Australian Government
Australian Signals Directorate

Security configuration guide: Viasat Mobile Dynamic Defense

First published: February 2021
Last updated: October 2021

Table of contents

Introduction

The Australian Signals Directorate (ASD) has developed this guidance to assist organisations to understand the risks of deploying and provide specific configuration requirements for the Viasat Mobile Dynamic Defense (MDD) system to handle classified data. This security configuration guide does not replace the *Information security manual* (ISM), however where a technical conflict arises the most current document shall take priority.

Audience

To use this guide, readers should be familiar with basic networking concepts, be an experienced mobile device system administrator, and be or have access to an experienced network administrator.

Parts of this guide will make reference to product features that will require the engagement of other software, networking equipment or other Mobile Device Management (MDM) vendors. While every effort has been made to ensure content involving any third-party vendor products is correct at the time of writing, organisations should always check with these vendors when planning their system implementation. Note, mention of third-party products is not a specific endorsement of that vendor over another, and they are used for illustrative purposes only.

Some security configuration instructions within this guide are complex, and if implemented incorrectly could reduce the security of the device, the network or the organisation's overall security posture. These instructions should only be implemented by experienced systems administrators and should be used in conjunction with thorough testing.

Purpose

This guide provides information for organisations on Viasat Mobile Dynamic Defense (MDD) and potential security risks that should be considered before being introduced into their mobile fleet. A threat risk assessment should be undertaken by organisations so that they completely understand the risks present in the deployment model they have selected.

This guide is to be used with the security configuration guides for mobile devices developed by ASD. Organisations are required to meet all existing **PROTECTED** level security configurations as outlined in the configuration guides for the mobile devices.

The advice in this guide relates to use of the MDD platform within Australia. Organisations and individuals seeking to use devices overseas should also refer to the *Travelling with mobile devices* publication.

System functionality and user experience will be affected by the implementation of this guide. Authorising officers should consider the balance of user requirements and security, as not all advice may be appropriate for every user or environment.

Organisations should seek approval from their authorising officer to allow for the formal acceptance of the risks. Refer to the *applying a risk-based approach to cybersecurity* section of the ISM for more information.

General advice

When newer versions of MDD are released, there is potential for new security implications and authorising officers should seek additional guidance if required. In the absence of additional guidance, ASD advises:

- Upgrade to the latest version of MDD as new versions provide security enhancements and address known vulnerabilities. This is consistent with ASD's advice to install the latest versions of software and patch operating system vulnerabilities as communicated in the ISM and the *Strategies to mitigate cybersecurity incidents*.

Mobile device vendors and software providers provide explanatory notes regarding the content of their security updates. This information may help organisations quantify the risk posed if they do not update.

Introduction to mobile device security

In this guide, mobile device security advice centres on the three security tenets of:

- device integrity
- data at rest
- data in transit.

ASD evaluates device cryptographic implementations, to determine the device configuration necessary to reduce handling requirements of devices used for the processing or storing of classified data. It is each organisation's responsibility to configure the device according to ASD advice, and assess that the applications implemented by an organisation use the available cryptographic protections appropriately.

Configuration advice regarding device integrity aims to provide a level of protection suitable for classified mobile devices. It assumes malicious actors may have physical access to mobile devices while powered on and in a locked state. Configuration advice draws upon an assessment of:

- key hierarchy and architecture evaluation
- cryptographic implementation assessment
- operating system architecture
- configuration assessment under typical deployment scenarios.

It is the organisation's responsibility to configure the device according to this advice in order to achieve the desired integrity outcomes.

Configuration advice regarding the protection of data at rest, aims to provide a level of protection suitable for classified data stored on mobile devices. This advice assumes malicious actors have physical access to the device while it is powered on and in a locked state. Configuration advice and device evaluation draw upon configuration assessment and details of application implementation including availability of security features.

Configuration advice regarding the protection of data in transit, aims to provide a suitable level of protection for the classified data traversing a network, while assuming malicious actors are able to intercept traffic.

It is each organisation's responsibility to configure their devices according to ASD advice and support and maintain appropriate VPN infrastructure to support the VPN tunnels. Such infrastructure is out of scope for this guide.

Supervised devices

ASD guidance advises that all devices handling classified data be supervised. Supervision is configured via MDD enrolment. Supervision of devices handling government data is necessary to ensure that the correct policies and configurations are applied throughout the lifecycle of a device.

