BlueFletch
ENTERPRISE
MOBILE
SECURITY

Android Security Solutions for Government Agencies

Increasingly, government agencies are deploying enterprise-grade Android smartphones and tablets to enable their workforce to complete critical tasks and better serve civilians.

As more and more functionality continues to move onto these dedicated Android devices, it's crucial that Federal agencies have a comprehensive mobile security strategy in place. Solely relying on mobile policies and managment solutions like EMM/MDM is no longer enough to protect government-issued devices and sensitive data.

Secure Login & Authentication | **Identify Device Threats** | **Mobile Threat Prevention**

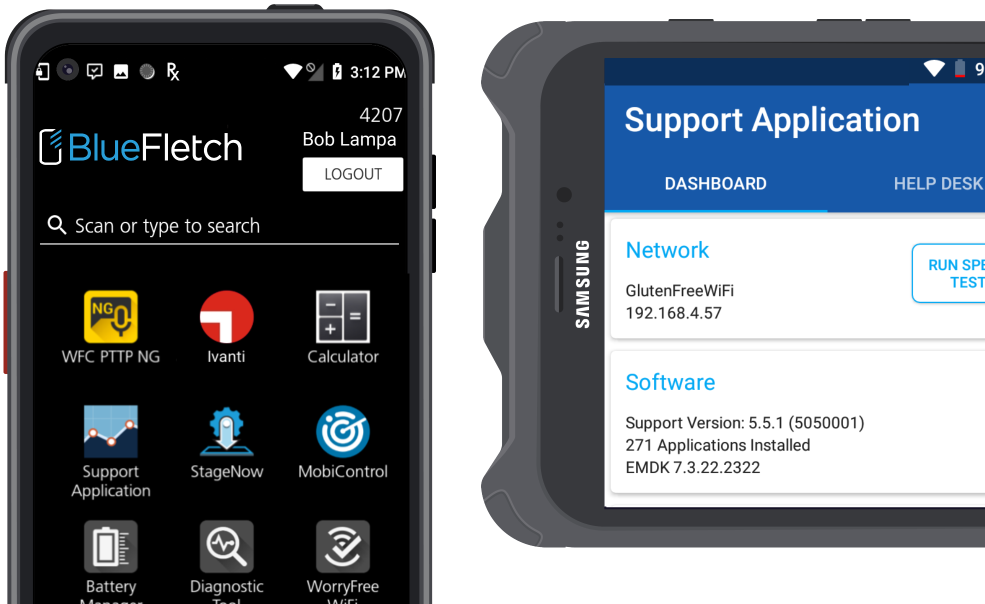
BlueFletch Enterprise Mobile Security (EMS) is a software toolset that helps secure government-owned Android devices while empowering the federal workforce to become more productive.

All product features are included in the EMS offering and the cost is based on an annual per-device licsense. Setup consulting, custom plugin development, and ongoing support is included.

Device and OS Support

EMS supports Android 5.0 and above and functions on rugged and consumer Android devices.

Additional EMS Resources:
bluefletch.com/ems



4207
Bob Lampa

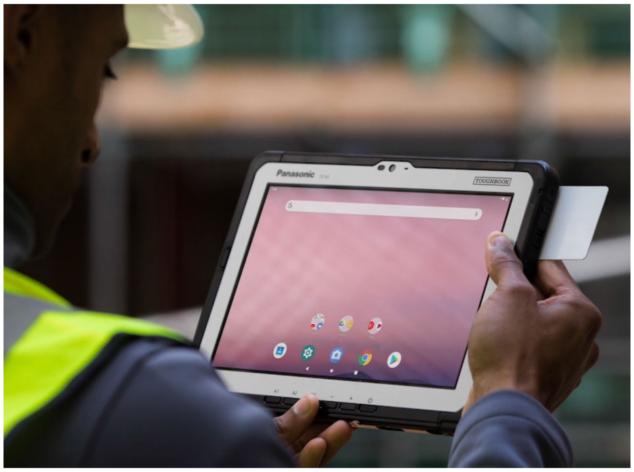
GlutenFreeWiFi
192.168.4.57

Support Version: 5.5.1 (5050001)
271 Applications Installed
EMDK 7.3.22.2322

Use Case:

Default Android Launchers offer limited security control for shared government devices

1 out of 3 government agencies have devices without a passcode or lock screen enabled, which poses a huge security risk. Default launchers that come with your newly purchased rugged Android devices aren't designed for shared-user scenarios. They offer minimal security control and functionality needed to lockdown devices and protect sensitive data.



Solution:

BlueFletch Launcher with custom security and lockdown controls

The BlueFletch Launcher was designed to provide security features government IT teams need to safeguard data and secure Android device fleets - without impeding employees' productivity and increasing support costs. Our launcher is more than a kiosk; it's a highly customizable and secure home screen that provides a single sign-on login experience for employees.

