Copyright & License Information

Copyright © 2017–2020 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, India.

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

This document is current as of the initial date of publication and may be changed by Quick Heal at any point of time.

**Trademarks**

Seqrite is a registered trademark of Quick Heal Technologies Ltd.

**License Terms**

Installation and usage of Seqrite Encryption Manager is subject to user’s unconditional acceptance of the Quick Heal end-user license terms and conditions.

To read the license terms, visit [www.seqrite.com/eula](http://www.seqrite.com/eula) and check the End-User License Agreement for your product.
About This Document

This manual covers all the information required to install and use Seqrite Encryption Manager. The following table lists the conventions that we followed to prepare this manual.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold Font</strong></td>
<td>Anything highlighted in bold indicates that it is a menu title, window title, check box, drop-down menu, dialog, button names, hyperlinks, and so on.</td>
</tr>
<tr>
<td>![i]</td>
<td>This is a symbol used for a note. Note supplements important points or highlights information related to the topic being discussed.</td>
</tr>
<tr>
<td>![💡]</td>
<td>This is a symbol used for a tip. Tip helps users to apply the techniques and procedures to achieve a task in an easy way.</td>
</tr>
<tr>
<td>![⚠️]</td>
<td>This is a symbol used for warning or caution. This is an advice either to avoid loss of data or damage to hardware.</td>
</tr>
</tbody>
</table>

| You | Admin |
| User | Endpoint, desktop, laptop, or Tablet users |
| Company | The organization who have registered with Seqrite SEM. |
| Enable | To turn on the button or to access the feature and its sub-sections. |

<table>
<thead>
<tr>
<th>Product Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEM</td>
<td>Seqrite Encryption Manager – Console</td>
</tr>
<tr>
<td>SVE</td>
<td>Seqrite Volume Encryption – Client application installed on the endpoints and managed by SEM console.</td>
</tr>
</tbody>
</table>
## Document History

<table>
<thead>
<tr>
<th>Release No</th>
<th>Change Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>September 2020</td>
<td>• Released SEM 1.2.3</td>
</tr>
</tbody>
</table>
Contents

1. **Introducing Seqrite Encryption Manager** ..........................................................................1
   Benefits of Seqrite Encryption Manager ........................................................................... 1
   SEM Architecture and Terminology .................................................................................... 3

2. **Getting Started** ............................................................................................................. 5
   Prerequisites ......................................................................................................................... 5
      Hardware Requirements for SEM Server ............................................................................ 5
      Supported operating systems for SEM Server (64 bit) ....................................................... 5
      Required software for SEM Server .................................................................................. 6
      Supported Web Browsers for SEM Console ...................................................................... 6
         *Desktop/Laptop web browsers* ....................................................................................... 6
         *For all browsers* ........................................................................................................... 6
      Hardware Requirements for SEM Client ........................................................................... 6
      Supported operating systems for SEM clients (32 and 64 bit) ......................................... 6
      Supported file systems for SEM client ............................................................................. 7
      Supported volume types by SEM client ............................................................................ 7
   Installation ............................................................................................................................ 7
      Installing Seqrite Encryption Manager ............................................................................. 7
      Updating MySQL configuration after installation or upgrade ........................................ 12
         Configuring MySQL while upgrading SEM ................................................................. 12
         Configuring MySQL on new installation of SEM on the latest version ....................... 13
      First login to SEM Console ............................................................................................. 14
      Forgot password ............................................................................................................. 14
         Using Forgot password link ........................................................................................ 14

3. **Dashboard** ....................................................................................................................... 16

4. **Management** .................................................................................................................. 18
   Company Page ...................................................................................................................... 18
   Add computer (Deploying Seqrite Volume Encryption client) ............................................. 19
      Download SEM Agent ....................................................................................................... 19
         Downloading SEM Agent .............................................................................................. 19
      Remote Installation Tool .................................................................................................. 20
         Adding computers with Remote Installation Tool ....................................................... 21
| Contents |
|-----------------|------------|
| 5. **Central Management of Seqrite Volume Encryption** .................. | 33 |
| Central Management of Seqrite Volume Encryption .................................. | 35 |
| Applying encryption policy .............................................................................. | 37 |
| Applying encryption policy to a group .......................................................... | 37 |
| Applying individual policy to a client computer .......................................... | 37 |
| Suspend Protection ......................................................................................... | 38 |
| Working with Suspend Protection .................................................................... | 38 |
| Rescue Procedures in Seqrite Encryption Manager ......................................... | 39 |
| Recovering computer that does not boot or repair a fixed volume ................. | 39 |
| Recovering encrypted removable USB drive .................................................. | 42 |

| 6. **Administration** .................................................................................. | 44 |
| Overview of the Seqrite Encryption Manager Database ................................ | 44 |
| SEM Database Encryption and Initialization .................................................. | 44 |
| *Client-server communication* ..................................................................... | 45 |
| *SEM Administration Console* ....................................................................... | 45 |
### Contents

Accounts ................................................................................................................................. 45
  Viewing user accounts ........................................................................................................ 46
  Creating new user account ............................................................................................... 46
  Editing user account .......................................................................................................... 47
Backup and restore .................................................................................................................. 47
  Company Backup ................................................................................................................ 47
    *Taking company backup* .................................................................................................. 48
Full Backup ............................................................................................................................ 48
  *Taking full backup* .......................................................................................................... 48
Restoring the backup ............................................................................................................ 49
Licenses ................................................................................................................................ 50
  Viewing license information ............................................................................................... 50
  Activating new license ....................................................................................................... 50
  Renewing license ................................................................................................................ 51
  Reactivating license ........................................................................................................... 51
  Blocked license .................................................................................................................. 52
Software Update .................................................................................................................... 52
  Checking available update .................................................................................................. 52
  Taking software update ..................................................................................................... 52
Software Upgrade .................................................................................................................. 53
  Manual SEM upgrade using setup file ................................................................................ 53
  SEM upgrade through update ............................................................................................. 54
Redirecting to new SEM Server ............................................................................................. 55
Reports .................................................................................................................................. 55
  Company report .................................................................................................................. 56
    *Generating company report* ........................................................................................ 56
Account activity report .......................................................................................................... 56
    *Generating account activity report* .............................................................................. 56
Computer report ..................................................................................................................... 56
    *Generating computer report* ...................................................................................... 56
Endpoint Activity Report ....................................................................................................... 57
    *Generating endpoint activity report* .......................................................................... 57
Active directory report ......................................................................................................... 57
    *Generating Active Directory report* ............................................................................ 57

7. **Uninstallation** ................................................................................................................ 58
   Uninstalling Seqrite Encryption Manager ......................................................................... 58
Uninstalling Seqrite Volume Encryption from client computers ........................................ 58
Uninstallation when client-server communication is present ........................................ 58
Uninstallation when client-server communication is disrupted ................................. 58

8. **Support** ........................................................................................................ 60
Technical Support .................................................................................................. 60
Introducing Seqrite Encryption Manager

Encryption – now-a-days is not an option, but a compulsion, as it helps protect sensitive corporate data while avoiding any unauthorized access to the computers.

Seqrite Encryption Manager (SEM) provides a wide range of data protection in the form of:

1. Full disk encryption
2. Media encryption for removable devices
3. Traveller tool to decrypt the encrypted USB devices from other system, where SVE is not installed.
4. Fail Safe mode to protect your data from unauthorized access or any intruder.

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. Combine variety of encryption algorithms and create a single encryption policy or use the pre-configured policies and assign to groups or computers.

