SEQRITE

Seqrite Encryption Manager 1.2

Release Notes

11 February 2019

Copyright Information

Phone: +91 20 66813232

Email: info@seqrite.com

Official Website: www.seqrite.com

Trademark

Contents

Revision History

Version	Date	Comment
1.2	11 February 2019	Seqrite Encryption Manager 1.2 Released

Build Information

Product Name	Release Date	MD5 Checksum	Build Version
SEM installer	11 February 2019	d16b82454a487f7091ad7436d711cd33	1.2
PreCheck Tool	11 February 2019	6a6f2f69ed92b2acf540951f16ecf7a6	1.2
Traveller Kit	11 February 2019	cac184fafe427861cb6b9184c16286b7	1.2
SEM Rescue ISO	11 February 2019	0163088ed17d723be3457ea2d01691b0	

Seqrite Encryption Manager

Seqrite Encryption Manager (SEM) is the robust encryption solution for security of business data

SEM protects corporate data residing on endpoints with strong encryption algorithms such as AES, RC6, SERPENT and TWOFISH. Full disk encryption supports Microsoft Windows Desktops and Laptops and prevents data loss occurring from loss/theft of endpoint. Seqrite Encryption Manager encrypts the entire contents on removable devices such as Pen Drives, USB Drives and makes it accessible to only the authorized users.

Benefits

- Centralized management and control of encrypted disk volumes.
- Ease of deployment and pre-requisites check
- Full disk and removable media encryption
- Default encryption policies
- Excellent rescue methods
- Automatic backup and upgrades

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 RS5 (Max version support 1809)
- Windows 8.x
- Windows 7
- Windows Vista SP2
- Windows Server 2008 R2 (minimum SP1)
- Windows Server 2012 and 2012 R2
- Windows Sever 2016
- Windows Server 2019 (Max supported version 1809)

Required software for SEM Server

- Oracle Java 8
- MySQL Server v5.5+
- Redis v2.8+
- Net framework 4.0
- Microsoft Visual C++ 2008 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 69, 70, and 71
- Mozilla Firefox 61, 62, and 63
- Internet Explorer 9, 10, and 11
- MS Edge
- Opera 59

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 Flavours)
- Windows Vista (All Flavours)
- Windows 7 (All Flavours)
- Windows Server 2003 (All Flavors)
- Windows server 2008 and 2008 R2
- Windows 8.0 (All Flavours)
- Windows 8.1 (All Flavours)
- Windows server 2012 and 2012 R2
- Windows 2016
- Windows 10 RS5 (Max support version 1809)
- Windows 2019 (Max supported version 1809)

What's New

Seqrite Encryption Manager (SEM) features:

- **Pre-check tool enhancement**
  - Pre-check tool is enhanced to collect HDD S.M.A.R.T.

    i.e Hard drive model, Hard drive Firmware, Hard drive temperature, Total Power On hours and Bad Sector remapped count.
- **SEM installer enhancement**
  - Seqrite Encryption Manager server installation is now possible with the help of host name also. The host name must be in FQDN format such as; comp1.abc.com
  - At the time of installation, you can change the SSL port to the desired free port.
- **Implement Forgot password to easily retrieve the password**
  - After six failed attempts of wrong password, your SEM account gets locked for six hours. Thus, you can use the Forgot password link to reset your password immediately.
  - It is recommended to create two different Administrator accounts at the time of SEM server installation. If one Admin forgets the password, then another Admin account can be used to reset the password.
- **Implemented Active Directory to deploy Seqrite Volume Encryption**
  - SEM provides another easy method to deploy SVE application on client computers.
- **Single Sign On**
  - New feature added to the SEM database. With this feature, the user gets the privilege to use a single set of login credentials for Windows.
  - The SEM Admin can enable or disable this policy on client computers or give complete control to the user if this policy is to be applied or not.
- **FailSafe Mode for security**
  - After 10 attempts of wrong passwords on the client computer, the computer goes into FailSafe mode. This adds one more layer of security for the client computers.
- **Implemented software upgrade**
  - SEM software upgrade made easy with;
    - Setup file: When you have the SEM setup file, you can have a manual upgrade.
    - Via Updates: This option helps you to upgrade the SEM applications. With updates, you can configure the automatic upgrade of the SEM applications whenever the update is available.
- **Reports enhanced with Active Directory reports**
  - Easily get the reports for Active Directories, groups and computers added to the Active Directory, SVE deployment status, Active Directory sync status, and activity log.

