EXTENSIONS (Mx)
FORTIFIED ANDROID™ FOR THE ENTERPRISE
WHAT IS Mx?

Extensions (Mx) by Zebra is a new layer of features that infuses standard Android with the features you need to take advantage of Android devices in your business.

INFUSING STANDARD ANDROID WITH:
- ENTERPRISE-CLASS SECURITY
- ENTERPRISE-CLASS MANAGEABILITY
- ENTERPRISE-CLASS DATA CAPTURE
- ENTERPRISE-CLASS WIRELESS CONNECTIVITY

Mx: ENABLING THE CREATION OF THE TRULY ENTERPRISE-CLASS ANDROID DEVICE.

Android has taken the world by storm; currently the operating system of choice in nearly 75 percent of the world’s consumer smartphones. Now, Android-based devices are crossing over from the consumer world to the enterprise, driven by the operating system’s simplicity and flexibility. With its contemporary user interface (UI) and support for touch input and gestureing, enterprises are now free to design application screens that make every step in a workflow as intuitive as possible. The result is a new class of business applications that is every bit as easy to use and engaging as today’s consumer applications, meeting the expectations of today’s workers — and virtually eliminating the need for training.

Zebra recognized the value Android could bring to the enterprise — but there was one major hurdle to clear before embarking on the creation of enterprise-class mobile computers based on Android: the Android operating system was built for the consumer world. Even though Android is constantly evolving and integrating new enterprise-class features, it still falls short of the features required in the enterprise.

Extensions (Mx) was created to address this issue. Mx adds a layer of features on top of the standard Android operating system — features that enable the creation of Android-based mobile computers that are truly enterprise-ready. Mx infuses Zebra Android-based mobile computers with a complete enterprise feature set — features that are missing in mobile devices that run standard Android, robust enterprise-class security and manageability, enterprise-class data capture features and business-class Wi-Fi connections that provide workers with a superior wireless experience.

...LACKING IN THE FEATURE SET YOU NEED IN YOUR ENTERPRISE...

Android now the most popular mobile operating system in the world... lacking in the feature set you need in your enterprise... until now.

WHAT IS Mx?

WHAT Mx IS NOT

FEATURES
Overview
Mx Security
Mx MDM
Mx Data Capture
Mx Wireless
THE ZEBRA Mx COMMITMENT
WHAT Mx IS NOT

While Mx includes platform features, it is not a proprietary version of Android that would give IT cause for concern, nor does it reduce any functionality in Android or create application compatibility issues.

Mx platform features are pre-installed on all of our Android devices. With Mx, you are always in charge — you decide which optional features you want to activate, and when.

And since Mx features are typically deployed through your current mobile device management (MDM) solution, implementing Mx couldn’t be easier. With Mx, you're in complete control of your Zebra Android-based mobile computers, maximizing risk and minimizing value.

Mx. ALL THE ENTERPRISE FEATURES YOU NEED IN ANDROID. DELIVERED.

IT IS NOT A PROPRIETARY VERSION OF ANDROID.
IT DOES NOT REDUCE ANDROID’S FUNCTIONALITY.
IT DOES NOT CREATE COMPATIBILITY ISSUES.
IT DOESN’T COST YOU A THING.
IT DOESN’T REQUIRE INSTALLATION – IT IS PRE-INSTALLED AND READY TO GO.

Mx OVERVIEW

There are five classes of Mx features that are layered in between the standard Android operating system and your applications.

Applications

Extensions (Mx)

Mx Security
- Device lockdown: Enterprise Home Screen
- Peripheral/Feature lockdown
- Government grade granular encryption
- Security updates

Mx MAM
- Mobile Application Management additions
  - Enterprise Applock: Multi-tap on lock
  - Application lock-on
  - Silent install

Mx MDM
- Mobile device management additions
  - Multi-user log-on
  - MDM compatibility
  - Optional chew management controls

Mx Data Capture
- Data Capture features that allow you to easily utilize all of our advanced enterprise data capture capabilities in your Android business application
  - DataWedge support— capture barcodes and more without programming
  - Integrated decode algorithms for superior scanning performance
  - DataCapture SDK

Mx Wireless
- Bluetooth/Wi-Fi/4G/LTE/LAN/WAN
  - Fast and intelligent roaming
  - Adaptive Authentication
  - Edge Awareness
  - Heterogeneous WLAN network support
  - Comprehensive Wi-Fi security protocol support

STANDARD ANDROID
YOU GET ALL THE ADVANTAGES OF THE ANDROID YOU WANT—with the SECURITY YOUR ENTERPRISE NEEDS.