Benefits of Seqrite Encryption Manager

1. Easy deployment of SEM client via SEM agent or Remote Installation Tool or Active Directory.
2. Client-Server communication is secured with public/private key encryption and happens over HTTPS channel.
3. Support for deployment automation using Windows Group Policy or third-party utilities (e.g., Microsoft SCCM, LANDesk).
4. Automatic updates of the SEM server and client software.
5. Monitor usage of encrypted disk partitions/volumes and gather information from client computers in a central SEM database.
6. Central management of encryption policy distribution via SEM console.
Introducing Seqrite Encryption Manager

7. Administrators have the option to encrypt removable disks, such as USB sticks, with password and can set individual security policies for non-encrypted removable disks to be read-only or forbidden entirely.

8. Troubleshoot or remotely reboot the encrypted computers using suspend protection by temporarily disabling the pre-boot password.

9. Store all rescue information in SEM database, allowing security administrators to recover encrypted client data in case of emergency or forgotten password.

10. Create global reports in HTML format and PDF format.

11. Fail Safe mode to protect your data from unauthorized access or any intruder. It gets enabled, if the user enters the wrong pre-boot password for 10 times.


13. Schedule automatic update of the software.

14. Schedule for automatic backups of the Seqrite Encryption Manager Database.

15. Controlled user access to perform encryption/decryption of disk volumes.

16. Allow users to manage encryption locally.

17. Multiple user accounts with different level of access.

18. Trace back important changes made to the configuration with activity report for all the accounts or a selected one within a specified period of time. A periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours.

19. Generate a report featuring information about active accounts, licenses, managed computers and their current state in just one click. Optionally, an account activity log can be included in this report. HTML and PDF formats are supported.

20. Combine variety of encryption settings into one encryption policy. Create and save encryption policies or use a number of pre-configured policies offered by Seqrite. Apply policies to computer groups or selected computers.

21. Use featured encryption algorithms that complies best with your company standards.

22. Browse for the log of selected computer or group of computers to see the full list of changes made or use the filter to view only Warnings or Errors reported. Additionally, it is possible to filter the unread messages.

23. Provision to view the pre-boot authentication password with help of the Tab key.

24. When you plugs-in Encrypted USB, the password prompt appears automatically. Enter the password to access the Encrypted USB.

25. When you download the rescue file, the name of the rescue file contains the host name for which it is downloaded. This helps to identify the host against the rescue file.
26. Provision to redirect the SVE client to a new SEM Server. For details, see Redirecting to new SEM Server.

27. Provision to identify system type (Legacy or UEFI).

28. Provision to identify last login user.

**SEM Architecture and Terminology**

The following picture illustrates how SEM modules are organized to correctly implement the architecture.

All client computers and computers or devices actively running the SEM console communicate with SEM server using HTTPS protocol. Every request from a connected computer is recorded as a change in the SEM Database.

For example, when an administrator uses the SEM Web console to change a policy for a client computer, the SEM console sends a request to the SEM server to save the new policy in SEM Database. Then, the SEM server notifies the SEM client that it should download updated policy. The client sends a request to the SEM server and receives its new policy from SEM Database.

The picture below illustrates flow of HTTPS requests and physical architecture of SEM software.

**SEM Terminologies**
The terminologies used in this document are as follows:

- **SEM server**: The computer where SEM database and SEM web console are running.
- **SEM web console**: The application that gives access to SEM functions and settings through a web browser using HTTPS protocol.
- **SEM agent**: The agent is generated by SEM server and used on the client computers to deploy, update, or uninstall the SEM client software. The agent automatically starts running on the client computer upon log in.
- **SEM client computer**: Computers where SVE client/agent software is installed.
- **SEM client software (SVE)**: The software that is deployed using SEM Agent and is intended to perform encryption/decryption on the client computers.
- **User account**: Multiple user accounts can be created and given authentication privileges as per user role to access SEM console.
- **SEM Administrator**: A user of SEM console with administrator rights and privileges.
Getting Started

To install Seqrite Encryption Manager, ensure that you comply with the following requirements:

**Prerequisites**

**Installation of Seqrite Encryption Manager**

**First login to SEM console**

**Prerequisites**

Seqrite Encryption Manager should meet following prerequisites and supports the following operating systems:

**Hardware Requirements for SEM Server**

- RAM 2 GB (min)
- Free disk space 6 GB

**Supported operating systems for SEM Server (64 bit)**

- Windows 10 (20H1) (Maximum version 2004)
- Windows 8.x (All flavors)
- Windows 7 SP1
- Windows Vista SP2
- Windows Server 2008 R2 (minimum SP1)
- Windows Server 2012 and 2012 R2
- Windows Sever 2016
- Windows Server 2019 (Maximum version 1903)
Required software for SEM Server

- Oracle Java 8 Update 91 and later
- MySQL Server v5.5+
- Redis v2.8+
- Net framework 4.0
- Microsoft Visual C++ 2015 Redistributable 64-bit package

Supported Web Browsers for SEM Console

SEM Console will run on any one of the compatible, HTTPS enabled web browsers listed below, regardless of operating system.

Desktop/Laptop web browsers

- Google Chrome 84, 83, and 81
- Mozilla Firefox 78, 76, and 75
- Internet Explorer 11, 10, and 9
- Microsoft Edge (Chromium) 84
- Opera 69

For all browsers

- HTTPS protocols must be enabled
- JavaScript must be enabled
- Cookies must be enabled
- Images must not be blocked

Hardware Requirements for SEM Client

- RAM 512 MB
- Minimum Disk Space 250 MB

Supported operating systems for SEM clients (32 and 64 bit)

- Windows XP (All Flavors)
- Windows Vista (All Flavors)
- Windows 7 SP1
- Windows Server 2003 (All Flavors)
- Windows server 2008 and 2008 R2
- Windows 8.0 (All Flavors)
- Windows 8.1 (All Flavors)
- Windows server 2012 and 2012 R2
• Windows 2016
• Windows 10 (20H1) (Maximum version 2004)
• Windows 2019 (Max supported version 1903)

**Supported file systems for SEM client**
FAT, FAT32, NTFS, exFat, GPT and ReFS

**Supported volume types by SEM client**
RAID 1 & 5, dynamic disks, basic disk, mirrored, spanned volumes, and storage spaces introduced in Windows 8.

To check for the latest system requirements, visit our website at [www.seqrite.com](http://www.seqrite.com).

**Installation**
The installation program installs Seqrite Encryption Manager Server. Before running the installation program, ensure the target computer meets the prerequisites to run the Seqrite Encryption Manager Server.

The Seqrite Encryption Manager Server setup program follows the standard Windows installation protocols and thus gives all the necessary explanation and instructions throughout the installation process.

The setup program has the following common buttons on all the installation dialogs:

• **Cancel**: Use this button to abort installation.
• **Next**: Use this button to proceed with the installation.
• **Back**: Use this button to return to the previous step.

**Installing Seqrite Encryption Manager**
To install SEM follow these steps:

1. The user will receive the SEM Agent installer download link via email at the time of product purchase. Open the email and click the download link.

2. The setup will check if Java is installed on the computer. If it finds older version of Java, then the user must uninstall it and install Java 8.

   If Java is not found, it will display the following message:
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.
SEM Server uses MySQL database. In MySQL database, a new database should be created, named **jcm_global_database**.

**Note:**

SEM server does not accept mysql login password as **ROOT**.

- If MySQL was already installed, open MySQL console and run commands:
  - For MySQL 8.0, run the following commands:
    ```
    mysql> grant all on *.* to 'username'@' %' ;
    mysql> flush privileges ;
    mysql> create database jcm_global_database;
    ```
  - For MySQL 5.5 or 5.7 run the following commands:
    ```
    mysql> grant all on *.* to 'username'@' %' identified by 'password' ;
    mysql> flush privileges ;
    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 command:

```
mysql> create database jcm_global_database;
```

8. The next Setup window 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. The cache server Redis is used by SEM for caching. SEM Server setup will verify if Redis is installed and properly configured:

![Connect Redis](image)

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.

