Mobile Shared Device Management Report

Mobility Public Safety

Mobile Device Provisioning & Management

Produced For: Department of Homeland Security (DHS)
Science & Technology Directorate (S&T)

Date Published: August 26, 2019

Prepared by: Mobility 4 Public Safety

Principle Author: Niki Papazoglakis

Contributing Authors: Michael Jumonville, Mobility 4 Public Safety
Sam Miller, Texas Division of Emergency Management

Please send comments to: Niki Papazoglakis
Principal
Mobility 4 Public Safety
1307 Waugh Dr #787
Houston, TX 77019
Phone: 346-291-5575
Email: niki@mobility4ps.com

Other Contributors and Agency Points of Contact

Name	Title	Agency
Brian Cantrell	Chief	Waller County Fire Marshal's Office - Office of Homeland Security and Emergency Management
Chris Collier	Emergency Service and Response Manager	Southeast Texas Regional Advisory Council (SETRAC)
Zachery Glover	Systems Support Analyst	Texas Division of Emergency Management (TDEM)
Sam Miller	CIS FieldOps Manager	Texas Division of Emergency Management (TDEM)
Jeff Newbold	State Coordinator, Critical Information Systems	Texas Division of Emergency Management (TDEM)
Colin Rizzo	Emergency Manager	Port of Houston Authority

Table of Contents

Executive Summary

As the public safety community adopts mobile broadband, departments are already beginning to purchase larger quantities of department issued cell phones. Some departments are issuing phones to individual users, while others are deploying caches of shared phones due to the cost constraints of providing all users individually assigned phones.

As in the early days of Personal Computers (PC), cell phones are currently designed predominantly around individual, consumer use. The tools and processes for provisioning and managing mobile phones are fundamentally different than those employed for other mobile assets such as laptop computers and radios. Information Technology (IT) and Communications personnel will need to employ new tools for deploying and managing large quantities of phones - whether individually issued or shared across personnel. The implications of these new technologies and methods should be considered by department executives when making decisions about the pace and scale of mobility adoption.

Smartphone Management Compared to Other Mobile Assets

Most enterprises today, particularly in government and public safety, deploy laptops and Mobile Data Terminals (MDTs) running the Operating System (OS) Microsoft Windows. Over the decades, Windows has evolved beyond supporting local hardware on a PC to supporting complex networked computers that allow the sharing of hardware with users across the enterprise. This evolution has been enabled by the deployment of a full ecosystem of tools that centralize user management, control access to hardware and information inside secure networks, and support the migration and/or replication of data from local storage on a PC to networked infrastructure accessible from most enterprise-connected devices.

IT departments build images with the necessary software packages, network settings, security tools and other customizations required by the organization. They use automation tools to quickly load the pre-configured image onto new PCs/laptops. Most updates are then pushed remotely over the network without manual configuration by a desktop support technician. User profiles and information are managed at the enterprise level, so an individual's credentials can be used on just about any networked PC in the organization to access their personal files.

Radios are programmed in a similar manner. Templates are built with designated channels and hardware settings which are then easily installed on large quantities of radios using automation tools. Unlike PCs and phones, radios do not require unique user credentials. Users have access to the channels programmed onto the radio. For deployments of shared/cached radios, channels are pre-configured into the radios. Often, instructions are provided to users for which channels to use for which type of communication or group to communicate with.

Mobile platforms such as smartphones and tablets are a relatively new technology and still in the early stages of maturity. While there are a number of hardware manufacturers, the mobile device market is dominated by two OS platforms: iOS and Android. Early use of mobile devices was predominantly personal. Private industry began operationalizing mobility technologies shortly after the launch of the Smartphone. And over the last decade, tools for automation and remote security have evolved. But the overall market is still rather immature for enterprise deployments, particularly for shared devices.

Project Overview

The public sector in general, and especially the public safety vertical, have only recently begun to operationalize these mobile technologies. This adoption is being fueled by the availability of reliable, mobile broadband networks. There are three models for enterprise mobile device deployments:

1) Individually issued devices funded and managed by the organization
2) Cache devices funded and managed by the organization and shared across users
3) Bring Your Own Device (BYOD) in which organizations allow personnel to use their personal device for work purposes which may or may not include some sort of stipend

Most organizations have systems and procedures in place for managing individually issued department devices. The BYOD model relies on department policies but leaves device acquisition, provisioning, and management to individual users with little or no burden on department resources. This assessment focuses on the management of shared devices. The shared device model offers reduced financial burden from individually issuing devices and improved security over BYOD; however, it brings with it the most challenges and complexities.

