

Seqrite Endpoint Security 8.2

Steps to Apply SP

Copyright Information

Copyright © 2008–2024 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited, Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies Ltd. is liable to legal prosecution.

Trademarks

Seqrite and DNAScan are registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

License Terms

Installation and usage of Seqrite Endpoint Security is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit <http://www.seqrite.com/eula> and check the End-User License Agreement for your product.

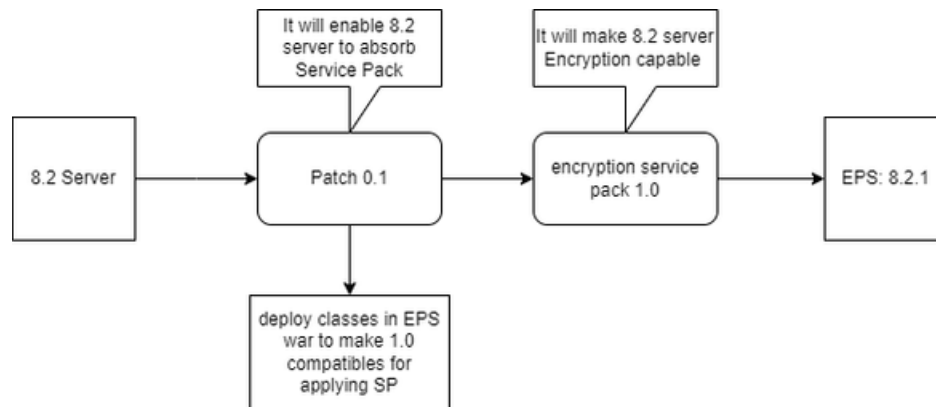
Contents

- 1. Overview 2
 - Execution Flow 2
 - What does SP 1.0 Contain? 2
- 2. Prerequisites 3
- 3. Steps to Apply the Patch 3
- 4. Application of Infra Service Pack 1.0..... 4
 - Apply SP Manually..... 5
 - Apply SP Automatically 8

Overview

EPS 8.2.1 release includes the BitLocker Encryption feature which will be applicable for EPS 8.2 and delivered as a bundle via Infra Service Pack.

Execution Flow



What does SP 1.0 Contain?

The service pack comprises the following items:

Policy Encryption

- eps.war
- cs-pushdata.war
- cs-pushaction.war
- cs-consumer.jar
- localization json file
- epscloudapi.property file
 - **qh.epscloud.requestConnectionTimeout=180000**
 - Mongo url Quartz password encryption.
 - Property Name: **qh.platform.quartz.scheduler.jobStoreMongoUri**

Help Content

Policy Encryption

Health Monitor

- Code for restarting consumer in case of policy pending issue.

- Location:
`/opt/Seqrite_EndPoint_Security/health_monitoring/health_monitoring_distributed_file/communication.sh`

Database Mongo

NA. Only SP specific collection changes

Redis

Code change for resolving critical vulnerability.

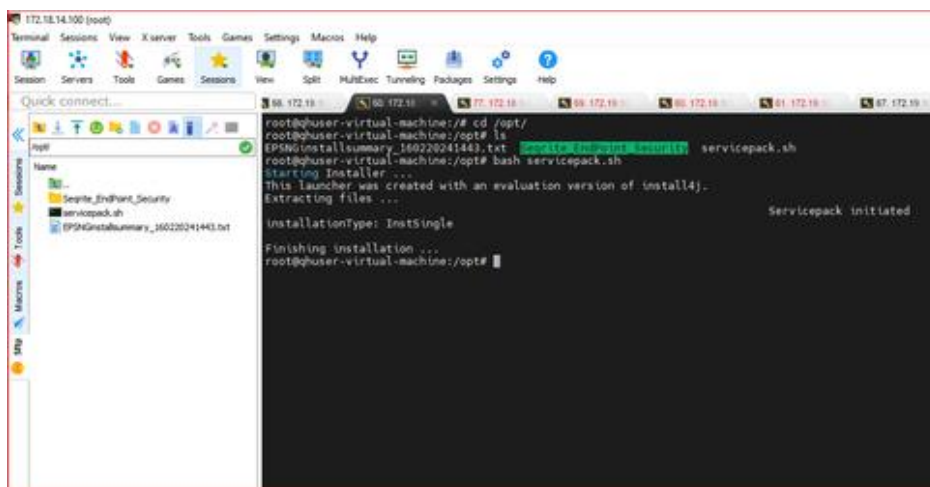
Prerequisites

Apply a patch script, **servicepack.sh** before applying SP 1.0. The purpose of applying this patch is to enable Infra SP.

