Seqrite **Workspace**

Frequently Asked Questions

1. Why will I need Seqrite Workspace?

Seqrite Workspace is designed to use primarily & exclusively for enterprises planning to roll-out BYOD functionality for its employees. The product helps employees to work on their personal devices seamlessly without jeopardizing enterprise collateral.

2. Does Seqrite Workspace support all Mobile Operating Systems?

Seqrite Workspace is available on Android as well as iOS Mobile Operating Systems.

3. How do I know if all my employees are working out of the Seqrite Workspace app?

Seqrite Workspace comes with an easy-to-understand, lucid dashboard through which you can easily analyze your employees' engagement rates about working from the Seqrite Workspace App.

4. What all capabilities are a part of Seqrite Workspace?

Along with the base package of E-mail, Calendar and Contacts, Seqrite Workspace additionally includes a secure browser, a vault which is a central repository securely holding enterprise documents, a secure camera and intelligent text-specific modules.

5. How will Seqrite Workspace support my corporate email ecosystem?

Seqrite Workspace integrates with Office 365 and G Suite.

6. How do I configure these capabilities to fit into my business framework?

Seqrite Workspace comes with a comprehensive console through which IT Admins can easily configure every capability according to business policy. The console is pre-loaded with a variety of policies and profiles to configure Seqrite Workspace capabilities as per business requirements.

7. Does Seqrite Workspace install if employee devices have been tampered with?

Seqrite Workspace will not get installed on rooted or jailbroken devices.

8. I want to set up employee internet access in Workspace a certain way. Is there a facility for this?

IT Admins can Whitelist & Blacklist websites based on URLs and keywords within the secure browser in the Workspace. Once you decide what you want to allow or disallow, your admins can deploy your choices in the blink of an eye.

9. Can I prevent my employees from uninstalling Seqrite Workspace?

No, you cannot deny the uninstallation of Seqrite Workspace since it is an employees' personal device. However, in an event where an employee uninstalls the app, the administrator will be alerted on the dashboard.

10. What happens when Seqrite Workspace is reinstalled – does it retain the data?

On re-installation, it works as a newly installed application. The employee needs to re-configure his official email inside the Seqrite Workspace email client. On doing so, emails and other related information (like contacts and calendar) will auto-populate. However, data saved inside the vault will be lost.

11. Can I delete complete enterprise data from employee devices?

Seqrite Workspace has an over the air function to wipe the Workspace from the device. This is a management command from the secure management console which can only be accessed by a qualified administrator and will wipe Seqrite Workspace and all data from the device.

12. Can I wipe data from the device if the device is not connected to the network?

Seqrite Workspace includes a policy for a feature called 'Time Bomb'. When enabled the administrator will define a period of time (i.e. 30 days) and if the Seqrite Workspace client on the device has not checked in with the secure management server, the Seqrite Workspace client on the device will automatically wipe itself.

13. Can I host my native organisation Apps inside Seqrite Workspace?

Seqrite Workspace has thoughtfully provisioned all the essential enterprise Apps for its users.

14. Can this product function without an EMM solution?

No, this product functions in conjunction with Seqrite's mSuite, a complete EMM solution. In order to obtain Seqrite Workspace, mSuite has to be pre-installed.

15. Will my IT Admins have access to employees' personal data on their phone?

Seqrite Workspace creates a virtual boundary between employees' personal data and enterprise data on phones. IT Admins can only control the use of Seqrite Workspace on employee phones.

16. Can Seqrite Workspace be hacked?

All software can, in theory, be hacked. However, Seqrite Workspace has taken all the necessary precautions that are available today to protect against hacking.

17. How many users can be supported by Seqrite Workspace?

Seqrite Workspace and the secure management server have been designed to scale according to the size of the deployment.

SEQRITE

Quick Heal Technologies Limited

Support Number: 1800-212-7377 | info@Seqrite.com | www.Seqrite.com

Follow us on: