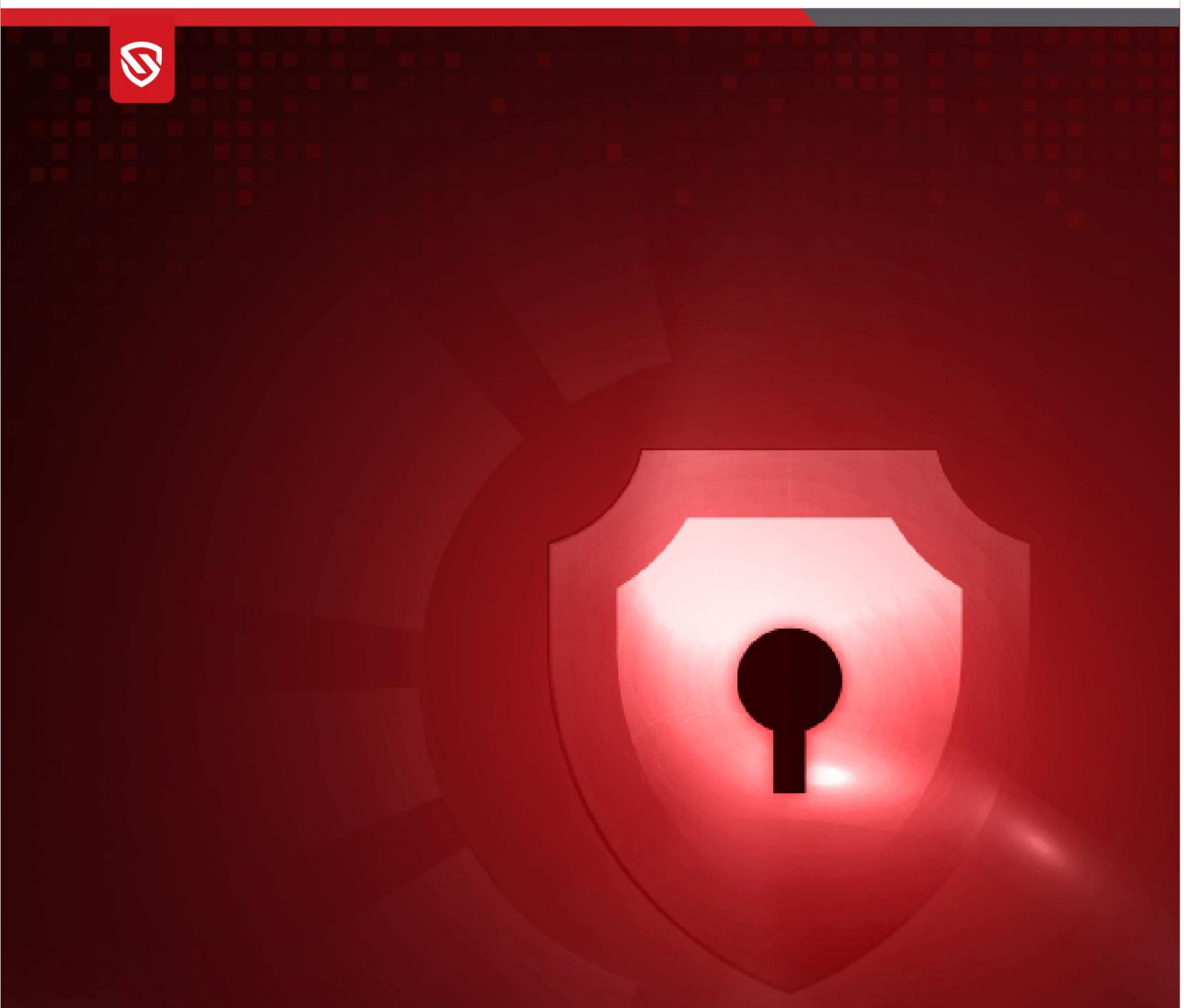
Seqrite

Endpoint Protection



Migration Guide

EPS 8.0 to EPP 8.3

www.seqrite.com

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Endpoint Protection is subject to the 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

Overview

Seqrite Endpoint Protection (EPP) is an integrated solution for managing and regulating multiple Endpoint Protection products across different geographical locations. IT administrators can easily connect to the server from any location to view the latest security status, configure product policies, receive notifications, and address critical network events from a single dashboard.