Advice to authorising officers

ASD has developed the *Strategies to mitigate cybersecurity incidents* to help organisations and their authorising officers mitigate cybersecurity incidents caused by various cyberthreats. The most prominent set of these mitigation strategies is known as the Essential Eight. While the strategies were developed for workstations and servers, much of the functionality described exists on modern smartphones as well. Consequently, the risks are just as important to consider on mobile devices.

The assessed MDD product interacts with Samsung Galaxy mobile devices. Users and administrators will need to implement all of the security configurations as specified in the *Security configuration guide: Samsung Galaxy S10, S20 and Note 20 devices* publication. The minimal configuration requirements for mobile devices shall target the **PROTECTED** level controls. The configuration guide outlines the risks of deploying and specific configuration requirements for the Samsung Galaxy mobile devices to handle classified data.

MDD platform features and risk considerations

The following table describes certain features within MDD and the risk considerations that users, administrators and risk owners will need to consider.

Feature	Description and Risk Considerations	Requirement at PROTECTED
'Whitelist', 'Signature Whitelist' and 'Blacklist'	The 'Whitelist' will allow third-party applications onto the device, but it does not disable system apps. 'Signature Whitelist' enables the ability to define a set of android application signatures to the 'Whitelist' on the provisioned device. When the device is provisioned, third-party applications are uninstalled. However, if third-party applications are installed through the MDD, they are automatically allowed. 'Blacklist' will block third-party applications and disable system applications. For simplicity, 'Whitelist' and 'Signature Whitelist' should be enabled and leave the accepted applications list blank, unless there is a use case the 'Blacklist' should be the focus of administrators to deny unrequired system applications. Without this control, unauthorised applications may be installed onto the mobile device and affect the security of the device and network.	Mandatory
Firewall	This control will allow mobile devices to connect to a specified set of Internet Protocol (IP) addresses, hosts or subnets. Enabling the firewall control allows devices to only connect to pre-defined networks.	Mandatory
Auditing	MDD allows administrators to configure the audit logging on the mobile device. Monitoring the logs of the mobile devices will provide administrators additional context regarding unusual or suspicious activity.	Mandatory
Actuations	Actuations allows configuration of mobile devices to perform certain actions when a specified event occurs on the device (e.g. A user enters their password incorrectly 5 consecutive times the phone, actuations can automatically reset the phone to factory defaults).	Organisation decision
Mandatory Apps	The behaviour of mandatory applications (installed or always running) on the device can be adjusted in accordance with operational requirements and threat risk assessments.	Organisation decision
Managed Wi-Fi	Configuration of Wi-Fi SSID 'Whitelist' will allow devices to only connect to known networks.	Mandatory
Password Policy	Configuration of type, history, screen timeout, lifetime, maximum number of failures until wipe, minimum password length, sequential and repeating characters and customisation of the lock screen banner. Refer to the ISM password controls for additional guidance.	Mandatory
Local Admin	Allow Local Administrator on the device. This allows for policy changes on device even after the device has been provisioned. If local admin is disabled, the only way to reprovision device is through a factory reset through the device, QR code or the MDD provisioning portal.	Organisation decision

Operator	Allows for operator mode on the device that can modify a defined subset of the basic policy configurations on the device.	Organisation decision
QR scanner	Reprovision/Modify device profiles without using USB tethered connection. There is a requirement for the client to trust a provisioning station before accepting QR code to modify profile settings.	Recommended
Managed certificates	QR certificate management for devices.	Mandatory if QR scanner is enabled.

MDD – Recommended configuration items

The following outlines the MDD configuration items on mobile devices and the requirement for use at the **PROTECTED** classification. Administrators must include a threat risk assessment matrix for **PROTECTED** and bespoke use cases, and have a complete understanding of the risks associated with their decision around implementing a particular control.