Steps to Apply the Patch

To apply the patch, follow these steps:

1. Go to the following path to get the SP 0.1 patch
<http://download.quickheal.com/builds/seqrite/82/en/build/ctrlldservicepack/sp01/servicepack.sh>
2. Login to the server machine as root user.
3. Place this **servicepack.sh** script into server machine `/opt/` directory.
4. Open terminal or console and go to `/opt/` directory from console and type **bash servicepack.sh** command and hit [Enter].



```
root@ghuser-virtual-machine:/# cd /opt/
root@ghuser-virtual-machine:/opt# ls
EPNInstallSummary_160220241443.txt  servicepack.sh
root@ghuser-virtual-machine:/opt# bash servicepack.sh
Starting Installer ...
This launcher was created with an evaluation version of Install4j.
Extracting files ...
InstallationType: InstSingle
Servicepack initiated
Finishing installation ...
root@ghuser-virtual-machine:/opt#
```

- Once you hit [enter], the script executes. It takes around three to four minutes to complete the execution.

You can check the execution status of patch script by checking logs present at the following location: **/opt/Seqrite_EndPoint_Security/log/SP_Logs.txt**

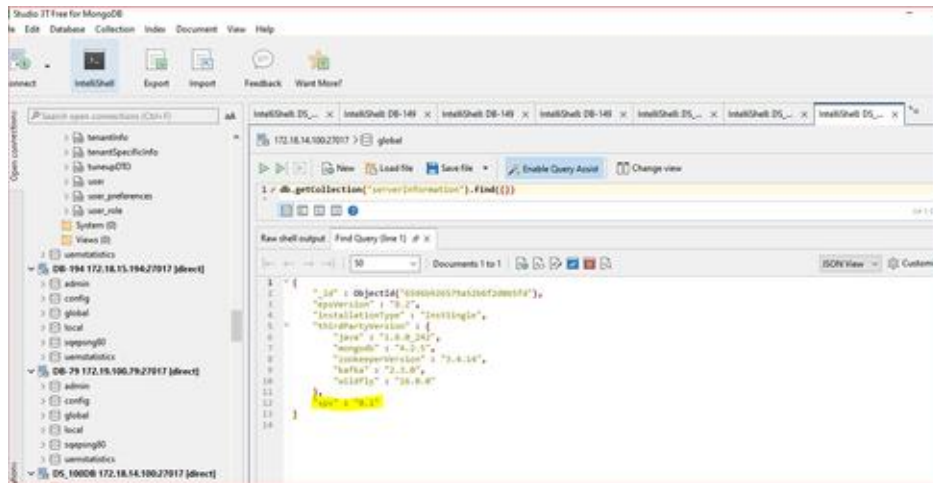
Note: In case of any failure, the script will roll back itself. No human intervention is required. Same can be checked in Rollback logs:

/opt/Seqrite_EndPoint_Security/log/SP_Rollback.txt

- Now, you can verify whether the patch has been applied by checking the logs and also by accessing the database.
 - Before accessing the mongo db by robo-3t or studio-3t, run this command to disable the authorization.

**sed -i -e 's,authorization: enabled,authorization: disabled,g' /etc/mongod.conf
systemctl restart mongod**

- Now access the mongo db by using host IP [for eg:- 172.18.14.100]
- Go to global collection > server information and check **spv =0.1**. We can assure that patch has been successfully applied.

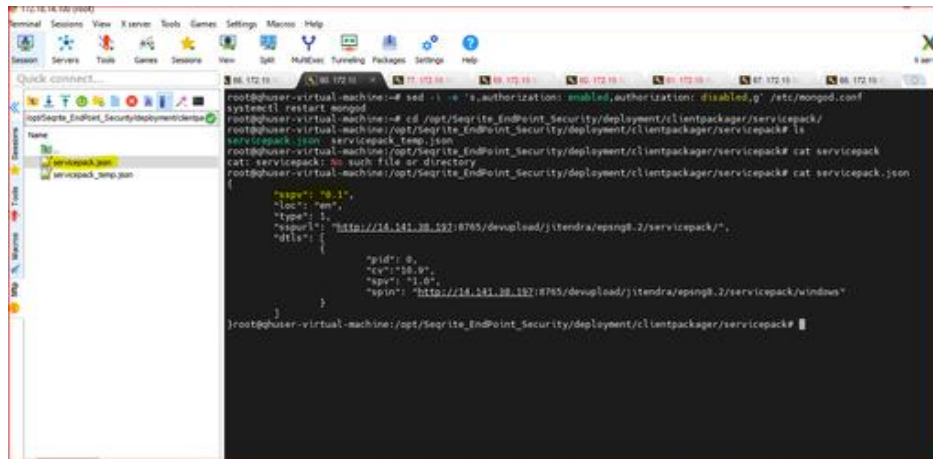


Application of Infra Service Pack 1.0

There are two ways to apply the SP:

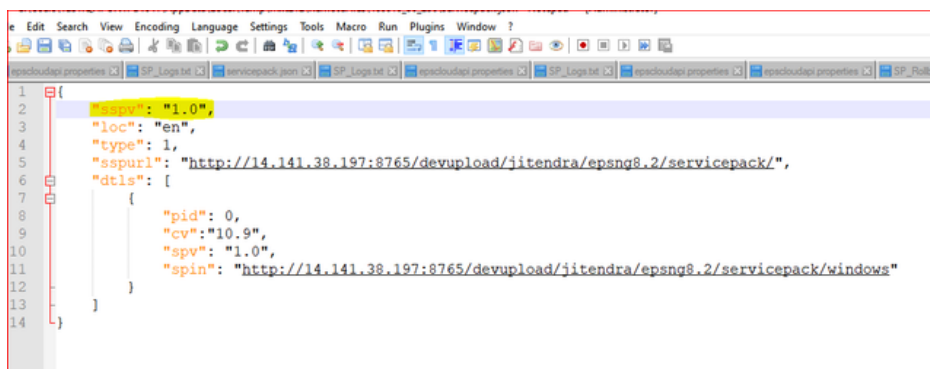
Apply SP Manually

1. Access following path to get the SP 1.0
<http://download.quickheal.com/builds/seqrite/82/en/build/ctrlservicepack/sp10/servicepack/servicepack.sh>
2. Login to server machine as root.
3. Place this **servicepack.sh** SP script into server machine.
4. Copy servicepack.sh file to `/opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack/server/` folder [If **server** folder does not exist then create it and place the servicepack.sh]
5. Assign permission 644 to servicepack.sh file [**chmod 644 servicepack.sh**]
6. Go to `/opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack/` folder and assign permission 644.
 - a. Edit servicepack.json
 - b. change "ssp": "0.1" to "spv": "1.0"
 - c. Save it.



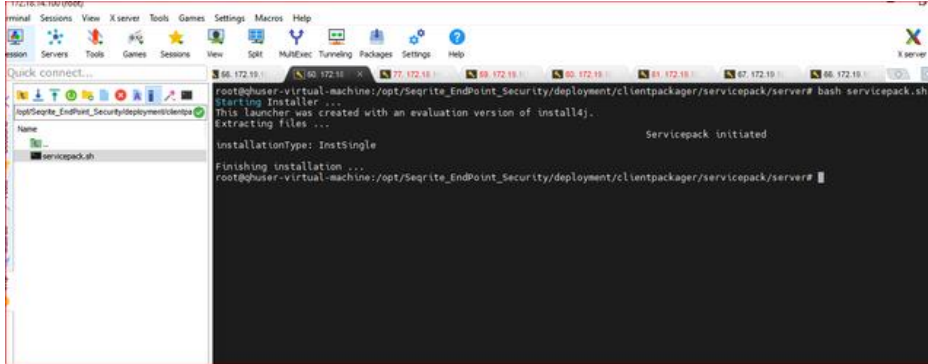
```
root@phuser-virtual-machine:~# sed -i -e 's.authorization: enabled,authorization: disabled,g' /etc/mongod.conf
systemctl restart mongod
root@phuser-virtual-machine:~# cd /opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack/
root@phuser-virtual-machine:/opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack# ls
servicepack.sh
root@phuser-virtual-machine:/opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack# cat servicepack
cat: servicepack: no such file or directory
root@phuser-virtual-machine:/opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack# cat servicepack.json
{
  "spv": "1.0",
  "loc": "en",
  "type": 1,
  "sspurl": "http://14.141.38.197:8765/devupload/jitendra/epsng8.2/servicepack/",
  "dtls": {
    {
      "pid": 0,
      "cv": "10.9",
      "spv": "1.0",
      "spin": "http://14.141.38.197:8765/devupload/jitendra/epsng8.2/servicepack/windows"
    }
  }
}
```

7. The json file looks like:



```
1 [{"spv": "1.0",
2
3 "loc": "en",
4 "type": 1,
5 "sspurl": "http://14.141.38.197:8765/devupload/jitendra/epsng8.2/servicepack/",
6 "dtls": {
7
8   {
9     "pid": 0,
10    "cv": "10.9",
11    "spv": "1.0",
12    "spin": "http://14.141.38.197:8765/devupload/jitendra/epsng8.2/servicepack/windows"
13   }
14 }
}
```