10. Click **Start Server**. Wait for the hyperlink **Start Console in a Web Browser** to become active. (Please wait, as this task may take some time)

![Seqrite Server Monitor](image)

11. Click **Start Console in a Web Browser** to open the SEM Console in the default Web browser. Alternatively, the SEM Console can be accessed in the following ways:
   - Using 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](https://localhost:8443)
Note:
- For SEM 1.2.3, 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.

Updating MySQL configuration after installation or upgrade

For the latest version of SEM, MySQL is mandatory. You can configure MySQL while upgrading SEM or while newly installing SEM.

Configuring MySQL while upgrading SEM

After installation, you can configure MySQL by stopping the server monitor.

1. To stop the server, click **Stop Server**.

2. Click **Configure MySQL**. MySQL Configuration Setting dialog box is opened.
3. Change User Name, Port, IP Address and click OK. MySQL configuration is updated successfully.

![MySQL Configuration Setting](image)

MySQL configuration updated successfully.

OK

**Configuring MySQL on new installation of SEM on the latest version**

1. At the time of new installation of SEM 1.2.3 server, you can check MySQL by clicking **Check MySQL**.

![Connect MySQL](image)

MySQL server gets configured properly.

![SEM Server Setup](image)

MySQL Server is configured properly.
Click Next to continue to other settings.

OK

2. Click **OK**.
First login to SEM Console

When SEM Console is opened for the first time, the program will ask you to create the first administrator account by typing the user name, company name, email address, and password.

It is recommended to create two different Administrator accounts. It will be helpful in case one Administrator forgets the login credentials, then the second Administrator can help retrieve the password.

The following steps will encrypt your company's computers with default settings:

1. After SEM installation, start the SEM server from SEM Monitor Application.
2. Open the SEM Web console.
3. Register the Administrator account by providing first name, last name, company name, email address, and password and click Create.
4. After creating the administrator account, user should login to SEM Web console.
5. On dashboard, click Administration and in the left pane, click Licenses.
6. Add in the purchased product key and click Add License.

Forgot password

Seqrite Encryption Manager gives you the privilege to reset your password for security reasons or if you forget your account password by using the Forgot password link available on the log in page.

Note:

It is recommended to create two different Administrator accounts to retrieve either accounts in case any of the Administrators forget the password.

Your account gets locked after six failed attempts of adding wrong password. When you use the Forgot password link, the password reset request is sent to the Administrator.

If your account gets locked, it will be unlocked in the next six hours automatically. But if you want to access your account immediately, you can either reset your password using Forgot password link or contact your Administrator.

Using Forgot password link

To change your account password, another user with Administrator rights can reset your password as follows:

1. The first Administrator should access the SEM log in page and click the Forgot password link.
   Password reset request is raised and is sent to the second Administrator.
2. The second Administrator has to login to SEM console and click **Administration > Accounts**. The Change Password link gets active for the second Administrator. 

![Accounts](image)

3. The second Administrator should click **Change Password**. The Change Password dialog is displayed.

Create new password and confirm the password. The password is reset for the first Administrator.
Dashboard

Dashboard is the default screen after you log on to the Seqrite Encryption Manager (SEM) console. Dashboard is unique and helps to navigate easily to all the sections of the SEM console.

SEM dashboard shows the following options:

- **Title bar**: Shows the product name and different menus such as Administration and Management.
  - **Administration**: Helps to perform backup and restore function. Also perform all administrative tasks such as manage accounts, licenses, software update and reporting.
  - **Management**: Helps complete management of company, computers, and Seqrite Volume Encryption application on different endpoints.
  - **User email ID**: shows the email ID of the administrator who is logged in the SEM console.
  - **Help**: Shows the help content for SEM console.
Dashboard

- **Logout**: Option to log out of SEM console.
- **Search computers**: Helps to search computers within the SEM database.
- **Company**: Just below search, the company name and the list of included computers is displayed.
- **License usage**: Shows the status of the license.
- **Add computer**: Helps to deploy SVE client application on the selected computers with the help of SEM agent or Remote Installation tool or Active Directory.
- **Seqrite Volume Encryption**: Encryption policies: Shows the list of all the default encryption policies applied.
- **Add new policy**: Helps to create a new encryption policy.
- **Computers and groups**: Shows a list of computers or group of computers or active directory groups added at the time of Active Directory sync up. In this section, you can create new groups, move computers or delete computers.
- **Settings**: Helps to configure company settings.
Management

Management is the default page, which is visible when you log in to Seqrite Encryption Manager (SEM) console.

Content of this chapter:

Company Page
Add Computer
Encryption Policies
Computer and Groups
Settings

Company Page

The company page is displayed as a default page when you log in to SEM console or if you select a company in the left pane. The global search helps you to find the computer with its name.
Add computer (Deploying Seqrite Volume Encryption client)

Methods to deploy SVE to the database

There are different ways with which you can deploy SVE application on client computers:

- Download and run the SEM Agent on the client computer.
- Download and run the Remote Installation Tool and then add the computers.
- Sync with Active Directory groups to deploy SVE.

Download SEM Agent

This process is beneficial when you want to install SVE client application on a single computer.

Downloading SEM Agent

To add a computer to the database with SEM agent, follow these steps:

1. Log on to SEM console.
2. On the company page, click Add computer.
3. In the new dialog, click the Download button for the installer.
   The SEM Agent installer will be downloaded automatically on the endpoint.
The name of the file has the following format:

\texttt{\texttt{jci\_setup\_JCM\_SERVER.IP\_PORT\_NUMBER\_COMPANY\_ID\_.exe}}

For example:

\texttt{jci\_setup\_207.154.213.48\_8443\_10002\_.exe}

\textit{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 should appear in the New computers group.

6. If the new computer should be added in other group, the “jci\_setup..” file should be run from Command Prompt with the parameter \texttt{-G} and the group name in the following format:

\texttt{\texttt{\textgreater \textless jci\_setup\_207.154.213.48\_8443\_10002\_.exe \_G\_#MY\_GROUP\_NAME\_#}}

If the group does not exist, the group will be created automatically, and the default encryption policy will be assigned.

**Remote Installation Tool**

Seqrite Remote Installation Tool is an integrated solution within Seqrite Encryption Manager. This solution eases the deployment of the Seqrite Volume Encryption client on all the supported Windows operating systems (OS). It also eases the deployment across multiple endpoints at a time.

The screenshot below shows the Remote Installation tool:
Adding computers with Remote Installation Tool

1. Log on to SEM console.
2. On the Company page, click Add computer.
3. In the new window, click the Download button for the Remote Installation Tool.
   The Remote Installation Tool is downloaded.
4. Add in all the required information and add the remote computers to the database. For detailed information, refer the Remote Installation Tool help file.
   To proceed further, refer the Remote Installation Tool help file.

Active Directory

You can sync a group with Active Directory and add the computers to the SEM database. When the group is synced, the Seqrite Volume Encryption (SVE) client gets downloaded and deployed on all the computers under your domain network in that group. You can also exclude any computer from installation of SVE client on it. You can exclude computers by host name, IP address, or by IP range. You can also manage the Active Directory by editing or removing the group after synchronization.

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.