Item	Description and Risk Considerations	Requirement at PROTECTED
New Admins	Enables new device administrator applications.	Organisation decision
Factory Reset	This configuration item will disable a local reset of the device to factory settings. If this setting is enabled and the device under goes factory reset, the device will be unsupervised.	Organisation decision
Android VPN	Allows the VPN to be specified in the device settings. All data communications for the Samsung Galaxy platform handling government data must be through an Always On 'StrongSwan' VPN. The Samsung Galaxy platform offers two versions of VPN client – OpenVPN and StrongSwan. The StrongSwan client is enforced via the kernel and therefore offers a stronger security claim for the VPN tunnel.	Recommended
Audio Recording	Disables applications from using audio recordings. If enabled applications may inadvertently record sensitive conversations.	Organisation decision
Autofill service	Enables the Autofill service application to be used. Similar to a password manager, the device stores user information such as usernames and passwords and then automatically completes forms when asked for them.	Recommended
Backup services	Disables applications from using the Samsung cloud services to back up data from the device. Enabling this service may allow the transfer of sensitive government data to the Samsung cloud service.	Not recommended
Bluetooth	Allows the device to use Bluetooth to connect to other devices and be used to increase location accuracy. If the use case does not require this feature, then this feature should be disabled. This will reduce the attack surface on the device.	Organisation decision
Bluetooth Tethering	Allows the mobile device to share their network connection to other device through Bluetooth connection. If this item is enabled, the network can be exposed to other devices.	Not recommended
Camera	Photos and videos taken with the camera application are stored locally and may be transferred automatically to locations that do not have sufficient protection for sensitive government data.	Organisation decision
Cell Data	Mobile devices can be enabled to use cell data for internet connectivity. The use of the always on StrongSwan VPN is recommended if using GSM cellular data.	Organisation decision

Certificate management	Disable the ability of the user to modify the certificates on the device. If this feature is enabled users will be able to manage the certificates on the device. This includes self-signed certificates.	Organisation decision
Developer mode	Developer mode can be enabled allowing for mobile application development. This configuration item will allow users to access system level controls and should only be used for testing and development.	Not recommended
External Encrypt	Enforces encryption of external storage such as SD cards. If this item is not enabled, external storage can be ejected from the mobile device and contents read on another device.	Mandatory
Google Auto Sync	Enables synchronisation of the data on a mobile device to a google account. This configuration item allows data on a mobile device to be stored and updated on an external server hosted by Google.	Not recommended
Google Backups	The mobile device is backed up with a google account. This configuration item allows data on a mobile device to be stored and updated on an external server hosted by Google.	Not recommended
GPS	This item configuration enables GPS to be used by the mobile device. Information based on the device's physical location is obtained and used by the mobile device and third-party applications for various location-based services.	Organisation decision
Lock Notifications	This will enable notifications to appear while the device is in a locked state. Applications can send notification to the device, which can reveal information and details of applications on the device.	Not recommended
Microphone	Applications requiring the devices microphone can be enabled or disabled. This configuration item provides an additional control on apps and services that are allowed to access the device microphone.	Organisation decision
MMS	Multimedia messaging service can be enabled on the device allowing images, videos or sound clips to be sent and received. Sensitive information can be transmitted through this service without appropriate safeguards in place.	Not recommended
Mock Locations	The location of the physical device can be specified, instead of using the device's actual location. This enabled when developer mode is on. This mode is usually used for testing and development purposes.	Not recommended
Over-The-Air Updates	The mobile device can be enabled to use Over-The-Air (OTA) android updates. This will enable wireless updates of the OS, firmware or application software.	Recommended
SD card	Enables SD cards to be used by the device. If the SD card contains malicious software, it can infect the mobile device. Furthermore, sensitive information can be stored on the SD card and easily transferred to another device. If enabled, the External Encrypt feature must also be enabled.	Organisation decision

Smart Lock	Android can allow the bypass of security locked screen based on constant movement (proximity to user), location, recognised voice or connection to a device.	Not recommended
SMS	Short message service (SMS) allows text messaging to be sent and received from the device.	Organisation decision
Unknown Sources	Disable the installation of APKs from Unknown Sources onto the device. If enabled, APKs from unknown source/s can be installed on to the device. Installing APKs from unknown sources can compromise the mobile device.	Recommended
USB Debugging	Enabled in conjunction with developer mode turned on, this configuration item allows applications to be copied via USB to the device. Applications with malicious code can be transferred to the device. This configuration is primarily used for testing purposes.	Not recommended
USB Host Storage	Allows the mobile device to act as a host for another device through a USB connection (i.e. with an On The Go [OTG] adapter). This configuration allows a mobile device to connect to external peripherals such as a USB storage device.	Not recommended
USB Mass Storage	Through a physical USB connection and enabling this configuration item, external mass storage such as flash drives and USB sticks can be connected to the mobile device. This would enable transfer of information between the device and external storage. This can expose the device to malicious applications or executables, and potentially unauthorised transfer of information.	Not recommended.
USB Tethering	The mobile device can be configured to share network connection to other devices via USB connection. If this configuration is enabled, the mobile device can act as an open gateway to the network.	Not recommended
Video Recording	Videos taken with the camera application are stored locally and may be transferred automatically to locations that do not have sufficient protections for government data.	Organisation decision
WAP Push	Wireless application protocol (WAP) push allows content such as web links to be pushed to the mobile device. Messages containing web links can direct users to untrusted websites, which can present additional risks to the user and the device. If there is a requirement to use this feature, organisations needs to understand and accept the risks. Infrastructure (push proxy gateway) will be required to support this feature.	Organisation decision
Wi-Fi	Enabling this configuration item will enable the mobile device to establish a Wi-Fi connection. System risk owners and administrators will need to assess risks associated with the type of network that the mobile device will be connecting too.	Organisation decision

Wi-Fi Direct	Wi-Fi Direct allows a mobile device to have a direct connection with another device, to transfer and receive data. If the connecting device is not with an organisation supervised device, transferring and receiving of sensitive government data will not have sufficient protection.	Not recommended
Wi-Fi Tethering	Wi-Fi tethering allows mobile device to share mobile data connection with external devices.	Not recommended

Knox – Recommended configuration items

The following table outlines the Knox configuration items available on Knox enabled mobile devices and the requirement for use at the **PROTECTED** classification. Administrators need to perform a formal threat risk assessment and have a complete understanding of the risks associated with their decision around implementing a particular control.

Item	Description and Risk Considerations	Requirement at PROTECTED
Airplane	Forces airplane mode to be on. The user will still be able to disable airplane mode but this will trigger a fault and audit event.	Organisation decision
Android Beam	Enable Android beam, a NFC data transfer.	Not recommended
Block Non-Mil Accounts	Switching this feature off will not block accounts which do not end in '.mil'. If this feature is switched on, only accounts ending in '.mil' are allowed to be accessed by the mobile device. All other accounts are blocked.	Organisation decision
Browser Autofill	Enables login and personal information to be stored and automatically filled into web forms. This will support different complex passwords/passphrases to be used on webpages.	Recommended
Cell Voice	Enabling this feature will allow voice calls to be made. A potential risk is communication of sensitive information.	Recommended
Crash report	Enabling this feature allows crash reports to be generated by the mobile device in the event of an application not responding. If disabled, technical reporting is not provided, making identification of technical errors or potentially malicious applications difficult to determine.	Organisation decision
Fingerprint Unlock	If disabled the mobile device will not be able to be unlocked through fingerprint recognition. Depending on the mobile device, the fingerprint recognition system and the reliability can vary.	Organisation decision
Google Play	Enable the Google play store application to run. Google play is a shop front for Android applications that can be installed onto the mobile device. Unauthorised or potentially malicious applications can be installed onto the device. The 'Whitelist', 'Signature Whitelist' and 'Blacklist' feature can minimise this risk.	Not recommended
Lockscreen Camera	Enable the camera icon to appear on the phone lock screen. If enabled, the camera can be easily used even when the mobile device is in a locked state. This allows sensitive material to be photographed.	Organisation decision
Lockscreen Icons	Icons such as phone will be allowed to appear on the locked screen. This will allow shortcuts to different applications (login will still be required). The associated risk depends on the application. If an application contains sensitive information then displaying the icon on the locked screen can expose the types of applications, and the role of the device, to malicious actors if the device is lost or stolen.	Organisation decision

Multi-user mode	This is applied to tablet devices, if enabled multiple users are able to access a single tablet device. As multiple users are able to access the tablet, users can potentially access sensitive data from other accounts on that tablet device.	Organisation decision
NFC	Enable Near-Field-Communication (NFC) will allow other devices to communicate with the mobile device.	Organisation decision
Samsung beam	Builds on the functionality of the Android beam feature, where content can be shared using NFC and Wi-Fi direct (peer-to-peer Wi-Fi connection). If enabled, peer-to-peer communication can occur between devices. A peer-to-peer connection to other devices, which may be external to the organisation fleet, can present high risk to the device and the network.	Not recommended
Samsung Voice Google Assistant Bixby	Personal voice activated assistant applications carry out the user's command by voice input. These applications may process conversation taking place around the device at any time. Should these applications be used, there is a risk that classified conversations will be transmitted, and the data could then be stored and processed by the voice assistant servers without sufficient protections for classified government data.	Not recommended
Share via list	Enable the 'Share Via' list to appear. If enabled, the user would be able to share sensitive information through different applications with insufficient protection for classified data.	Not recommended
YouTube	Enable the use of the YouTube application. Allows videos to be streamed to the device. User activities can also be monitored and tracked by the application.	Not recommended

MDD Premium – Recommended configuration items

The following table outlines the MDD premium configuration items. It requires a premium Samsung Knox licence. The table displays the requirement for use at the **PROTECTED** classification. Administrators need to perform a formal threat risk assessment and have a complete understanding of the risks associated with their decision around implementing a particular control.

Item	Description and Risk Considerations	Requirement at PROTECTED
Audit Log	Enable Knox audit logging. If disabled, monitoring the device activities will become difficult for error identification and detecting possible security breaches.	Recommended
Auto Touch sensitivity	If enabled the touchscreen sensitivity is enabled, the device is able to automatically adjust the touchscreen's sensitivity.	Organisation decision
Bluetooth low energy	Enables Bluetooth low energy which is used for increased location accuracy and connection to devices. If the use case does not require this feature, then this feature should be disabled. This will reduce the attack surface on the device.	Organisation decision
Certificate revocation	Enable Knox certificate revocation. Without this enabled, certificates will not be validated for against a known list of revoked certificates. This can potentially allow invalid and untrustworthy certificates to be used on the mobile device.	Recommended
LED indicator	Disable the light emitting diode (LED) indicator on the device. The LED indicator is used to indicate the status of the device and for application notifications.	Organisation decision
Online certificate status protocol	The online certificate status protocol (OCSP) is an internet protocol used to obtain the revocation status of certificates. If disabled, the status of revocation certificates will be unknown to the device.	Recommended
Tactical mode	The mobile device is forced into airplane mode. User will not be able to disable airplane mode. If disabled the mobile device is not locked down and able to communicate.	Organisation decision
Wi-Fi scanning	Disables Wi-Fi scanning for increase location accuracy. If enabled, the mobile device will use the Wi-Fi antenna to complement the GPS and mobile tower information to increase the location accuracy of the device.	Organisation decision

Glossary of cybersecurity terms

Term	Meaning
application control	An approach in which only an explicitly defined set of approved applications permitted to execute on systems.
ASD Cryptographic Evaluation	The rigorous investigation, analysis, verification and validation of cryptographic software and equipment by ASD against a stringent security standard.
authorising officer	An executive with the authority to formally accept the security risks associated with the operation of a system and to authorise it to operate.
classification	The categorisation of information or systems according to the business impact level associated with that information or system.
Common Criteria	An international standard for software and IT equipment evaluations.
cryptographic software	Software designed to perform cryptographic functions.
cybersecurity	Measures used to protect systems and information processed, stored or communicated on such systems from compromise of confidentiality, integrity and availability.
cybersecurity incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of systems or information.
data at rest	Information that resides on media or a system.
data in transit	Information communicated across a communication medium.
integrity	The assurance that information has been created, amended or deleted only by authorised individuals.
Internet Protocol Security (IP Sec)	A suite of protocols for secure communications through authentication or encryption of Internet Protocol packets as well as including protocols for cryptographic key establishment.
IT equipment	Any device that can process, store or communicate electronic information.
key management	The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.

media	A generic term for hardware, often portable in nature, which stores information.
mobile device	A portable computing or communications device. For example, a laptop, mobile phone or tablet.
NFC	Near-Field-Communication, a set of communication protocols used between two electronic devices in close proximity.
passphrase	A sequence of words used for authentication.
password	A sequence of characters used for authentication.
patch	A piece of software designed to remedy vulnerabilities, or improve the usability or performance of software and IT equipment.
product	A generic term used to describe software or hardware.
protective marking	An administrative label assigned to information that not only shows the value of the information but also defines the level of protection afforded to it.
Protection Profile	A document that stipulates the security functionality that must be included in Common Criteria evaluation to meet a range of defined threats. Protection Profiles also define the activities to undertaken to assess the security function of an evaluated product.
security risk	Any event that could result in the compromise, loss of integrity or unavailability of information or resources, or deliberate harm to people measured in terms of its likelihood and consequences.
server	A computer that provides services to users or other systems. For example, a file server, email server or database server.
system	A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.
system manager	An individual that the system owner has delegated the day-to-day management and operation of a system.
system owner	The executive responsible for a system.
user	An individual that is authorised to access a system.
Virtual Private Network	A private data network that maintains privacy through a tunnelling protocol and security procedures. VPNs may use encryption to protect traffic.
workstation	A stand-alone or networked single-user computer.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).