One objective of the Mobility Acceleration Coalition (MAC) is to explore methods for streamlining the management of device caches to enhance scalability for the public safety industry. The MAC sought to evaluate existing technologies and procedures, identify gaps and document current best practices in order to:

1. Provide feedback to industry partners to build and/or enhance tools available to automate shared device management and enhance the affordability and scalability for public safety
2. Document lessons learned from tools and processes tested to help public safety agencies accelerate mobility adoption

The lessons learned in this report were derived from a combination of:

1. Multiple shared device deployments for pre-planned events
2. Interviews with other departments managing large caches of phones
3. A tabletop exercise to compare tools and procedures

Device Provisioning

In order for phones to be useful, they must be provisioned with the necessary apps and settings. This is true whether the use is personal or business. For personal use, users must install their apps of choice for messaging, shopping, social media, banking, games, photo editing and a whole host of other uses. This process has evolved in recent years with cloud-based back-ups which allow for automating many of the previously manual tasks associated with configuring a new phone.

The technology is continuing to evolve for the management of mobile devices used for business purposes. Provisioning phones includes 1) configuring device settings 2) installing applications and 3) logging into apps. Individuals use personal preferences to configure device settings, install the apps they want, and use personal credentials for each app they acquire. Organizations typically have security policies such as requiring a PIN to unlock the phone, set sleep and lock times, and possibly even prevent the use of open Wi-Fi networks. Organizations also typically control app usage by whitelisting (allowing only “approved” apps to be installed) or blacklisting (blocking the installation of “unauthorized” apps). These policies are enforced through tools known as Mobile Device Managers (MDM) or Unified Endpoint Managers (UEM). This section will outline the tasks associated with each of the three models employed by the MAC.

The physical tasks of unboxing, labeling, and powering on/off phones are the same across all methods of provisioning. When managing large volumes of mobile devices - workspace, charging infrastructure, transportability, storage, and network bandwidth all significantly impact efficiency. Examples of ways to improve efficiencies include:

1. Multi-unit charging banks
2. Multi-unit transport cases
3. Augmented bandwidth at provisioning facility
4. Batch label making

Manual

A cache of Sonim XP8s was utilized for the 2019 Chevron Houston Marathon. Due to delays for procuring the MAC devices associated with the federal government shutdown, FirstNet built by AT&T loaned us the necessary phones to conduct this planned deployment. The phones were brand new and in their original state, other than having the FirstNet SIMs pre-installed.

The tasks and associated times were logged for a sample of 15 phones to determine the average time to manually provision devices. It is important to note that provisioning activities can vary significantly based on factors such as:

- Hardware
- SIM: pre-installed or requires installation
- OS and version

- Network connectivity - app installation times can vary significantly
- Number of apps being installed
- Accessibility of apps - available in public app stores or acquired through another manner
- User proficiency with device and applications
- Type of labels/label maker (if used)

For the 2019 Houston Marathon, device assignments and app account creation were completed prior to the start of device provisioning and not included in this assessment. Depending on the complexity of the deployment, these activities can be quite time-consuming.

As demonstrated in the table below, the provisioning of 15 devices with 2 mobile apps took 3 hours and 27 minutes with an average of 14 minutes per device.

Step	Task	Start Time	End Time	Total Time	Time / Phone
1	Power on phone and attach inventory label	9:15	9:40	0:25	0:01
2	Update AT&T software and reboot phones	9:40	9:59	0:19	0:01
3	Add device assignment labels	9:47	10:02	0:15	0:01
4	Login to Google Play	10:03	10:30	0:27	0:01
5	Install collaboration app	10:31	10:38	0:07	0:00
6	Install Situational Awareness (S/A) app	10:40	11:03	0:23	0:01
7	Login S/A app and set user icons	11:04	11:20	0:16	0:01
8	Move app icons to home screen	11:22	11:33	0:11	0:00
9	Login collaboration App	1:35	1:45	0:10	0:00
10	Clean-up Collaboration timelines	1:45	2:14	0:29	0:01
11	Create channels in Situational Awareness app	2:14	2:29	0:15	0:01
12	Set phone security settings (PIN, Lock screen & Sleep)	2:30	2:35	0:05	0:00
13	Remove Gmail account	2:35	2:40	0:05	0:00
	Total			**3:27**	**0:14**