Importing Active Directory

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

1. Log on to SEM console.
2. In Computer and groups section, click Add > Import active directory.
   ▪ To exclude any computer from installation of SVE client, click Exclusion.
   i. In Excluded computer dialog, select the options with which you want to exclude the computers; Exclude by Host Name, Exclude by IP address, and Exclude by IP Range.
   ii. Depending on your selection, the next field changes. Add in the required information and click Add.
   iii. 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.
   iv. 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.

6. Active Directory is loaded. 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 then 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 the confirmation screen, click **OK**.

**Managing Active Directory**

With this option, you can easily manage the Active Directory and the synced groups.

To edit or delete the Active Directory synchronization, follow these steps:

1. Log on to SEM console.

2. In Computer and groups section, click **Add > Import active directory > Manage Active Directory**.

   A list of groups synced with the Active Directory, is displayed with the details such as; name of the Active Directory, sync status, sync interval, and different actions.

3. You can perform different actions and manage the active directory. The action icons are displayed in front of every group such as:

   ▪ **View Details**: Click this option to view a complete information about the computers in synced Active Directory such as: computer name and IP, deployment status, and policy applied.

   ▪ **Edit**: Click this option to change the active directory synchronization information such as settings and sync interval.

   ▪ **Delete**: Click this option to delete the synced Active Directory. Then on the confirmation dialog, click **OK**.

**Activity log**

The Activity log gives all the information about the activities carried out on the groups in the active directory. The Activity log gives following information such as; group name, date and time of the activity, and the activity information.

**Encryption Policies**

You can protect the data on the client computers by assigning an encryption policy. Seqrite Volume Encryption installed on the client computer applies the encryption policy, assigned by the administrator. After SEM installation, number of encryption policies are created
automatically. The default policy is Encrypt, which will be applied on newly created groups or SVE deployment using Agent installer or Remote Installation tool.

Encryption policy is a group of settings to manage encryption on all local volumes, and fixed and removable devices on the client computers. The encryption policy is implemented using Seqrite Volume Encryption software installed on the client computers.

About encryption policies
You can define encryption policies with different actions for fixed drives and removable devices, and by using appropriate encryption algorithms.

Fixed drive action: With the following actions for fixed drives, you as an Admin, can manage the encryption policies.

- **Encrypt**: When you apply this policy, you ask the user on the client computer to enter a password and start the encryption process. With this policy, all the local volumes will be encrypted. However, the mapped network drives will not be encrypted.
- **Decrypt**: When you apply this policy, you initiate the decryption process on the client computer.
- **Manage locally**: With this option, you give the rights to the user to manage the encryption process on the local or single computer.
- **Encrypt volumes without drive letter (mount points)**: You can select this check box, if you want to encrypt mount points.

Removable devices: With this option, you can configure different settings for removable devices in a policy.

- **Encrypt**: When this check box is selected and a removable device (i.e. a USB drive) is connected to the computer, the user will be asked to enter a password and start the encryption of the removable device. If the user refuses to encrypt, then the access to the removable device will be restricted. The restriction on the removable device will read-only or blocked depending on the other option selected. When this check box is not selected, the user will not be forced to encrypt the removable device.
  For an encrypted removable drive, the user will be able to enter the password either to decrypt or continue using it.
  - **Read-only access if media is not encrypted**: You can select this option to provide read-only access to the removal device if the user resist to encrypt the removable device.
  - **Block access if media is not encrypted**: You can select this option to block complete access to the removal device if the user resist to encrypt the removable device.

- **Encryption algorithm**: You can use different encryption algorithms to manage the policies. SEM provides different algorithms such as; AES, RC6, Twofish, and Serpent.

- **Single Sign On Action**: The SEM Administrator can apply Single Sign On policies on the endpoints using the Single Sign On actions such as:
Management

- **User Control**: With this action, the Administrator gives the endpoint user the privilege to associate with Single Sign On authentication on their own. It is user’s choice to enable Single Sign On or not.

- **Enable**: When this option is selected, the Administrator directly applies the Single Sign On authentication policy. The user will receive continuous prompt on the computer to opt for Single Sign On until the user accepts it after the encryption of the volumes.

- **Disable**: When this option is selected, the Administrator disables the applied Single Sign On authentication policy.

**Creating new encryption policy**

To create a new encryption policy:

1. Log on to SEM console.
2. On dashboard, in the encryption policies section, click **Add new policy**.

3. Add the new policy name.
4. Enter the action for fixed drives;

```plaintext
Add new policy

Policy name: New policy

Fixed drives action:
- Encrypt

Removable Devices:
- Encrypt
  - Read-only access if media is not encrypted
  - Block access if media is not encrypted

Encryption Algorithm: AES

Single Sign On action:
- User Control
  - Note: If two users use the same pre-boot password, then the first user's Single Sign On gets dissociated.

Add
```
▪ Encrypt: Select this option to encrypt the drives.
▪ Decrypt: Select this option to decrypt the drives.
▪ Manage locally: Select this option to give authority to the user to either encrypt or decrypt the local computer.
▪ To encrypt the mount points, you can select the check box.

5. To encrypt the removable device, select the Encrypt check box. Depending on your policy, you can either block or provide read-only access to the removable device if the user does not encrypt the removable device.


7. Select the SSO Action and click Add.

The encryption policy is created and is listed under the encryption policy section.

**Editing encryption policy**

You can edit the existing encryption policy.

1. Log on to SEM console.

2. On dashboard, in encryption policy section, click the policy name that is to be edited.

3. In the Edit policy dialog, make the necessary changes and click Save.

**Deleting encryption policy**

You can easily delete the encryption policy.

1. Log on to SEM console.

2. On dashboard, in encryption policy section, click the policy name that is to be deleted.

3. In the Edit policy dialog, click Delete. On confirmation dialog, click Delete.

**Note:**

You can delete only that policy, which is not applied to any group.

**Computer and groups**

Segrite Encryption Manager provides convenient way for managing groups of computers. The first (default) group is created automatically by the setup program and the group is given the name “New computers”. You cannot delete this default group. Newly added computers will appear in this group, unless the SEM Agent Setup file is launched with the special key -G.

There is no limit to the number of groups that can be created. You can add maximum of 100 computers to a group. Client computers can be distributed among these groups in any way by the SEM administrator such as physical location, security policy, or any other attribute. Both
Management

computer groups and the computers within a group are displayed in ascending alphabetic order.

You can assign encryption policy to a group or to a computer. A group policy is applied on a Group page, while an individual policy is applied on a Computer page. If an individual policy is assigned to a computer, the computer is marked with the gear icon in the list.

The Admin can sync a group with active directory and add the computers to the SEM database. Such group is created with the following nomenclature: DomainName.OuName. Thus, such Active Directory groups are beneficial to deploy SEM client on different computers.

The Computer and groups section allows the SEM Administrator to perform following useful functions:

- Creating new computer group
- Renaming existing group
- Deleting an empty computer group
- Moving a computer to another group
- Deleting one or several computers from the databases
- View the encryption policies assigned to computers and groups
- View the status of computers in the database (whether they are online or offline)
- See which computers in the database are 'policy-compliant'
- View what client software is installed as well as the version number and date of the last update
- Install/uninstall client software

This is an example of simple view of Company page with computer groups:
About Group Page

If a group is selected in the left pane, the Group page is displayed in the right pane as follows:

- **General information**: Shows information about number of computers that are policy non-compliant, number of computers having errors and warnings. The edit icon (pencil) helps to edit the group name.
- **Group Settings**: Helps to manage Seqrite Volume Encryption on all the computers in the group, apply or change the encryption policy, and enable or disable Suspend protection option.
- **Activity Log**: It shows the activity logs for all the computers included in the group. The log can be filtered to show only the errors or warnings.

