

# CODEPROOF LG ENTERPRISE MOBILE SECURITY

## (CLOUD VERSION)



Codeproof partnered with LG to integrate the LG Android operating system software with the Codeproof cloud-based enterprise mobile security platform. LG enterprise customers can now use the Codeproof central cloud console to remotely manage and secure LG smartphones and tablets, in addition to Samsung and Apple devices.

## CONTENTS

Device Restrictions Policies .....	3
App Restrictions & Whitelisting/Blacklisting Policies.....	4
Website Whitelisting and Content Filter (Secure Browsing).....	5
WiFi Management.....	6
Kiosk Mode .....	6
Kiosk Mode App Management .....	7
Locate the device including location history .....	8
MDM Tools .....	9
App Deployment.....	10
Email Configurations .....	11
Reporting.....	12
Miscellaneous features.....	12
What's next?.....	13

## DEVICE RESTRICTIONS POLICIES

IT Admins can centrally enable or disable various device features including WiFi, Bluetooth, USB, Airplane mode, SMS, Phone, Roaming, Email, OS OTA Update and Camera, among over 100 other policies. Configure restriction policies simultaneously at the group level from the Codeproof cloud console and apply these policies to all devices enrolled in the future automatically. As a result, Administrators don't have to manually configure each device individually.

The screenshot displays the Codeproof Mobile Policy Manager interface. The top navigation bar includes 'Codeproof', 'Dashboard', 'Policy Manager', 'EMM', 'Reports', and 'Administration'. The user 'sshetty@codeproof.com' is logged in. The left sidebar shows a navigation menu with categories like 'Home', 'Android Devices', 'Bring Your Own Devices (BYOD)', 'Galaxy Devices', 'iOS Devices', 'LG Devices', 'North America', and 'Supervised Devices'. The main content area is titled 'MOBILE POLICY MANAGER' and shows tabs for 'Android Security', 'iOS Security', 'Samsung Security', and 'LG Security'. Under 'LG Security', there are sub-tabs for 'Mobile Antivirus', 'Agent Policy', 'Kiosk Mode', 'Kiosk App Management', 'App Restrictions', 'Device Restrictions', 'Passcode Policy', 'WiFi Policy', 'Secure Browsing', 'Encryption Policy', 'Misc Policy', and 'Email Policy'. The 'Device Restrictions' tab is active, showing a list of 30 policies, all of which are checked and enabled. The policies are organized into three columns:

Device Restriction	Device Restriction	Device Restriction
<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Allow Hardware Factory reset	<input checked="" type="checkbox"/> Allow Sending SMS
<input checked="" type="checkbox"/> Allow Airplane Mode On	<input checked="" type="checkbox"/> Allow Hotspot	<input checked="" type="checkbox"/> Allow Shortcut Key
<input checked="" type="checkbox"/> Allow Android Beam	<input checked="" type="checkbox"/> Allow Infrared Port	<input checked="" type="checkbox"/> Allow Tethering
<input checked="" type="checkbox"/> Allow Auto Restore	<input checked="" type="checkbox"/> Allow LG VPN	<input checked="" type="checkbox"/> Allow USB
<input checked="" type="checkbox"/> Allow Auto Sync	<input checked="" type="checkbox"/> Allow Microphone	<input checked="" type="checkbox"/> Allow USB Debugging
<input checked="" type="checkbox"/> Allow Background Process Limit	<input checked="" type="checkbox"/> Allow Miracast	<input checked="" type="checkbox"/> Allow USB Host Storage
<input checked="" type="checkbox"/> Enable Bluetooth	<input checked="" type="checkbox"/> Allow Cellular Data Network	<input checked="" type="checkbox"/> Allow USB MTP
<input checked="" type="checkbox"/> Enable Bluetooth Pairing	<input checked="" type="checkbox"/> Allow Mock Location	<input checked="" type="checkbox"/> Allow USB PTP
<input checked="" type="checkbox"/> Enable Bluetooth Profiles	<input checked="" type="checkbox"/> Allow Multiple Users	<input checked="" type="checkbox"/> Allow USB Tethering
<input checked="" type="checkbox"/> Enable Bluetooth Tethering	<input checked="" type="checkbox"/> Allow Native(Basic) VPN	<input checked="" type="checkbox"/> Allow Developer Options In Settings
<input checked="" type="checkbox"/> Allow Bluetooth Visible	<input checked="" type="checkbox"/> Allow NFC	<input checked="" type="checkbox"/> Allow Native & LG VPN
<input checked="" type="checkbox"/> Enable Outgoing Calls In Roaming	<input checked="" type="checkbox"/> Allow OS OTA Update	<input checked="" type="checkbox"/> Allow VPN Split Tunneling
<input checked="" type="checkbox"/> Allow Manual DateTime Change	<input checked="" type="checkbox"/> Show Owner Info In The Lock Screen	<input checked="" type="checkbox"/> Allow Factory Reset
<input checked="" type="checkbox"/> Allow Manual Timezone Change	<input checked="" type="checkbox"/> Allow Passive Provider	<input checked="" type="checkbox"/> Allow Wireless Location
<input checked="" type="checkbox"/> Allow Clipboard	<input checked="" type="checkbox"/> Require EAS Complex Password	<input checked="" type="checkbox"/> Allow Wireless Storage
<input checked="" type="checkbox"/> Allow Contact Info Access		