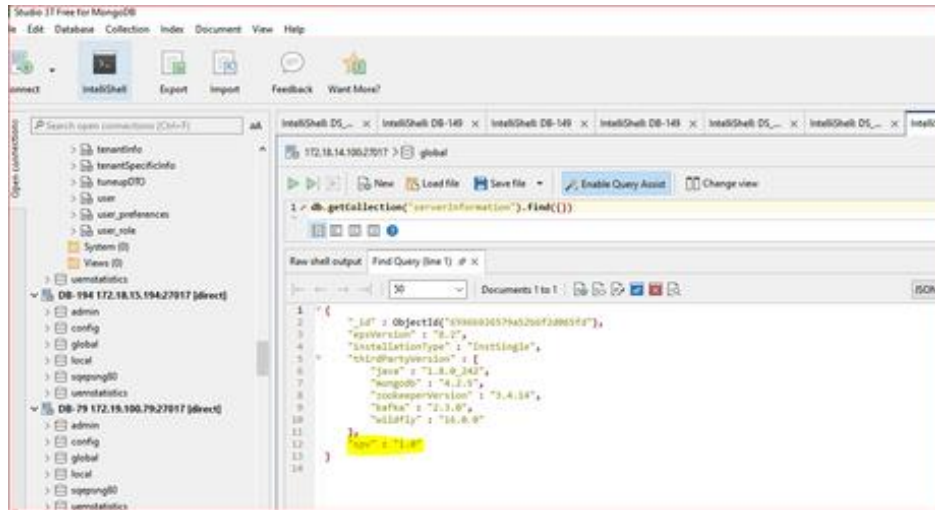
8. Execute **bash servicepack.sh** from terminal/ console from this path:
/opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack/server/
9. Once the user executes the command then human interaction is not recommended.
Here is the successful execution snap:



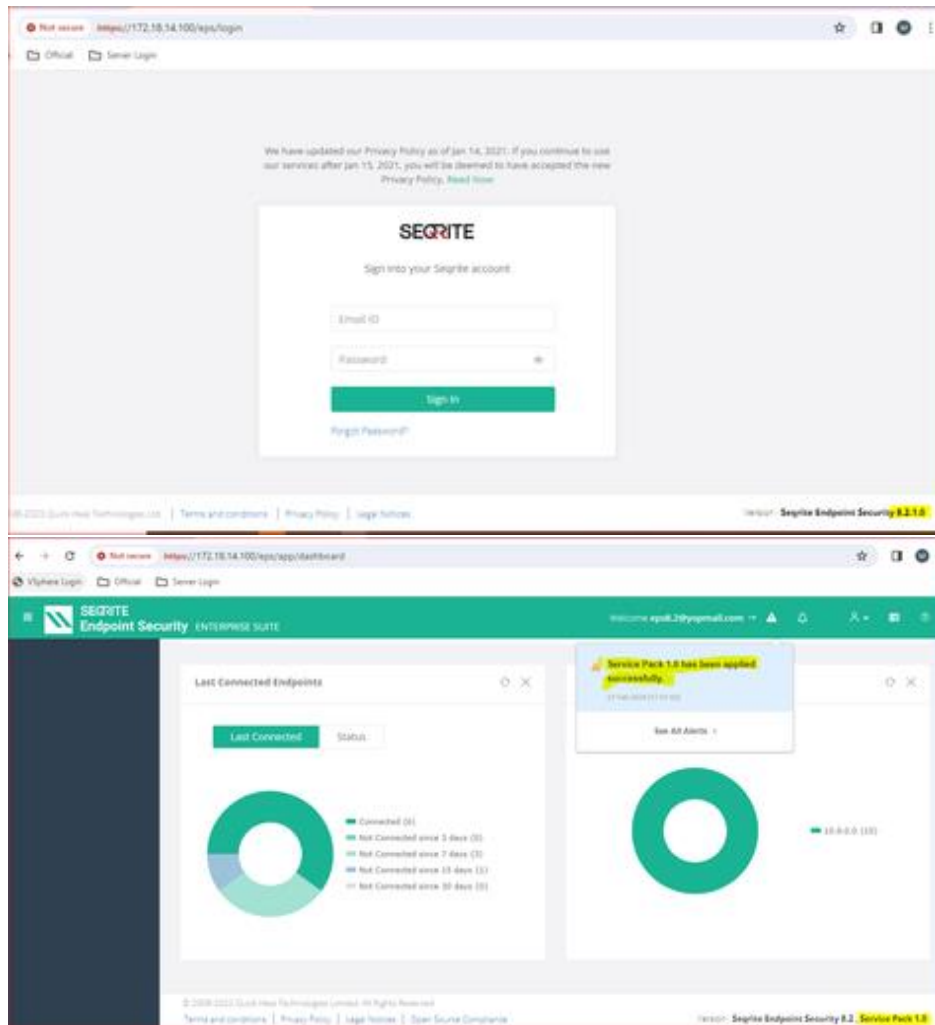
10. Wait for the installation successful or rollback message.
11. If a rollback message is displayed, it indicates that the Service Pack was not applied due to errors. In such cases, the Service Pack will initiate contingency measures to restore the server to its original state.
12. You can check the execution status of SP script by checking logs present at this location:
/opt/Seqrite_EndPoint_Security/log/SP_Logs.txt

Note: In the event of any failure, the script will automatically initiate a rollback process. [No human intervention is required]. Same can be checked in Rollback logs:
/opt/Seqrite_EndPoint_Security/log/SP_Rollback.txt

13. You can verify whether the patch has been applied by checking the logs and also by accessing the database.
 - a. Before accessing the mongo db by robo-3t or studio-3t, run this command to disable the authorization.
sed -i -e 's,authorization: enabled,authorization: disabled,g' /etc/mongod.conf
systemctl restart mongod
 - b. Access the mongo db by using host IP [for example: 172.18.14.100]
 - c. Go to global collection > server information and check **spv =1.0**. The patch has successfully been applied.



d. Same can be verified by accessing server console on login page.



