

Boas práticas para utilização segura de Smartphones Samsung Knox

SAMSUNG Knox



Documento produzido por:





Introdução

Na nova era digital, o Smartphone tem assumido cada vez mais um papel central, deixando de ser uma pura ferramenta de comunicação assente em voz e SMS, evoluindo ao ponto de ser possível a sua transformação num posto de trabalho, seja no tratamento de correio electrónico ou uso de aplicações internas.

As novas tendências *Bring-Your-Own-Devices* (BYOD), *Corporate-Owned Personally Enabled* (COPE) e *Corporate Owned Business Only* (COBO), não só tem acelerado a proliferação de aplicações para todo o tipo de negócios e necessidades pessoais, como também, tem promovido uma crescente mistura de contextos, tipos de informação e plataformas de acesso, que requerem uma correta avaliação dos riscos inerentes.

Esta mudança de paradigma levanta uma série de questões de segurança que servem de base para a elaboração deste guia.

Contexto

As recomendações deste guia assentam no uso de equipamentos e implementação de soluções, que enumeramos de seguida:

- Sistema Operativo Android 8 e 9
- Smartphones/Tablets Samsung com a plataforma Samsung Knox 3.x.
- Solução de MDM para gestão centralizada dos dispositivos móveis



Samsung Knox Platform for Enterprise (KPE)

A plataforma Samsung Knox é considerada uma das plataformas de gestão de mobilidade mais seguras da indústria, tendo recebido mais certificações de segurança por parte de entidades independentes e agências governamentais (>30) do que qualquer outra plataforma ou solução.

Assente nesta plataforma temos o Knox Container - um container que separa os dados e aplicações profissionais dos dados pessoais do utilizador, garantido a integridade da informação e possibilitando aos gestores de IT um controlo granular do smartphone.



Considerações para as organizações

Mobile Device Management (MDM)

A escolha da solução de MDM a implementar ficará sempre a cargo do Administrador de IT. A Samsung trabalha em parceria com os principais *players* neste campo para assegurar o suporte às Knox APIs. Contudo, deve o Administrador de IT assegurar que a solução de MDM suporta os princípios e políticas de segurança constantes neste guia.

Alguns dos principais MDM - Samsung Knox Manage; BlackBerry UEM; Citrix Endpoint Manager; Microsoft Intune; MobileIron UEM; SAP Cloud Platform Mobile Services; SOTI MobiControl; Samsung SDS EMM; VMware Workspace ONE UEM.



Knox Mobile Enrollment (KME)

A solução Knox Mobile Enrollment permite a automatização do registo/inscrição dos equipamentos móveis Samsung na plataforma de MDM, aplicando as políticas pré-definidas. As vantagens desta solução são claras, poupando tempo e custos às organizações na configuração dos equipamentos em massa e retirando complexidade na configuração inicial aos próprios utilizadores.

Esta solução é também compatível com os principais MDM existentes no mercado. Para mais informações, visite a página:

<https://www.samsungknox.com/en/solutions/it-solutions/knox-mobile-enrollment>

Como mitigar os principais riscos e ameaças

Existem várias plataformas Samsung, cada uma com o seu suporte personalizado. Para efeitos de identificação e caracterização utilizámos a solução Samsung Knox Manage, e listamos seguidamente para um conjunto riscos alguns mecanismos de segurança, assim como, políticas possíveis de serem aplicadas a um dispositivo móvel e ao Knox Container:

Perda ou roubo de equipamento:

Mecanismos de segurança	Recomendação
Aplicação de políticas de segurança	O uso de uma solução de MDM será fundamental para aplicar e gerir de forma centralizada as políticas de segurança definidas nos dispositivos, assim como preparar os mesmos para uso no ambiente profissional, automatizando as configurações de e-mail, VPN, aplicações profissionais, etc.
Resposta a incidentes	Uma brecha na segurança, que pode passar pelo simples extravio de um equipamento a um OS comprometido, pode ser rapidamente mitigada através de acções como bloquear/remover o <i>container</i> , revogar o acesso à VPN, e-mail, ou mesmo apagar todo o dispositivo.

1. Criação de um novo perfil de políticas de segurança: Profiles » Device Management Profile » New registration
2. Devices & Users » Devices (seleccionar o dispositivo comprometido)» Device Command



Frequently Used	Apply latest Device/App mgmt profiles
Compliance	Lock/Unlock device
App Management	Reset screen password
Device Management	Factory reset + Initialize SD Card
EMM	Send message
Device Info Sync	Collect device/app info

Fraca proteç o do sistema operativo:

Mecanismos de seguranc�a	Recomendaç�o
Proteç�o de bin�rios	<p>A recomendaç�o das entidades acreditadoras passa por incluir nos smartphones e tablets as seguintes proteç�es de bin�rios:</p> <ul style="list-style-type: none"> - RELRO - Canary - NX - Pie
Mecanismos de verificaç�o de integridade do SO	<p>Os equipamentos m�veis dever�o possuir mecanismos pr�prios para garantir a integridade do dispositivo desde o <i>boot</i> at� ao <i>runtime</i>.</p> <ul style="list-style-type: none"> - Secure/Trusted Boot (Samsung KPE) - Real-time Kernel Protection (Samsung KPE) - Attestation (Samsung KPE)
Atualizaç�es de software	<p>� de todo o interesse das organizaç�es controlar as vers�es de sistema operativo instaladas nos seus equipamentos m�veis, garantido assim que n�o existem disrupç�es na operaç�o e as �ltimas atualizaç�es de seguranc�a.</p> <p>O Samsung Knox E-FOTA pode garantir esta gest�o atrav�s da plataforma de MDM ou soluç�o Cloud/On-premise dedicada. Desta forma, o administrador de IT pode decidir para quem e quando s�o instaladas as actualizaç�es.</p>



- Profiles » Device Management Profile » Android (Legacy) » Security » Attestation

Attestation ● ?

- Action when verification fails ●

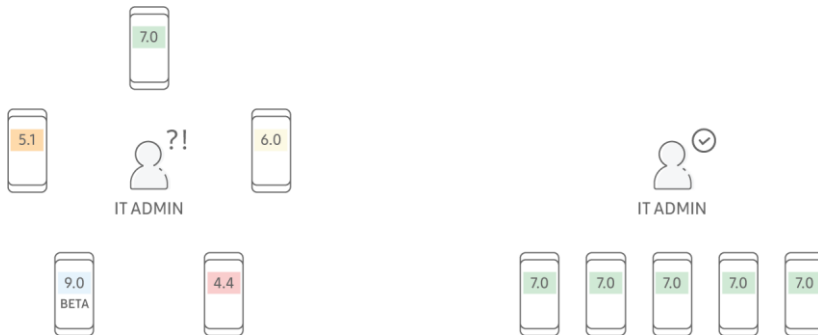
- Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » System » Trusted Boot Verification

Trusted Boot Verification ?

- Profiles » Device Management Profile » Android (Legacy) » System » OTA upgrade

OTA upgrade ● ?

- Profiles » E-FOTA Management (necessita de licença válida para E-FOTA on MDM)





Fraca identificação e autenticação:

Mecanismos de segurança	Recomendação
Dupla autenticação	Deverá ser aplicada uma política de identificação e autenticação para acesso ao dispositivo e ao container, de acordo com os requisitos da organização, sendo passível o uso de autenticação biométrica.

- *Profiles » Device Management Profile » Android (Legacy) » Policy » Security*

The screenshot shows the 'Security' settings page for an Android (Legacy) profile. The left sidebar lists various categories: Security (selected), Interface, Application, Kiosk, Phone, Browser, System, Scheduler, Logging, Firewall, and DeX. The main content area is titled 'Device Password' and includes the following settings:

- Minimum strength: Must be alphanumeric
- Maximum Failed Login Attempts: 10
- If maximum failed login attempts exceeded: Lock device
- Minimum length: 8
- Expiration after (days): 0-365
- Manage password history (times): 0-10
- Device lock timeout (min): 15
- Maximum length of sequential numbers: 1-10
- Maximum length of sequential characters: 1-10
- Block function setting on lock screen: Apply
- Block functions on lock screen: All, Camera, Trust Agent

- *Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » Security*

The screenshot shows the 'Security' settings page for a LightWeight Knox profile. The left sidebar lists various categories: System, Interface, Browser, Container Data, Application, Security (selected), and Firewall. The main content area is titled 'Device Password' and includes the following settings:

- Enterprise Identity Authentication: Do not use
- Minimum strength: Must be alphanumeric
- Maximum Failed Login Attempts: 3
- Action for failing allowed count to retry password: Lock Knox Container
- Expiration after (days): 90
- Manage password history (times): 1
- Minimum length: 8
- Minimum number of letters: 1
- Minimum number of lowercase letters: 1-10
- Minimum number of capital letters: 1-10
- Minimum number of non-letters: 1-10
- Unlock with fingerprint: Allow
- Unlock with iris: N/A
- Enforce Multi factor Authentication: Use



Separação entre dados pessoais e dados profissionais:

Mecanismos de segurança	Recomendação
Protecção dos dados armazenados	Toda a informação armazenada no Knox Container está encriptada por defeito e inacessível a aplicações fora do <i>container</i> .

1. Profiles » Device Management Profile » Knox » Add (para criar o Knox Container)
2. Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » Container Data

- Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » System » Share via apps

Instalação e utilização de aplicações terceiras:

Mecanismos de segurança	Recomendação
Lista de aplicações permitidas	De forma a limitar o risco de instalação de aplicações maliciosas, o administrador de IT deverá aplicar através da consola de MDM uma política restritiva, só deixando instalar aplicações verificadas. No limite, poderá bloquear o acesso à Play Store ou Galaxy Store.



- Por defeito, na criação do Knox Container não são adicionadas aplicações comuns à área pessoal, como a Câmara, Galeria, Internet ou E-mail. Estas terão de ser adicionadas manualmente pelo administrador de IT através do package name (Ex. Câmara - com.sec.android.app.camera).
- *Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » Application » General area app installation list*

System	- General area app installation list	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Add +</p> <table border="1"> <tr> <td>com.sec.android.app.camera</td> <td>×</td> </tr> <tr> <td>com.sec.android.app.sbrowser</td> <td>×</td> </tr> </table> <p>App Data deletion protection list ▾</p> <p>Add + Add all app +</p> <table border="1"> <tr> <td>.*</td> <td>×</td> </tr> </table> <p>Add + Add all app +</p> <table border="1"> <tr> <td>None</td> <td></td> </tr> </table> <p>N/A ▾</p> <p>N/A ▾</p> </div>	com.sec.android.app.camera	×	com.sec.android.app.sbrowser	×	.*	×	None	
com.sec.android.app.camera	×									
com.sec.android.app.sbrowser	×									
.*	×									
None										
Interface										
Browser										
Container Data	App Data deletion control setting ?									
Application	- App Data deletion protection list									
Security										
Firewall	- App Data deletion protection exception list									
	Application force stop prohibition list setting ?									
	Show ProgressBar when installing apps ?									

- Desabilitar aplicações Google no Knox Container: *Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » Application » GMS application*

System	- Application installation blacklist	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Add +</p> <table border="1"> <tr> <td>None</td> <td></td> </tr> </table> <p>Add + Add all app +</p> <table border="1"> <tr> <td>None</td> <td></td> </tr> </table> <p>N/A ▾</p> <p>N/A ▾</p> <p>N/A ▾</p> <p>N/A ▾</p> <p>Disallow ▾</p> <p>N/A ▾</p> </div>	None		None	
None						
None						
Interface						
Browser						
Container Data	- Application installation whitelist					
Application	App Execution Blacklist Setting ?					
Security	Application execution prevention list setting ?					
Firewall	Application uninstallation prevention list Setting ?					
	App installation authority whitelisting settings ?					
	GMS application ?					
	TIMA CCM profile whitelist ?					



- Desabilitar aplicações no dispositivo: *Profiles » Device Management Profile » Android (Legacy) » Policy » Application (App Installation Black/Whitelist; Application execution Black/Whitelist)*

- Instalar aplicações internas: *Applications » Internal Applications » Add (+)*



Falta de monitorização contínua:

Mecanismos de segurança	Recomendação
Ativação dos registos de auditoria (audit logs)	Através da consola de MDM, o administrador de IT pode recolher também informação do dispositivo como as aplicações instaladas, as políticas de segurança aplicadas, localização, definir alarmística, etc.

- *Devices & Users » Devices » pressionar no "Mobile ID" para aceder aos detalhes*

Security

<p>Lock Device: Unlocked</p> <p>- Unlock Code: 136055210</p> <p>Password Policy Compliant: ● Normal</p> <p>Password Failure Count: N/A</p> <p>- Password Failure Policy: N/A</p> <p>Password [?]: ?</p> <p>Knox Password [?]: ?</p> <p>EMM Login Failed: 0/5</p> <p>-Login Failed Policy: None</p>	<p>+ More</p>	<p>KeepAlive [?]: ● Unset</p> <p>Compromised OS: ● Normal</p> <p>Compromised App: ● Normal</p> <p>Fingerprint authentication: Supported</p> <p>Iris recognition: Not supported</p> <p>E-FOTA: Disabled</p> <p>Attestation [?]: ● Normal</p>	<p>+ More</p>
---	---------------	--	---------------

Device Information

<p>Device location</p> <p>Memory: 2.44G of 109.93G used + More</p> <p>Battery Level: 35% Remaining</p> <p>Mobile Number</p> <p>MAC Address: 6C:C7:EC:90:D1:64</p> <p>Firmware: PPR1.180610.011.G970FXXU1A SD4</p>	<p>+ More</p>	<p>IMEI/MEID: 352248100325181</p> <p>Serial Number: R38KB0FADGF</p> <p>ICCID information: 8935101811643408005</p> <p>Manufacturer: samsung</p> <p>Activation Type [?]: ● Match</p> <p>- User Settings / Device Activation: Android / Android</p> <p>Android Enterprise Method: Legacy</p>
---	---------------	---

- Para configuração de alarmística: *Service Overview » Alerts*

Audit Events

Audit Events

Event Category	Audit Events
<input type="checkbox"/> Email	Send Mail To User
<input type="checkbox"/> Email	Update SMTP Settings
<input type="checkbox"/> Email	Add Mail Template
<input type="checkbox"/> Email	Delete Mail Template
<input type="checkbox"/> Email	Modify Mail Template
<input type="checkbox"/> Settings	Activate API User
<input type="checkbox"/> Settings	Deactivate API User
<input type="checkbox"/> Settings	Delete API User
<input type="checkbox"/> Settings	Add API User
<input type="checkbox"/> Settings	Invalidate API User Tokens
<input type="checkbox"/> Settings	Modify API User
<input type="checkbox"/> Email	Send Tizen Wearable Installation Info.
<input type="checkbox"/> Email	Send Mail To User (Async)
<input type="checkbox"/> Email	Send Mail To Device (Async)
<input type="checkbox"/> SMS	Change SMS settings

Page 1 of 59 View 20

Total Events (272)

Audit Events

Alert Category	Audit Events	Level	Result
<input type="checkbox"/> Failed Policies	Agent Device Control Fail ...	Error	Failed
<input type="checkbox"/> Security Violation	Report policy violation	Critical	All
<input type="checkbox"/> Security Violation	Check Point MTP Malware...	Warning	All
<input type="checkbox"/> Changes In Device Status	Change to Disconnected s...	Info	All
<input type="checkbox"/> Failed Policies	Close container app (Devic...	Error	Failed
<input type="checkbox"/> Failed Policies	Delete container app data ...	Error	Failed
<input type="checkbox"/> Failed Policies	Delete container app (Devi...	Error	Failed
<input type="checkbox"/> Failed Policies	Apply security policy (Devi...	Error	Failed
<input type="checkbox"/> Failed Policies	Distribute the latest app m...	Error	Failed
<input type="checkbox"/> Failed Policies	Agent Request to disallow ...	Error	Failed
<input type="checkbox"/> Failed Policies	Agent Respond to the requ...	Error	Failed
<input type="checkbox"/> Failed Policies	Agent Request to lock scre...	Error	Failed
<input type="checkbox"/> Failed Policies	Agent Respond to the requ...	Error	Failed
<input type="checkbox"/> Failed Policies	Agent Request to unlock d...	Error	Failed
<input type="checkbox"/> Failed Policies	Agent Respond to the requ...	Error	Failed
<input type="checkbox"/> Failed Policies	Agent Request to reissue c...	Error	Failed

