LG ANDROID 6.x STIG CONFIGURATION TABLES

Version 1, Release 1

09 May 2016

Developed by LG and DISA for the DoD

Note: The logic of some of the configuration settings in the following table may differ from one MDM product to another. For example, the policy rule "Disable GooglePlayStore" may appear as "Allow GooglePlayStore" in some MDM consoles. In this case, the rule should be set to "Disable" instead of "Enable" as indicated below.

Note: The title of each policy group and policy rule may differ from one MDM product to another.

Table 1: Configuration Policy Rules

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments	Activation Type	
								COPE #1	COPE #2
Password Restriction	Enforce password	Enable/Disable	X		Enable	LGA6-201001-01		X	X
Password Restriction	Password length	0	X		6 or more characters	LGA6-201002-01		X	X
Password Restriction	Maximum time to lock	0	X		15 minutes or less	LGA6-201003-01		X	X
Password Restriction	Max repeating characters	0	X		More than 2	LGA6-201004-01		X	X
Password Restriction	Max sequential characters	0	X		More than 2	LGA6-201004-01		X	X
Password Restriction	Maximum failed password attempts	0	X		10 or less	LGA6-201005-01		X	X
Application Restriction	Allow GooglePlayStore	Enable/Disable	X		Disable	LGA6-201006-01		X	X
Android Restriction	Allow unknown sources	Enable/Disable	X		Disable	LGA6-201006-02		X	X
Application Restriction	Application whitelist configuration (install)	Configure/Not Configure	X		Add approved applications	LGA6-201007-01	Allow user to install applications only on whitelist	X	X

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments	Activation Type	
								COPE #1	COPE #2
Android Restriction	Allow notification on LockScreen	Enable/Disable	X		Disable	LGA6-201008-01	Disallow to display notification when the device is locked	X	X
Android Restriction	Allow Wi-Fi tethering	Enable/Disable		X	Disable			X	X
Android Restriction	Allow Bluetooth tethering	Enable/Disable	X		Disable	LGA6-201009-02		X	X
Android Restriction	Allow USB tethering	Enable/Disable	X		Disable	LGA6-201009-03		X	X
Android Restriction	Allow development mode	Enable/Disable	X		Disable	LGA6-201010-01		X	X
Android Restriction	Device encryption	Enable/Disable	X		Enable	LGA6-201011-01	Protect data at rest on built-in storage media	X	X
Android Restriction	Storage card encryption	Enable/Disable	X		Enable	LGA6-201012-01	Protect data at rest on removable storage media	X	X
Android Restriction	Enforce Warning Banner	Configure/Not Configure	X		Add text	LGA6-201015-01	Add DoD required advisory warning message	X	X
Android Restriction	Allow USB mass storage	Enable/Disable	X		Disable	LGA6-201016-01	Disallow a USB mass storage mode	X	X
Android Restriction	Allow USB host storage	Enable/Disable	X		Disable	LGA6-991000-03	Disallow a USB host storage mode	X	X
Application Restriction	Allow LG backup	Enable/Disable	X		Disable	LGA6-201017-01	Disallow backup to locally connected systems	X	X

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments	Activation Type	
								COPE #1	COPE #2
Android Restriction	Allow Google backup	Enable/Disable	X		Disable	LGA6-201018-01	Disallow backup to remote systems	X	X
Android Restriction	Allow Google crash report	Enable/Disable	X		Disable	LGA6-201021-01	Disable automatic transfer of diagnostic data to an external device other than MDM service	X	X
Android Restriction	Allow Fingerprint	Enable/Disable	X		Disable	LGA6-201022-01		X	X
Android Restriction	Allow Smart Lock	Enable/Disable	X		Disable	LGA6-201022-02		X	X
Network Configuration	VPN	Configure/Not configure	X		Add VPN Profile	LGA6-201025-01	Enable VPN protection	X	X
Application Restriction	Application blacklist configuration (launch)	Configure/Not configure	X		Add disapproved applications	LGA6-201026-01 / LGA6-991000-10	Disallow user to launch applications on blacklist	X	X
Android Restriction	Allow Bluetooth Data Transfer	Enable/Disable	X		Disable Data transfer	LGA6-201027-01		X	X
Android Restriction	Allow VPN Split Tunneling	Enable/Disable	X		Disable	LGA6-201029-01		X	X
Application Restriction	Application blacklist configuration (launch)	Configure/Not configure	X		Add FOTA client application	LGA6-201031-01	Disable automatic firmware updates	X	X
Certificate Configuration	Install CA Cert	Configure/Not configure	X		Add certificate	LGA6-991000-01	Install DoD root and intermediate PKI certificates on the device	X	X

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments	Activation Type	
								COPE #1	COPE #2
Application Restriction	Application blacklist configuration (install)	Configure/Not configure	**X**		Add disapproved applications	LGA6-991000-10	Disallow user to install applications on blacklist	**X**	**X**
Application Restriction	Allow Voice Command	Enable/Disable	**X**		Disable	LGA6-991000-04		**X**	**X**
Android Restriction	Allow NFC	Enable/Disable	**X**		Disable	LGA6-991000-05		**X**	**X**
Android Restriction	Allow DLNA	Enable/Disable	**X**		Disable	LGA6-991000-06	Disable connection to nearby devices	**X**	**X**
Android Restriction	Allow removal of device administrator rights	Enable/Disable	**X**		Disable	LGA6-991000-07		**X**	**X**
Android Restriction	Allow system time changes	Enable/Disable	**X**		Disable	LGA6-991000-08	Disable manual date time changes	**X**	**X**
Android Restriction	Set CC mode	Enable/Disable	**X**		Enable	LGA6-991000-09	Set Common Criteria mode	**X**	**X**