Apply SP Automatically

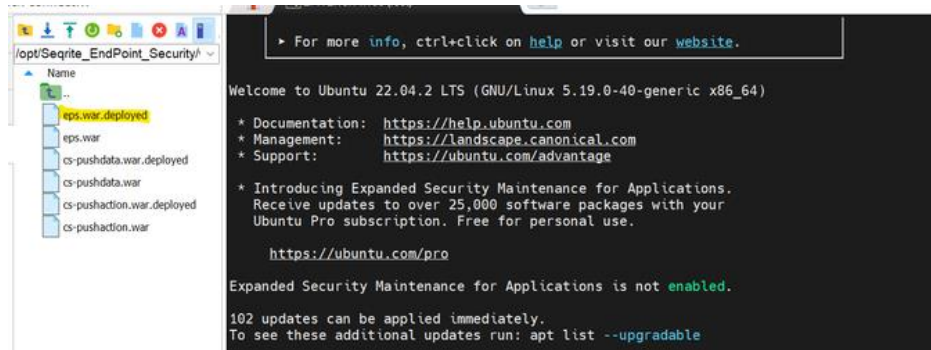
1. After patch [servicepack.sh] is applied to system, edit **epscloudapi.properties** in /opt/Seqrite_EndPoint_Security/config/.
 - a. Edit epscloudapi.properties.
 - b. Change
qh.epscloud.cdnServerUrl=<http://download.quickheal.com/builds/seqrite/82/en/build/> to
qh.epscloud.cdnServerUrl=<http://download.quickheal.com/builds/seqrite/82/en/build/>/ctrlIdservicepack/sp10/ [This url used for local testing & can be used for controlled SP].

```
1 #####
2 # Framework Properties
3 #####
4 qh.epscloud.app-info.id=eps
5 spring.mvc.view.prefix=/WEB-INF/views/
6 spring.mvc.view.suffix=.jsp
7 qh.epscloud.downloadUrl=https://172.18.14.100/s3
8 qh.epsonprem.helpUrl=https://172.18.14.100:s3/seqrite-endpoint-security-ng/
9 qh.epscloud.defaultUrl=https://172.18.14.100:443/s1/
10 qh.epscloud.kafkaProducerBaseUrl=NA
11 spring.cache.type=NONE
12
13 # Spring mongo properties
14 spring.data.mongodb.authentication-database=admin
15 spring.liquibase.change-log=classpath:/db/changelog/db.changelog.xml
16
17 qh.epscloud.cdnServerUrl=http://download.quickheal.com/builds/seqrite/82/en/build/
18
19 # Security configuration
20 security.filter-order=5
21 security.ignored=/v1/eps/**,/v1/upgradation/,/v1/reports/csvexport/selectiveclients,/v1/reports/csvexport,/v1/repor
  */export/download/**,/api-doc/**,/v2/**,/v1/servicepack/,/v1/notifyinstall/setupdetails,/v1/notifyinstall/crea
  */epsuser/deleteall,/v1/reports/csvexport/**
22 server.servlet.context-path=/eps
23 #####
24 # EHCache configuration
25 #####
```

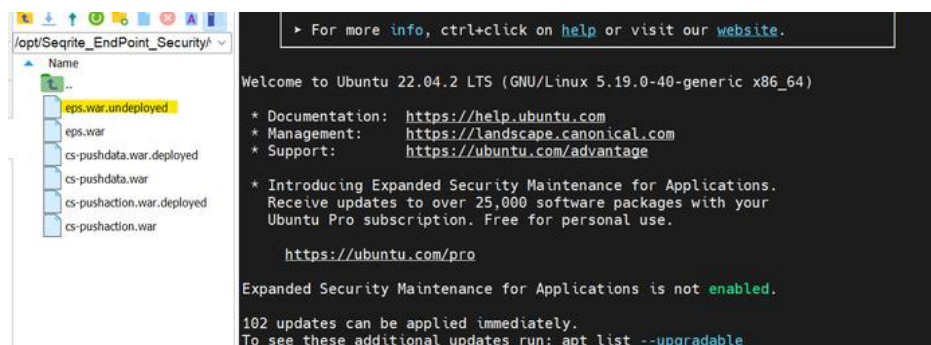
2. The **epscloudapi.properties** file looks like this:

```
1 #####
2 # Framework Properties
3 #####
4 qh.epscloud.app-info.id=eps
5 spring.mvc.view.prefix=/WEB-INF/views/
6 spring.mvc.view.suffix=.jsp
7 qh.epscloud.downloadUrl=https://172.18.14.100/s3
8 qh.epsonprem.helpUrl=https://172.18.14.100:s3/seqrite-endpoint-security-ng/
9 qh.epscloud.defaultUrl=https://172.18.14.100:443/s1/
0 qh.epscloud.kafkaProducerBaseUrl=NA
1 spring.cache.type=NONE
2
3 # Spring mongo properties
4 spring.data.mongodb.authentication-database=admin
5 spring.liquibase.change-log=classpath:/db/changelog/db.changelog.xml
6
7 qh.epscloud.cdnServerUrl=http://14.141.38.197:8765/qaupload/jitendra/epsng8.2/
8
9 # Security configuration
0 security.filter-order=5
1 security.ignored=/v1/eps/**,/v1/upgradation/,/v1/reports/csvexport/selectiveclients,/v1/reports/csvexport,/v1/repor
  */export/download/**,/api-doc/**,/v2/**,/v1/servicepack/,/v1/notifyinstall/setupdetails,/v1/notifyinstall/crea
  */epsuser/deleteall,/v1/reports/csvexport/**
2 server.servlet.context-path=/eps
3 #####
4 # EHCache configuration
```