About Computer Page

The computer page shows detailed information about selected client computer as follows:

- **General information**: This section shows information about the computer, connection status, policy compliance, warnings and errors, operating system and IP address. The computer icon indicates the current status of the device.
- **Main window**: Shows settings to manage Seqrite Volume Encryption on the computer and the activity log.
• Deployment: Shows information about deployment status, version of client software installed, last update date, and uninstall option.

Depending on computer's state and settings, additional icons may appear near the computer name in the left panel:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Individual policy is set</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Protection is suspended</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Error occurs on the computer</td>
</tr>
</tbody>
</table>

### Adding a group

You can add a regular group as well as an Active Directory group.

To add a group:

1. Log on to SEM console.
2. In Computers and group section, click **Add group**.
3. In Add group dialog, add group name and then select and apply the encryption policy.
4. Click Add. The new group is listed in the Computers and group section.

*i* Note:
Whenever a group is synced with the Active Directory, the group is also listed in Computers and group section.

**Renaming existing group**

To rename the existing group:
1. Log on to SEM console.
2. In Computers and group section, click the edit (pencil) icon.
3. In Rename group dialog, change the group name and click Rename.

**Move Computer(s)**
You can easily move computers from one group to another.

If a computer is moved from Group1 to Group2, the computer gets the encryption policy of Group2. If the computer is already encrypted and the “move” operation would cause change of encryption algorithm, then the program will ask to decrypt the computer first and then attempt to move the computer again.

**Moving computer from one group to another**
To move computer:
1. Log on to the SEM console.
2. In Computers and group section, select the check box for single or multiple computers or the computers in the group.
3. Click **Move computers(s)**. If you have selected multiple computers, the dialog displays the number of computers that were selected to be moved.

4. Select a group from **Select group** list.

5. Click **Move**. The computer is moved successfully to the new group and new group encryption policy is applied.

**Delete computer(s)**

Seqrite Encryption Manager (SEM) console provides an option to delete a computer from SEM database. If a computer is deleted, then that computer will not be managed by the SEM and both the Seqrite client software and SEM agent will be uninstalled.

**Deleting computers from a group**

You can initiate computer deleting operation, i.e. mark a computer for deletion in two different ways:

1. Log on to SEM console.

2. In the Computers and groups section, select one or several computers, and click **Delete computer(s)**:

3. On the confirmation dialog, click **Delete computer**.
4. Further you can perform the automatic or manual deletion depending on the server connectivity.

**Automatic computer deletion**

When the client computer is rebooted and the connection with the SEM server is established, the following actions are performed automatically:

- For encrypted computers: All the volumes are decrypted.
- After reboot or re-logon: Seqrite client software is uninstalled.
- After next reboot: SEM agent is uninstalled.

The computer is completely deleted from database, the computer page disappears.

**Manual computer deletion**

If the client computer cannot be connected to the server then you can perform the deletion procedure manually:

1. Download **agent_uninstaller** using the hyperlink provided on the computer page for the “marked for deletion” computer.

2. Run the **agent_uninstaller** on the client computer. It is recommended to run this program from Command Prompt to see program reports.

3. For encrypted computers - decrypt all the volumes.

4. Reboot the client computer.

To completely remove the computer from the database, go to the computer page of that computer and click **Force delete**. Its computer page disappears.
Note:
The action marked for deletion is irreversible, however, while the computer is not deleted, the rescue information is still stored in SEM database. Thus, if the computer is encrypted and cannot be decrypted for some reason, “marked for deletion” page provides the link to download the recovery information for rescue decryption. Encrypted volume should be decrypted before deleting the computer from the SEM server.

Settings
The Settings options helps to make some company setting changes.

Editing company setting
1. Log on to SEM console.
2. On Management page, at the lower right section, click Settings.
3. In Company settings dialog, you can change the following:
   - Company name: Edit the company name.
   - Seqrite Volume Encryption: To install SEM Agent with SVE application on the computers, you must always keep this check box selected.
4. Click Save.
Central Management of Seqrite Volume Encryption

Seqrite Volume Encryption (SVE) is the client software installed on the client computers.

This chapter includes:

**Central Management of SVE**
**Applying encryption policy to a group**
**Suspend Protection**
**Rescue Procedures in SEM**

Seqrite Volume Encryption (SVE) software allows the user to encrypt all the data on existing disk partitions and disk volumes. This includes both basic and dynamic disk volumes as well as boot/system partitions. The main window of SVE software is as mentioned below.

Seqrite Volume Encryption (SVE) is managed by Seqrite Encryption Manager (SEM), its management completely depends on the encryption policy applied by the SEM administrator.
If the policy forces encryption, then before starting the process, the user will be asked to enter a password twice. As soon as the encryption process starts, the user must enter the password at boot time.

If the policy forces encryption or decryption process, the process runs in the background, but its progress is displayed:

![Encryption and Decryption Progress](image)

The User can stop (pause) the process, but it automatically resumes after a sometime. The process can also be resumed after restarting or hibernating the computer.

If the policy forces encryption or decryption process, the SVE main window can be opened, but most of the functions are not active. The following commands are available in this mode:

- Mount/Dismount encrypted volume (Volume menu).
- Decrypt with Rescue File (Rescue menu): The option is used in case if the volume is damaged and the standard decrypt operation does not work. The command is available for dismounted volumes.
- Recover/Change Boot Password (Rescue menu): This option changes the master password or resets it using the Administrator password generated by SEM Server. In both the cases, the corresponding message will be sent to the SEM Server.
- Manage Boot Passwords (Volume menu): Change/add/remove additional boot passwords.

If the policy is set to Manage locally, all the standard SVE commands are available on the client computer. The user can encrypt or decrypt volumes and change various settings. As soon as the Encrypt policy is applied, the program will ask user to enter boot-time password and volume password to make all volumes encrypted with single master password:
If volumes were encrypted with different encryption algorithms, it will not be changed, but the computer will be considered as policy non-compliant even after the encryption process is finished. The same behavior is applied in case if the client computer was previously encrypted with standalone version of SVE (not managed by SEM).

To reduce the risk of losing encrypted data, SVE always creates and updates the rescue file necessary to recover encrypted disk volumes in case of an emergency. With Seqrite Encryption Manager, all the rescue information from the client computers is saved securely in the SEM Database. As a result, the SEM administrator can run a recovery process on client computers encrypted by SVE without any user's activity.

Encryption policy also includes the option for removable devices. If it is set to force the encryption, then when inserting a non-encrypted USB drive, the user will be asked to enter the password to encrypt the device. If the user refuses to encrypt it, access to the device will be blocked or restricted. If the policy does not force encryption of removable devices, then when inserting encrypted USB disk, the user will be asked if the device should be decrypted or not.

**Central Management of Seqrite Volume Encryption**

After the successful deployment of Seqrite Volume Encryption (SVE) on remote computers, administrator can manage SVE on client computers through Seqrite Encryption Manager Console:
Seqrite Encryption Manager Database receives and displays the following information from SVE software running on the client computers:

- Information about all disk volumes (partitions) on the computer including sizes, labels, and volume types.
- Status of every disk volume (encrypted/partially encrypted/not encrypted/error).
• Log information about SVE events (encrypting/decrypting volumes, installation of new disk volumes, volume errors, etc.).

• Rescue information about all the encrypted volumes.

Additionally, the administrator can click Recovery Options to prepare rescue file or rescue bootable disk to recover encrypted disk volume on the selected computer.

**Applying encryption policy**

The SEM Administrator can manage client computers by applying encryption policies to the whole group or to the selected computer.

