

Release Notes - Zebra MC33x Android Oreo LifeGuard Update 16 Release (NGMS)

[Introduction](#)

[Description](#)

[Component Contents](#)

[Installation Requirements](#)

[Installation Instructions](#)

[Device Compatibility](#)

[Known Issues and Limitations](#)

Introduction

Zebra MC3300 is the next generation key-based, rugged mid-range hand-held mobile computing device. MC3300 supports multiple form-factors offering a combination of different physical keys, data capture and memory options. Running on a stable Android-O (8.1.0) OS, MC3300 offers the Zebra Value Adds software solutions to enhance your Enterprise workflow.

The MC3300 is the professional-grade Android device built from the ground up for the Enterprise.

- Zebra's Mobility Extensions (Mx)
- Mobility DNA, a suite of mobility enabling applications, development tools and utilities
- Most advanced scan engine with longer range data capture capability
- Rugged and ready for every day Enterprise use inside and outside the four walls

Description

This release contains the following software package which is compatible with the MC33x products.

LifeGuard patches are cumulative and include all previous fixes that are part of earlier patch releases.

Component Contents

Package Name	Package Description
CFE_ATLAS_02-13-15.00-ON-U16-STD.zip	OTA incremental CFE v16 update software for NGMS build compatible for MC33x product.

Component Version Info

Component / Description	Version
Product Build Number	02-13-15.00-ON-U16-STD
Android Version	8.1.0
Linux Kernel	3.10.84
Android SDK Level	27
Platform	QC8956
Bluetooth Stack	4.1
Flash Size	16/32GB
RAM Size	2/4GB
Scanning Framework	22.0.6.1
DataWedge	7.3.22
EMDK	7.3.18.2318
MXMF / OSX	MXMF : 9.0.3.1 / OSX : QCT.81.8.8.2
WiFi	FUSION_BA_2_11.0.0.024_O
NFC	Radio: BA_2_11.0.0.017_O
	Application: BA_2_11.0.0.012_O
	Middleware: BA_2_11.0.0.015_O
	Firmware: 7.35.205.8_20181002
	NFC_NCIHALx_AR003C.8.3.0_O_OpnSrc
PTT	3.1.39
Touch FW	26
RxLogger	5.4.12.0
Bluetooth Pairing Utility	3.14
Zebra Data Service	3.5.0.1162
Files	8.1.0
Stage Now	3.3.1.2000
Battery Swap	1.0
User Guide	1.0
Zebra Volume Control (ZVC)	2.1.0.14
Battery Manger	1.4.2
ActiveEdge	2.5.16

WorryFree WiFi Analyzer	3.2.20
Device Central	2.1.0.9
Zebra Software License Manager	3.1.1
Audio	0.8.0.0
Acoustic Profiles	General: DO3.1 Cellular: N/A
OemInfo	1.0.1.1128
OemConfig	9.0.1.0
Enterprise Keyboard (EKB)	2.1.1.3
Diagnostic Tool	1.17.0.9
WebView	73.0.3683.90
Finger Print	Zebra/MC33/MC33:8.1.0/02-13-15.00-ON-U16-STD/96:user/release-keys Zebra/MC33/MC33C:8.1.0/02-13-15.00-ON-U16-STD/96:user/release-keys
Security Patch Level	July 01 2019

1. CFE v16 Updates:

❖ CFE_ATLAS_02-13-15.00-ON-U16-STD.zip (NGMS)

1. **Android Security Patch Level: July 01, 2019.**

Use the link below to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

2. Updated below mentioned components: For more detail please refer

<http://techdocs.zebra.com>

- DataWedge – Version 7.3.22
 - a. SYMBOL_TRIGGER_6 virtual key can be mapped using KeyManagerCSP to any physical keys and the mapped physical keys can then be used to trigger RFIDWedge.
- MXMF – Version 9.0.3.1
 - a. SPR36768 - Resolved an issue wherein EHS Hostname in title was not reflecting updated Hostname after device reboot.
- EKB – Version 2.1.1.3
 - a. SPR37353 - Enabled remapping of the right-side emoji icon in the EKB, both left and right emoji icons will be remapped to same key.
- EMDK – Version 7.3.18.2318
- OSx – Version QCT.81.8.8.2
- Zebra Data Service – Version 3.5.0.1162
- OemInfo – Version 1.0.1.1128