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments	Activation Type	
								COPE #1	COPE #2
Application Restriction	Application blacklist configuration (launch)	Configure/Not configure	X		Add LG browser and Chrome browser applications	LGA6-991000-12	Disallow user to use the browsers, including encryption modules that are not FIPS 140-2 validated LG browser does not apply to Verizon smartphones.	X	X
Android Restriction	Set owner info	Configure/Not configure		X	Add text		DoD sites should consider displaying the DoD warning banner and/or the following message: "If this mobile device is found, please call the following phone number xxx-xxx-xxxx." When called, the phone number should not identify itself as a DoD organization.	X	X

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments	Activation Type	
								COPE #1	COPE #2
Android Restriction	Disallow owner info	Enable/Disable		X	Disable			X	X
Password Restriction	Password complexity	Pattern Pin Alphabetic Alphanumeric Complex		X	Complex			X	X
Android Restriction	Allow contact info access on LockScreen	Enable/Disable		X	Enable			X	X
Android Restriction	Allow auto sync	Enable/Disable	X		Disable	LGA6-991000-14		X	X
Android Restriction	Allow Android Beam	Enable/Disable	X		Disable	LGA6-991000-15		X	X
Android Restriction	Allow Wi-Fi Direct	Enable/Disable		X	Disable			X	X
Android Restriction	Allow Miracast	Enable/Disable		X	Disable			X	X
Android Restriction	Allow download mode	Enable/Disable	X		Disable	LGA6-991000-18		X	X
Password Restriction	Password expiration	0		X				X	X
Password Restriction	Min uppercase	0		X				X	X
Password Restriction	Min lowercase	0		X				X	X
Password Restriction	Min numeric	0		X				X	X

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments	Activation Type	
								COPE #1	COPE #2
Application Restriction	Application blacklist configuration (uninstall)	Configure/Not configure		X	Add applications		Disallow user to uninstall applications on blacklist	X	X

Table 2: Configuration Policy Rules for Android for Work "Work Profile"

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments	Activation Type	
								COPE #1	COPE #2
Account Management	Allow addition of Google Accounts (for Work Profile)	Enable/Disable	**X**		Disable	LGA6-991000-51	Disallow to add Google accounts in Work Profile.		X
Application Restriction	Whitelisted Android apps (for Work Profile)	Configure/Not configure	**X**		Add approved preloaded applications to Work Profile whitelist	LGA6-991000-52	Preloaded apps added to the Work Profile whitelist should be AO-approved		X
Application Restriction	Set permitted input methods (for Work Profile)	Configure/Not configure		**X**			Control adds IME apps to an IME whitelist and is redundant to the app whitelist		X
Application Restriction	Set uninstall not allowed for mandatory Work Profile apps	Configure/Not configure	**X**		Add applications	LGA6-991000-55	Disallow uninstalling mandatory applications in Work Profile		X
Android Restriction	Allow screen capture (for Work Profile)	Enable/Disable		**X**	Disable				X
Android Restriction	Allow camera (for Work Profile)	Enable/Disable		**X**	Disable				X

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments	Activation Type	
								COPE #1	COPE #2
Android Restriction	Allow Bluetooth contact sharing (for Work Profile)	Enable/Disable		**X**	Disable		Disallow Bluetooth devices accessing work contacts.		X
Android Restriction	Allow Cross-Profile CallerId (for Work Profile)	Enable/Disable		**X**	Disable		Disable showing caller-Id information from the Work Profile in the Personal Profile (e.g., incoming calls).		X
Android Restriction	Allow copy/ paste between Work Profile and Personal Space (for Work Profile)	Enable/Disable	**X**		Disable	LGA6-991000-60	Disallow copying to the clipboard between Work and Personal Profiles		X
Android Restriction	Allow Install apps (for Work Profile)	Enable/Disable		**X**	Enable		Allow installing applications in Work Profile		X
Android Restriction	Allow share location (for Work Profile)	Enable/Disable		**X**	Enable		Allow turning on location sharing for Work Profile		X
Certificate Configuration	Install CA Cert (for Work Profile)	Configure/Not configure	**X**		Add CA certificate	LGA6-991000-57	Install DoD root and intermediate PKI certificates on the device		X
Certificate Configuration	Install KeyPair (for Work Profile)	Configure/Not configure		**X**	Add certificates and private key pair		Install a certificate and private key pair		X

Policy Group	Policy Rule	Options	Required	Optional	Settings	Related Requirement Number	Comments	Activation Type	
								COPE #1	COPE #2
Certificate Configuration	Uninstall all user CA Certs (for Work Profile)	Command		**X**	Uninstall		Uninstall all custom trusted CA certificates from the profile		X
Android Restriction	Allow content sharing (for Work Profile)	Enable/Disable	**X**		Disable	LGA6-991000-58	Disable sharing data in Work Profile to Personal Profile (e.g., contacts in Work Profile)		X