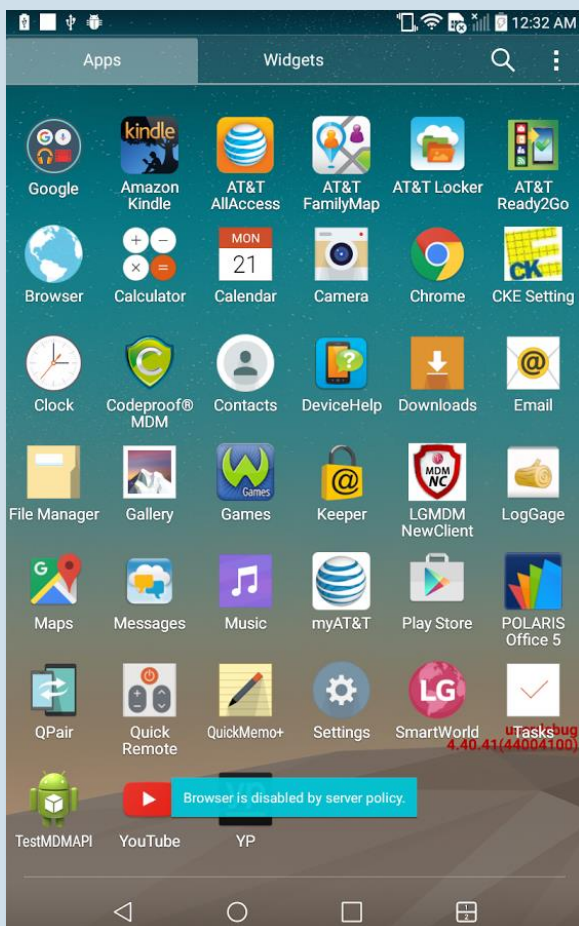
## APP RESTRICTIONS & WHITELISTING/BLACKLISTING POLICIES

From the App restrictions tab in the console, IT admins can block users from changing device Settings and Configurations, app installations, accessing Web browsers and task manager, among other features as per custom organizational policies for Whitelist/Blacklist.

### Admin Panel

The screenshot displays the Codeproof Admin Panel. The top navigation bar includes 'Codeproof', 'Dashboard', 'Policy Manager', 'EMM', 'Reports', and 'Administration'. The user 'sshetty@codeproof.com' is logged in. The left sidebar shows a tree view of device categories: Home, Android Devices, Bring Your Own Devices (BYOD), Galaxy Devices, iOS Devices, LG Devices (selected), LG Device [LG-V496], LG GPad [LG-V410], North America, and Supervised Devices. The main content area is titled 'MOBILE POLICY MANAGER' and has tabs for 'Android Security', 'iOS Security', 'Samsung Security', and 'LG Security'. Under 'LG Security', there are sub-tabs: 'Mobile Antivirus', 'Agent Policy', 'Kiosk Mode', 'Kiosk App Management', 'App Restrictions' (selected), 'Device Restrictions', 'Passcode Policy', 'WiFi Policy', 'Secure Browsing', 'Encryption Policy', 'Misc Policy', and 'Email Policy'. The 'App Restrictions' tab is active, showing a list of policies with checkboxes: 'Enable' (unchecked), 'Allow App Installation By End User' (checked), 'Allow App Un-Installation By End User' (checked), 'Allow Running Of Unsigned App' (checked), 'Allow Sideload (Manual APK Installation)' (checked), 'Enable Settings Changes By End User' (checked), 'Enable Google Playstore' (checked), 'Enable Web Browsers' (checked), 'Enable YouTube' (checked), 'Enable LG Backup' (checked), 'Enable Task Manager' (checked), and 'Enable Voice Dialer' (checked). Below this list are sections for 'App Whitelist' and 'App Blacklist', each with an 'Add Apps' button. A table header for the whitelist is visible with columns 'App Name' and 'Package Name'.

### Device Screen:



## WEBSITE WHITELISTING AND CONTENT FILTER (SECURE BROWSING)

Using the [Codeproof Secure Browser App](#), IT Administrators can remotely block website access in the device. Some of the supported features include:

- Remotely allow only the required websites (whitelist)
- Remotely block certain websites (blacklist)
- Remotely block websites based on a keyword in the content
- Remotely block websites based on a keyword in the URL
- Remotely block all advertisements
- Remotely block malicious websites
- Setting homepage & web shortcuts

The screenshot shows the 'Secure Web Browsing' configuration page in the Codeproof Policy Manager. The page is titled 'Secure Web Browsing' and includes a note: 'Restrict user access to websites in the devices. NOTE: In order for this feature to work, Please install Codeproof browser app from Playstore'. The configuration is divided into two main sections: 'Url access control' and 'Content access control'. In the 'Url access control' section, the 'Enable' checkbox is checked. Under 'Allow only these websites(whitelist)', there is a table with one entry: 'http://www.google.com' with the title 'google'. Below this, the 'Block only these websites(blacklist)' section is currently empty. The 'Content access control' section has a checkbox for 'Block sites which contains following keywords(seperated by comma)' which is unchecked. A text input field contains 'porn, sex, ...'. There are two checked checkboxes: 'Scan keywords in the Url' and 'Scan keywords in the website content'. At the bottom, there is a text input field for 'Skip urls with following extensions(seperated by comma)' containing 'jpg,png,gif'.

The screenshot shows a mobile browser interface. At the top, there is a search bar with the number '2' and the word 'Search'. Below the search bar, there is a list of website shortcuts: 'Codeproof website', 'Google website', 'Apple Website', and 'Microsoft website'. At the bottom of the screen, there is the Codeproof logo and the text 'CODEPROOF® A Mobile Managemant Company'.

## WIFI MANAGEMENT

- Allow or block specific known WiFi hotspots.
- Remotely create and manage WiFi and APN profiles

The screenshot displays the Codeproof Mobile Policy Manager interface. The left sidebar shows a navigation menu with categories like Home, Android Devices, Bring Your Own Devices (BYOD), Galaxy Devices, iOS Devices, and LG Devices. The main content area is titled 'MOBILE POLICY MANAGER' and is currently on the 'LG Security' tab. Under the 'WiFi Policy' sub-tab, there are several configuration options: 'Enable' (unchecked), 'Allow WiFi' (checked), 'Allow WiFi Auto Connection' (checked), 'Allow Wifi Direct' (checked), 'Allow End User Profile Management' (checked), and 'Allow WiFi Scan' (checked). Below these are three sections for managing hotspots: 'Configure WiFi Hotspot' with an 'Add WiFi Hotspot' button, 'WiFi Hotspot WhiteList' with an 'Add WiFi SSID' button, and 'WiFi Hotspot Blacklist' with an 'Add WiFi SSID' button. Each section contains a table with columns for 'SSID' and 'Encryption Type'.