FirstNet Built by AT&T provided 100 loaner Sonim XP8s for the Los Angeles Marathon. Every phone has a unique identifier called an International Mobile Equipment Identifier (IMEI). FirstNet Built by AT&T requires that the SIM card be tied to the IMEI of the specific device in order to activate public safety priority and preemption. Due to the delay in the purchasing approval process, the loaners were provided just days before the event. With such short notice, the phones were shipped with the SIMs not installed. The process of matching the SIM to each individual phone was incredibly time-consuming. Once the SIMs were matched to the correct phones, they then had to be installed. The overall process added approximately 14 hours, or roughly 8.4 minutes per phone, to the provisioning process.

Manufacturer's Provisioning Tool

Some manufacturers offer provisioning tools to aid in inventory management and automate some device provisioning activities. MAC members tested the provisioning tool, Sonim SCOUT, for a jail communications pilot. The findings below are not an exact comparison against the manual provisioning process. Due to the secure nature of the jail environment, the key feature was the use of the Kiosk Mode which restricts what users are able to access on the device. The time to develop and test the Kiosk configuration inside of Sonim SCOUT was not measured.

The table below outlines the tasks required for provisioning devices utilizing Sonim SCOUT.

Step	Task
1	Power on phone and attach inventory label
2	Update software and reboot phones
3	Add device assignment labels
4	Scan Sonim SCOUT QR Code
5	Sonim SCOUT tool automatically installed apps & configured phone settings
6	Login App(s)

Utilizing a manufacturer's tool allows some settings to be provisioned automatically that most third-party tools cannot or often do not support such as setting the device PIN. It is estimated that the use of Sonim SCOUT reduced the time for provisioning by 75-80% over manual provisioning (excluding the time to create and test the Kiosk profile). The biggest limitation of the tool was the network bandwidth to provision numerous devices simultaneously.

As a provisioning tool, it is designed to assist in initial device configuration rather than full device management. Over-the-Air (OTA) update capabilities are limited, so updates typically require each device to be physically touched. Updates can be done very easily by creating a new QR code for individual changes such as adding a new application or the entire profile can be updated through a single QR scan.

The SCOUT kiosk mode provides more flexibility in managing what device settings can be accessed while in kiosk mode. Administrators can block Settings altogether or manage which settings can be adjusted from kiosk mode. One advantage of the SCOUT tool is the ability to securely set fingerprints within kiosk mode without having to completely exit kiosk mode.

Mobile Device Manager / Unified Endpoint Manager

The use of an MDM or UEM is important for automation, security and inventory management. The MAC used MobileIron as the UEM to provision and manage the majority of devices acquired for this project. We also conducted interviews with the Texas Division of Emergency (TDEM)

followed by a tabletop exercise to compare tools and processes to document best practices for managing device caches.

The MAC acquired 200 Sonim devices. By utilizing MobileIron, the provisioning process was very similar to the process used with Sonim SCOUT. The major difference is that devices are populated in the Sonim SCOUT portal through importing a CSV file. Devices are automatically registered in the MobileIron portal once the username and password are entered and the device contacts the MobileIron server through the MobileIron Go app.

As with the jail deployment, kiosk mode was used for the LA Marathon and other MAC deployments. The kiosk profile was built prior to device provisioning. Below is the list of tasks for device provisioning with MobileIron.

Step	Task
1	Power on phone and attach inventory label
2	Tap screen 6 times to exit “Setup” mode and open the QR scanner
3	Scan the QR code to install MobileIron Go
4	Enter MobileIron username / password
5	Set device PIN
6	MobileIron auto-configured phone
6	Add device assignment labels
7	Login App(s)

One significant advantage of UEMs is the ability to support OTA updates. The apps deployed differed across events and user groups. For example, a survey app was utilized by fire/medical personnel during the LA Marathon to track patient contacts. Law enforcement did not use this app. Therefore, we utilized two kiosk profiles with the survey app being included in the fire/medical profile but not law enforcement.

As the devices were used for different deployments, the kiosk profiles were updated in the admin portal and changes were pushed automatically to specific devices.