**Applying encryption policy to a group**

To apply an encryption policy to a group:

1. Log on to SEM console.
2. In the left pane, select the group name to which you want to apply the encryption policy.
3. In Group settings, click the current encryption policy name.
4. In Select encryption policy dialog, in Select policy list choose the required policy.
5. Click **Apply**.

![Select encryption policy dialog](image)

**Applying individual policy to a client computer**

To apply an individual policy to a client computer:

1. Log on to SEM console.
2. Select the computer in the left pane and select the **Use individual encryption policy** option.
Central Management of Seqrite Volume Encryption

The dialog Select encryption policy will appear.

3. Choose the required policy and click **Apply**.

Computers with individual policies are marked with the gear icon in the list of computers:

[DESKTOP-02807HF]

If the applied policy forces the SVE software to encrypt fixed disks (in the policy, Fixed drive action = Encrypt), SVE will ask the user on the client computer to enter a password to encrypt the volumes. The encryption will start and will be performed in the background. The process can be stopped, but it will be automatically resumed after a short time or after reboot. As soon as the encryption process starts, the user will be asked to enter the password at boot.

**Important:**

The automatic encryption may not start (or not resume) for the following reasons:

- The client computer was not rebooted after installation.
- SVE main window is open on the client computer.
- The client-server connection has been lost.

**Suspend Protection**

The SEM Administrator can temporarily suspend the client protection (i.e. remove boot-time authentication). In this case, the volumes will remain encrypted. This feature may be required to allow the computer(s) to restart automatically (Windows Updates, backup purposes, etc.). The feature is especially necessary when managing servers that are required to function around the clock.

**Working with Suspend Protection**

1. As soon as the administrator enables this option, it is reported by the SEM Console to the log file: “Server: Suspend Protection set for computer 'compluter name’”

2. After that, if the client computer is ON, another report in the log file is expected: “Client: Suspend Protection set for computer 'compluter name’”

3. If the client computer is OFF, it will receive the setting and send this report to the SEM console when it is turned on. Upon receiving this confirmation from the client, boot-time authentication is removed.

4. As soon as the administrator disables this option, two records appear in the log file:

   “Client: Suspend Protection unset for computer 'compluter name’”

   “Server: Suspend Protection unset for computer 'compluter name’”
5. At this point, the boot-time authentication is restored.

6. Computers with “Suspend protection” option enabled are marked with the Pause icon in the list of computers:

Further, the status of such computer is set to “yellow” on the computer page with the following warning:

```
<table>
<thead>
<tr>
<th>JULVM-W1064</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline, policy complied</td>
</tr>
<tr>
<td>Warning: protection suspended</td>
</tr>
</tbody>
</table>
```

**Note:**

The option, Suspend Protection exposes a security risk. For example, someone can take access of the computer by taking it outside the company’s network and gain access to the data.

It is always recommended to disable this option as soon as automatic reboot is no longer required.

### Rescue Procedures in Seqrite Encryption Manager

The Seqrite Encryption Manager (SEM) database stores recovery information for disk volumes (partitions) encrypted on remote client computers with Seqrite Volume Encryption (SVE) software.

When you download the rescue file, the name of the rescue file contains the host name for which it is downloaded. This helps to identify the host against the rescue file.

**Recovering computer that does not boot or repair a fixed volume**

1. Log on to SEM console.

2. In the left pane, select the client computer. Click the **Recovery Options** on the computer page.

The following window appears:
3. Choose Computer / volume on fixed media and click Next.

4. Choose the appropriate option:
   - **Password is lost / forgotten/ FailSafe**: Select this option, if unable to recall the password for the encrypted computer or FailSafe mode is enabled on the endpoint because of wrong password attempts. Decryption is not required in such case. A recovery password will be automatically generated, which can be used to boot the computer.

   Note:
   - After booting the computer with the recovery password, it is possible to change the password on the client computer using the menu: **Rescue > Recover/Change Boot Password**.
   - To change the recovery password, the user must decrypt and then encrypt the system again.
   - **Encrypted volume is damaged**: Select this option to repair a non-system volume. The program will generate a Rescue File. The file can be generated with the same password
that was used to encrypt the volume, or with a new password. The following window provides the options with detailed instructions on how to use the Rescue File:

**Encrypted computer won’t boot:** Select this option to recover the client computer that will not boot. In this case, a bootable USB disk is created that can be used to boot the computer and run rescue decryption. The following window shows the detailed instructions:
Recovering encrypted removable USB drive

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

   ![Recovery options - Step 1](image)

   Select Removable media and then click Next.

   ![Recovery options - Recover removable drive](image)

   3. Follow the instructions to get the ID for the corrupted USB drive.

   **Note:**

   You can locate the cursor inside the ID field and press Spacebar, the program will display a list of all the IDs registered in the database. Choose the appropriate ID and click Next.
5. Select the option that corresponds to the issue, either the password is lost, or the removable device has been corrupted. 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 an corrupted fixed volume.
Administration

Overview of the Seqrite Encryption Manager Database

Seqrite Encryption Manager (SEM) encrypts sensitive information in its database and in the communication channel between SEM Client computers and SEM Server. SEM utilizes public/private key technology to provide this functionality.

This chapter includes:

- SEM Database Encryption and Initialization
- Accounts
- Backup and restore
- Licenses
- Software Update
- Software Upgrade
- Redirecting to new SEM Server
- Reports

SEM Database Encryption and Initialization

When SEM Console runs for the first time, the program automatically creates the first company and the first administrator account. At that time, two public/private key pairs are generated. The generation procedure runs on a local computer where the SEM Administrator starts initializing the SEM database. The generated keys are password protected. As the keys are generated on the local computer, the keys are transferred to remote database in a secure form.

**The two key pairs function in the following manner:**

1. The first key pair is a Company Key. It is used to encrypt all sensitive information in SEM Database.
2. The second encryption key pair is an Administrator Key. It is used to encrypt the Company Key. SEM allows creating user accounts with different roles (Administrator, Operator, and Auditor). Multiple persons can manage SEM database with different user roles, thus each person should have their own password and key pair. A personal key can be used to encrypt the Company Key. This two-level key architecture allows the addition and removal of user accounts that can gain access to different portions of the sensitive data stored in the SEM database.

When SEM generates an Administrator Key, it asks for a password to encrypt the private key. Then SEM generates a Company Key and encrypts it with the Administrator’s public key. This means that the Company Key can only be decrypted by this Administrator’s private key which, in turn, has been encrypted by a key derived from the Administrator password.

Client-server communication

SEM secures the communication channel between the server and its clients using HTTPS protocol.

As part of the SEM Server installation, the SEM Setup program generates a public/private key pair and creates a server root certificate. When the SEM Client computer connects to the server for the first time, it receives the server certificate, generates its own private/public key pair, and sends a request to the server to sign the keys. After the successful completion of this process, a client can verify the server since the client has the server certificate. Additionally, the server can verify all further requests from the client, since it has signed the client keys.

The communication channel between client and server is protected, because all the information sent by the client to the server is encrypted by the server public key. When the client receives an encryption policy or any other data from the server, it can validate that the data comes from a proper server by ensuring the data is signed by the proper certificate.

SEM Administration Console

The administration console allows number of administrative functions:

- Control the SEM console and manage user accounts.
- Backup/restore the SEM database and configure settings for automatic backup.
- Update the software and configure settings for automatic updates and upgrade.
- Perform SEM server activation.
- Create and view different types of reports.

Accounts

You can access Seqrite Encryption Manager (SEM) console from any device using HTTPS protocol for communication with SEM Server. SEM Console uses standard web browser to access the interface. When the database is created, it initializes the first user that has access to SEM Console. The user has administrator rights and can perform any action provided by the
software. This first administrator can create another user account and assign a role for each user.