Audience

This guide is for users upgrading from version 8.0 to version 8.3. The upgrade provides users with comprehensive features and ensures a seamless transition of version 8.0 data.

Server Upgrade

This section provides information on upgrading from v8.0 to v8.3 in the server environment. For help or support during the upgrade process, refer to the product documentation or contact Support.

Note: *It is important to migrate the server from 8.0 to 8.2 and then follow the process for further migration to 8.3*

Migration from 8.0 to 8.2 on IP to IP/Hostname

If customer has EPSNG Server **8.0** installed on CentOS machine, follow these steps to upgrade to version **8.2**.

1. The EPSNG 8.0 server includes data such as policies, configurations, custom packages, administrative settings, feature reports, etc. all the respective data will be retained well post migration.
2. **Backup Data (8.0)**: To back-up the data, follow these steps:
    a. Open Mobaxterm or terminal on CentOS machine, and navigate to "**/opt/Seqrite_EndPoint_Security"**
    b. Copy these above files from this location: http://dlupdate.quickheal.com/builds/seqrite/uemcp/epsng/docs/8.0_to_8.2_Forward_compatibility.zip
    Note that you need to extract the zip before taking any further actions. Click here to view the folder structure.
    c. **Standalone server**: **run_backup.sh** and **backup_standalone.sh** files on your server machine at "**/opt/Seqrite_EndPoint_Security"**.
    Distributed Server: "**run_backup.sh** and **backup_distributed.sh"** files on your server machine at "**/opt/Seqrite_EndPoint_Security"**.
        i. ***Above should be done on App Server Machine***
    d. Go the terminal and assign 755 permissions to **both** the files with this command: **chmod 755 file_name.**
    e. Execute the **run_backup.sh** file with the following command: **bash run_backup.sh 19**.
    f. The success message appears as **Backup is completed.**
    The **exportDump<Date_time>** and **MongoDump<Date_time>** directories get created at the **/opt/Seqrite_EndPoint_Security/Backup/** location (*for both standalone and distributed*).
    g. Download the above **Backup** directory to any other machine or any NFS, or shared drive, or any removable drive disk, so in case of machine crash, your backup is not affected.

    Note: Minimum space requirement validation is 1GB. Ensure you have enough space to back up your data.

3. After the backup is completed and copied to the new location (refer point: **f**), shut down 8.0 server machine.
4. Take new machine with Ubuntu 22.04 LTS installed. Assign the same IP (IP that was assigned to the 8.0 server) to Ubuntu machine that will be used for 8.2 server installation.
   Note: Ensure that all the below 8.2 prerequisites are met before the installation starts. Please find the prerequisites listed here-

   Prerequisites: Disk Space Requirements:
   - **Download**: At least **20 GB** disk space must be available.
   - **Installation**: At least **16 GB** disk space must be available. **(Ubuntu 22.04)**
5. Install 8.2 with **Activate Later** option with basic configurations.
   a. If it is IP based Installation, then proceed with next steps.

   If it is a Hostname based installation, then the server machine Hostname needs to be properly FQDN configured. Refer the steps to set FQDN here.