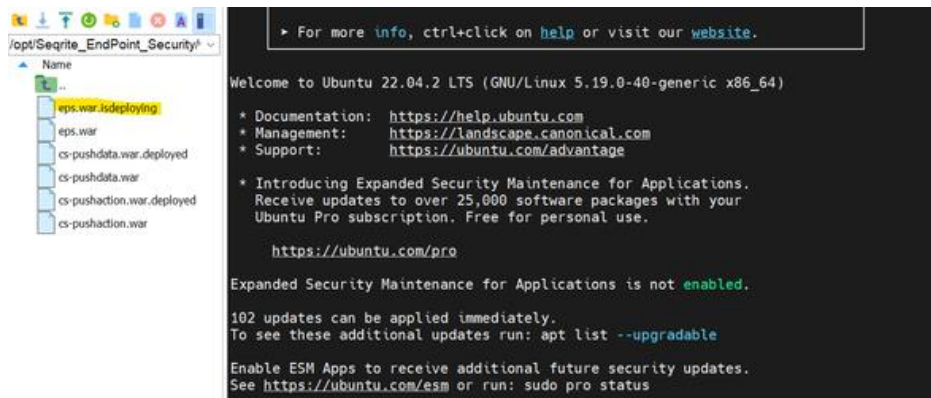
3. After making changes in properties, redeploy the eps war from /opt/Seqrite_EndPoint_Security/wildfly/standalone/deployments/
4. Steps to redeploy eps war:
 - a. Remove the existing eps.war.deployed or from console [rm eps.war.deployed]



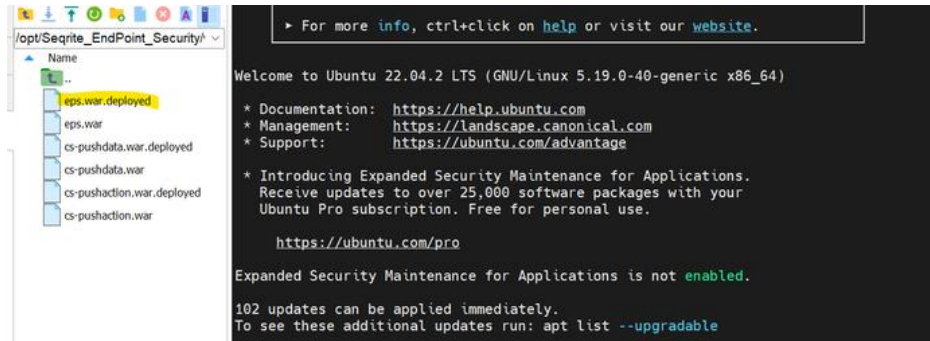
- b. Now after refresh remove eps.war.undeployed also or from console [`rm eps.war.undeployed`].



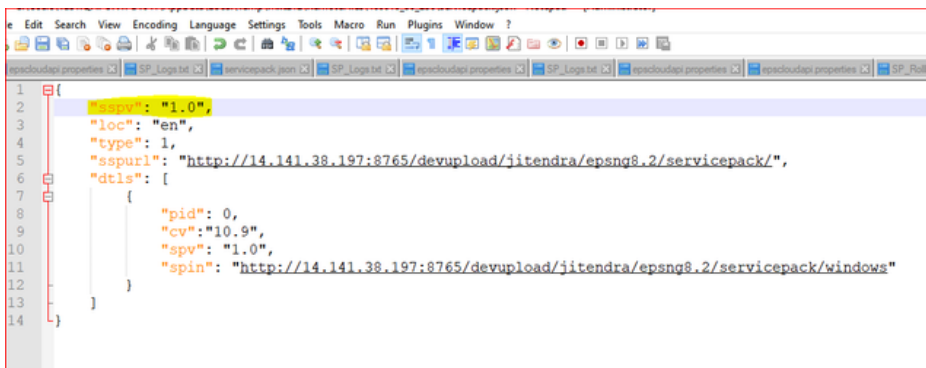
Now, upon refreshing, you should be able to observe that eps.war is deploying.