Update



Falha no estabelecimento de comunicações móveis seguras:

Mecanismos de segurança	Recomendação
Protecção dos dados transmitidos	Uso de VPN: - Apenas Knox Workspace - Todo o dispositivo
Protecção de conectividade externa	O uso de interfaces de conectividade como Wi-Fi, USB, Bluetooth, NFC ou cartão de memória poderão ser limitados ou mesmo desactivados de acordo com as especificidades da organização.

- Profiles » Device Management Profile » Android (Legacy) » Policy » Interface

The screenshot displays the configuration for the 'Interface' policy. The settings and their corresponding dropdown options are as follows:

- Wi-Fi: N/A
- Wi-Fi hotspot: Disallow
- Wi-Fi SSID whitelist setting: N/A
- Wi-Fi SSID Blacklist setting: N/A
- Wi-Fi auto connection: N/A
- Wi-Fi minimum security level setting: N/A
- Bluetooth: Allow
- Desktop PC connection: Disallow
- Data transfer: Disallow
- Search mode: N/A
- Bluetooth tethering: Disallow
- Bluetooth UUID Black/Whitelist: N/A
- NFC control: Disallow
- PC connection: Disallow
- USB tethering: Disallow
- USB host storage (OTG): Disallow
- Set usb exception allowed list: N/A
- USB exception allowed list:
 - Audio
 - Cdc Data
 - Communication
 - Hid
 - Mass Storage
 - Miscellaneous
 - Still Image
 - Vendor Spec
 - Wireless Controller
- USB debugging: Disallow
- Microphone: N/A
- GPS: N/A



- Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » Interface

System	Add a new Wi-Fi network ?	Disallow
Interface	Microphone ?	N/A
Browser	Camera ?	N/A
Container Data	Allow USB access ?	Disallow
Application	- Allow access of USB devices	
Security		Package Name
Firewall		Vendor Id
		Product Id
		None
	Bluetooth Low Energy ?	N/A
	Phone Book Access Profile (PBAP) via Bluetooth ?	Disallow
	NFC control ?	Disallow

- Profiles » Device Management Profile » Android (Legacy) » Settings » Generic VPN

Category ?	Generic VPN
Configuration ID *	
VPN name *	
Description	
Remove available	-
VPN vendor name *	Cisco
VPN client vendor package name *	com.cisco.anyconnect.vpn.android.avf
VPN type *	SSL
Entering methods for Generic VPN *	Manual Input
Generic VPN profile	
VPN route type *	per-app vpn
Server address *	
User authentication *	<input checked="" type="radio"/> Use <input type="radio"/> Do not use
Connection type *	<input checked="" type="radio"/> KEEP ON <input type="radio"/> On Demand
Chaining *	Default
UID PID *	<input checked="" type="radio"/> Use <input type="radio"/> Do not use



Conclusões

A elaboração deste guia resulta do trabalho conjunto do mundo académico (Adyta), empresarial (Samsung) e governamental (GNS) e visa dotar as organizações de uma maior consciência não só para a sua segurança como também para o aumento da produtividade através do uso de ferramentas de mobilidade.

Como apontado ao longo deste guia, cabe às organizações a escolha das soluções que melhor assentam as suas necessidades, mas consideramos vital que estejam cada vez mais atentas a estas temáticas aquando da elaboração da sua estratégia interna de mobilidade.

Referências

Samsung Knox™ Security Solution White paper

Knox Platform for Enterprise White paper

SAMSUNG Knox Manage Administrator's Guide

Knox STIG API tables for Android 8 and Android 9