
MOTOTRBO ION

# SECURITY IS ON

MOTOTRBO Ion helps you stay safe from cyber threats. A defense-in-depth approach provides multiple layers of security to help prevent unauthorized device access and malicious activity, and to safeguard your critical data. With the highest level of device and network security, combined with real-time threat monitoring, Ion lets you use data and Android apps with confidence — even on public networks.

## DEVICE SECURITY TO PREVENT UNAUTHORIZED ACCESS

MOTOTRBO ION HELPS PREVENT HOSTILE CODE FROM RUNNING ON THE DEVICE AND UNAUTHORIZED USERS GAINING ACCESS.

### TRUSTED EXECUTION ENVIRONMENT (TEE)

A TEE provides end-to-end security by implementing ARM's TrustZone technology and handles critical functions and services. It runs on the same processor as the Android operating system but is completely isolated from the rest of the system. This isolation ensures that critical data is stored, processed and protected in a secure environment.

### TRUSTED FIRMWARE

A secure boot process verifies both firmware and software integrity. With secure boot, each stage of the boot process is cryptographically signed with approved keys, which prevents malicious attacks and unauthorized software updates, providing a safe and secure OS launch.

### THE ANDROID KEYSTORE SYSTEM

The Android Keystore prevents unauthorized use of cryptographic keys. In addition, apps must specify authorized uses of their keys, and enforce these restrictions outside of the apps' processes, providing further restrictions on how and when keys are used.

### DEVICE ACCESS SECURITY

Single- and multi-factor authentication mechanisms are supported on MOTOTRBO Ion — from simple PIN to other authentication factors such as password, pattern, etc. Valid users will have access to only the data, applications and services for which the users are authorized.

### THE NIST CYBERSECURITY FRAMEWORK

All MOTOTRBO systems and devices strictly adhere to the NIST cybersecurity framework.

NIST security practices are based on continuous monitoring, diagnosis, mitigation options and remediation. We use a risk-based approach throughout our entire product development, implementation and operational support life-cycle. Our protection and response-based controls are built in consultation with industry-leading experts, processes and technologies.

For more details on MOTOTRBO systems' security practices as part of the NIST framework, please click here to view.



MOTOROLA SOLUTIONS

# APPLICATION SECURITY TO PREVENT MALICIOUS ACTIVITY

MOTOTRBO ION ENABLES SECURE OPERATION BY HELPING TO PREVENT MALWARE, PHISHING AND OTHER MALICIOUS ACTIVITY.

## MOBILE DEVICE MANAGEMENT AND MANAGED GOOGLE PLAY

Device security policies, including application management, are best implemented using a Mobile Device Management (MDM) solution. IT administrators, who typically are responsible for the configuration and management of these devices, can use an MDM to define and set policies for application use, creating a customized and secure application management framework tailored to their specific needs.

Key to this implementation is the Android Enterprise and the Managed Google Play framework, which provides APIs to MDM vendors to manage apps on Android devices. This applies to both public applications available from the Google Play Store and private applications built for corporate use.

Through MDM's, IT admins can:

- Remotely distribute approved apps through the Managed Google Play Store and block malicious apps or remove apps
- Define and enable/disable app access for users depending on their profile
- Setup real-time notifications on device usage to monitor for malicious activity or non-compliance of security policies

## GOOGLE PLAY PROTECT

Google Play Protect is a powerful threat detection service built into the Google Play Store, that actively scans 24x7 for harmful applications and protects the devices, their data and apps, from malware. Users are notified upon detection of apps containing malware. Google Play Protect may also remove or disable malicious apps automatically as part of its prevention initiative and use the information it gathers to improve the detection of Potentially Harmful Applications (PHAs). In addition, the user can also opt to have unknown apps sent to Google for analysis.

## SAFETYNET

SafetyNet is a set of services and APIs that developers may use to protect apps against security threats and mitigate against device tampering, bad URLs, PHAs and fake users.