Verizon Wireless provided 100 of the loaner Sonim devices for the LA Marathon. At the end of the event, the phones were required to be factory reset prior to returning them to Verizon. The process was incredibly simple using MobileIron. The Verizon phones were filtered in the MobileIron portal and a bulk “Wipe” command was sent. As each phone was powered on, it would begin the factory reset process immediately upon connecting to the network. Once the factory reset process was complete, phones were powered down and put back into their assigned bag for shipping.

TDEM manages a cache of approximately 7,500 iPhones for disaster response around the entire state of Texas. Over the past several years, TDEM personnel have acquired tools and developed sophisticated processes for device management. Unlike MAC deployments for pre-planned events and daily operations with dedicated support personnel, TDEM deployments are typically in support of no-notice events around the entire state. TDEM devices are generally deployed for single application use such as evacuation tracking, Push-To-Talk (PTT), personnel tracking, damage assessments, etc.

TDEM uses the MDM Airwatch to provision and manage their cache of phones. Due to the dynamic nature of TDEM deployments, their basic configuration provides an Airwatch App Catalog containing approved apps that end-users can install based on operational requirements.

Other General Provisioning Considerations

Network Connectivity

The single biggest limitation to provisioning phones is network bandwidth. TDEM has expedited this process by caching data locally on an Apple laptop and connecting the phones via a USB cable. This wired provisioning significantly improves download and update speeds. If network bandwidth cannot be optimized, staff must be increased as the device number increases to get them provisioned quickly enough.

The location of device provisioning is important. If a strong commercial LTE signal is available and devices have cellular service activated, provisioning can be done directly over the carrier network using any of the methods of device provisioning outlined above. If commercial signal is poor or the devices do not have active service, they must be put on a Wi-Fi network if wired provisioning is not supported. The number of devices that can be provisioned simultaneously depends on the available bandwidth. TDEM has built a robust Wi-Fi network at its headquarters facility dedicated to the provisioning of cached phones. This augmented infrastructure has reduced the overall time and manpower required for device management.

Automation

Provisioning mobile devices involves significantly more manual tasks than provisioning computers or radios. Having tools that allow the device to be plugged into a powered USB hub on a computer allows auto-population of things that must be entered multiple times such as MDM credentials, Wi-Fi network information, etc.

Another mechanism for automating manual device management tasks is through the use of QR or barcode scanning for items that must be done manually on each phone. Tasks such as connecting to Wi-Fi, setting a device PIN, and entering credentials can be significantly expedited through the use of QR/barcode scanning.

Charging

Ensuring devices stay charged is important for provisioning and deployment. Multi-port charging banks, cables, and power strips should be acquired to support the number of devices being managed. For longer-term deployments, charging cables should be sent with the device. Having a second set of power cables that can be permanently installed at a central provisioning facility can reduce the time for unpacking and plugging/unplugging cables. While this may seem trivial, it can become quite time consuming when managing large quantities of mobile devices. Some manufacturers such as Sonim provide multi-bay charging banks similar to radio charging banks. In lieu of this, multi-port USB charging banks and extra cables can be used. It is important to estimate the amount of power required to charge the types of devices being managed and to factor that into the type of charging banks purchased as well as the number and type of power strips/surge protectors used.

Device Management

Inventory management for shared mobile devices is in some ways similar to shared radios; however, there are distinct differences.

Service

Radios are privately owned and operate on dedicated networks. Most mobile devices require active cellular service unless exclusively used in dedicated facilities operating on a local wireless network. Commercial carriers offer different types of plans for public safety agencies that allow for service to be activated for periods of deployment and then deactivated or suspended between operations. Service is activated/deactivated through an administrative portal. Processes must be developed to support rapid service activation of designated devices, especially for no-notice events.

Asset Management

Mobile devices are identified through IMEIs and/or phone numbers. Most organizations utilize internal asset management systems to track equipment inventory. Tracking the issuance of laptops, radios and other mobile equipment is typically done by assigning a user in the organization's directory to the asset in the asset management system. To date, the majority of public safety deployments of cached phones support temporarily assigned phones to users across different agencies for different operations. Traditional asset management systems and processes do not support this type of deployment model.