## KIOSK MODE

IT administrators can remotely turn LG smartphones and tablets into kiosk devices. In Kiosk mode, you can allow to run a single or a defined set of apps, and block the notification bar, back key, menu key, recent key, Qslide, Split screen window and a range of unnecessary features.

You can also assign an app to the home key. This app will be displayed in full screen mode.

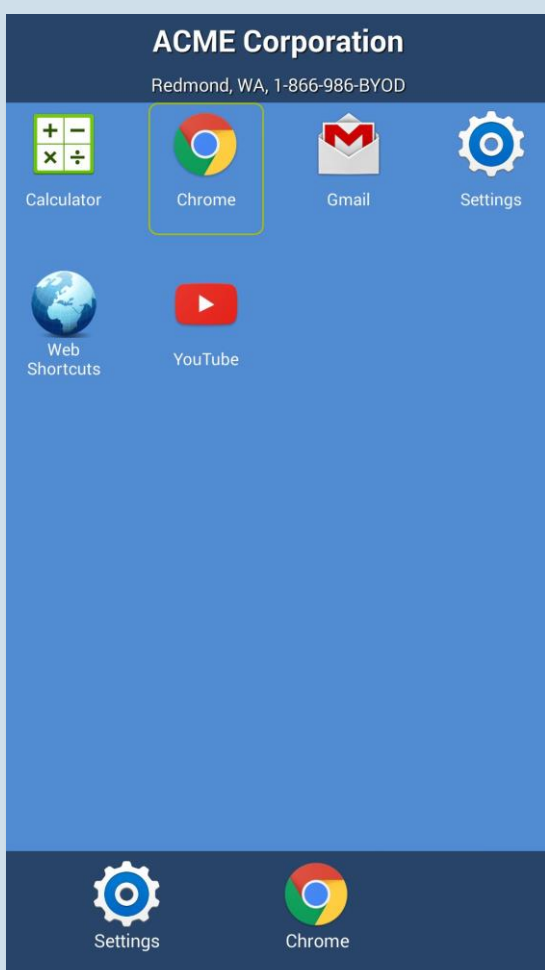
The screenshot displays the Codeproof Mobile Policy Manager interface, specifically the 'Kiosk Mode' configuration page for LG Security. The left sidebar is the same as in the previous screenshot. The main content area is titled 'MOBILE POLICY MANAGER' and is on the 'Kiosk Mode' sub-tab. The configuration options include: 'Enable ( Enable Kiosk mode policies. )' (checked), 'Enable Single App Full Screen View ( Enable full screen kiosk application. )' (unchecked), a text input for 'Kiosk App Package Name' with a 'Browse' button, 'Allow Back Key ( Allow back key in the device. )' (checked), 'Allow Home Key ( Allow home key. )' (checked), 'Allow Menu Key ( Allow menu key in the device. )' (checked), 'Allow Recent Key ( Allow recent key in the device. )' (checked), 'Allow Status Bar Expansion ( Allow status bar expansion in the device. )' (checked), 'Allow Split Screen View ( Enable or disable split screen view. )' (checked), and 'Allow Lock Screen Notifications ( Enable or disable keyguard customizations. )' (checked). At the bottom, there is an 'Inherit from parent ( Inherit policies from parent node )' checkbox (checked) and a 'SAVE' button.

## KIOSK MODE APP MANAGEMENT

Codeproof Platform includes the *Kiosk app management* feature that allows administrators to selectively run apps while blocking the rest. This capability is achieved using the Codeproof Kiosk App (home app). The Codeproof Kiosk App can be downloaded from the Google Play Store [here](#).

