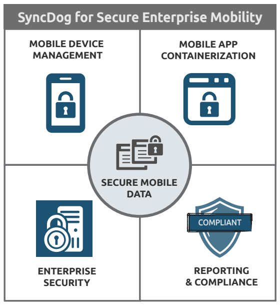
# SENTINELSECURE™ FAQs

SyncDog SentinelSecure™ is a secure data platform that encrypts and transports data between an enterprises' backend and a secure, "sandboxed" application workstation on a mobile device. SentinelSecure is more than just messaging software that offers encrypted e-mail, calendar, and contacts to smart phones. More information on SentinelSecure can be found in this FAQ document.



Q. *What platforms is SentinelSecure available for?*

A. Currently iOS and Android with Windows Mobile expected in early 2016

Q. *Do you have to have your smartphone managed by an MDM to use SentinelSecure?*

A. No, unlike Android for Work or Samsung KNOX, an MDM is not required to manage the SentinelSecure workspace. SentinelSecure is MDM-agnostic and can be used with an MDM solution or as a standalone solution.

Q. *Can I add applications to my instance of SentinelSecure workspace?*

A. Yes, any natively developed iOS or Android application can be applied to SentinelSecure. The application will need to be placed within the framework of SentinelSecure by a SyncDog engineer.

Q. *If I have 3rd party applications I use for business on my smartphone can they be protected by SentinelSecure?*

A. Yes, for 3rd party business applications not embedded into the secure workspace, SentinelSecure provides the ability to wrap the application in encryption for protecting data at rest and in transit.

Q. *How does SentinelSecure work with my corporate e-mail system?*

A. SentinelSecure provides applications for e-mail, calendar and contacts connectivity. Currently SentinelSecure supports Microsoft Exchange and Office 365 implementations out of the box. Custom installations can be completed for mail systems like Lotus Notes and others.

Q. *How secure is SentinelSecure?*

A. SentinelSecure provides AES 265 bit encryption for all data at rest and in transit between the smartphone and the enterprise network.

Q. *Does SentinelSecure require a VPN Solution?*

A. No, SentinelSecure does not require a 3rd party VPN solution to connect to the network securely. The SentinelSecure workspace connects to the Sentinel management server via a relay in the DMZ using an AES 256 bit encrypted SSL tunnel between the device and the management server behind the firewall.

Q. *Can SentinelSecure be hacked?*

A. All software can, in theory, be hacked, but SentinelSecure has taken all methods that are available today to protect against hacking. The client is protected, among other methods, with code obfuscation and runtime memory heap protection

Q. *Is SentinelSecure vulnerable to a man-in-the-middle attack?*

A. No, SentinelSecure's secure transport methodology protects against MIM attacks.

Q. *Does SentinelSecure store encryption keys in the local key store of the device?*

A. No, SentinelSecure uses a multi-part key structure which disseminates the key in various places, but is also composed of several key components in order to be fully secure.

Q. *How many applications can be put into SentinelSecure?*

A. There is no limit to the number of applications which can be embedded into SentinelSecure. The only limit would be based on the maximum physical storage capacity of the device.

Q. *Can I store and retrieve documents in SentinelSecure?*

A. Yes, SentinelSecure provides both the ability to store and sync documents with a network drive or desktop, as well as open and edit the documents, spreadsheets or slide decks in an Office Suite within SentinelSecure workspace.

Q. *Can I use my smartphone to view internal LAN pages on my company intranet?*

A. Yes, SentinelSecure provides a secure browser which does not connect to the internet directly via the device, but by the secure connection on the Sentinel management server through the encrypted SSL tunnel.

Q. *Can I run SentinelSecure on multiple devices?*

A. Yes, the SentinelSecure device client can be installed on multiple devices and will sync content between the devices so you can start an e-mail on your iPhone and finish it on your iPad.

*Q. Can I have multiple mailboxes on an instance of SentinelSecure?*

A. No, currently SentinelSecure can only support a single connection to Microsoft Exchange or Office 365. Multiple mailbox functions are on the SentinelSecure roadmap and will be available in a future release.

*Q. Can I run multiple instances of SentinelSecure on a single device?*

A. Multiple versions of SentinelSecure can be made available if required

*Q. How many users can be supported by SentinelSecure?*

A. SentinelSecure and the Sentinel management server have been designed to scale according to the size of the deployment. When implemented, the Sentinel Management server and the Sentinel relay can be installed in multiple locations and geographies to maximize the capacity and provide redundancy for the deployment.

*Q. What applications are available with SentinelSecure?*

A. Along with E-mail, Calendar and Contacts, SentinelSecure also includes a secure browser, an Office Suite for documents, a secure text application, and an application to connect to your MS Lync or corporate Google Talk account. Along with a secure camera and maps application, SentinelSecure also includes applications for local file management and network / PC file sync between SentinelSecure and your network file share or PC.

*Q. Can you copy data from SentinelSecure to an application on the device?*

A. No, you are not able to copy and paste data from the SentinelSecure application to other device applications running outside of the secure workspace. You are able to use copy and paste between applications running within the secure workspace.

*Q. Can you take screenshots of screens within SentinelSecure and save on the device?*

A. No, screen captures are disabled when you are running within SentinelSecure.

*Q. Can I wipe the device or specific data from the device?*

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

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

A. SentinelSecure 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 SentinelSecure client on the device has not checked in with the Sentinel management server the SentinelSecure client on the device will automatically wipe itself.

## About SyncDog

SyncDog is the leading independent software vendor (ISV) for containerized application security for enterprise mobile computing. SyncDog's flagship product SentinelSecure™ provides defense-grade secure mobile device partitions or "containers" that can secure e-mail & contacts, calendar items, IM apps, Internet browsers, mobile file stores and other business apps provisioned on personal devices to be used in a BYOD or COPE (corporate owned personally enabled) setting. SentinelSecure protects both data at rest and data in transit through Federal Information Processing Standard or FIPS 140-2, AES 256 bit encryption.

For more information on SyncDog products, please visit www.syncdog.com.

**SyncDog, Inc.**
1818 Library St.
Suite 500
Reston, VA 20190
Tel: (703) 430-6040
Fax: (703) 997-8667

SYNCDOG