## APPLICATION SIGNING

Android requires that all apps be digitally signed with a developer key prior to installation and uses the corresponding certificate to identify the application's author. When the system installs an update to an application, it compares the certificate in the new version with the existing version and only allows the update if the certificate matches.

# DATA SECURITY TO SAFEGUARD CRITICAL DATA

MOTOTRBO ION SAFEGUARDS CRITICAL DATA, AT REST AND IN TRANSIT.


## DATA AT REST SECURITY

### SECURE STORAGE

Credentials, certificates and keys are securely stored in hardware-backed trusted storage on the device.

### CERTIFICATE HANDLING

Certificate authorities are critical for providing secure communications over a network using the public key infrastructure. With Android 7.0 and above, all compatible devices, including MOTOTRBO Ion will implement only the standardized system certificate authorities maintained in AOSP. All Ion devices will ship with the same certificate authority store.

### WORK PROFILE

For company-owned devices, IT administrators can implement one of two deployment options to manage the corporate data on these devices:

- Fully managed device in which the device is used exclusively for work purposes. IT admins can enforce the full range of management policies to the entire device
- Fully managed work profile option, in which the device supports the work profile and a personal profile simultaneously

In the second option, the work profile creates a separate, self-contained profile which holds corporate applications and data and isolates those from personal apps and data. Using MDM, device policies can be configured to prevent sharing of files and data from the work profile.

### DEVICE POLICIES

Device can be configured using MDM to prevent or restrict data transfer to/from the device such as:

- Preventing transfer of files using Bluetooth
- Preventing transfer of files from the device via USB
- Prevent access to external storage such as SD card
- Preventing mounting of physical external media
- Disallowing access to debugging capabilities
- Setting device passcode policies
- Disabling camera
- Disabling screen capture
- Allowing installation of apps from known sources such as the Google Play store

## DATA IN TRANSIT SECURITY

Ion implements the industry-standard secure protocols used for data-in-transit, such as SRTP, HTTPS, etc. Available industry standard protocols and security requirements for connectivity interfaces such as WiFi, USB, BlueTooth and VPN have been implemented. In addition, Android provides secure communications over the Internet for web browsing, email, instant messaging and other Internet apps, by supporting Transport Layer Security (TLS).

### WI-FI

Android 10 supports the Wi-Fi Alliance's Wi-Fi Protected Access version 3 (WPA3) and Wi-Fi Enhanced Open standards, which improve overall Wi-Fi security by providing better privacy and robustness against known attacks.

### VPN

Android supports securely connecting to an enterprise network using VPN.

# ADDITIONAL SECURITY MEASURES

## ANDROID SECURITY UPDATES

Every month, Google publishes Android Security Bulletins to update users, partners and customers on the latest fixes. These security updates are available for Android versions for three years from the date of release.

## ANDROID ENTERPRISE RECOMMENDED PROGRAM

The Android Enterprise Recommended program from Google provides a set of specifications for enterprise devices and services for hardware performance, deployment, security updates and user experience. These include security updates that are delivered to devices within 90 days of release from Google. In addition, OEMs receive an enhanced level of technical support and training.

## INDUSTRY STANDARDS AND CERTIFICATIONS

Android Enterprise has received ISO 27001 certification and SOC 2 and 3 reports for information security practices and procedures for Android Management API, zero-touch enrollment and managed Google Play. This designation ensures these services meet strict industry standards for security and privacy.

Certifications include:

- FIPS 140-2 CAVP
- Common Criteria/NIAP Mobile Device Fundamentals Protection Profile
- DISA Security Technical Implementation Guide (STIG)
- General Data Protection Regulation (GDPR)


MOTOTRBO ION

For more information, please visit
**motorolasolutions.com/ion**



Triangle Communications SC
SECURITY & COMMUNICATIONS
Helping you prepare for critical moments

www.trianglesc.com

940 West Main Street
New Holland, PA 17557
717.656.2211

99 15th Street
New Cumberland, PA 17070
717.774.7455