Below is an overview of multiple inventory tracking methods employed for mobile devices:

1) **Spreadsheet** - the least sophisticated method of tracking inventory is to have a spreadsheet with a list of each device. Columns can then be added to track the individual, agency and contact information of device assignments. This method is highly manual and

prone to mistakes. When doing large deployments with multiple support personnel issuing phones, using a cloud-hosted spreadsheet that each team member can update simultaneously has proven to be easier to keep accurate and updated than individual, locally stored files that require version control and reconciliation.

2) **Manufacturer tool** - Our only experience is with Sonim CLOUD. This tool allows you to import a list of devices and assign them to groups and/or users. If adequately maintained and kept up to date, the tool provides a database that is searchable.
3) **MDM/UEM** -

   Airwatch requires an Active Directory account, so TDEM created a generic Active Directory account which is tied to a single Airwatch account used for all shared phones. Since all devices use one generic account, Airwatch uses the phone # or IMEI to identify individual devices.

   MobileIron can be deployed with or without an Active Directory account. If using an enterprise version of MobileIron which requires an AD account, one method employed was to create generic AD service accounts for each device. In this model, we created service accounts with the format LTExxxxx with the x's representing the last five numbers of the IMEI.

   Alternatively, the cache of phones managed by the MAC were not tied to Active Directory. Each device was assigned a MAC inventory number which was assigned to the phones in MobileIron.

Labeling

When dealing with large quantities of devices, it is important to have an inventory label where it can be easily identified. Some departments put the inventory label with return contact information on the inside of the battery cover. This model can work for individually issued devices; however, when provisioning phones for shared deployments, it is important to have a label visible from the outside identifying the specific phone - either an assigned inventory number, phone number or reference to the IMEI (i.e. LTE-XXXXX with the last 5 digits). After multiple deployments, we have found that a straight-forward, consecutive numbering system is much easier for locating and provisioning large quantities of phones than utilizing IMEI or phone numbers which are longer strings of numbers and not consecutively numbered.

When transporting phones in pelican cases with foam cutouts, labels on printer sheets do not seem to adhere as well as the label tape. Printing sheets of labels is much quicker and easier than printing on commercial label maker machines.

Finally, the type, size, color, and placement of labels should be considered with a small group of test phones before labeling large quantities of devices.

Device Updates

When managing cached phones, there are often gaps between deployments. During that time, there are often updates to firmware, operating systems, and apps. TDEM has implemented a process where cache phones are turned on and updated once per quarter. Based on the size of Texas and the time to get phones distributed to no-notice events, TDEM changed the model of storage from all centrally stored in San Antonio to being distributed around the state. Phones are assigned to a local "Device Manager" from a particular organization. That person is responsible for following the TDEM device management guidelines. This process also ensures that batteries and overall device health are verified quarterly to ensure they are in good condition and can be rolled out quickly for no-notice events.

User Assignments

When sharing devices, it is important to know who will need to be assigned a device. This process varies significantly based on operational requirements. In general, there are 3 operational contexts for device sharing:

1) Pre-planned events
2) Daily operations
3) Incident response

Hardware, apps, automation tools, and department policies and procedures can differ widely throughout the industry, so this report will provide example use cases for assigning shared devices under each of the 3 operational models listed above. These examples are intended to provide general guidance for considerations in developing shared device programs, but each deployment must take into account the specifics associated with the hardware, apps, automation tools, staffing/support resource availability, and department policies and procedures to ensure a successful mobility deployment.

Special Event Device Assignments

Pre-planned events have the advantage of knowing resource requirements in advance of the operational period. By working with event planners, device users should be identified during the planning process based on the Concept of Operations (ConOp) for how mobility technologies will be utilized and assigned based on the Event Action Plan (EAP). The operational requirements of the event should drive the type of devices and apps utilized as well as which resources should be assigned devices. In many cases, the individual person may not be known until shortly before the event, but the number and types of resources should be known in advance.

The device assignment models for the MAC deployments during the 2019 Chevron Houston Marathon and Sketchers Los Angeles Marathon are the basis for this assessment. Tasks included:

1. Identify resources
2. Confirm quantity of devices required
3. Validate apps used by user group

For large special events, users are often identified by resource or post rather than the individual name or ID number. This is useful in being able to pre-assign devices and allow for staffing changes without impacting device provisioning activities. Device assignments can be managed electronically through an asset management tool or spreadsheet.