   Note: Do Not activate unless you execute the following steps.
6. **Restore Data**:
   a. Place the backup folder on your machine using the **removable drive** or get it from **shared drive** or any **NFS**. **OR**
   b. Open **Mobaxterm** and provide the server machine IP to log in to the backend of your server. From the left panel, go to this location to copy the backup **/opt** directory or from the CMD prompt **cd/opt** hit [Enter].
   c. Copy /Download exportDump<Date_time> and MongoDump<Date_time> and **outputFilePath.txt** file from backup directory to **/opt** directory.
   d. Rename **exportDump<Date_time>** and **MongoDump<Date_time>** directories to MongoDump and exportDump.
   e. **Standalone Server**: **run_restore.sh**, **restore_standalone.sh** and **backward_compatibility_8.2.js** in /opt directory and give 755 permissions to all the files with this command: **chmod 755 file_name**
      Distributed Server: run_restore.sh, **restore_distributed.sh** and **backward_compatibility_8.2.js** in /opt directory and give 755 permissions to all the files with this command: **chmod 755 file_name**
   f. Execute **run_restore.sh** file using the **bash run_restore.sh 19** command on terminal. Wait till you get a restoration success message, **Restoration is Completed.**
7. **With the above steps completed, we need to activate the 8.2 server using the below steps.**
   a. first reset the **AFG** flag with the help of activation team for the same key.
   b. Once the above stage is completed, now **activate** the server with the **same key** used for 8.0 server.
8. If roaming service was enabled in 8.0 server, then;
   a. on 8.2 server you need to enable it again.
   b. Navigate to **Configurations>Roaming Service>Connect to Cloud Platform** and select **Automatic** mode.

9. Now, Roaming Clients will start connecting to the server.
   Note: Wait until all the roaming clients are connected and showing status- Roaming.

Just to double check, validate that all your previous data is retained as-it-is.

Now your 8.0 server is migrated to 8.2 server successfully and your endpoints are on 10.7. Check if the endpoints are connected to the server well. Do not proceed for client upgrade till server version becomes 8.3.4.

Server Upgrade from 8.2 to 8.3 on IP to IP/Hostname

This section provides information on upgrading from v8.2 to v8.3 in the server environment. For help or support during the upgrade process, refer to the product documentation or contact Support.

Prerequisites

1. **Product Key Conversion**: To convert the product key from version 8.2 to version 8.3 for activation, contact the Support team.
2. **Ensure v8.2 Service Pack (version 0.1) Installation**: The service pack must be installed on the Server before starting the upgrade process for v8.3 Server.

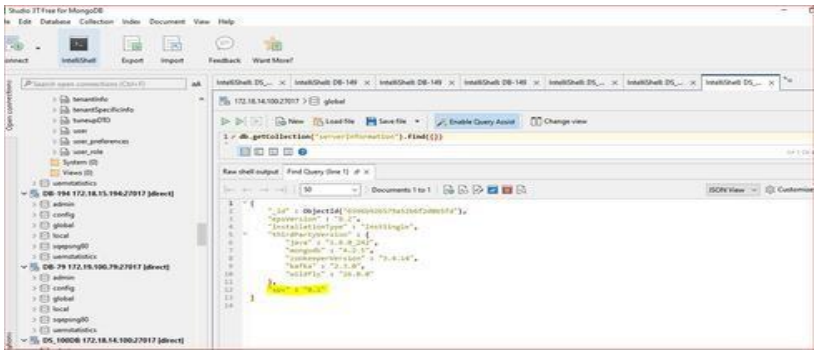
   To apply the service pack 0.1, follow these steps:

   1. Go to the following path to get the SP 0.1 patch http://download.quickheal.com/builds/seqrite/82/en/build/ctrldservicepack/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 click Enter.
   5. 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

   6. Now, you can verify whether the patch has been applied by checking the logs and also by accessing the database.
      a. Connect to MongoDB with these steps
      b. Now access the mongoDB by using host IP [for eg:- 172.18.14.100]
      c. Go to global collection > server information and check **spv=0.1.** We can assure that 0.1 SP successfully applied.



