SEQRITE ENCRYPTION MANAGER COOKBOOK

Seqrite Encryption Manager and Seqrite Volume Encryption both work together to perform seamless encryption and decryption process.

Content

Introduction

Seqrite Encryption Manager works on Client-Server architecture and the communication is secured with public/private key encryption over HTTPS channel. SEM features different encryption algorithms that complies best with any organizational standards. Privilege to combine variety of encryption algorithms and create a single encryption policy or use the pre-configured policies and assign to groups or computers.

Prerequisites

MySql pre-requisites

- SEM server installation methods:
  i. Local/intranet network
     a) On MySQL dialog box, the user must enter only the loopback IP Address (127.0.0.1).
  ii. For roaming users, public/static IP address
     a) User must enter loopback IP address (127.0.0.1) on MySQL dialog box.
     b) MySQL communication for the outside network should be blocked or not allowed.
     c) MySQL password MUST be strong.
- MySql communication port number should be allowed in firewall.
- jcm_global_database named database must be created.

Redis Server

- Redis server communication port should be allowed in firewall.

Java

- Java 8 Update 91 must be installed.
- Older versions of Java are not supported.

Seqrite Encryption Server

- SEM default port (8443) should be allowed and it should not be used by any other application.
- If SEM server is configured with hostname then the SEM server must be accessible from the clients through SEM hostname.
- SEM server must be running and accessible from the client (SVE), where encryption/decryption process is running. So that the rescue information can be communicated to SEM Server.

Other specifications

- The laptop should have enough battery life.
- Make sure the desktop is connected to the power source.
- The laptop/desktop performance may decrease when encryption or decryption is in progress.
- The ISO image should be prepared before the encryption is done.
- In distributed deployment:
  - The recovery ISO USB should be sent before the encryption is done.
  - Every location's IT Admin should be trained for all the recovery mechanism.
- It is mandatory to take back up of your hard disk and USB before encrypting any fixed drive or removable drives.
- To avoid any hardware compatibility issue before rolling out encryption to large number of machines, a pilot testing should be conducted in customer premises on some test machines.

Installation

Downloading and installing SEM

Before installing SEM, make sure the target computer meets the prerequisites.

To install SEM, follow these steps:

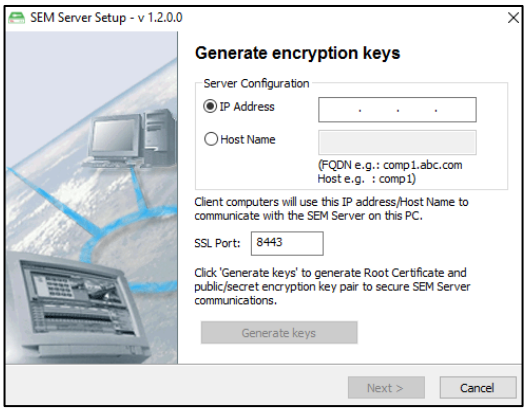
1. Open the email received from Seqrite and click the SEM Agent download link.
2. The setup will check for Java on the computer; if older version is found, a prompt is displayed to uninstall the old version and download Java 8. Click **Download and Install Java**.

After verifying the correct version of Java, the setup will continue with the installation.

The Welcome screen is displayed.

3. Read and accept the end user license agreement.
4. Select the Destination Directory.
5. Choose the name of the Program Folder as it will appear in the Start menu.

   The local files will be copied during this step.
6. Set the SEM server IP address or Host name and click **Generate Keys** to generate a root certificate and encryption keys.
7. You can change the default communication port from 8443 to the desired free port.

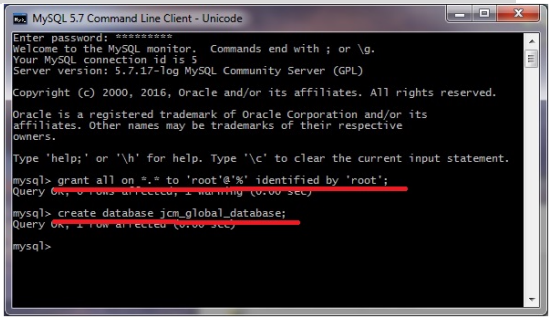


8. In MySQL database, a new database should be created, named, jcm_global_database. Also, a MySQL user should exist with the custom user name, custom password and administrator privileges.