- Screen lockdown & a custom home screen
- Remotely turn on/off apps from the home screen
- Custom branding text and background company logo

The screenshot shows the Codeproof Kiosk App Management interface. The top navigation bar includes Dashboard, Policy Manager, EMM, Reports, and Administration. The left sidebar lists device categories like Android, iOS, and LG Devices. The main content area is titled 'Kiosk App Management' and contains a notification about installing the 'Codeproof App Manager' app. Below this, there are radio buttons for 'Allow Settings App', 'Allow All apps', and 'Allow Selected apps'. The 'Allowed App Whitelist' section contains a table with columns for 'App Name' and 'Package Name', listing 'Android Web Browser' and 'Phone'. There is also a section for 'Add Webshortcuts' with a table for 'Url' and 'Title', listing 'http://www.google.com' and 'Google Website'. At the bottom, there are fields for 'Enable Branding', 'Branding Title' (ACME Corp), 'Branding Subtitle' (1-866-986-BYOD), and 'Branding Image Url'.



## LOCATE THE DEVICE INCLUDING LOCATION HISTORY

Codeproof platform offers a complete device location history including GPS coordinates and physical addresses. Currently location history is stored for up-to three days. Location history can be exported and downloaded as a spreadsheet in an Excel format.

### Location History Export:

ReportedTime	Latitude	Longitude	Accuracy	PhysicalAddress
3/23/2016 8:58	39.5124	-85.7886036		12 806 St Joseph St, Shelbyville, IN 46176, USA
3/23/2016 8:45	39.50195	-85.78806745		48 2325 S Miller St, Shelbyville, IN 46176, USA
3/23/2016 8:20	39.71084	-86.00333191		24 I-74, Indianapolis, IN 46239, USA
3/23/2016 7:59	39.94507	-86.15796182		8 10801 N Meridian St, Indianapolis, IN 46290, USA
3/23/2016 7:31	39.95876	-86.16011947		8 11725 N Illinois St, Carmel, IN 46032, USA
3/23/2016 7:06	39.95543	-86.1609186	32.4679985	11590 N Meridian St, Carmel, IN 46032, USA
3/23/2016 6:48	39.95545	-86.16097845		96 11590 N Meridian St, Carmel, IN 46032, USA
3/23/2016 6:16	39.97479	-86.15751788		6 12900 N Meridian St, Carmel, IN 46032, USA
3/23/2016 6:06	39.84864	-86.04510834		6 I-465, Lawrence, IN 46226, USA
3/23/2016 5:47	39.5892	-85.82947324		4 I-74, Fairland, IN 46126, USA
3/23/2016 5:36	39.5046	-85.7582016	71.69300079	1168-1192 E McKay Rd, Shelbyville, IN 46176, USA
3/23/2016 4:25	39.51248	-85.7885596		20 806 St Joseph St, Shelbyville, IN 46176, USA
3/23/2016 3:25	39.51248	-85.7885599		20 806 St Joseph St, Shelbyville, IN 46176, USA
3/22/2016 15:07	39.51248	-85.7885545		20 806 St Joseph St, Shelbyville, IN 46176, USA
3/22/2016 14:41	39.51249	-85.78856		20 806 St Joseph St, Shelbyville, IN 46176, USA
3/22/2016 14:16	39.52168	-85.7769494		16 300 S Harrison St, Shelbyville, IN 46176, USA
3/22/2016 13:51	39.78437	-85.76919833		8 1 Court House Plaza, Greenfield, IN 46140, USA
3/22/2016 13:31	39.79764	-85.76927976		48 2-98 Ellis Dr, Greenfield, IN 46140, USA
3/22/2016 13:12	39.79787	-85.76913457		24 1031 N State St, Greenfield, IN 46140, USA
3/22/2016 12:47	39.81705	-85.92184051		24 I-70, Greenfield, IN 46140, USA
3/22/2016 12:24	39.78865	-86.1627613	43.89400101	280-298 W 16th St, Indianapolis, IN 46202, USA
3/22/2016 12:03	39.80273	-85.9629018		50 11432-11448 Cosmo Ct, Indianapolis, IN 46229, USA
3/22/2016 11:23	39.79449	-85.765895	20.84399986	300 E Boyd Ave, Greenfield, IN 46140, USA
3/22/2016 10:08	39.79448	-85.7658651		20 300 E Boyd Ave, Greenfield, IN 46140, USA
3/22/2016 9:45	39.79578	-85.7678955		20 HRH Private Dr, Greenfield, IN 46140, USA
3/22/2016 9:05	39.79571	-85.7680465	159.9730072	HRH Private Dr, Greenfield, IN 46140, USA
3/22/2016 8:30	39.79595	-85.76791721		48 HRH Private Dr, Greenfield, IN 46140, USA
3/22/2016 8:11	39.79574	-85.7679682	161.9900055	HRH Private Dr, Greenfield, IN 46140, USA
3/22/2016 7:51	39.80549	-85.77427944		8 200 Green Meadows Dr, Greenfield, IN 46140, USA