3. **Offline Server**: An offline upgrade is possible; however, offline key reactivation is required. Contact the Support Team to activate the offline key.
4. **Non-Complaint**: After the 8.2 to 8.3 upgrade, the Host Integrity policy requires all clients to have version 10.11. Any client earlier than 10.11 will show as non-compliant.

Manual Procedure for 8.2 to 8.3 Server

1. Access the following path to get the upgrade pack: https://dlupdate.quickheal.com/builds/seqrite/83/en/upgradepack/pack/upgradepack.sh
2. Log in to the server machine as root using Vsphere, MobaXterm, or a physical machine.
3. Place the upgradepack.sh script on the server machine.
4. Copy the **upgradepack.sh** file to "**/opt/Seqrite_EndPoint_Security/deployment/clientpackager/upgradepack"**
5. Set permissions for upgradepack.sh to 644 (e.g., chmod 644 upgradepack.sh).
6. Ensure that the SP0.1 service pack is installed before applying upgradepack.sh .
7. Execute **bash upgradepack.sh** from the terminal/console. Execute the script from /opt/Seqrite_EndPoint_Security/deployment/clientpackager/upgradepack/ .
8. Once executed, avoid human interaction (e.g., interrupting with ctrl+c or ctrl+z).

Note:

- After a successful upgrade, the user will be redirected to the EPP 8.3 console and can log in with EPS 8.2 credentials.
- Check the execution status in the logs located

Application of 8.3.4 SP

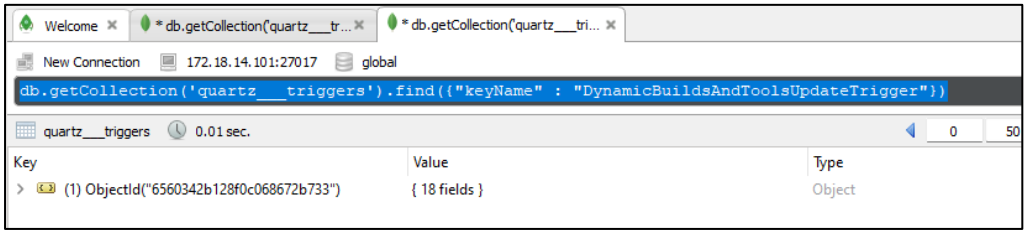
- Now apply, 8.3.4 SP on 8.3 console following the deployment guide provided here- https://docs.seqrite.com/wp-content/uploads/2025/03/Endpoint-Protection-EPP-OnPrem-_-Service-Pack-8.3.4.0-Deployment-Guide.pdf

Note: After a successful upgrade, the user will be redirected to the EPP 8.3.4 console.

Mandatory Steps to Update Builds

This describes the process of replacing the existing latest builds manually for online customers. Below are mandatory steps to be followed.

1. Connect to MongoDB with Steps to open MongoDB
2. Once the connection is established, go to **global** > **collections** > **quartz___triggers** > **DynamicBuildsAndToolsUpdateTrigger** from the left panel.
3. Double click the **quartz___triggers**.
4. Enter this query in a connection grid bar: **db.getCollection('quartz___triggers').find({"keyName" : "DynamicBuildsAndToolsUpdateTrigger"})**.



5. It fetches the record. Right click on the record and select **Edit Document**. The document opens.

Note: It is recommended to save this json in a separate doc file before you make any changes.

6. Once the backup is done, update the **nextFireTime** by adding five to seven minutes to your current UTC time. For example, if my current UTC time is 05:31, then your next fire time would look like:

“nextFireTime" : ISODate("2023-11-30T05:36:00.000Z")

7. Click **Save.** Wait for the Cron execution to complete for about five minutes. Then go back to the same database record to check the previous fire time. It should be the same as last saved **next fire time**. The next fire time should reset to the default value.

Note:

- For offline customers, please follow the manual procedure to update the builds.
- Please use below provided offline activation tool for 8.3.4 Server https://dlupdate.quickheal.com/builds/seqrite/83/en/offlinesupportactivation_watermark.zip

Perform the Major Upgrade

Follow these steps to perform the major upgrade on migrated clients from 10.7 to 10.11 CA version.