Labeling devices is critical to the successful deployment and management of pre-assigned devices. Unlike radios, app credentials are unique to the user and are typically logged in prior to device distribution. More details will be provided later in this report on the use of app credentials for resources (as opposed to individual users). In addition to the standard inventory label, shared device deployments typically require a user label identifying the resource it is assigned.

Daily Operations

Shared devices for daily operations can vary significantly based on operational requirements. The two examples provided include a jail communications pilot at the Harris County Sheriff's Office (HCSO) and "Connected Cop" deployment with the Inglewood Police Department.

Jail Pilot

The jail deployment represented a challenging operational environment to support shared devices due to the current state of technology. One requirement based on the secure nature of the facility was to use fingerprints to unlock the device and only allow supervisors to know the unlock PIN in the event a device reboot is required. It also posed a challenge for creating user accounts. Due to scheduling complexities and staff shortages for such a large facility, personnel often move around to different posts. The ConOp was designed around knowing the position that you needed to reach as opposed to the individual person (i.e. 3rd Floor Control Center or Pod 5A). Devices were assigned to each designated post.

Connected Cop

Another pilot under the MAC was to test the feasibility of replacing the Mobile Data Computer (MDC) in the police cruisers at Inglewood Police Department (IPD) with a smartphone which would wirelessly cast information from the phone worn on the officer's body onto a "dummy" tablet mounted to the dashboard with a swivel keyboard installed on the passenger side to allow the keyboard real estate of a computer when officers needed to write reports or do more typing than simple queries from the touchscreen.

IPD had a more straight-forward device assignment model due to the consistent nature of their staffing. Prior to the launch of the Connected Cop pilot, IPD had restructured its staffing to have 4 officers assigned to each patrol vehicle - one from each of their 4 shifts. Given the predictability of users, devices were assigned to the cruiser and the fingerprints of the 4 officers were pre-provisioned into the phones by the IPD Administrator.

No-Notice Events

To support the diverse requirements of different types of "No-Notice Events", TDEM utilizes an app catalog or pre-approved mobile apps that can be downloaded when the phones are assigned to the users. Each operation typically uses 1-2 apps, so users are provided instructions with the phone packet on how to download from the Airwatch app catalog.

The cache of phones is distributed around the state for rapid deployment. Incident commanders and communications personnel determine device assignments.

User App Credentials

One of the most challenging aspects of deploying mobile apps is the creation of secure app accounts and assignment of user credentials. Integrating app credentials to a department's directory and utilizing Single Sign-On (SSO) is the most straightforward method of managing user credentials. Public safety mobile app adoption is still in its infancy, so very few departments have the tools available to support SSO. Multi-organizational deployments pose a greater challenge when supporting users from different organizations who all have separate organizational directories.

The methods and technologies for managing and securing user credentials, particularly across organizations and apps, is a broad and complex topic that is rooted in Identity, Credential, and Access Management (ICAM). This report will address the current processes for issuing app credentials in shared device deployments. Additional information on this subject can be found in various mobile ICAM publications including the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) Special Publication 1800-13 Mobile Application Single Sign-On: Improving Authentication for Public Safety-First Responders[1].

In most public safety operations, there are users who need to be identified by name such as Incident Commanders, Supervisors and other special detail personnel. Other users need to be identified by the position/post they fill or resource ID.

Individual

Individually-assigned accounts typically utilize a person's email address or some other unique username with a private password. The user is identified in the application by name or callsign indicating their rank and/or position in the event/incident.

Shared

Other users need to be identified by 1) the post they are filling such as "Gate 6" or "Hazmat Team 1" or 2) the resource type such as Quick Response Vehicle (QRV) - QRV3. In large-scale operations,

[1] https://www.nccoe.nist.gov/publication/1800-13/

many members may not know the person staffing each particular post or resource type. In these situations, they need to be able to find the person in a particular location or with particular skills and/or equipment such as Advanced Life Support (ALS) versus Basic Life Support (BLS). In these cases, user accounts are created based on the post or resource. Shared devices are pre-configured with the apps necessary for the operation and apps are often pre-logged in. The management of who was actually issued the device at a particular time is managed through the device distribution process described below.

Device Distribution & Collection

Distribution & Collection

Shared devices must be distributed/collected in different ways for different types of operations. Below are some examples of the different models which can be considered during implementation planning.

Pre-planned events - the size, footprint, and duration of events will impact the distribution strategy.