DEVICE LOCKDOWN WITH AN ENTERPRISE HOME SCREEN

Many users only need to access one line-of-business application. With this feature, when workers turn on their mobile computer, it will automatically launch and lock into that application. Since users are unable to exit, the Enterprise Home Screen effectively creates a single-purpose mobile computer that protects productivity and secures corporate data by preventing access to other business applications, or downloading of personal social networking or game applications. And since you have the flexibility to allow users to exit the application, the Enterprise Home Screen can also provide workers with the convenience of instant access to their most used application every time they power up their mobile computer.

PERIPHERAL AND FEATURE LOCKDOWN

The mobile computer you purchase may have features that pose security risks, but off-the-shelf Android doesn’t provide a means to disable those features. For example, you may want to disable the USB port to eliminate the possibility of a user copying sensitive data on to a USB stick — or loading an unapproved application that could contain malware. This feature gives you complete control over the feature set your workers can access, allowing you to restrict user access to peripheral interfaces such as USB and Bluetooth, as well as device features such as GPS and near field communication (NFC).

GOVERNMENT GRADE GRANULAR DATA ENCRYPTION

Data encryption is not only crucial in order to protect corporate data, in numerous industries it is a requirement. For example, Payment Card Industry (PCI) regulations require protection for sensitive customer payment card information, and the Health Insurance Portability and Accountability Act (HIPAA) U.S. government mandate requires proper protection of personal patient healthcare information.

The latest versions of standard Android now provide basic encryption features — you can choose to encrypt the entire internal drive as well as any installed SD card. Mx builds on this feature to improve flexibility and protect device performance by allowing you to select the data you want to encrypt. You simply create encrypted file systems that appear as folders — everything in the folders is automatically protected with government-grade AES 256 encryption. The advantage? Since only sensitive data is encrypted, the impact encryption often has on device performance is minimized.

Another key difference is the generation and management of the encryption keys. With standard Android, keys are generated and secured directly on the mobile device, eliminating the ability to move the SD card to another device — a major inconvenience if a user needs to swap devices or give data to a supervisor or other worker. Mx provides best IT practices for encryption key management — keys are generated and provisioned in a centralized location. The result? Unlike standard Android, the SD card can be moved to another device — with the press of a few buttons, IT can remotely and remotely provision the new device with the proper encryption keys required for access.

YOU GET ALL THE ADVANTAGES OF THE ANDROID YOU WANT—with the SECURITY YOUR ENTERPRISE NEEDS. Mx SECURITY UPDATES

When the Android Open Source Community releases a security patch, how do you know it’s available? And how can you make sure that patch is deployed in a timely manner to help prevent security breaches? Until today, enterprises and consumers alike have been dependent upon the cellular carrier to test, certify and distribute the patch. But for the enterprise customer, time is of the essence — enterprises need to plug any security weaknesses the moment a patch is available.

HOW DOES Mx IMPROVE SECURITY?

You can lock users into a single application. You can lock users out of specific device features — such as USB or Bluetooth. You can select the files you want to protect with government grade encryption, helping ensure that the security your need doesn’t come at the cost of device performance. And since encryption keys are centrally managed, you have the flexibility to move SD cards to other devices when needed.

That’s why Zebra created a dedicated internal team responsible for a process known as DARN—Discovery, Assessment, Remediation and Notification. This team monitors all reported Android security issues and their related patches. Depending upon the priority of the patch, it is either made available immediately or in Mx maintenance releases. Customers with products under warranty who have purchased Zebra’s Security from the Start support program for their Android-based Zebra mobile computer will receive notification via email whenever a patch is available. A link in the email allows the enterprise to instantly download the new Android Mx image, complete with the patch. The updated image can then be instantly deployed to all mobile devices via a compatible Mobile Device Management (MDM) application.

GOVERNMENT GRADE GRANULAR DATA ENCRYPTION

Data encryption is not only crucial in order to protect corporate data, in numerous industries it is a requirement. For example, Payment Card Industry (PCI) regulations require protection for sensitive customer payment card information, and the Health Insurance Portability and Accountability Act (HIPAA) U.S. government mandate requires proper protection of personal patient healthcare information. The latest versions of standard Android now provide basic encryption features — you can choose to encrypt the entire internal drive as well as any installed SD card. Mx builds on this feature to improve flexibility and protect device performance by allowing you to select the data you want to encrypt. You simply create encrypted file systems that appear as folders — everything in the folders is automatically protected with government-grade AES 256 encryption. The advantage? Since only sensitive data is encrypted, the impact encryption often has on device performance is minimized. Another key difference is the generation and management of the encryption keys. With standard Android, keys are generated and secured directly on the mobile device, eliminating the ability to move the SD card to another device — a major inconvenience if a user needs to swap devices or give data to a supervisor or other worker. Mx provides best IT practices for encryption key management — keys are generated and provisioned in a centralized location. The result? Unlike standard Android, the SD card can be moved to another device — with the press of a few buttons, IT can remotely and remotely provision the new device with the proper encryption keys required for access.