**Note:**
It is mandatory to create two different Administrator accounts with admin privileges. It helps to retrieve the forgot password.

The user role determines the assigned privileges. Different user roles are as follows:

- **Administrator:** Has complete authority of SEM console. The Administrator can manage and control accounts, backup and restore, companies and licenses, software update and upgrade, and reports.
- **Operator:** Has privilege only to backup and restore, manage companies and licenses, manage reports (without activity reports) available under Administrator account.
- **Auditor:** Manages only reports (without activity reports) that are available under Administrator account and view current configuration and generate reports.

**Note:**
If the user account gets locked, it will be unlocked automatically in next 6 hours. But, if the user wants to unlock the account immediately, then contact the Administrator or use the Forgot password link.

**Viewing user accounts**

1. Log on to SEM console.
2. On title bar, click **Administration**.
3. In left pane, click **Accounts**.

   By default, Accounts page is displayed with the list of user accounts.

**Creating new user account**

1. Log on to SEM console.
2. On title bar, click **Administration**.
3. In left pane, click **Accounts > Create new account**.
4. Enter the first name, last name, and email ID of the account user.

5. Select the user role that is to be assigned to the user.

6. Create the password and confirm it again.

   After the account is created, the user can login to SEM Console using the email and the password as authentication.

7. Click Create.

   Private key is generated for the user account.

**Editing user account**

1. Log on to SEM console.

2. On title bar, click Administration.

3. In left pane, click Accounts.

4. To edit the user account, click Edit link available in front of it.

5. Make the changes and click Save.

**Backup and restore**

You can easily take back up of SEM database with company backup and full database backup.

**Company Backup**

Company back up can be performed manually or you can schedule it. You can take backup of the following data:

- A list of client computers
- All groups of computers
- A list of encryption policies
- The assigned policies for groups and computers
Taking company backup

To create a backup or change backup settings for a company use company backup.

1. Log on to SEM console.
2. On title bar, click Administration.
3. In left pane, click Backup and restore.
4. Click the client computer arrow to access the information.
   - To schedule the company backup, select the Backup automatically every check box. Provide schedule, by selecting Day, Week, or Month. Then select the duration for which the backup is to be maintained in SEM database such as One Week, One Month or Forever.
5. To take company backup, click Backup now.
6. In Backup now dialog, add the comment and click Create backup.

   Backup is taken successfully.

Full Backup

It is always beneficial to take full backup of all the database. You can take full backup manually by SEM or MySQL administrator.

Note:

- If the SEM Server's host computer is no longer operational, it is strongly recommended to regularly take full backup and store them on another computer.
- Full Backup & Restore functionality is applicable only for the same product versions.

Taking full backup

To take full back up:

1. Save the following files and subfolders from the directory where SEM Server is installed to a backup location (external drive or other computer is recommended):
   - key.jks
   - cacerts.jks
   - application.properties
   - cert (subfolder)
   - backup (subfolder)
2. Take back up of MySQL database:
   ▪ Open command prompt as Administrator
   ▪ Go to MySQL installation directory and “bin” subfolder
   ▪ Run the command: “mysqldump.exe -u user name -p(password) --all-databases>dumpfilename.sql"

   ![Note]
   In the above command, you must use the user name and password used for MySQL database connect.
   ▪ The backup is stored in the file “dumpfilename.sql”

3. Save the file to a backup location on an external drive or other computer.

**Restoring the backup**

In this process, you can restore the backups taken manually.

![Note]
New SEM server must have same MySQL version installed to restore the database.
If any computer is added lately after taking this backup, then that computer will be uninstalled.

1. Log on to SEM console.
2. On title bar, click **Administration**.
3. In left pane, click **Backup and restore**.
4. Click the **arrow** to list down the backups.
5. To restore the backup, click the **Restore from this link** of that backup.
6. On confirmation dialog, click **Restore**.
7. Conduct a fresh install of SEM Server. The IP address of that machine should be same as that of old server.
8. Stop SEM Service (or otherwise ensure it does not start).
9. Copy the files and subfolders from the backup location to the directory where SEM Server is installed
   ▪ key.jks
   ▪ cacerts.jks
   ▪ appplication.properties
   ▪ cert (subfolder)
   ▪ backup (subfolder)
10. Restore MySQL database:
    i. Open the command prompt as Administrator.
    ii. Go to MySQL installation directory and “bin” subfolder
    iii. Run the command: “mysql.exe -u user name -p(password) <ltdumpfilename.sql”
    iv. Start SEM service.

Licenses

You can add new licenses to your company with Licenses option. Every new company will be given a product key that is to be activated. If the license expires, you can easily renew your license. Also, if you want to reactivate the license, you can reactivate it on the same computer or on different computer.

Viewing license information

The license page gives information about the company and license. To view license information, follow these steps:

1. Log on to SEM console and click Administration.
2. In the left pane, click Licenses.
   The license page shows the following information:
   ▪ Company: Shows company name.
   ▪ Product key: Shows the licensed product key.
   ▪ Corporate email: Shows the company’s corporate email ID.
   ▪ No. of license: Shows the total number of licenses allocated and the used licenses.
   ▪ Expiry date: Shows the expiry date of the license.
   ▪ Update license button: You can update the license after any renewal, activation, or addition of additional licenses. This helps to update the license information.
     o Click Update license button to sync with the server and update the license information.

Activating new license

When you access the license page, if you have newly purchased the product, you have to activate the license. Company name, first and last name, and corporate email is displayed automatically. Further, fill in the form and activate the license. If all the information is correct, the license gets activated.

1. Log on to SEM console.
2. On title bar, click Administration.
3. In the left pane, click Licenses.
4. If it is a new license, a form will be displayed. Add in the product key and fill all the information and click **Register Now**.

![Registration Form]

### Renewing license

After license expiry, you must renew the license. On SEM portal, Renew link is displayed for easy product renewal.

To renew the product license, follow these steps:

1. Log on to SEM console.
2. On title bar, click **Administration**.
3. In the left pane, click **Licenses**.
4. Renew now link is displayed on the Management page and License page. To renew your license, click the Renew now link and **contact the sales person**.

### Reactivating license

You can reactivate the product key on SEM server on the same computer until the license is valid. However, if you want to reactivate the product key on a different computer, within 30 days, contact the Support team.

1. Log on to SEM console.
2. On title bar, click **Administration**.
3. In the left pane, click Licenses.

4. A form will be displayed. Add in the product key and fill all the information and click Register Now.

**Blocked license**

In some scenarios, your license may be blocked. Upgrade and update functionality will not work if your license is blocked. To unblock the license, you must contact the Support team.

**Software Update**

You can use this option to update the Seqrite Encryption Manager (SEM) server, SEM Agent, Seqrite Volume Encryption or to change the software update settings. The software update can be scheduled to be installed automatically.

**Checking available update**

In SEM console > click Administration > Software update > Check now.

Available updates will be displayed.

**Taking software update**

1. Log on to SEM console.

2. In title bar click Administration.

3. In the left pane, click Software update.

4. You can add a schedule to regularly install the updates:
   - Select the Check for updates check box and select the duration.
   - Select the Install automatically at check box and then select the timing by clicking the arrows.

5. To update the software immediately, click Update now.

   The Version column shows the current version numbers for SEM Agent, SEM Server, and SVE software. If update is available, the Latest Version column will show the new versions of the modules.

   **Note:**

   If SEM Server is updated, then the SEM Service will restart and then the users have to log in again to the SEM Console.

   At the time of update, if Java 8 update 91 and later version is not found, then the user will receive following message to update Java to latest version.
Software Upgrade

You can easily upgrade SEM server, SEM agent, and SVE applications. SEM upgrade can be done manually with setup file or using the updates.