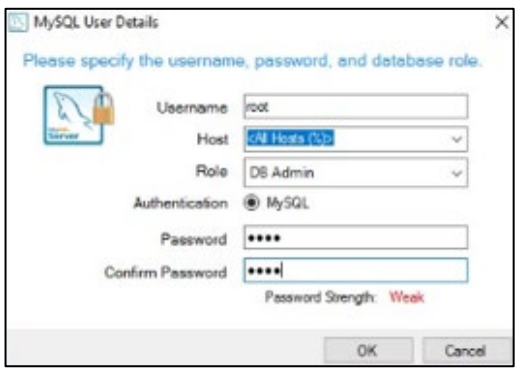
   If MySQL is already installed, open MySQL console and run these two commands:

*mysql>grant all on *.* to 'user name'@'%' identified by 'password';*

mysql>create database jcm_global_database;



- If you install MySQL right now, you can create the user during installation:

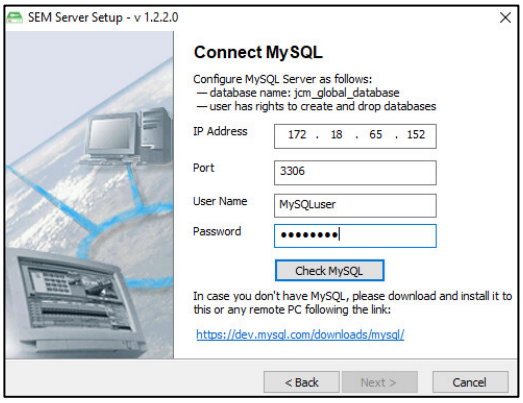


Be sure that the user Role is set to "DB_admin" and Host is set to "All hosts".

After installation is completed, open MySQL console and run the following command:

mysql>create database jcm_global_database

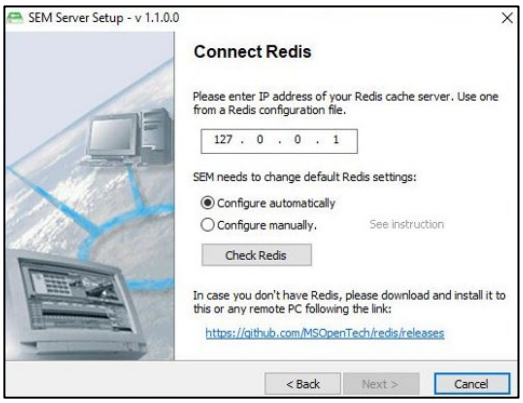
Program checks for the correct MySQL configuration.



If MySQL is not configured and if you want to see which configurations are applied, click **Check MySQL**.

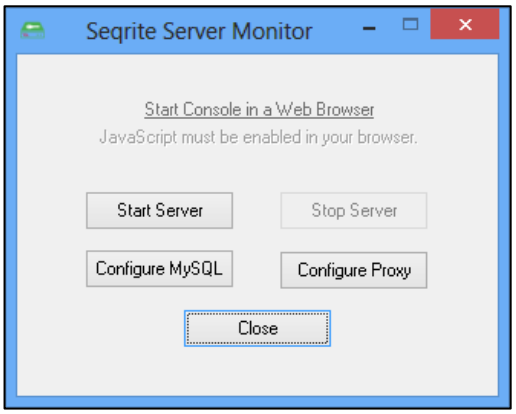
Note: On MySQL configuration dialog box, you must enter the loopback IP address (127.0.0.1).

9. SEM Server setup verifies if Redis is installed and properly configured.



- If you have not changed the default Redis configuration, leave this field as is "127.0.0.1".
- Otherwise, type the IP address that is reported in the file "redis.windows-service.conf" in the Redis program folder by clicking **Check Redis**. Click **Next**.

10. In new dialog box, click **Start Server** and then click **Start Console in a Web Browser.**



The SEM console opens in the default Web browser.

Alternatively, the SEM console can be accessed in the following ways:

- Use the link, https://*.*.*.*:8443 (where *.*.*.* is the IP address of the SEM server computer).
- If the server was installed on the same computer where SEM console is open, use the link; https://localhost:8443

Note

- For SEM 1.2.2, it is mandatory to configure MySQL. You can configure MySQL while upgrading SEM or even at the time of new installation.
- Log is not generated for any changes related to MySQL configuration.

