SAP Afaria

Extend Corporate Security Policies to the Android Platform

Advanced Enterprise Security with the SAP® Afaria® Mobile Device Management Solution

SAP and Samsung are working together to address the management and security concerns commonly faced by IT when deploying Samsung Android devices. The intent is to enable IT to allow mobile workers access to enterprise assets using the device of their choice – both personally and corporate-owned Android devices. IT can now confidently extend corporate security policies to the Android platform. The SAP® Afaria® mobile device management solution reduces the complexity of managing Android devices by automating over-the-air deployments, configuration, and application management without the need for user intervention.

SAP Afaria offers advanced enterprise security for Samsung Android devices, empowering IT with comprehensive device management capabilities for Android version 2.3 or later. The solution is offered for the following policy groups:

- Application control policy group
- Bluetooth policy group
- Exchange account management
- Firewall policy group
- Location policy
- Hardware and software information
- Password policy group
- Restriction policy group
- Roaming policy group
- Security policy group
- Wi-Fi policy group

PROVIDE MOBILE ACCESS TO ENTERPRISE SYSTEMS

Providing employees with access to corporate e-mail via mobile devices is important, but your mobile strategy must also extend to provide workers in the field 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. SAP and Samsung are collaborating extensively to make the mobile experience for enterprises easier, more secure, and more consistent.

PLATINUM MEMBER
SAMSUNG
ENTERPRISE ALLIANCE PROGRAM

DELIVER EXTENSIVE SECURITY

If security is top of mind for your organization, then SAP Afaria offers exactly what you need to confidently adopt Android devices. In the event that a device is lost or stolen, IT can easily lock 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 SAP Afaria.

TAKE ADVANTAGE OF SAP INNOVATION

In short, SAP and Samsung are working to help you:

- Reduce the complexity of managing Android devices
- Improve the experience of using mobile devices for enterprises, making it easier, more secure, and more consistent
- Give IT control over applications running on Android devices

FOR MORE INFORMATION

To learn more about SAP and its innovative products and solutions, please visit www.sap.com/mobile. For a full list of features, see the table below.

FEATURES OF SAP® AFARIA® FOR SAMSUNG ANDROID PLATFORMS

(Please read "Important Information" on the final page.)

Policy Group	Policy Description
Application control policy group	• Application black list management • Application white list management • Delete managed application information • Disable/enable Android market • Disable/enable application • Disable/enable application installation • Disable/enable application uninstallation • Disable/enable blocking all applications except black list • Disable/enable blocking all applications except white list • Install/remove/update application • Wipe application data
Bluetooth policy group	• Turn off/on Bluetooth • Disable/enable Bluetooth • Disable/enable desktop/laptop connectivity • Disable/enable scan devices
Exchange account management	• Add exchange accounts • Remove exchange accounts • Modify exchange accounts
Firewall policy group	• Disable/enable IP proxy rule with IP address and port • Proxy configuration for browser
Location policy	• Disable/enable GPS location provider

Policy Group	Policy Description
Hardware and software information	• Bluetooth and Wi-Fi information and status • Current network operator/type • Get paired devices • IMEI (international mobile equipment identity)/MEID (mobile equipment identifier)/ICC ID (integrated circuit card identifier) • Information of restricted policies applied • Information of security policies applied (password, encryption, and so on) • Installed application ID/name/version • Installed certificates • Last known IP address, SMS address • Phone number/type • Phone SIM operator name/country ISO/state • Platform OS version, maker, model • Wi-Fi enabled/SSID/assigned IP address • Wi-Fi status and information
Password policy group	• Allow simple values for password • Get/set password time-out • Invalid password attempts before device factory reset • Maximum number of failed attempts before device is wiped • Maximum password age in days • Minimum complex characters in password • Minimum password length • Password change enforcement (do not let user cancel out) • Password history • Remote reset • Require alphanumeric values for password
Restriction policy group	• Disable/enable apps installation from unknown source • Disable/enable backup my data • Disable/enable Bluetooth • Disable/enable cut/copy/paste • Disable/enable external storage (SD card) • Disable/enable settings changes • Disable/enable Bluetooth tethering • Disable/enable USB tethering • Disable/enable USB debugging • Disable/enable USB mass storage • Disable/enable USB media player • Disable/enable Wi-Fi • External storage encryption status • Proxy configuration for device • Status/disable/enable background data (cellular) • Status/disable/enable camera • Status/disable/enable microphone

www.sap.com/contactsap

CMP18913 (12/08) ©2012 SAP AG. All rights reserved.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, SAP HANA, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase Inc. Sybase is an SAP company.

Crossgate, m@gic EDDY, B2B 360°, and B2B 360° Services are registered trademarks of Crossgate AG in Germany and other countries. Crossgate is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Policy Group	Policy Description
Roaming policy group	• Disable/enable automatic sync while roaming • Disable/enable push while roaming • Disable/enable roaming data
Security policy group	• Device encryption • All user contents wipe • Credential storage password • Device wipe (factory reset) • External storage encryption (SD card) • Install/clear certificate • Internal storage encryption status • Managed apps data wipe • Clear installed certificates
Wi-Fi policy group	• Connect to specific access point • Disable/enable Wi-Fi • Get assigned IP address • Get current Wi-Fi AP's hidden SSID • Get current Wi-Fi AP's SSID • Turn off/on Wi-Fi

Important Information

- Listed features are for Samsung Android platforms with mobile device management–enabled OS V4.0.x or higher.
- Listed features are available on SAP Afaria V7.0SP1 (as of June 30, 2012).
- Please contact Samsung Electronics or SAP for supportability of listed features on old Samsung models (V2.x or 3.x).
- The supported features above are as of June 29, 2012.

The Best-Run Businesses Run SAP™