>Note:

It is always recommended to take back up of your database before performing the upgrade function.

Manual SEM upgrade using setup file

You can have a manual upgrade when you have the SEM setup.

1. Run the higher version of SEM setup.
2. In the Welcome setup dialog, click Next.
3. In License Agreement dialog, select the **I accept the Agreement** and the **Consent** check box and click **Next**.

![License Agreement dialog](image)

4. In SEM setup dialog, click **Finish**. Seqrite Server Monitor dialog will be displayed.

5. To start SEM Console in a Web browser, click **Start Server**.

![Seqrite Server Monitor dialog](image)

**SEM upgrade through update**

With update, you can upgrade to the higher SEM version. The updates provide you with the options to frequently check for updates and also set time to automatically install the higher version of the SEM application whenever available.
To automatically upgrade SEM with the help of updates:

1. Log on to the SEM server and click **Administration**.

2. In the left pane, click **Software update**. Whenever the upgrade is available, a notification will be displayed next to Software update and the **Update now** button will be enabled on the page.

3. On the Software Update page, click **Update now**.

   If you have already configured the **Check for updates** and **Install automatically at** check boxes, then the upgrade of all the applications will be done as per the configuration.

4. In the Upgrade information dialog, click **Update**.

5. Seqrite Encryption Manager server upgrade will start and the server will not be available to the client computers until the server resumes the services. You need to reload the page again after some time.

### Redirecting to new SEM Server

You can redirect the SVE client to new SEM Server by re-installing the client agent setup of new SEM Server. You can do client redirection to new SEM Server using Agent installer.

1. Deploy new SEM Server on other system.

2. Download agent installer from New SEM server.

3. Run the agent installer on existing clients.

   A dialog appears with message, “It seems that SVE agent was already installed for different SEM server Do you want to re-install the SVE agent for the new SEM server."

4. Click **Yes**. The server information is updated. The client will be redirected to the new SEM Server. If you click **No**, you will exit the agent installer.

5. Restart the system when the Restart prompt appears.

### Reports

Seqrite Encryption Manager (SEM) gives options to create different types of reports such as company report, account activity report, computer report, active directory report.
Company report

The company report gives information about user account, license information, backup information, Active Directory information, and current state of all the computers. This report can be generated in either PDF or HTML format for the selected group (or for all groups). You can also include activity log for a specific time.

Generating company report

1. Log on to SEM console and on title bar click Administration.
2. In left pane, click Reports.
3. In Company Reports section, from Groups list, select All groups or specific computer.
4. Select the Include activity log for a time period check box and then select the date range.
5. Select the Report format either PDF or HTML.
6. Click Generate Report.

Account activity report

You can generate report for user accounts and their activities for specific time. It shows the following user actions; login/logout, create/Edit/Assign an encryption policy, add/delete/move computers, create/edit/delete user account, add a license, retrieval of rescue information, set/reset Suspend protection option, synced Active Directory, changes in passwords, create backup and change backup settings, and restore from backup.

Generating account activity report

1. Log on to SEM console and on title bar click Administration.
2. In left pane, click Reports.
3. In Account activity report section, in Select an account list, select the user account.
4. Select the date range from Time period option.
5. Select the Report format option and click Generate report.

Computer report

This report informs about the current state of the computers and the respective activity logs. The report generates the following information; computer name, computer group, deployment status, encryption policy assigned, computer status with policy non-compliance reason, operating system, IP address, versions of SEM Agent and client software installed, number of errors/warnings, volume list and encryption status of each volume, and activity log for a time period (optional).

Generating computer report

1. Log on to SEM console and on title bar click Administration.
2. In left pane, click **Reports**.
3. In Computer report section, select a group and computer from the respective lists.
4. Select the **Include activity log for a time period** check box and select the date range.
5. Select the **Report format** option and click **Generate report**.

**Endpoint Activity Report**

With this report you get information about the endpoint activities in the selected group. The report generates the warning messages or the errors shown by the endpoints in given specific time, in PDF or HTML format.

**Generating endpoint activity report**

1. Log on to SEM console and on title bar click **Administration**.
2. In left pane, click **Reports**.
3. In Endpoint activity report section, select the group.
4. Select appropriate time period from the calendar.
5. In Activity log section, select the logs such as warning messages or errors or all the logs.
6. Select the **Report format** option and click **Generate report**.

**Active directory report**

This report generates information about all the Active Directories in the SEM database.

**Generating Active Directory report**

1. Log on to SEM console and on title bar click **Administration**.
2. In the left pane, click **Reports**.
3. In Active directory report section, from Select AD list, select the Active Directory.
4. Select **AD report type**, date range, and report format.
5. Click **Generate report**.
Uninstallation

Uninstalling Seqrite Encryption Manager

If you need to uninstall Seqrite Encryption Manager software, use Add/Remove Programs feature of Windows.

1. From the Start menu, launch Windows Control Panel and click Programs > Programs and Features.

2. From the list, select SEM Server and then click Uninstall/Change. In Remove Program dialog, if you want to delete the MySQL database, select the Uninstall MySQL database check box.

3. Click Start. SEM is successfully uninstalled.

Note:

It is recommended to take full backup of SEM database, if you are going to install the SEM server again or if the volumes of the endpoints are encrypted.

Uninstalling Seqrite Volume Encryption from client computers

You can uninstall SVE application from the client computers in two scenarios.

Uninstallation when client-server communication is present

1. Log on to Seqrite Encryption Manager.

2. Select the computer which you want to remove/delete/uninstall.

3. Click Delete.

Uninstallation when client-server communication is disrupted

1. Log on to SEM console.

2. Select the computer which you want to remove/delete/uninstall.

3. Click Delete.
4. Click **Force Delete**.
5. Download the Agent_uninstaller.
6. Open the command prompt as Administrator on the endpoint to remove/delete/uninstall forcefully.
7. Navigate to Agent_uninstaller directory.
8. Run the agent_uninstaller.exe
9. Decrypt the encrypted volumes.
10. From Control Panel, open the Windows Add remove program.
11. Select the Seqrite Volume Encryption client and click **Uninstall/remove**.
12. Restart the computer.

**Note:**

If any volume is encrypted, then SVE app shows a message that the encrypted volume is found.
Support

Technical Support
The Support option includes FAQ where you can find answers to the most frequently asked questions, options to submit your queries, send emails about your queries, or call us directly.

Support includes the following options:

- **Web Support:** Includes Visit FAQ (Frequently Asked Questions) and Visit Forums – where you can submit your queries to get an appropriate answer.
- **Email Support:** Includes Submit Ticket that redirects you to our Support web-page. Here you can read some of the most common issues with answers. If you do not find an answer to your issue you submit a ticket.
- **Live Chat Support:** Using this option, you can chat with our support executives.
- **Phone Support:** Includes phone numbers. You can call our support team and get your issues resolved.
- **Remote Support:** This support module helps us easily connect to your computer system remotely and assist you in resolving technical issues.

**Phone Support**
The contact number for phone support: 1800 212 7377.

To know more phone numbers for support, visit: [https://www.seqrite.com/contact-support](https://www.seqrite.com/contact-support)

**Head Office Contact Details**
Quick Heal Technologies Limited
(Formerly known as Quick Heal Technologies Pvt. Ltd.)
Reg. Office: Marvel Edge, Office No.7010 C & D, 7th Floor,
Viman Nagar, Pune 411014, Maharashtra, India.

Official website: [www.seqrite.com](http://www.seqrite.com)

E-mail: [support@seqrite.com](mailto:support@seqrite.com)