☑

Display apps based on the user's permission level and control access to settings to prevent misuse

☑

Automatically uninstall foreign apps that aren't whitelisted

Clear running apps and cached data upon logout

☑

Configure custom logout rules such as session timeouts, no device motion, or device cradled

Additional EMS Resources:
bluefletch.com/ems

Use Case:

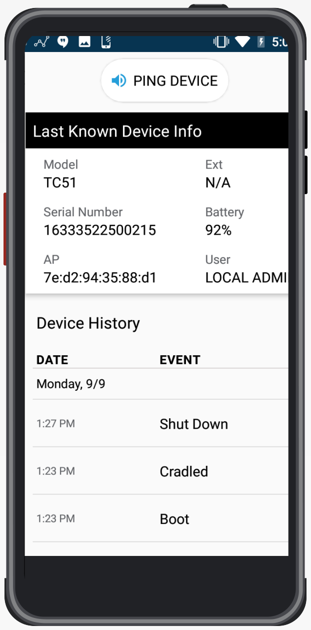
Asset management and visibility

IT and security resources for government agencies often lack real-time visibility of their device fleets. Not knowing a device’s whereabouts, health, last known user, network, and software information makes it difficult for teams to securely manage and support their rugged Android devices in the field.

Solution:

BlueFletch Support Agent for total device, user, and data awareness

The BlueFletch EMS toolset empowers government IT teams with complete visibility of their device fleet in real-time. EMS can be implemented to any Android device running 5.0 and above, so it is the optimal solution for gaining actionable data across your mixed device fleet and environment.

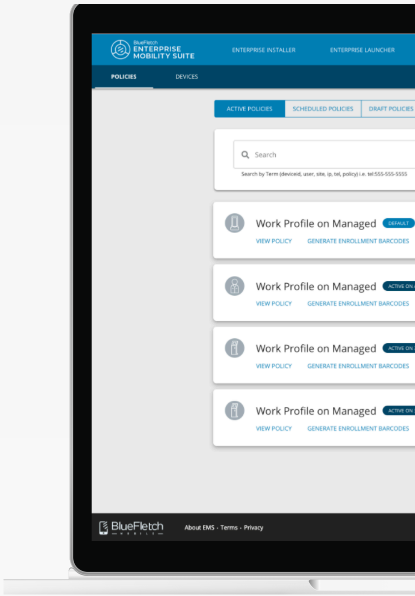


Last Known Device Info

Model TC51	Ext N/A
Serial Number 16333522500215	Battery 92%
AP 7e:d2:94:35:88:d1	User LOCAL ADMI

Device History

DATE	EVENT
Monday, 9/9	
1:27 PM	Shut Down
1:23 PM	Cradled
1:23 PM	Boot



Search by Term (deviceid, user, site, ip, tel, policy) i.e. tel:555-555-5555

Work Profile on Managed

Work Profile on Managed

Work Profile on Managed

Work Profile on Managed

☑ Use Check-Out and Check-In data to know which frontline employees currently have what device and when they last used them

☑ View devices’ remaining battery campacity to proactively order battery replacements before you’re down a device in the field

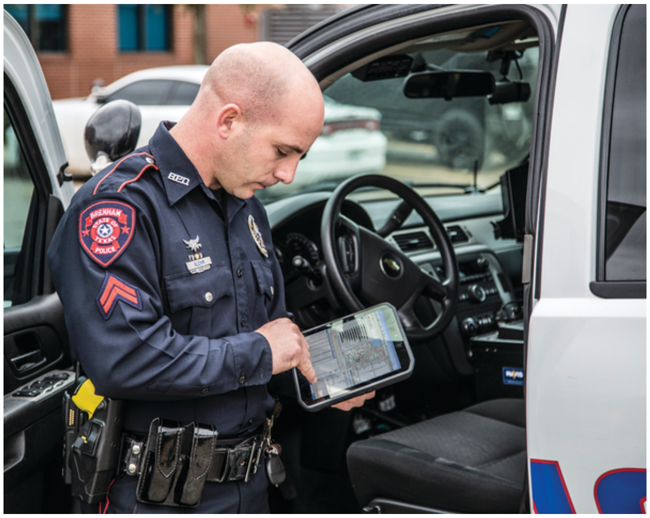
☑ Use the Device Finder and GPS integrations to verify the location of your rugged Android devices for accurate inventory tracking

Additional EMS Resources:
bluefletch.com/ems

Use Case:

Governmenet workers need quick access to their apps

Government employees use many apps at work and they need a distinct password for each. This actually puts organizations at risk because users are reluctant to create multiple complex passwords and instead adopt bad password habits, like using the same password across all their apps. Given that 80% of hacking-related breaches are due to weak or stolen credentials, government agencies need to ensure their employee login and authentication process is secure.



Solution:

BlueFletch Launcher with Single Sign-On

BlueFletch Launcher offers a fast and frictionless login process by using single sign-on to securely authenticate users and give them immediate access to the business apps tied to their role or permission level. With BlueFletch's single sign-on support for any mobile, web, legacy, or third-party application, the government workforce can spend less time fumbling with passwords and more time tending to civilians and carrying out critical tasks.

☑

Integrate with your existing Identity Provider to secure app access in a way that works best for your business

☑

Streamline the login experience for your workforce, providing immediate and secure access to all their business apps

☑

Reduce authentication time from 30 seconds to less than a second, potentially saving minutes each day for field workers

Additional EMS Resources:
bluefletch.com/ems