1. SPR35991 - Resolved an issue wherein when soft-keyboard is switched, sometimes scan data stops to transmit to apps.
2. SPR36946 - Resolved an issue wherein System UI crashes whenever user tries to open settings related options on user screen in EHS.
3. SPR36967 - Resolved an issue wherein downgrading LG patch will cause "Error Zebra Plugin Stopped" popup.
4. CHINA/Indonesia SKU Support - LTE/4G network option/capability is disabled for China/Indonesia SKU's.

2. CFE v15 Updates:

❖ CFE_ATLAS_02-13-15.00-ON-U15-STD.zip (NGMS)

3. **Android Security Patch Level: June 01, 2019.**

Use the link below to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

4. Updated below mentioned components: For more detail please refer

<http://techdocs.zebra.com>

- DataWedge – Version 7.3.21
 - a. SPR37060 - Resolved an issue wherein Datawedge was not disabling the scanner upon resume during app transition from background to foreground causing intermittent scanning failures.
 - b. SPR37124 - Resolved an issue wherein ADF rule with crunch spaces was removing last character from barcode data with space.
 - EMDK – Version 7.3.17.2317
 - b. SPR36925: Resolved an issue wherein scanner was not available for second app when an ANR or crash occurred on the first app.
 - MXMF – Version 9.0.2.9
 - a. SPR36994 - Resolved MX initialization issue wherein EHS was calling MX before completion of MX initialization process.
 - EKB – Version 2.1.1.2
 - Device Central – Version 2.1.0.9
5. SPR 35943 - Added WebView version 73.0.3683.
 6. SPR36961 - Fixed an issue wherein User installation of RFID apps does not persist on non-RFID devices after reboot.
 7. SPR36897: Added dun type to Telstra-M2M APN.
 8. SPR37175 - Fixed an issue wherein Two apps can enable the same scanner without one app releasing it.

9. SPR36927 - Resolved an issue wherein scanner was not available for any app when multiple apps enabled the scanner and any app among them disable the scanner when it moves to background.

3. CFE v14 Updates:

- ❖ CFE_ATLAS_02-13-15.00-ON-U14-STD.zip (NGMS)
- 5. **Android Security Patch Level: May 01, 2019.**
Use the link below to see the Android Security bulletin for more information:
<https://source.android.com/security/bulletin/>
- 6. Updated below mentioned components: For more detail please refer <http://techdocs.zebra.com>
 - DataWedge – Version 7.3.18
 - StageNow – Version 3.3.1.2000
 - EMDK – Version 7.3.14.2314
 - MXMF – Version 9.0.2.4
 - DDT – Version 1.17.0.9
 - EKB – Version 2.1.1.0
 - OemConfig – Version 9.0.1.0
 - Scanning Framework – Version 22.0.6.1
 - a. DotCode Symbology support is added for SE4750, SE4850, SE4710 and Camera Scanning.
 - b. Digimarc barcode decoding support is added for Camera Scanning.
 - c. Support for new Symbologies named FebraBan and Gridmatrix is added.
 - d. Instant Data Reporting (MultiBarcode) feature support is added.
 - OSx – Version QCT.81.8.7
- 10. SPR36846/36693 – Fixed an issue wherein SIP shown area was patched up with white background when "Show Virtual Keyboard" setting is off and web page is opened.
- 11. SPR36170 - Fixed an issue wherein ntp sync does not work when parameters are updated using Stagenow.
- 12. SPR36143 - Resolved an issue wherein remapping of control modifier keys were not persisting across a reboot.
- 13. SPR36697 - Resolved an issue wherein alpha keys do not work properly on 29-key keyboard.