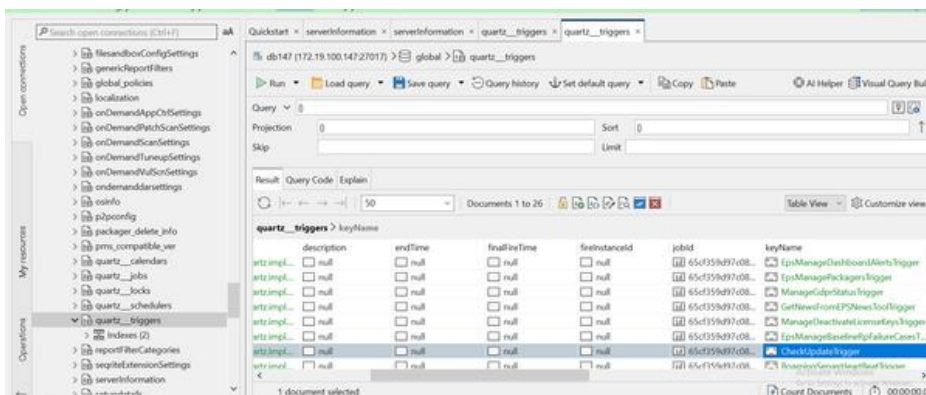
- c. Please wait for some time. You will notice that eps.war has been deployed.



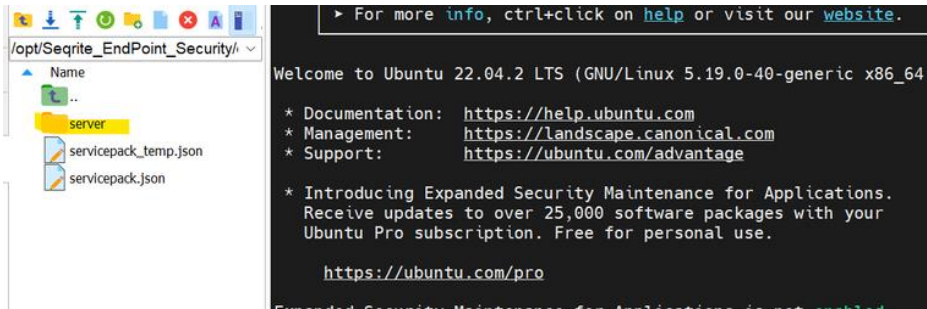
5. Make sure that `servicepack.json` with `"sppv": "1.0"` is uploaded at: <http://14.141.38.197:8765/qaupload/jitendra/epsng8.2/> SP.



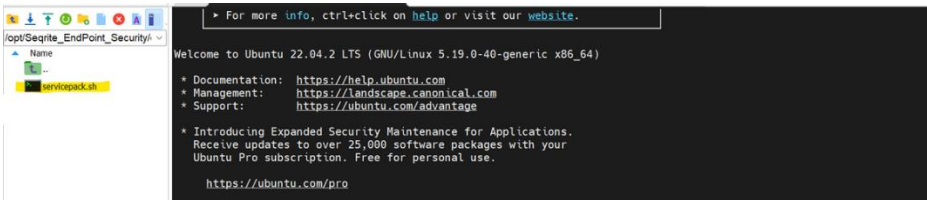
5. Now access mongo db from Robo 3T and go to global > quartz_triggers and trigger the Cron named Keyname > **CheckUpdateTrigger**.



6. After the cronjob is triggered, it will compare servicepack.json file on machine and one on cdn and after finding latest on CDN it will create a folder name server at this location: `/opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack/`