1. For smaller events with a single roll call location, administrators or other operational personnel assigned to distributing devices can stage equipment at the roll call/staging location in a manner similar to radio distribution. The only difference is that phones must be assigned based on the post or user it is configured for as opposed to just keeping a log of which person took possession of which device #.
2. Larger events, especially that span multiple days and/or have multiple staging locations, typically work better by having an individual assigned by the department to be responsible for distributing, charging, and collecting a pre-assigned cache of devices at the end of each shift and returning them at the conclusion of the operation.
3. Larger events with pre-defined staging and demobilization areas can incorporate distribution and collection activities at these specified locations.

Daily Operations - the operational environment again impacts the best management and accountability of shared devices.

1. For operations in fixed facilities such as a jail, having a secure, permanent location with ample charging banks and space for distribution/collection at shift change is necessary. Defining roles for administering the checking out and in of devices is important. This is typically a supervisor or their designee.
2. For mobile deployments like in patrol vehicles, assigning the phone to a particular unit and coupling it with a Mobile Data Computer (MDC) can improve accountability versus having officers pick them up from a central location during or after roll call. This can also

assist when using Bluetooth devices such as mobile fingerprint scanners to ensure that paired equipment stays together.

Incident Response - deploying large numbers of phones during a no-notice event presents additional challenges and requires more sophisticated processes and tools for rapid deployment and distributed collection. TDEM has distributed its cache of phones in strategic locations throughout the State of Texas assigned to Device Managers in various state and local agencies. These phones are issued as-needed in a kit that includes the original box with charging accessories, including an AC adapter, and a pre-paid FedEx return envelope. At the end of a operation, responders simply package the phone with all accessories into the FedEx envelope and drop-off at any nearby location.

User Check Out/In

Several asset management systems were evaluated to find a low-cost, stand-alone, out-of-the-box inventory management system to support the check-out/in process for shared phones across different organizations. No viable platform was identified in time for the exercises and deployments conducted under this program. The primary limitations were:

1. Lack of enterprise asset management system for multi-jurisdictional users across multiple directories
2. Cost
3. Ease of use

Prior to the 2019 LAM deployment, device distribution was managed through spreadsheets and/or paper logs. This method of check out/in is not scalable and prone to errors. While exploring automated solutions for managing device check out/in, M4PS contacted TDEM on their lessons learned from managing thousands of phones across the State. Due to limitations of funding to procure a solution and technical skills to build a system in-house, TDEM provided instructions on how to create a web form to capture user contact information and log when the user received the phone. This was a method employed early by TDEM before building a custom database which integrates to their WebEOC platform.

Web Form

A Google Form was created to populate contact information of the person receiving a loaner phone. A custom URL was created for each device with the device number being pre-populated to prevent user data entry errors.

The phones were deployed in MobileIron kiosk mode which placed a link to the custom URL on the home screen of each phone. As each phone was distributed, users clicked the link to enter name, phone number, email address, department, and position worked. Once submitted, the information was logged and time-stamped.

Conclusion

It is clear that mobile devices and apps offer tremendous potential to improve public safety communications by augmenting voice radio with tools such as personnel location tracking, Push-To-Talk (PTT), evacuation tracking, collaboration, situational awareness, and many more. The adoption of these tools will continue to grow as the availability of reliable, mobile broadband networks becomes more ubiquitous.

The use of shared, cache devices can accelerate the availability of these technologies until public safety agencies have the budgets to provide all first responders with department-issued smartphones. Cache devices also support interoperability by allowing responders from outside agencies secure access to mobile apps during joint operations.

As outlined in this paper, the provisioning and management of smartphones is a complex task. Department executives should carefully consider the implications of device management when deciding how many devices to purchase and the rate of adoption.

As with the evolution of personal computers, many of these challenges can be lessened as the industry matures products to support multiple users. Industry advancements for supporting multiple user profiles and using temporary facial recognition to unlock phones offer significant potential for expanding the viability of shared device deployments.

M4PS would like to offer a special thanks to TDEM for sharing their lessons learned over recent years in managing thousands of phones across the very large State of Texas. Tips and tricks they shared have helped streamline the provisioning, distribution, and collection of hundreds of cache phones for the various MAC deployments to-date saving countless hours and ensuring all equipment was successfully returned after each operation.