YOU GET ALL THE ADVANTAGES OF THE ANDROID YOU WANT—with the SECURITY YOUR ENTERPRISE NEEDS. Mx SECURITY UPDATES

When the Android Open Source Community releases a security patch, how do you know it’s available? And how can you make sure that patch is deployed in a timely manner to help prevent security breaches? Until today, enterprises and consumers alike have been dependent upon the cellular carrier to test, certify and distribute the patch. But for the enterprise customer, time is of the essence — enterprises need to plug any security weaknesses the moment a patch is available.

HOW DOES Mx IMPROVE SECURITY?

You can lock users into a single application. You can lock users out of specific device features — such as USB or Bluetooth. You can select the files you want to protect with government grade encryption, helping ensure that the security your need doesn’t come at the cost of device performance. And since encryption keys are centrally managed, you have the flexibility to move SD cards to other devices when needed.
WHITE-LISTING allows you to control what applications can be downloaded and launched. Simply create a list of approved applications, known as a white list. Users will be unable to download or run applications that are not on the list. The opportunity for the installation of malicious or personal applications that could compromise data security and reduce employee productivity is eliminated.

SILENT INSTALL
With standard Android, you can use your existing MDM application to request an application install. However, users are alerted of the pending installations and have the power to accept or delay the install, making it difficult to enforce timely application and security updates. With Mx, you can install applications silently, without alerting users. And if the application update contains critical security patches or updated features, you can force the device to reboot once the installation is complete to instantly activate the updated software.

WITH Mx, YOU COMPLETELY CONTROL WHICH APPLICATIONS CAN BE INSTALLED, AS WELL AS THE APPLICATION UPDATE PROCESS.

APPLICATION LOCKDOWN WITH WHITE-LISTING
While whitelisting allows only whitelisted applications to be downloaded and launched, simply create a list of approved applications, known as a white list. Users will be unable to download or run applications that are not on the list. The opportunity for the installation of malicious or personal applications that could compromise data security and reduce employee productivity is eliminated.

SILENT INSTALL
With standard Android, you can use your existing MDM application to request an application install. However, users are alerted of the pending installations and have the power to accept or delay the install, making it difficult to enforce timely application and security updates. With Mx, you can install applications silently, without alerting users. And if the application update contains critical security patches or updated features, you can force the device to reboot once the installation is complete to instantly activate the updated software.

WITH Mx, YOU COMPLETELY CONTROL WHICH APPLICATIONS CAN BE INSTALLED, AS WELL AS THE APPLICATION UPDATE PROCESS.

APPLICATION LOCKDOWN WITH WHITE-LISTING
White-listing allows you to control what applications can be downloaded and launched. Simply create a list of approved applications, known as a white list. Users will be unable to download or run applications that are not on the list. The opportunity for the installation of malicious or personal applications that could compromise data security and reduce employee productivity is eliminated.

SILENT INSTALL
With standard Android, you can use your existing MDM application to request an application install. However, users are alerted of the pending installations and have the power to accept or delay the install, making it difficult to enforce timely application and security updates. With Mx, you can install applications silently, without alerting users. And if the application update contains critical security patches or updated features, you can force the device to reboot once the installation is complete to instantly activate the updated software.

WITH Mx, YOU COMPLETELY CONTROL WHICH APPLICATIONS CAN BE INSTALLED, AS WELL AS THE APPLICATION UPDATE PROCESS.
THE ZEBRA MC COMMITMENT

Mx Wireless

Mx Wireless gives you wired-style dependable Wi-Fi connectivity, right to the very edge of your wireless LAN.

All Wi-Fi radios are not created equally. The consumer-grade radios in standard Android devices typically lack the features required to maintain a robust wireless connection. In the enterprise, this resulting connectivity gap can translate into dropped voice calls and the need to re-enter data, frustrating workers and reducing productivity. Mx Wireless addresses this issue with Fusion—an enterprise-grade Wi-Fi radio with a feature set that delivers wired-style quality of service in every inch of your managed WLAN network. The result? Your workers experience superior speed, throughput and dependability—even in managed heterogeneous WLAN network environments.

Fast and Intelligent Pre-emptive Roaming

Since our Fusion Wi-Fi radio is network aware, it can scan for and connect to the best signal and allow users to roam to that access point to prevent signal degradation.

Adaptive Authentication

With network awareness, our Fusion Wi-Fi radio pre-authenticates users on all of your access points, then scans for the best access point and authenticates when workers are on the move through your facility. Our Wi-Fi radios minimize de-authentication, improving battery cycle times, and roaming efficiency so the roaming experience is significantly improved.

Edge Awareness

Maintaining service quality at the literal edge of your wireless network is always a challenge. The Fusion Wi-Fi radio takes awareness when users have moved to the last access point and triggers a special feature that protects the network connection and the user experience. The result? Productivity is preserved, even at the very edge of your WLAN.