- **Disabled Seqrite Volume Encryption uninstallation from client computers**
  - Only the SEM Administrator is authorized to uninstall SVE application from the client computers.
- **Rescue ISO (WinPE) enhancement**
  - ISO is upgraded from Win7PE to WinPE 10 RS5
  - Added Team Viewer support to provide robust support
  - Take Full backup of SEM server if SEM server's OS gets corrupted

Note:

Seqrite Encryption Manager client (SVE) encrypts all the data available on your hard disk. To avoid the possibility of data loss, we strongly recommend to take a backup of the system data on any other hard drive, network storage, etc. Also make sure that the data can be easily restored.

Usage Information

Following are the usage information for Seqrite Encryption Manager (SEM):

- **Deploying SEM client on Virtual Box**.
  1. Open VirtualBox Manager.
  2. Click the machine.
  3. Click **Settings** or right-click the machine of Virtual Machine (Guest OS).
  4. Click **System** and then select the **Enable I/O APIC** check box.
  5. Click **Acceleration** and turn off the **Paravirtualization interface** by selecting **Not Present** or **None**.
- Dual Boot encryption can be done only with **Manage locally** mode

  To encrypt a dual boot system, you must operate Seqrite Volume Encryption Enterprise Client in **Manage Locally** mode.

  To encrypt a dual-boot computer with System A and System B, follow these steps:
  1. Create a policy that uses **Manage Locally**.
  2. **Add** System A to the SEM Database.
  3. Assign **Manage Locally** mode to System A.
  4. Run Seqrite Volume Encryption as Administrator.
  5. Encrypt the volumes marked as **System**, **Boot** or **System & Boot**
  6. **Restart and load** System B.
  7. Repeat the steps 2 through 5 for System B. Use the same password used for System A.

     Now you can encrypt non-system volumes (if any) from either System A or System B.

     Note: The Seqrite Volume Encryption prompt for password appears first and then the OS Selection.
- At the time of encryption, the client system should be in network

  To send the rescue details during encryption, you must make sure that the client system is in network and connected to SEM server.
- Single encryption policy applicable for removable drive

  At a time, you can use a single encryption policy on your removable drive. You can either use Seqrite Endpoint Security or Seqrite Encryption Manager or any third-party encryption tool.
- Account creation on console may display page unresponsive message

  When creating account from console, at times, you may receive page unresponsive message. In such scenario, do not kill or close the browser, but wait till the process is complete.
- Master password given to non-system volume while performing manual encryption cannot be changed. However, if user forgets the master password then decryption policy can be applied from server and get the volumes decrypted.

- Extra time is taken to reboot after SME installation

  After installing the SME, the fast reboot option gets disabled. The reason for disabling fast reboot is to ensure that the encryption drivers are loaded on next reboot after the SME installation. Following the serial reboots, it is expected that the keys are flushed out of RAM after the reboot. But if the fast reboot option is not disabled, the keys may not flush

- **Single Sign On**
  - Single Sign On will not work if auto login is enabled by user using third party tool or using Windows auto login.
  - Single Sign On is supported on Windows Vista and later versions.
  - Single Sign On will not work if suspend protection is enable on Endpoint.
  - User needs to re-enroll Single Sign On if Windows login credential is changed.
- **Active Directory Sync**
  - Active Directory authentication using FQDN is not supported.
  - If the admin has already configured client deployment using the AD Sync and if the Agent installer is run manually on any computer; which is already present in the Active Directory, then such client computer will be shown in AD group instead of New Computer.
  - Installation via Active Directory using SSL is not supported.
- **Forgot password**
  - It is mandatory that the user create two different administrator accounts to recover/change password.
- **SEM Upgrade/Update**
  - It is recommended to take the full backup of SEM server before starting upgrade/update.
- **Pre-Check tool**
  - Pre-check tool does not support virtual machine to collect S.M.A.R.T
  - Pre-check tool works on Windows Vista and later versions.
- **FailSafe**
  - User must decrypt/encrypt the computer to use FailSafe mode on legacy computer after SVE update/upgrade.
- **Installation on Live/public IP Address**

  SEM server must be installed on Hostname and client must be able to communicate with server using Hostname.

Critical Bug Fixes

Bug Id	Summary
SEM-1229	Encryption/Decryption process is suspending automatically if the power is cut down abruptly.
SEM-1076	Decryption process automatically suspends in some specific scenarios.
SEM-1225	Systems are getting into Auto-Recovery mode post SEM encryption 1.1

Note for SEM-1225: USB rescue will restart the system if Pre-boot password prompt is recovered.

Known Issues

1. Some extra lines are visible if SEM console is accessed in Windows 10 RS4 having Microsoft edge version 42.17134.1.0.
2. Encryption process is getting suspended for USB drive if USB drive disconnected at 0% encryption stage.
3. Removable drive status during encryption is not displayed on console sometimes if Fixed drive encryption is in progress.
4. Mark As read button for AD logs is not working in IE 11.
5. SVE client takes some time to open if Internet is connected using USB dongle.