SEQRITE

Seqrite Encryption Manager 1.2.2

Release Notes

25 September 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	25 September 2019	Seqrite Encryption Manager 1.2.2 Released

Build Information

Product Name	Release Date	MD5 Checksum	Build Version
SEM installer	25 September 2019	398cdcf4605bee7ece57ae3cbf4cf302	1.2.2
PreCheck Tool	25 September 2019	a84924ad0372fd171c71c126666bf1e3	1.2.2
Traveller Kit	25 September 2019	ccd684afbd63f88d6906cba97d10c1cd	1.2.2
SEM Rescue ISO	25 September 2019	0b87a181dbae2029bcc3242da19b70e1	

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 RS6 (19H1) (Maximum version 1903)
- Windows 8.x
- Windows 7 SP 1
- Windows Vista SP2
- Windows Server 2008 R2 (minimum SP1)
- Windows Server 2012 and 2012 R2
- Windows Sever 2016
- Windows Server 2019 (Max supported 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 77, 76, and 75
- Mozilla Firefox 69, 68, and 67
- Internet Explorer 11, 10, and 9
- 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 SP 1 (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 RS6 (19H1) (Maximum version 1903)
- Windows 2019 (Max supported version 1903)

What's New

Seqrite Encryption Manager (SEM) features:

- Enhanced supported operating systems:
  - SEM server now support Windows 10 RS6 (19H1) (Maximum version 1903) and Windows Server 2019 (Maximum version 1903).
  - SEM client now supports Windows 10 RS6 (19H1) (Maximum version 1903) and Windows Server 2019 (version 1903).
- Implemented a complete licensing support
  - Product licensing made easy with product key.
  - Easily renew and reactivate the license.
  - The license can be reactivated on the different computer after 30 days, but for immediate reactivation on different computer, you can contact the Support team.
  - The license may be blocked for some reasons and in such condition, upgrade and update functionality may not work.
- Proxy support to download update/activation
- Custom MySQL credential support
  - For latest versions of SEM, MySQL is mandatory. SEM Server will not accept MYSQL login password as "Root".
  - While configuring MySQL, a loopback IP address (127.0.0.1) is required.
  - While installing SEM server, user can provide following information for MySQL user name, password, IP address, port number, and administrator privileges.
  - If MySQL was already installed, make following change to the command:
    - mysql>grant all on *.* to 'user name'@'%' identified by 'password'
- Implemented new report type: Endpoint Activity Report
  - With this report, the activities of endpoints are generated for the selected group. The report gives information about the warning messages or the errors shown by the endpoints in the given specific time, in PDF or HTML format.

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

1. Randomly SEM client systems are getting freeze while volume encryption and after completion of encryption | SEM 1.2.1
2. Clients showing offline on Console
3. While Installing the SEM Client Getting Error: SEM Agent Setup Encountered Error - "Root certificate file of SEM Server (jcmCA.crt) not found."
4. SEM 1.2.1 | Windows upgrade | File guard module error message is getting displayed after Windows upgradation.

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.
6. City list is not populating on first attempt in activation page.
7. Last sector of the unmounted volume does not get encrypted after SEM upgrade.
8. Decryption speed is getting slow gradually on HP ProBook 440 G5 & Dell Latitude 3490.