Deploying SVE on different computers

You can deploy Seqrite Volume Encryption on your computers using either options.

Downloading SEM Agent

To add computer to SEM database with SEM agent:

1. Log on to SEM console.
2. On company page, click **Add computer**.

3. In the new dialog, box click the **Download** option available for SEM Agent installer.

   The installer will be downloaded automatically. The name of the file has the following format:
   jci_setup__JCM_SERVER_IP_PORT_NUMBER_COMPANY_ID__.exe
   For example:
   jci_setup__207_154_213_48_8443_10002__.exe

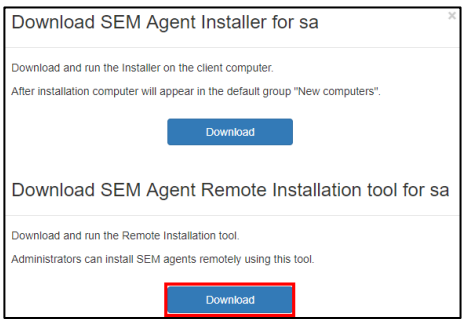
   Note: Do not rename the downloaded file.
4. Run the downloaded .exe file on the target computer that is to be encrypted.
5. After successful installation of SEM Agent, the computer name appears in the New computers group.

   If the new computer should be added in other group, the "jci_setup.." file should be run from Command Prompt with the parameter -G and the group name in the following format:
   >jci_setup__207_154_213_48_8443_10002__.exe -G#MY GROUP NAME#
   If the group does not exist, it will be created automatically, and the default encryption policy will be assigned.

Adding computers with Remote Installation Tool

You can install SEM agent on multiple computers with the help of Remote Installation Tool.

1. Log on to SEM console.
2. On the Company page, click **Add computer**.



3. In the new dialog box, click the **Download** button for the Remote Installation Tool. The Remote Installation Tool is downloaded.
4. Run the .exe file.
5. In the Remote Installer dialog box, enter the required information and click **Install**.

   For more information, refer the Remote Installation help file.

Importing Active Directory

You can import the Active Directory and sync the group with it and deploy the SVE.

1. Log on to SEM server.
2. In Computer and groups section, click **Add** > **Import active directory**.
   - To exclude any computer from installation of SVE client, click **Exclusion**.
   - In Excluded computer dialog box, select the options with which you want to exclude the computers; Exclude by Host Name, Exclude by IP address, and Exclude by IP Range.
   - Depending on your selection, the next fields change. Add in the required information and click **Add**.
   - The information gets listed in the Excluded endpoints list. You can delete a single computer or use Delete All to delete all the listed computers in the excluded computers list.
   - Click **Save**.
3. In Domain Authentication section, add parent domain credentials such as URL, user name and password, and then click **Next**.

   For example: ldap://example.com:3268
4. Select Domain and then click **Next**.
5. Add in domain authentication credentials: user name and password.

   Active Directory is loaded.
6. Select the group or computer(s) and click **Next**.

7. In Settings section, select the check box to automatically install the SVE client software on the new computers added to a group, and click **Next**.
8. In Settings section, set the time interval for SEM console to synchronize with the Active Directory container and click **Finish**.
9. On confirmation screen, click **OK**.

> Note: If the user has selected the Deploy SVE client on newly detected computer option, then any new computer added to the group, which is already synced with the Active Directory, will have the SVE client automatically installed on that computer.

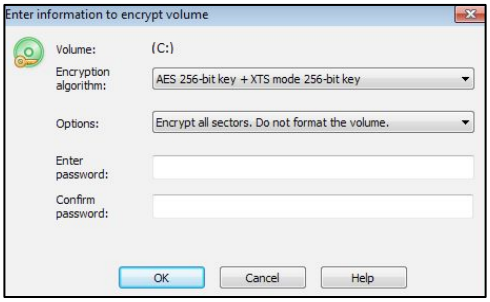
Volume Encryption

Seqrite Encryption Manager (SEM) and Seqrite Volume Encryption (SVE) are designed to provide encryption of all the data stored on fixed and removable disk devices using multiple encryption algorithms.

