

Sybase Afaria

Advanced Enterprise Security (AES) for Android

PRODUCT DATASHEET



Sybase and Samsung are working together to address the management and security concerns commonly faced by enterprises when deploying Android devices. This partnership provides the comprehensive capabilities that IT requires to allow mobile workers access to enterprise assets using the device of their choice. IT can now confidently extend corporate security policies to the Android platform, allowing for the adoption of both personally-owned or corporate owned Samsung Android devices.

Afaria Advanced Enterprise Security (AES) for Android empowers IT with comprehensive device management capabilities on the Samsung Android devices (Android version 2.3 or later), including:

- **Security management** – enforce device encryption, remote lock/wipe, strong password security, and corporate sandbox management
- **Application management** – deliver and control the applications that run on Samsung Android devices
- **Configuration management** – provide control over various ports (Bluetooth, WiFi, camera, microphone), roaming, and network configuration
- **Exchange Client Configuration** – configure native email client
- **Asset Tracking** – granular hardware and software collection and reporting

Sybase Afaria reduces the complexity of managing Android devices by automating over-the-air (OTA) deployments, configuration and application management without the need for user intervention.

Empower employees with mobile access to enterprise systems

Providing employees with access to corporate email is important, but it is also critical to extend your mobile strategy to empower mobile workers with access to business applications and data. This is what empowers you to transform your entire organization, bringing unprecedented levels of productivity to your employees. Samsung and Sybase are collaborating extensively to make the mobile experience for enterprises easier, more secure, and more consistent.

Deliver extensive security

If security is top of mind for your organization, then Afaria offers exactly what you need to confidently adopt Samsung Android devices. In the event a device is lost or stolen, IT can easily lock, unlock or wipe a device remotely. For extended security requirements, data can be fully encrypted. Application control can increase corporate security and employee productivity by providing the ability to uninstall or disable any application on the device that was provisioned by Afaria.

SYBASE AFARIA CAPABILITIES FOR ANDROID

	Feature	Afaria Capabilities with Native Android V2.2	Afaria AES for Samsung Galaxy S (V2.3) and Galaxy S2
Application Management	List authorized enterprise applications based on user groups		•
	Install & remove enterprise applications		•
	Enable & disable enterprise applications		•
	Enterprise applications information		•
	Remove managed applications		•
	Update application		•
	Certificate installation		•
	Prevent uninstall applications by user		•
	Check if application installed		•
	Check if application currently running		•
	Add/Remove applications to/from blacklist		•
	Enable uninstall application by user		•
	Enable & disable applications		•
	Wipe application data		•
Configuration Management	Enable & disable camera		•
	Allow automatic synchronization while roaming		•
	Disable push while roaming		•
	Remove managed exchange account and data		•
	Check WiFi is enabled or disabled		•
	Enable & disable WiFi	•	•
	Access point control		•
	Enable & disable Bluetooth		•
	Start/Stop Bluetooth discovery		•
	Enable & disable microphone		•
Exchange Server Policies	Active Sync host		•
	Create new exchange account		•
	Set exchange account display/account name		•
	Set exchange account sync interval		•
	Set exchange account protocol version		•
	Set exchange account sender name		•
	Set exchange account sender signature		•

SYBASE AFARIA CAPABILITIES FOR ANDROID

	Feature	Afaria Capabilities with Native Android V2.2	Afaria AES for Samsung Galaxy S (V2.3) and Galaxy S2
Exchange Server Policies	Set exchange account setting to always vibrate on email notification		•
	Set exchange account setting to vibrate when silent only on email notification		•
	Set exchange account setting to use TLS		•
	Set exchange account setting to accept all		•
	SSL related certificates		•
	Set Active Sync client auth certificate		•
	Set the Exchange user		•
	Set user's email address		•
	Use SSL		•
	Domain		•
	Password		•
	Number of past days to sync		•
Hardware and Software Inventory	SSID of wireless network		•
	Hidden network		•
	IMEI / MEID	•	•
	ICC ID		•
	Current carrier network	•	•
	SIM carrier network	•	•
	Phone number	•	•
	Data roaming setting		•
	Phone type	•	•
	Current network type	•	•
	Phone SIM operator	•	•
	Phone SIM country ISO	•	•
	Phone SIM state	•	•
	Bluetooth status	•	•
	Get assigned IP address		•
	Get paired devices		•
	List all installed application	•	•
	Application ID		•
Application name	•	•	
Application version	•	•	

SYBASE AFARIA CAPABILITIES FOR ANDROID

	Feature	Afaria Capabilities with Native Android V2.2	Afaria AES for Samsung Galaxy S (V2.3) and Galaxy S2
Password Policy	Allow simple values for password	•	•
	Require alphanumeric values for password	•	•
	Minimum password length	•	•
	Maximum password age in days		•
	Minimum complex characters in password		•
	Password history		•
	Get device password		•
	Set device password		•
	Maximum number of failed attempts before device is wiped		•
Security Management	Remote lock & unlock	•	•
	Remote wipe		•
	Remote reset		•
	Remove configuration data		•
	Ability to lock management on phone		•
	Full device encryption		•
	Wipe encrypted data		•
	SD card encryption		•
	Add blacklist		•
	Remove blacklist		•
	Disable application		•
	Enable application		•
Wipe application data		•	

Learn more about Sybase and its innovative products and solutions at www.sybase.com/android