SEQRITE

Seqrite
Encryption Manager 1.1
Release Notes

9 July 2018

Copyright Information

Phone: +91 20 66813232

Email: info@seqrite.com

Official Website: Seqrite.com

Trademark

Contents

Revision History

Version	Date	Comment
1.1	9 July 2018	Seqrite Encryption Manager 1.1 Released

Build Information

Product Name	Release Date	MD5 Checksum	Build Version
Seqrite Encryption Manager	9 July 2018	50C3B6123CFB1DF17C890F5B0346D9E9	1.1
Prerequisite Tool	9 July 2018	9AECAE5637BD9A009EBA475C93D311E0	1.0
Recovery ISO	9 July 2018	A8C7C0C7A64A4E3656767497FF6D7DB8	1.1
Traveller Kit	9 July 2018	A3ED8DC04FC08901274FF1B33D7EE7F4	1.1

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
- Windows 8.x
- Windows 7
- Windows Vista SP2
- Windows Server 2008 R2 SP1
- Windows Server 2012 and 2012 R2
- Windows 2016 (Max supported Version 1709)

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 65, 66, and 67
- Mozilla Firefox 58, 59, and 60
- Internet Explorer 9, 10, and 11
- MS Edge
- Opera 53.0
- Safari 11

Mobile Browsers

- Android 4.2+
- iOS 8+

For all browsers

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

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 (Max supported Version 1709)
- Windows 10 RS4 and below

What's New

Seqrite Encryption Manager (SEM) features:

- **Group-wise Installation**
  - Group-wise installation of the computers has been implemented. SEM client will be part of that group and the policy would be applied automatically. So there will not be a need to move the client from one group to another group manually.

    In this implementation, the packager itself (jci_setup_****....exe) is not group-specific, but it can be run with a special parameter -G and a group name.

    For example, if the new computer is to be added in other group, the "jci_setup..." file should be run from Command Prompt with the parameter -G followed by the group name using the following format:

    jci_setup__207_154_213_48_8443_10002__.exe **-G#MY GROUP NAME#**
  - If the group does not exist, it will be created automatically, and the default encryption policy will be assigned.
- **Group wise suspension option**

  Bypass pre-boot authentication for groups as well as computers.
  - If the Suspend Protection option is set/reset on the group page, it is automatically set/reset for each computer in the group and for new computers appeared in that group.
  - If the Suspend Protection option is set on the computer page, it is considered as an individual setting and takes preference over the group setting. But if group setting is changed after that it becomes equal to the group setting.
- **Implemented Search option**

  This is global search and administrator can find the computers using its name.
- **Enhancement in reports section**
  - Company report can now be generated for all groups or for a selected group of computers.
  - Computer reports can now be generated with the option to include Activity Log for a time period, for the specified computer.
- **Implemented three pre-boot authentication passwords**
  - Added the boot time password-related commands such as; change master password, add password, remove additional password, and change additional password.
  - Every action for adding/changing/removing additional passwords is logged in SEM Console.
- **Introduced Remote Installation Tool**

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

- **Pre-requisites check tool**
  - The Pre-requisites check tool scans the system for different parameters and checks the prerequisite of SEM client. It also gives the message if the system is ready for installation.
  - Download the Pre-requisite check tool from Seqrite website.

    Working of tool

    Pre-requisites tool will check your system status for Seqrite Volume Encryption installation. The tool will check the following information.
    - System Information
    - BIOS Information
    - OS Information
    - CPU Information
    - Hard disk Information
    - Logical Disk Information
    - RAM Information
    - Keyboard Information
    - HotFix Information
    - Installed Software Information
    - MBR Status

    Above mentioned check must be passed to install Seqrite Volume Encryption.

    Note: Pre-requisites tool is supported on Windows Vista and later versions.

- **Traveller Kit**
  - Seqrite Traveller kit helps to quickly access the volumes encrypted by Seqrite Encryption Manger. This helps to access the required data easily even when travelling. It supports volumes encrypted by any algorithm and any key generator in SEM.
  - Download Seqrite Traveller kit from Seqrite website.
  - After running a single executable file, Seqrite Volume Encryption application is accessible. Thus, the user can decrypt the volume and access the data.

- **Note**:

  Seqrite Encryption Manager client 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.

Critical Defect Fixes

1. System BSOD with "Unmountable boot volume" error is received after the SEM client installation and reboot of the system - SEM 1.0
2. Unable to boot OS with the error "no boot device found", due to system crash at the time of encryption.

Usage Information

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

- 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.

Known Issues

1. If Windows Surface\Tablet is encrypted using Seqrite Volume Encryption, then a keyboard will be required to enter the password at boot time.
2. If the system volume is encrypted with Seqrite Encryption Manager, then the encrypted hard disk should not be removed from its original encrypted system and connected to the another system.
3. The user should turn off the Secure boot (UEFI) for recovery of the damage volume using the bootable ISO.