Encrypting the volume

To encrypt the volume, follow these steps:

1. Open Seqrite Volume Encryption.
2. On dashboard, select the volume.
3. On the menu, click **Volume** > **Encrypt Volume**. The following dialog appears:



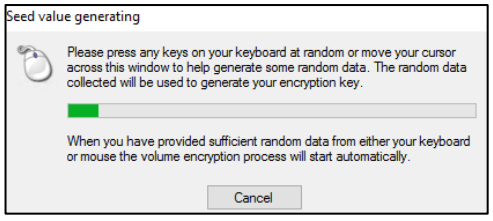
4. From the Encryption algorithm list, select the required algorithm.

   Initial encryption of disk volume runs with a speed about 30 - 60 sec/GB. Thus, it will require about 30 hours to encrypt 2 terabytes volume.

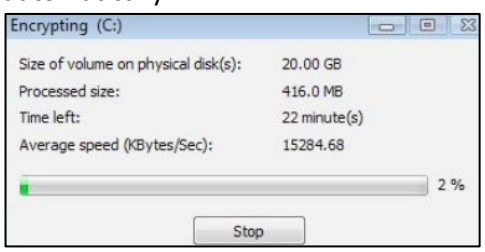
5. In the Options list, select the required option as follows:
   - Format the volume. Minimal initial encryption: In case of new hard disk, you may choose this option to format the volume and encrypt only the initialized filesystem data on the volume.
   - Erase whole volume. Format. Minimal initial encryption: With this option, SVE helps you to write random data to the volume before formatting it. Thus, no one can identify if the volume is full of encrypted data or stores nothing.
   - Encrypt all sectors. Do not format the volume: With this option, SVE helps to initiate full encryption of the volume that already stores data and must not be formatted.

   > The format option is not available for boot/system volumes, as they store system files and cannot be formatted.

6. Enter the password and confirm password, and then click **OK**.
7. To get random numbers for the seed, the program will display a dialog box and ask you to move the mouse or press keys on the keyboard randomly.



When enough random data is collected, encryption process will start automatically.



- If you want to suspend the encryption process, click **Stop**.

If volume encryption is not complete, SVE will remind you about the incomplete encryption of the volume. You can continue with the process at any time.

- To complete the encryption process, which was disrupted, select the volume and click **Volume** > **Encrypt Volume**.

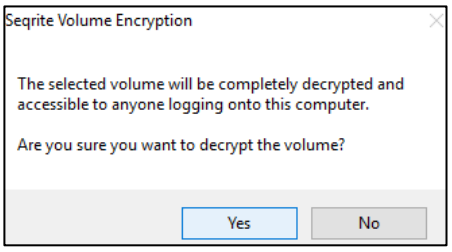
After the encryption process completes, a success message is displayed.

The encrypted volume header color on SVE dashboard turns green.

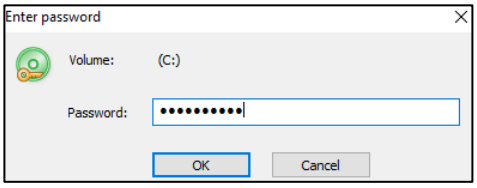
Volume Decryption

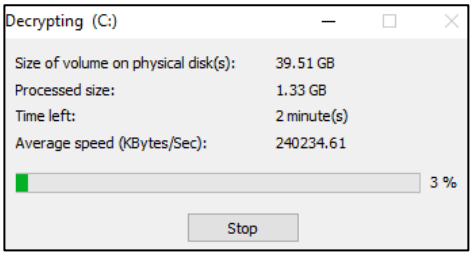
To decrypt the volume, follow these steps:

1. Open Seqrite Volume Encryption.
2. On dashboard, select the volume.
3. On the menu, click **Volume** > **Decrypt Volume**. The following dialog box appears:



4. Click **Yes**.
5. Enter the password and click **OK**.





6. After the decryption process is completed, a success message is displayed.

When the volume is decrypted, the color of volume header on SVE changes to blue.

