SAMSUNG Galaxy

Boas práticas para utilização segura de Smartphones Samsung Knox

SAMSUNG Knox

Documento produzido por:

GNS Gabinete Nacional de Segurança PORTUGAL

U.PORTO UNIVERSIDADE DO PORTO CENTRO DE COMPETÊNCIAS EM CIBERSEGURANÇA E PRIVACIDADE C3P

adyta SAMSUNG

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, politicas 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 *container*, 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 proteção do sistema operativo:

Mecanismos de segurança	Recomendação
Protecção de binários	A recomendação das entidades acreditadoras passa por incluir nos smartphones e tablets as seguintes protecções de binários: - RELRO - Canary - NX - Pie
Mecanismos de verificação de integridade do SO	Os equipamentos móveis deverão possuir mecanismos próprios para garantir a integridade do dispositivo desde o *boot* até ao *runtime*. - Secure/Trusted Boot (Samsung KPE) - Real-time Kernel Protection (Samsung KPE) - Attestation (Samsung KPE)
Atualizações de software	É de todo o interesse das organizações controlar as versões de sistema operativo instaladas nos seus equipamentos móveis, garantido assim que não existem disrupções na operação e as últimas atualizações de segurança. O Samsung Knox E-FOTA pode garantir esta gestão através da plataforma de MDM ou solução Cloud/On-premise dedicada. Desta forma, o administrador de IT pode decidir para quem e quando são instaladas as actualizações.

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

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

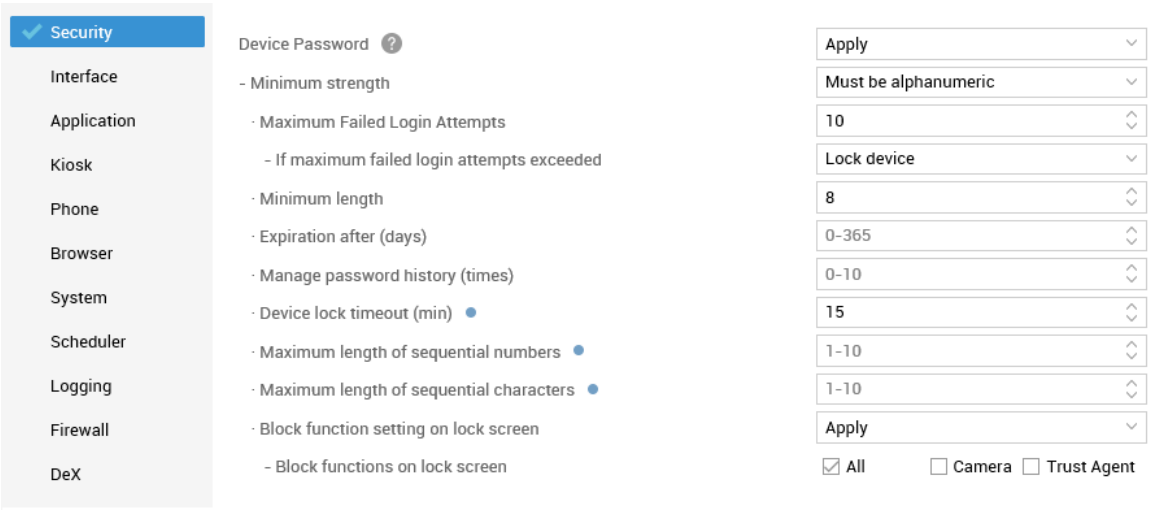
- *Profiles » Device Management Profile » Android (Legacy) » System » OTA upgrade*

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

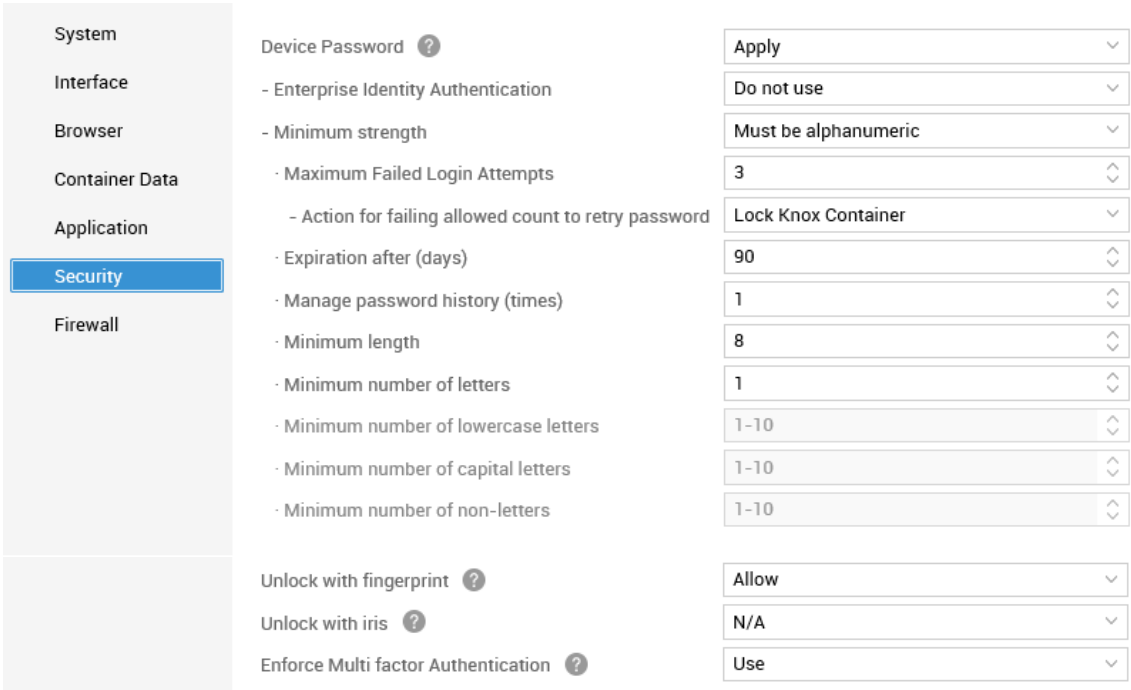
Fraca identificação e autenticação:

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*



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

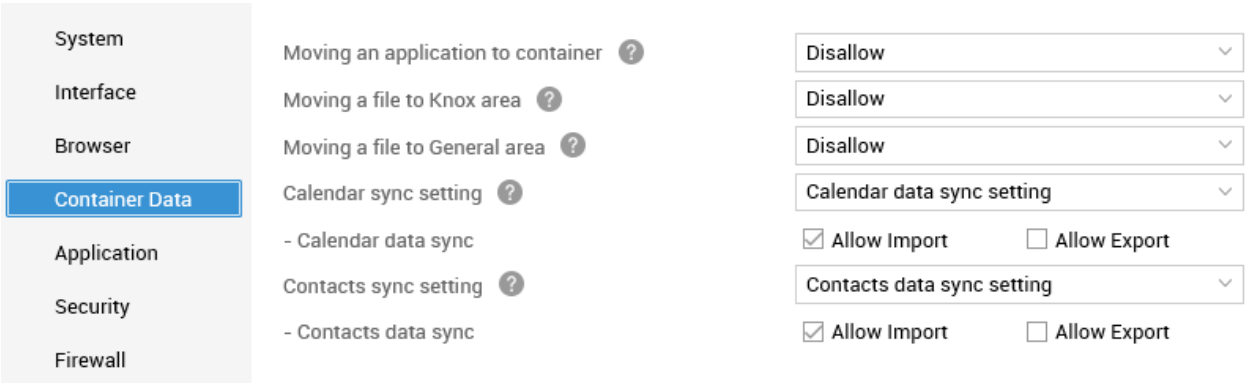


Separação entre dados pessoais e dados profissionais:

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 *container*.

1. *Profiles » Device Management Profile » Knox » Add (para criar o Knox Container)*

2. *Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » Container Data*



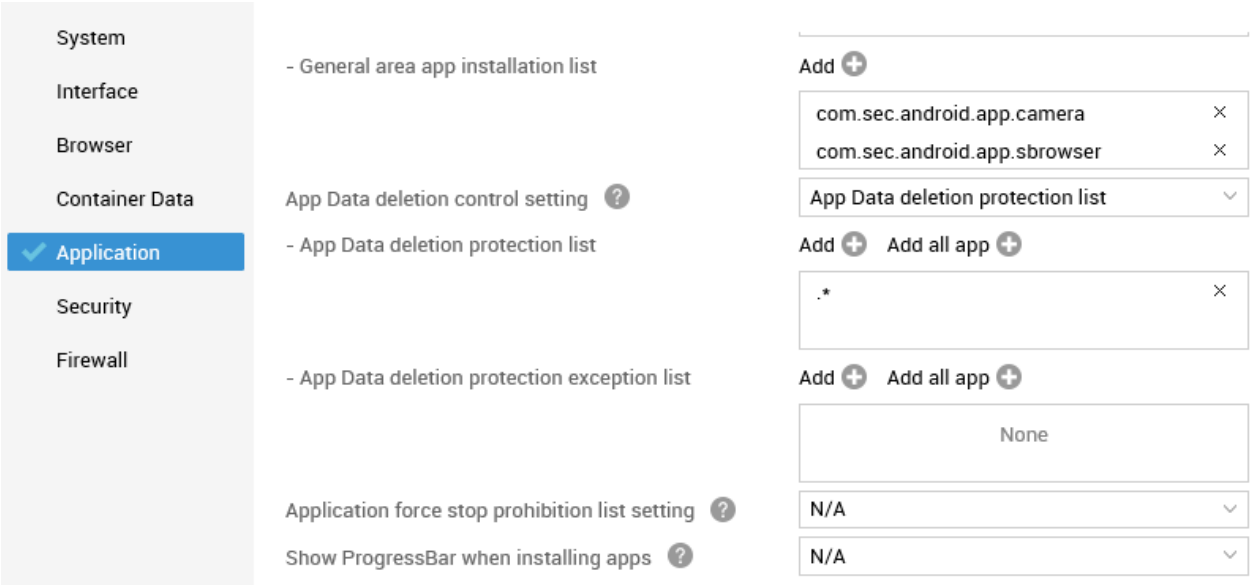
- *Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » System » Share via apps*

Instalação e utilização de aplicações terceiras:

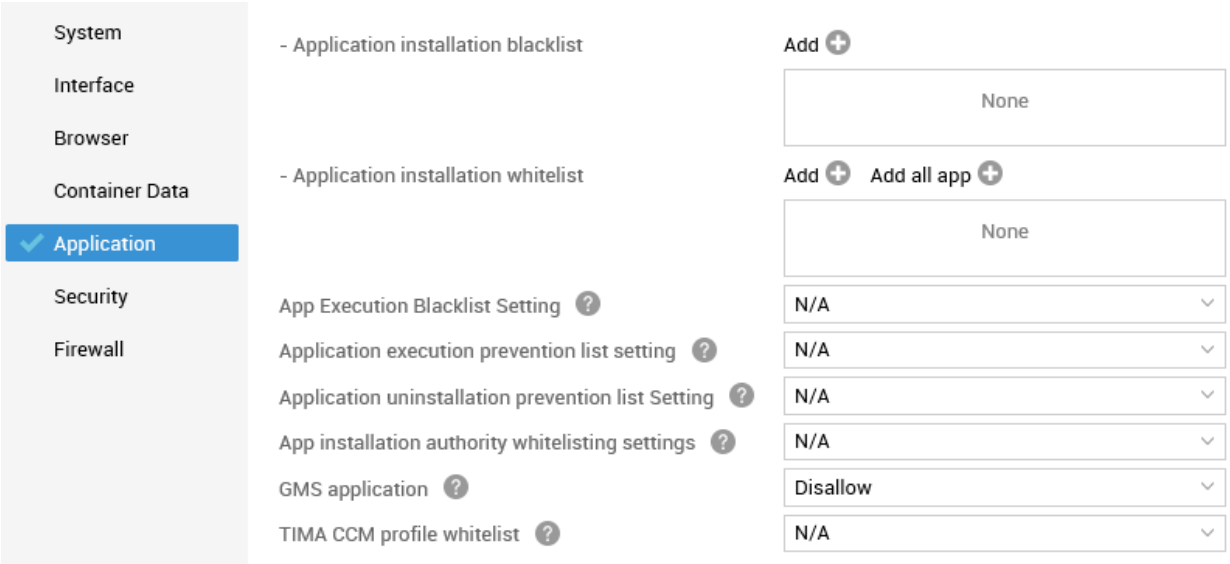
Mecanismos de segurança	Recomendação
Lista de aplicações permitidas	De forma a limitar o risco de instalação de aplicações maliciosas, o administrador de IT deverá aplicar através da consola de MDM uma política restritiva, só deixando instalar aplicações verificadas. No limite, poderá bloquear o acesso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

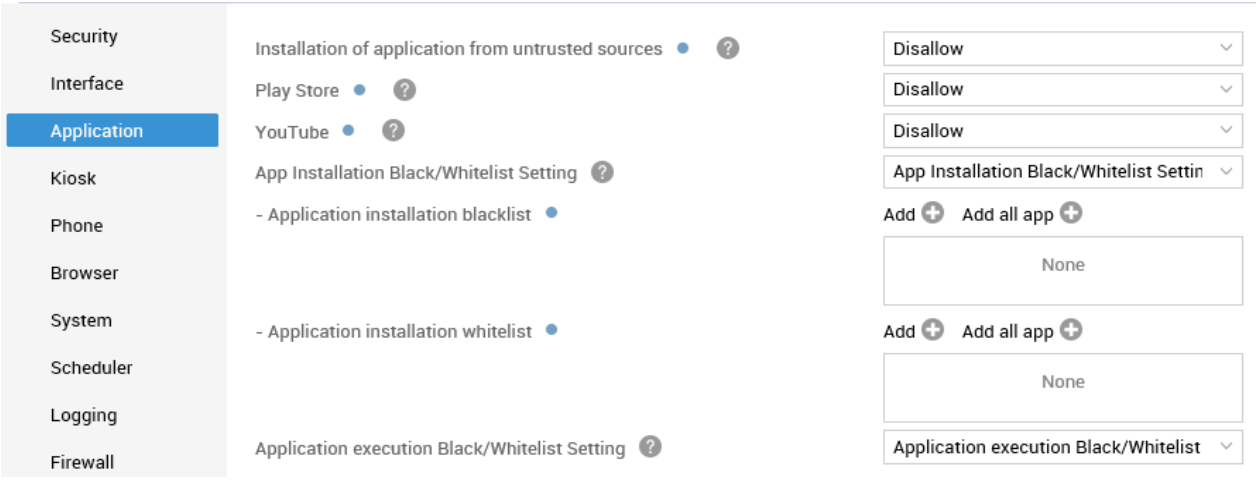
- *Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » Application » General area app installation list*



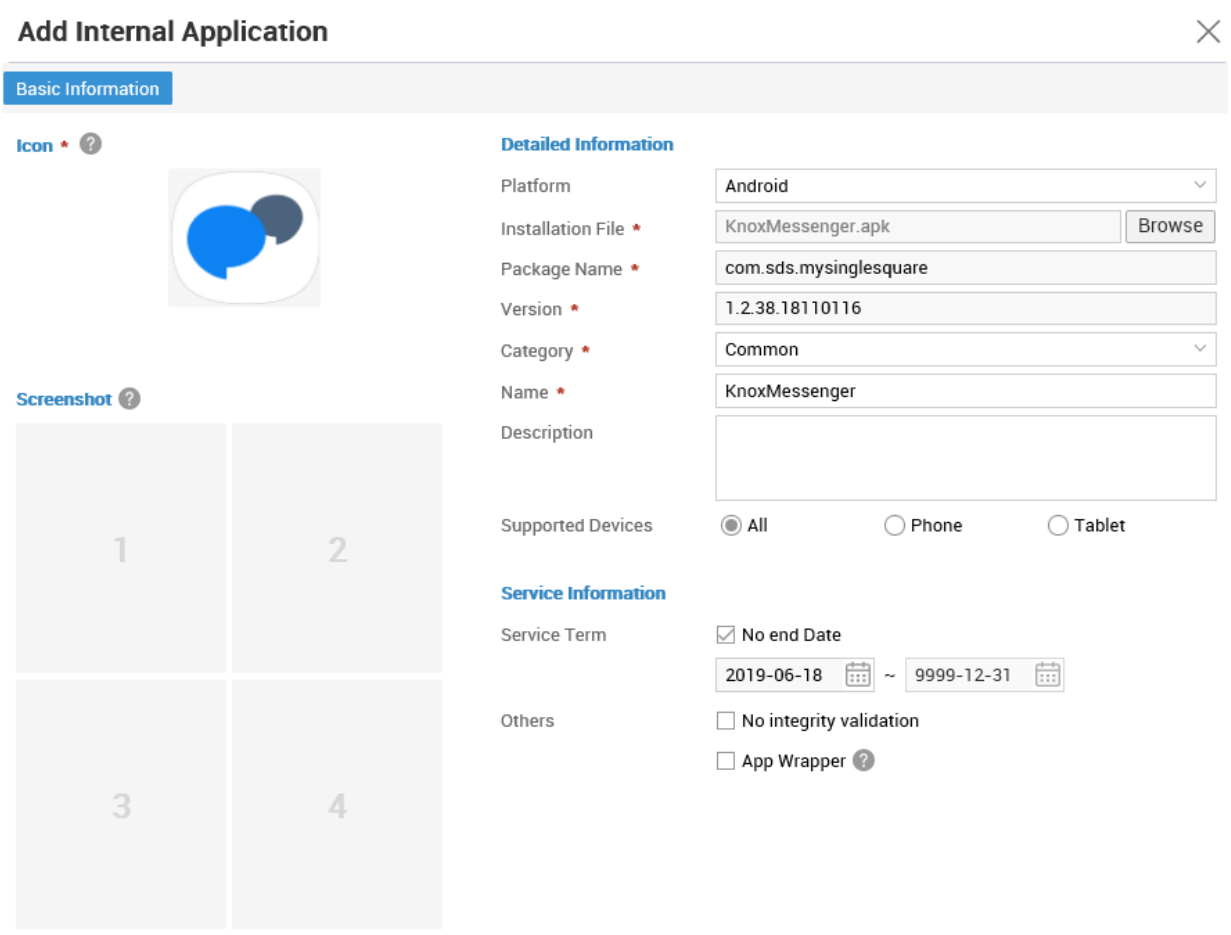
- Desabilitar aplicações Google no Knox Container: *Profiles » Device Management Profile » Knox » LightWeight Knox » Policy » Application » GMS application*



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



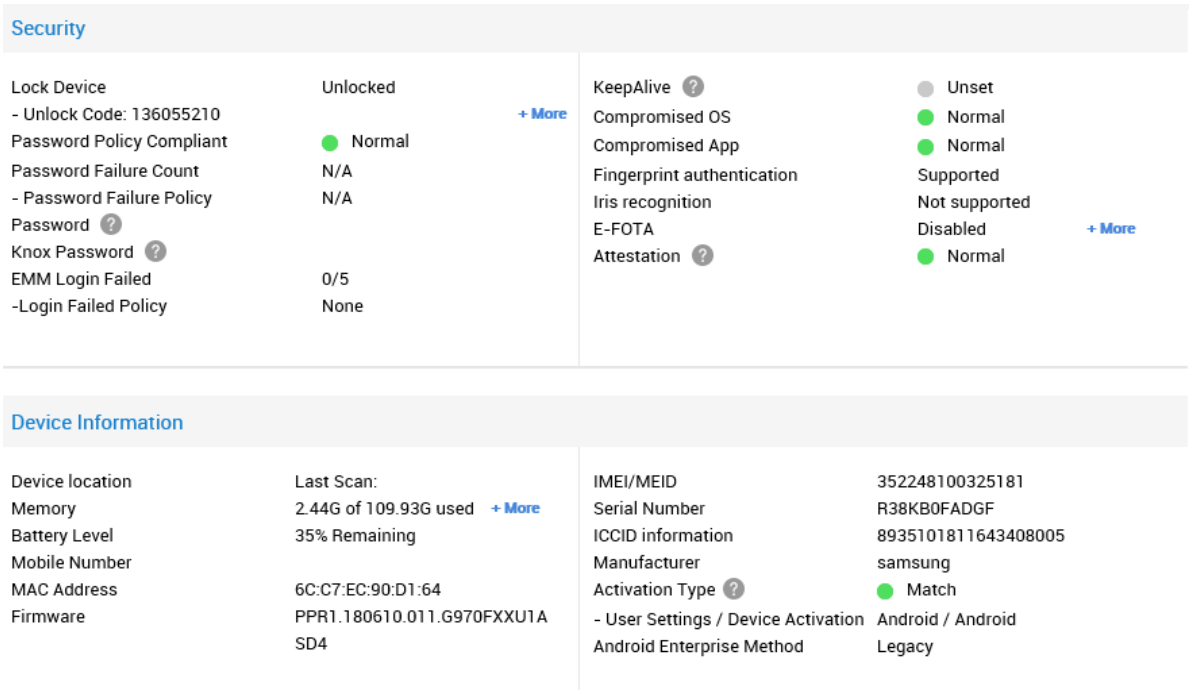
- Instalar aplicações internas: *Applications » Internal Applications » Add (+)*



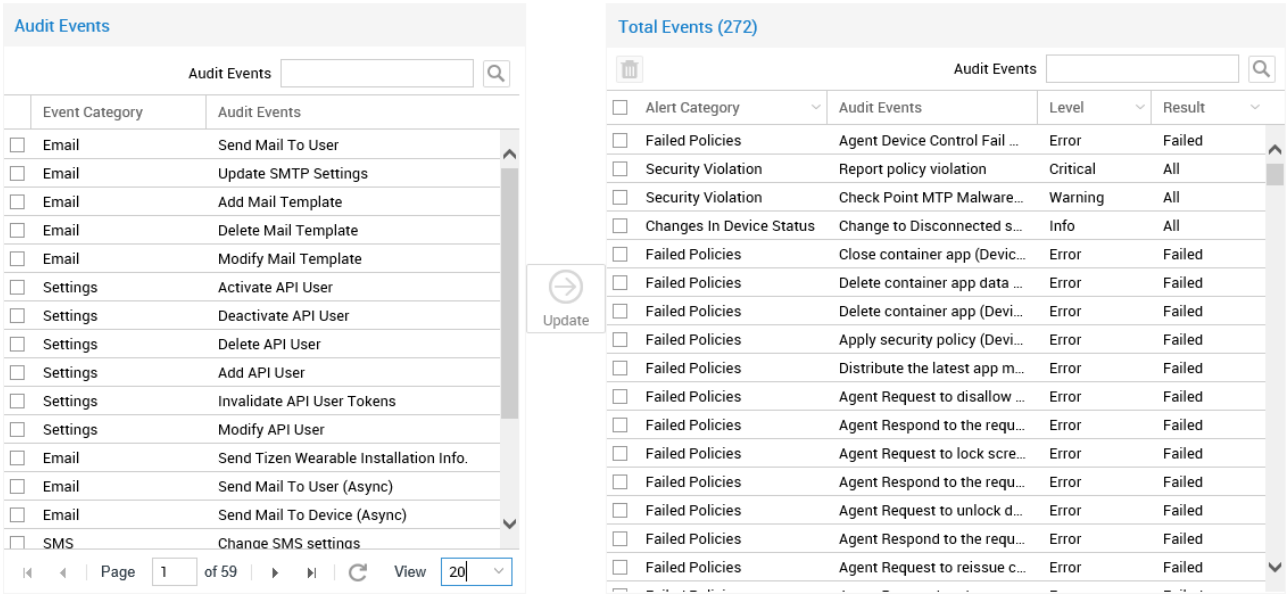
Falta de monitorização continua:

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*



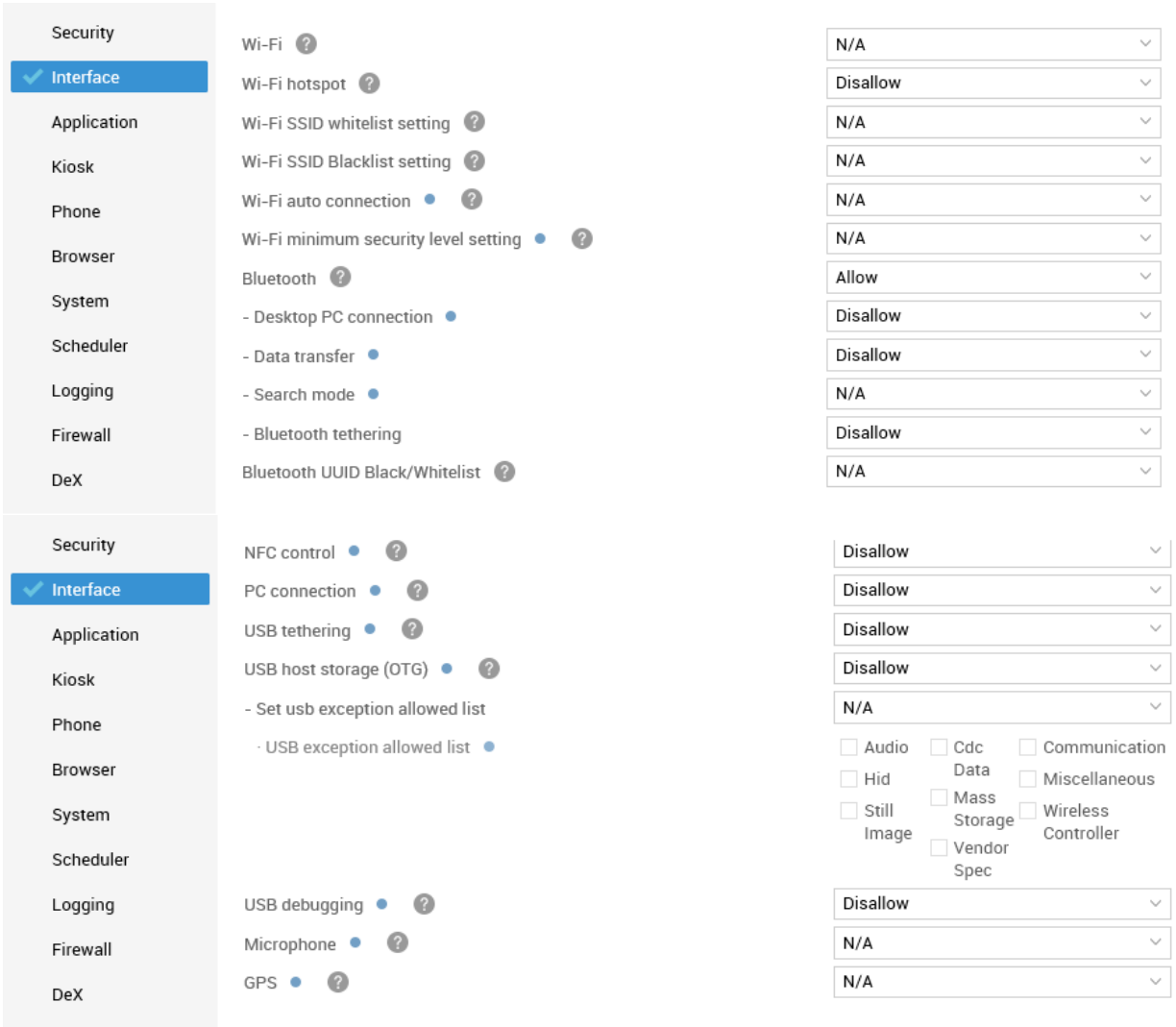
- Para configuração de alarmística: *Service Overview » Alerts*



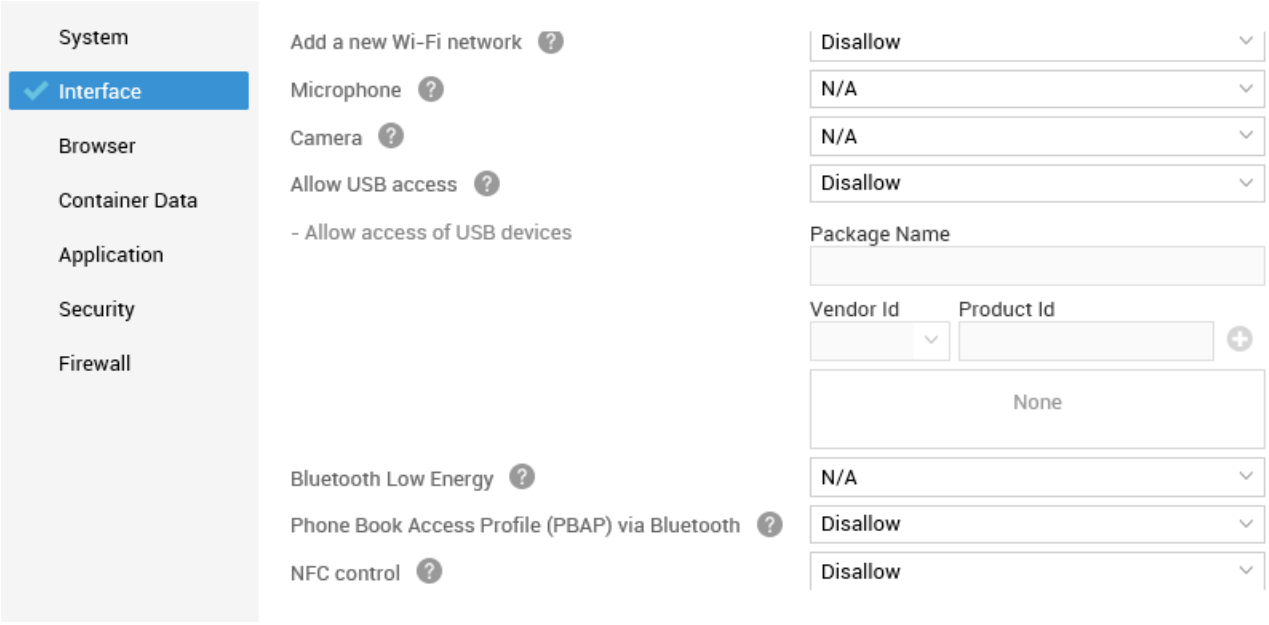
Falha no estabelecimento de comunicações móveis seguras:

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.

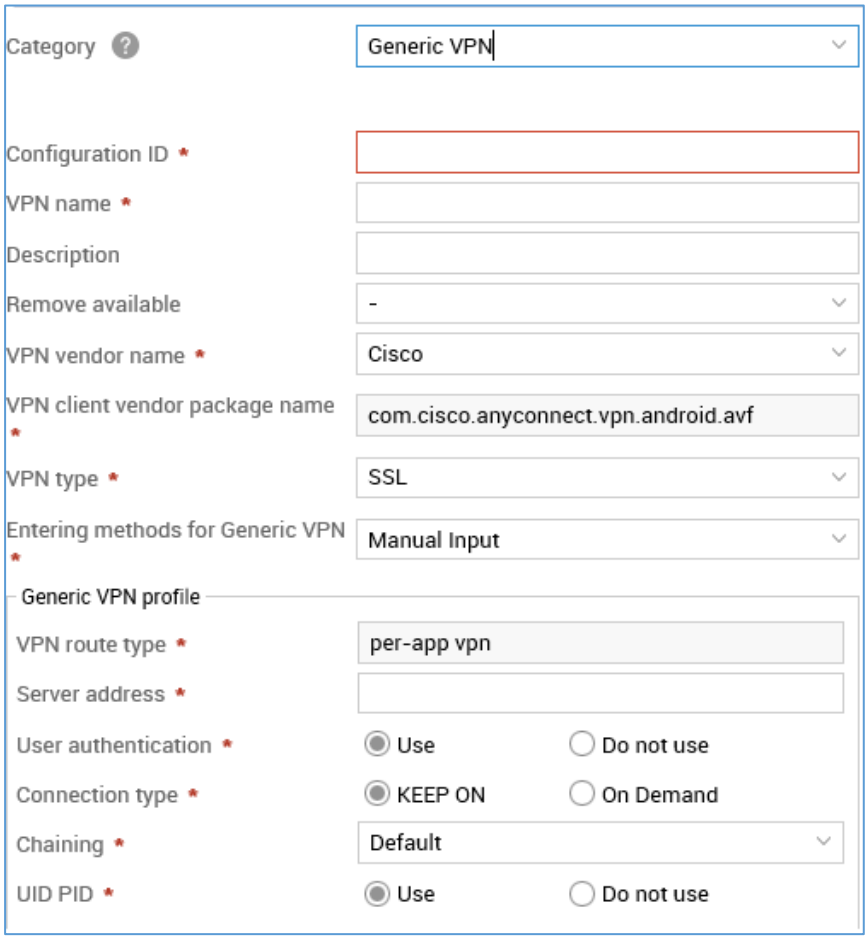
- *Profiles » Device Management Profile » Android (Legacy) » Policy » Interface*



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



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



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 KnoxTM 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