an error in the configuration file. You may observe an error such as `Upload failed: scp`, in such cases re-trigger `plugins_install.sh` to install the plugins. Likewise, ensure to review the configuration file carefully and proceed with the execution of `plugins_install.sh` to install only the plugins.

## Pod Out of Memory

During the mongo restore step of the application upgrade process, the pod may go into an out of memory state (exit code 137 as in the screenshot below). In this case resume the upgrade by rerunning the `upgrade.sh` command.

```
2024-02-19T06:21:47.060+0000  creating collection appviewx.hsmDeviceSettings_files.chunks with no metadata
2024-02-19T06:21:47.345+0000  restoring appviewx.hsmDeviceSettings_files.chunks from /appviewx/dependencies/logs/mongo_backup_Mon_Feb_19_11_15_14_IST_2024/appviewx/
mDeviceSettings_files.chunks.bson
2024-02-19T06:21:47.444+0000  [#####.....]          connectedPlatform.apiListenerData  76.1MB/284MB  (26.8%)
2024-02-19T06:21:47.444+0000  [#####.....] appviewx.visualworkflow_request_inputoutput  43.2MB/73.5MB  (58.8%)
2024-02-19T06:21:47.444+0000  [#####.....]          appviewx.archive-logging  46.0MB/56.7MB  (81.2%)
2024-02-19T06:21:47.444+0000  [#####.....]          appviewx.hsmDeviceSettings_files.chunks  43.2MB/43.2MB  (100.0%)
2024-02-19T06:21:47.444+0000
2024-02-19T06:21:50.444+0000  [#####.....]          connectedPlatform.apiListenerData  76.8MB/284MB  (27.0%)
2024-02-19T06:21:50.444+0000  [#####.....] appviewx.visualworkflow_request_inputoutput  43.9MB/73.5MB  (59.7%)
2024-02-19T06:21:50.444+0000  [#####.....]          appviewx.archive-logging  48.3MB/56.7MB  (85.3%)
2024-02-19T06:21:50.444+0000  [#####.....]          appviewx.hsmDeviceSettings_files.chunks  43.2MB/43.2MB  (100.0%)
2024-02-19T06:21:50.444+0000
command terminated with exit code 137
Error in restoring mongo backup
Failed during DB restore
```