7. The ServicePack file gets downloaded in this folder.

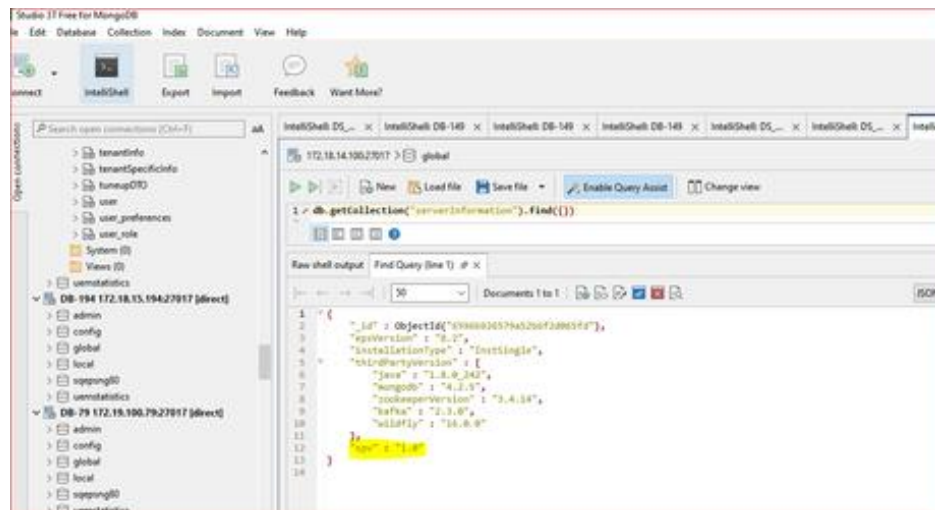


8. After downloading the ServicePack, it automatically executes the ServicePack.
 9. You can check the execution status of SP by checking logs which is present in following location:

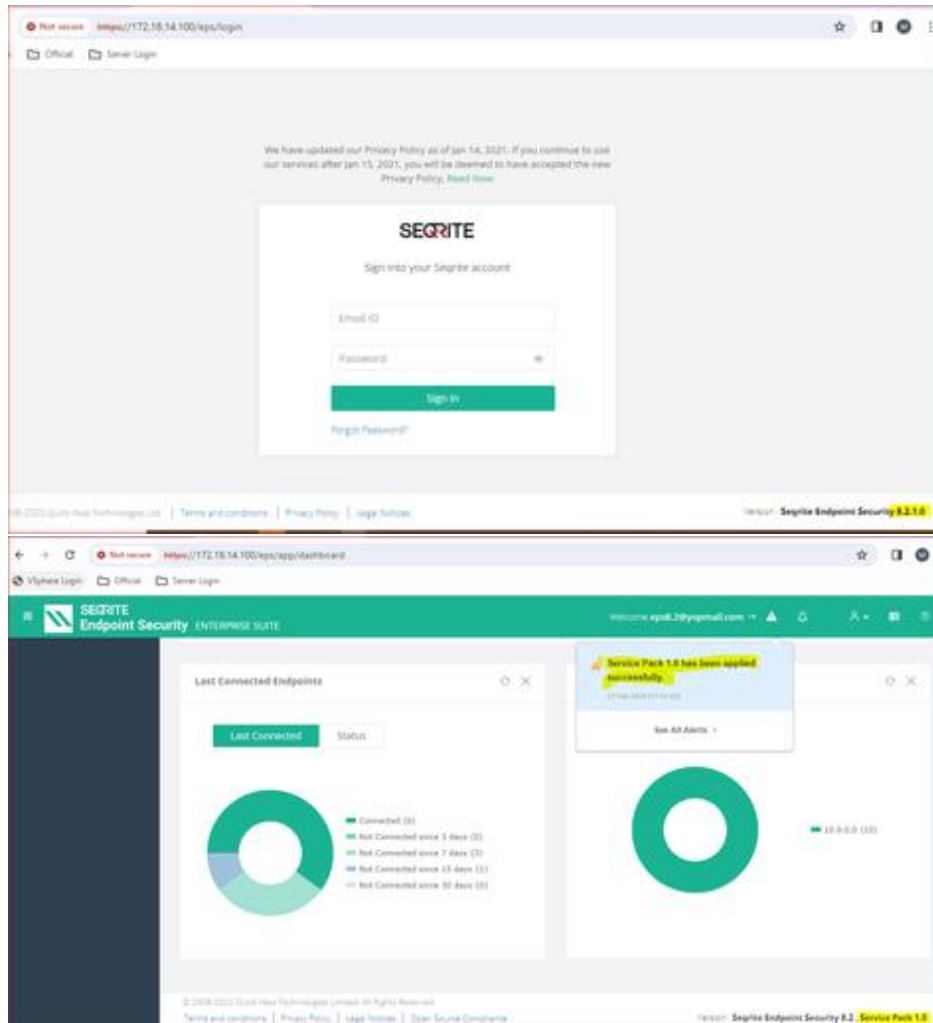
/opt/Seqrite_EndPoint_Security/log/SP_Logs.txt

10. Now you can check the SP is applied on logs and also can verify by accessing DB.

- a. Before accessing the mongo db by robo-3t or studio-3t, run following command to disable the authorization.
**sed -i -e 's,authorization: enabled,authorization: disabled,g' /etc/mongod.conf
 systemctl restart mongod**
- b. Now access the mongo db by using host IP [for example: 172.18.14.100]
- c. Now go to global collection > server information and check **spv=1.0**. The patch has been successfully applied.



d. Same can be verified by accessing server console on login page.



Note: In the event of any failure, the script will automatically initiate a rollback process.
/opt/Seqrite_EndPoint_Security/log/SP_Rollback.txt