Recovery Options/Rescue Procedures

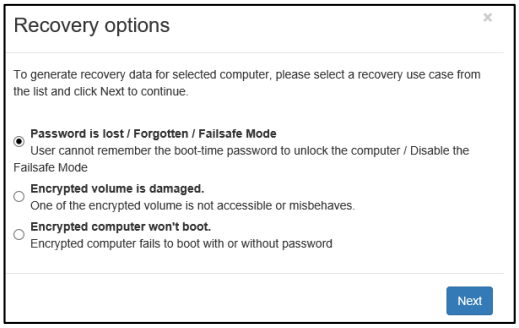
SEM provides different options to rescue computer, volume, or removable media.

Recovering computer or volume on fixed media

In this rescue method a recovery/administrator password is generated, which can be used to rescue the computer or the volume.

1. Log on to SEM console.
2. In the left pane, select the client computer. Click **Recovery Options** on the computer page. The following window appears:

3. Choose **Computer / volume on fixed media** and click **Next**.
4. In the new dialog box, choose the appropriate option and click **Next**.



- Administrator/recovery password is generated. It can be used by the SVE

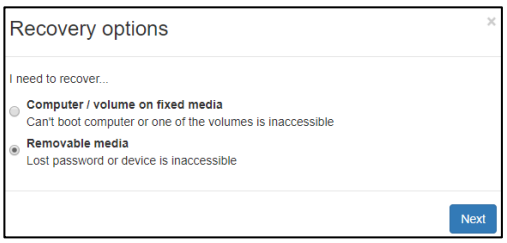
user to boot the computer or disable the Failsafe mode.

- To reset lost password, follow the instructions on the dialog box.

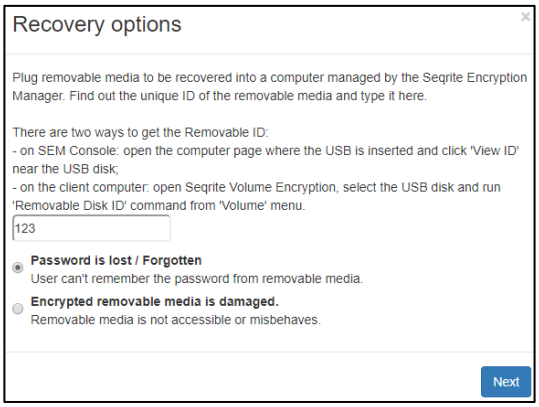
5. Click **OK**.

Recovering encrypted removable media

1. Log on to SEM console.
2. In the left pane, select client computer. Click **Recovery Options** on the Computer page.
3. In new dialog box, select **Removable media** and then click **Next**.



4. Plug removable media to be recovered into a computer managed by SEM and find the Removable ID. The dialog box instructs how to find removable ID; follow the instructions. Enter the ID in Removable ID field. Choose the appropriate reason for recovery and click **Next**.



- If a password has been lost, decryption is not required, just use the new password to mount the encrypted removable disk.
- In case of a corrupted removable drive, a Rescue File will be created in the same way as in the case of corrupted fixed volume.

Accessing encrypted USB drive using Traveller mode file

You need to download the Traveller kit file from www.seqrite.com, and perform the following steps:

1. Download and extract the Traveller_Kit file on your computer/laptop, which doesn't have SVE installed on it.
2. Connect the encrypted USB drive.
3. Run the bcfmgr.exe
4. Right click the USB drive.
5. Click the **Mount** option.
6. Enter the password.

USB drive will be mounted and become accessible.

Rescue using WinPE?

To rescue using WinPE:

On your computer, download the Rescue ISO (WinPe) from link (http://dlupdate.quickheal.com/builds/seqrite/sem/0122/en/ga/tools/Rescue_SEM1.2.2.ISO).

1. Download the Refus from https://rufus.ie/
2. Run the Rufus.exe
3. Select the downloaded ISO file by clicking the **Select** button.
4. Connect the USB drive.
5. Click the **Start** button.

   It will create the Bootable USB with rescue ISO. You must perform the following steps on the affected computer:

   i. Boot the computer from bootable USB drive.
   ii. Computer starts through rescue ISO.
   iii. On desktop, double-click the **Seqrite Volume Encryption** icon.
   iv. In the SVE application, right-click the encrypted volume and click **Decrypt**

Volume option or on menu, click the **Decrypt**  button.

v. On the confirmation dialog box, click **Yes** and then enter the master boot password.
Decryption process starts.