Windows:

1. Open the EPSNG server console.
2. Go to **Status** page and select the endpoint.
3. Select the Client Action as **Upgrade Clients**.

Linux:

Follow these steps to upgrade client when old client is already installed in new console:

1. Go to the console.
2. Go to **Deployment** section.
3. Download the required Linux package that is, 32/64 bit.
4. Go to the Client and log in as a root user.
5. Go to downloaded package location.
6. Unzip the package using this command: **tar -xvf package_name**
7. Check if all these files are present:
    - bu`ildNumber.txt
    - clagnt.dat
    - epslin64.tar.gz/epslin32.tar.gz
    - install
    - readme.txt
    - validation
8. Provide full permission to install file using this command: **chmod 777 install**
9. Run install by command: **./install**

Mac:

N/A

Note: Ensure that all Windows/Linux clients are upgraded to 10.11. Go to the **Status** page on the console and check the client agent version and the VDB.

How to Upgrade to Patch Management Server

Before upgrading Patch Management services:

- Administrators must upgrade from version 8.2 to 8.3 server to access the 8.3 Patch Management Server features.
- Users need to upgrade both the Patch Management server and the client to access the updated Patch Management feature. Feature functionality will remain unchanged.
- Ensure both the Patch Management server and the endpoints are upgraded to the latest 8.3 version after the server upgrade.

Note:

- Post patch management server upgrade, re-add the latest patch server to the upgraded EPP 8.3 console.
- Perform patch sync and reconfigure the updated Patch server to the defined policies to use the Patch Management feature.
- Perform patch scan and patch install on the registered endpoints.

Steps to Set FQDN

1. Login as a root user.
2. Check the status of hostname file using this command: **hostname –fqdn**. Check if it is within the domain, if not proceed with the following steps:
3. Set hostname using this command: **hostnamectl set-hostname *VMNAME***
4. Edit hosts file using this command: **nano /etc/hosts**.
5. Add this entry: VMIP vmname.qh.lan vmname.
   Example: 172.18.14.78 UEMQAC75x64-027.qh.lan UEMQAC75x64-027

Click here to go back to continue with the remaining steps

Steps to open MongoDB:

1. Login into the server machine.
2. Login in as a root user.
3. Go to **/etc.** directory.
4. Then run this command **nano mongod.conf** on terminal.
5. Use a down arrow to search for **security** > **authorization** which is by default enabled. Make it **disabled**.
6. Hit [Ctrl X]. It asks if you want to save. Press [Y] and [Enter] to save the changes.
7. Restart the **Mongod** service by using this command: **systemctl restart mongod.**
8. Now you need to open the database. Follow these steps to create a new DB:
   a. Download and install Robo 3T on your machine if it is not already available.
   b. Open Robo 3T.
      Note: In case of multiple server entries, make sure that the current saved server is selected.
   c. Under the **Connection** tab, select the **Type** from the drop-down list.
   d. Enter the name for the database in the **Name** field.
   e. Enter the **IP** address in the **Address** field.
   f. Test the connection by clicking the **Test** button.

Click here to go back to continue with the remaining steps.

Migration_8.0_to_8.2 Folder Structure

- **8.0_to_8.2_Backup_and_Restore**
  - 8.0_to_8.2_Forward_compatibility
    - Distributed
      - backup_distributed.sh
      - backup_distributed_instruction.txt
      - backward_compatibility_8.2.js
      - restore_distributed.sh
      - run_backup.sh
      - run_restore.sh
    - Standalone
      - backup_standalone.sh
      - backup_standalone_instruction.txt
      - backward_compatibility_8.2.js
      - restore_standalone.sh
      - run_backup.sh
      - run_restore.sh

Click here to go back to continue with the remaining steps.