Heterogeneous Wi-Fi Support

The Fusion Wi-Fi features are backward compatible with all Wi-Fi standards, ensuring that the Mx Fusion Wireless device will work, regardless of whether your WLAN includes only Zebra access points or other access points from other manufacturers.

Comprehensive Wi-Fi Security Support

Our Fusion Wi-Fi radio takes your mobile workforce to the next level. Our secure, proprietary technology, such as Cisco, supports a multitude of Wi-Fi security protocols, including WPA, WPA2 (AES), CCXv4 and much more. Our Fusion Wi-Fi radio is truly enterprise-class, with support for all of the latest Wi-Fi security protocols, including IEEE 802.11i, 802.11w and much more. As a result, your data is safe. Every Fusion network contains access points with proprietary technology, such as Cisco. Comprehensive Wi-Fi security protocol compliance sets our Fusion Wi-Fi radio apart from any other Wi-Fi radios and ensures your sensitive data is protected.

WITH Mx, IT’S EASY TO TAKE COMPLETE ADVANTAGE OF ALL OF OUR ENTERPRISE-CLASS DATA CAPTURE FEATURES TO MAXIMIZE THE VALUE OF OUR ANDROID-BASED MOBILE COMPUTERS.

DATA WEDGE FOR EASY CAPTURE OF BAR CODES AND OTHER BASIC ENTERPRISE DATA — WITHOUT PROGRAMMING

In the enterprise, bar code scanning is a core capability that will be used day-in and day-out to improve business efficiency and back-end data. Without native support, enabling enterprise-class bar code scanning with standard Android can be time-consuming and costly.

With Mx, your workers can scan, and with scanning bar code data is closer, instead of weeks or months. Mx offers native support for Datadex, an easy-to-use Zebra utility that enables the capture of bar code data from virtually any type of scanning technology — 1D laser, 1D linear imager, 2D imager and readers — as well as from magnetic stripe readers. The Advanced Data Formatting (ADF) function allows you to extract and filter data from whatever format your application requires. For example, the first five characters captured may be entered into one field and the following six characters into a different field — or you may need to remove all blank spaces or add a special keystroke, such as Tab or Enter. Once the data is formatted correctly, it is delivered into the application, where it is received keystroke-by-keystroke, such as Tab or Enter. This complimentary utility can be downloaded at no charge from the Zebra website.

EASILY INTEGRATE COMPREHENSIVE DATA CAPTURE FUNCTIONS IN NATIVE ANDROID APPLICATIONS WITH OUR DATA CAPTURE SDK

With the same first-time every-time bar code scanning performance for which Zebra is known, even if bar codes are poorly printed, dirty or damaged, our algorithms enable the successful first-pass scanning that keeps business moving and workers productive.

EASILY INTEGRATE COMPREHENSIVE DATA CAPTURE FUNCTIONS IN NATIVE ANDROID APPLICATIONS WITH OUR DATA CAPTURE SDK

If you’re creating native Android applications, we make it easy to take advantage of the advanced data capture features on our Android-based mobile computers. Our entire Android-based mobile device portfolio is fully compatible with the standard Android operating system, so developers can use standard and familiar Android development tools for the majority of the application development effort, such as Google’s Android Software Development Kit (SDK). But the Android SDK does not cover all of the enterprise-class data capture features on our mobile computers, creating a potentially time-consuming and resource-intensive development effort. To fix this gap and reduce development time and cost, we created the Zebra DataCapture SDK. Our DataCapture SDK incorporates a multitude of enterprise-class data capture functions in our Android-based mobile computers, whether the feature is native to the device (such as an integrated bar code scanner) or available through an attached accessory (such as a payment card reader).

INTEGRATED SUPPORT FOR DECIDE ALGORITHMS

With Mx in support of Zebra’s world-class decode algorithms, workers get the same first-time every-time scanning performance for which Zebra is known. Even if bar codes are poorly printed, dirty or damaged, our algorithms enable the successful first-pass scanning that keeps business moving and workers productive.

THE ZEBRA MC COMMITMENT

Mx gives you wired-style dependable wireless connectivity, right to the very edge of your wireless LAN.
WE PLEDGE A SOLID COMMITMENT TO Mx

As an industry leader in enterprise mobility, we are as committed to Mx as we are to the mobile computers and wireless infrastructure we manufacture. Today, there are over 30 Mx features, with over 50 more currently in development and a roadmap that reaches many years into the future. It’s obvious that the Android operating system is here to stay — so is Mx. You can count on Mx to evolve and keep pace with standard Android, new mobile device requirements and new mobility trends.

TAKE ADVANTAGE OF ANDROID IN YOUR ENTERPRISE WITH THE POWER OF Mx.
FOR MORE INFORMATION, PLEASE VISIT WWW.ZEBRA.COM/MXEXTENSIONS