Using the command center, administrators can perform the following actions to the device instantly:

- Remotely lock the device
- Remotely wipe the device and/or the external memory card
- Send the scream sound
- Send the Push Message
- Remotely rebooting the phone
- Remotely power off the phone
- Remotely launch the App in the phone
- Remotely wipe ALL App data
- Remotely un-install apps

The screenshot displays the Codeproof Mobile Policy Manager interface. The top navigation bar includes 'Codeproof', 'Dashboard', 'Policy Manager', 'EMM', 'Reports', and 'Administration'. The left sidebar shows a navigation menu with categories like 'Home', 'Android Devices', 'Bring Your Own Devices (BYOD)', 'Galaxy Devices', 'iOS Devices', 'LG Devices', 'North America', and 'Supervised Devices'. The main content area is titled 'MOBILE POLICY MANAGER' and is currently on the 'LG Security' page. The 'Command Center' tab is active, showing a 'Select a command to create:' dropdown menu with options: '(Select Command)', '(Select Command)', 'Screen lock command', 'Wipe Device(Factory Reset)', 'Send Scream', 'Send message to User', 'Install Application', 'Uninstall Application', 'Reboot Device', 'Power Off Device', 'Start Application', and 'Wipe Application Data'. Below the dropdown is a table with columns: 'Result', 'Status', 'Last Updated', 'Notes', and 'Created by'.

## APP DEPLOYMENT

IT administrators can centrally deploy a business app (APK) to all enrolled LG devices simultaneously simply by adding the APK download URL to the Codeproof console. Apps will be installed in the device silently.

After adding the APK URL, make sure to select the “deploy” checkbox. After that, send a ping command to device to perform a force policy update. Apps will be installed instantly. Complete instructions are available [here](#).

The screenshot shows the Codeproof App Store interface. The 'Add App' dialog box is open, displaying the following information:

- Name: ACME Business App
- Publisher: ACME Corp
- OS: Android
- Package Type: APK
- Value: <https://www.acmecorp.com/download/app.apk>
- Deploy:

The dialog box also includes 'Cancel' and 'Save' buttons and a link to 'Click here for instructions'.

Device Ping:

The screenshot shows the Codeproof Mobile Policy Manager interface. The 'LG Security' tab is selected, and the 'Kiosk Mode' sub-tab is active. The 'Ping Device' option is highlighted in the left sidebar menu.

The main content area displays the following settings:

- Enable ( Enable Kiosk mode policies. )
- Enable Single App Full Screen View ( Enable full screen kiosk application. )
- Kiosk App Package Name
- Allow Back Key ( Allow back key in the device. )
- Home Key ( Allow home key. )
- Allow Menu Key ( Allow menu key in the device. )
- Allow Recent Key ( Allow recent key in the device. )
- Allow Status Bar Expansion ( Allow status bar expansion in the device. )

## EMAIL CONFIGURATIONS

IT Administrators can remotely create IMAP/POP/SMTP Email accounts in the LG device.

The screenshot displays the Codeproof Mobile Policy Manager interface. The main window is titled 'MOBILE POLICY MANAGER' and includes tabs for 'Android Security', 'iOS Security', and 'Samsung Security'. Under the 'iOS Security' tab, there are sub-tabs for 'Mobile Antivirus', 'Agent Policy', and 'Kiosk Mode'. A sidebar on the left lists various device categories, with 'LG Devices' selected. The 'Add Email Configuration' button is visible in the 'Agent Policy' section. A modal dialog box titled 'Add Email Config' is open, showing fields for: Account Name, Account Type (set to IMAP), Email Address, POP/IMAP Server Address, POP/IMAP Security (set to SSL), POP/IMAP Server Port (set to 993), POP/IMAP Username, POP/IMAP Password, SMTP Server Address, SMTP Security (set to SSL), SMTP Server Port (set to 465), SMTP Username, SMTP Password, Maximum Mails To Show (set to 100), Retrieve Interval (minutes) (set to 15), Maximum Attachment Size(KB) (set to 10240), and Signature (set to 'The device is secured by Codeproof'). The dialog box has 'Cancel' and 'Add' buttons at the bottom.

## REPORTING

The following reports are available and can be printed or downloaded as PDF files.

- Apps Report
- Device Asset report
- Last communicated report
- Mobile Carrier report
- Mobile OS Report
- Security Compliance report
- Android Permission report

### Acme Corporation Mobile OS Report

Generated on: 3/31/2014 5:46:16 AM

Generated by: sshetty@codeproof.com

OS Name	OS Version	Model Name	Num Devices
Android	4.1.2	SGH-T999	4
Android	2.3.6	GT-S5360	2
Android	4.3	Nexus 7	2
iPhone OS	6.1.3		1
iPhone OS	7.1	iPhone	1
Android	2.3.4	Kindle Fire	1

### Acme Corporation Access Phone Contacts Permission Report

Generated on: 3/31/2014 5:51:29 AM

Generated by: sshetty@codeproof.com

App Name	Package Name	Version	Reported time	Enrollment ID	Agent ID
BACKLog	com.backlog	1.0.3	3/28/2014 4:48:55 PM	Ga test[Nexus 7]	3ced3fc1-fdfd-4538-9320-7f0b0b5830e8
Epic Raiders	com.gamevil.epicraiders.google	1.0.7	3/28/2014 4:48:55 PM	Ga test[Nexus 7]	3ced3fc1-fdfd-4538-9320-7f0b0b5830e8
Facebook	com.facebook.katana	1.9.10	3/28/2014 4:48:55 PM	Ga test[Nexus 7]	3ced3fc1-fdfd-4538-9320-7f0b0b5830e8
Facebook	com.facebook.katana	7.0.0.26.28	3/30/2014 7:05:01 PM	Final test[SGH-T999]	a89596e6-24e5-452d-9142-c15fb63990b8
Google Play services	com.google.android.gms	4.2.43 (1035512-010)	3/7/2014 5:15:54 PM	Samsung galaxie [GT-S5360]	13ef132a-05e9-4d68-ab0f-c3edb6beaa9
GroupMe	com.groupme.android	4.2.9	3/30/2014 7:05:01 PM	Final test[SGH-T999]	a89596e6-24e5-452d-9142-c15fb63990b8
ICS 4.0 StatusBar	com.calsto.statusbar.ics	1.2.1.3	3/28/2014 4:48:55 PM	Ga test[Nexus 7]	3ced3fc1-fdfd-4538-9320-7f0b0b5830e8
WhatsApp	com.whatsapp	2.11.186	3/30/2014 7:05:01 PM	Final test[SGH-T999]	a89596e6-24e5-452d-9142-c15fb63990b8

## MISCELLANEOUS FEATURES

Other supported features include configurations for passcode policy, encryption policy, jailbreak or rooted detection, collecting browser history, collecting phone call and SMS information etc.

## WHAT'S NEXT?

1. For a free trial signup click [here](#).
2. Go to device and Install Codeproof LG Security App from Google Playstore [here](#)  
(app url: <https://play.google.com/store/apps/details?id=com.codeproof.lg.security> )
3. Launch the Codeproof app and enroll the device.
4. Remotely manage from the Codeproof Cloud Console [here](#)

---

Document last updated on March 25, 2016

For more information, visit <http://codeproof.com>

Questions/comments, email to [support@codeproof.com](mailto:support@codeproof.com)

"LG Life's Good" is a registered trademark of LG Corp and/or its related entities.

Google and Android are registered trademark of Google, Inc.