4. CFE v13 Updates:

- ❖ CFE_ATLAS_02-13-15.00-ON-U13-STD.zip (NGMS)

1. **Android Security Patch Level: April 01, 2019.**

Use the link below to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

2. Updated below mentioned components: For more detail please refer

<http://techdocs.zebra.com>

- PTT - Version 3.1.39
- Device Central - Version 2.0.22.1
- OSX - Version QCT.81.8.6_4
 - a. SPR36117/36095 – Resolved an issue wherein the scanned data would not come to the Apps, Airplane menu item was missing in the Power key menu and Home and recent buttons were not functional.

5. CFE v12 Updates:

❖ CFE_ATLAS_02-13-15.00-ON-U12-STD.zip (NGMS)

1. **Android Security Patch Level: February 01, 2019.**

Use the link below to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

2. Updated below mentioned components: For more detail please refer

<http://techdocs.zebra.com>

- WorryFree WiFi Analyzer – Version 3.2.20
- MX: 8.4.1.3
 - a. SPR35665 – Resolved an issue wherein Google Keyboard settings was not persisting.
 - b. SPR35491/35856 – Resolved an issue wherein Analytics Manager was throwing "Index out of bound error " when a StageNow Barcode is scanned.
 - c. SPR35928 – Resolved an issue where Clock Manager CSP accepts timezone id in "/Etc" Olson format.
 - d. SPR35908 – Resolved an issue wherein admin and user generated certificates could not be downloaded from external server.
 - e. SPR34771 – Resolved synchronization issue while checking with accessmanager.
- StageNow client: 3.2.1.0
- OEMConfig: 8.4.0.1
- Datawedge: 7.2.5
- EKB: 2.0.1.9
 - a. SPR35603 – Fixed an issue wherein Enterprise Keyboard was getting disappeared when external Keyboard was connected.
- EMDK: 7.2.2.2202
- DDT: 1.16.1.3

3. SPR36019 – Resolved an issue wherein serial port control signals were not working as expected.

6. CFE v11 Updates:

❖ CFE_ATLAS_02-13-15.00-ON-U11-STD.zip (NGMS)

1. **Android Security Patch Level: December 01, 2018.**

Use the link below to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

2. Updated below mentioned components: For more detail please refer

<http://techdocs.zebra.com>

- WLAN - Version FUSION_BA_2_11_0.0.024_O
- ZVC - Version 2.1.0.14
- OemInfo - Version 1.0.0.1059

Installation Requirements

- ADB installed on the PC (including adb drivers)
- USB debugging turned ON (from Developer options)
- MC33 has at least:
 - Version 02-13-15.00-ON-U01-STD

Installation Instructions

CFE software update procedure for MC33x:

The installation instructions assume you have ADB installed on your PC (the adb drivers etc..) and your MC3300 has developer options enabled and USB debugging ON. Instructions on HOW TO enable ADB is also captured in the user guide.

1. Connect the MC33x to the PC using the USB data cable or through the cradle.
2. You may need to pull down the top menu and if you see “USB for charging”, touch it and then change it to “File transfers”.
3. Open Command Prompt, run “adb devices” and check if you can see the device’s serial number... If yes, proceed... if not, you will need to get the PC set up with the proper drivers or install an External SD Card.
4. You may also get a pop up on your PC (Win 7) that you will be connected as a Portable

Media Player... this can be ignored.

❖ Download Image

- a) CFE_ATLAS_02-13-15.00-ON-U16-STD.zip listed above in content section
5. Entering Recovery Mode
 - a. Choice 1: In Command Prompt, type *“adb reboot recovery”* and click enter.
 - b. Choice 2:
 - Reboot the device while holding the Pistol Grip Trigger (**GUN Device**) or the Right Scan Trigger (**BRICK Device**)
 - When Zebra Technologies logo appears on the screen release the trigger
6. Your MC33x will reboot and put you on the Android Recovery screen.
7. If applying update via sideload Method
 - a. Use the Volume + and – to highlight, *“Apply update from ADB”* and press the Power key to select it for applying OS upgrade package
8. if applying update via External SD card
 - a. Use the Volume + and – to highlight *“Apply update from SD card”* and press the Power Key to select it
 - b. Use the Volume + and – to highlight package CFE_ATLAS_02-13-15.00-ON-U16-STD.zip and press the Power Key to select it.
 - c. Go to Step 10 once above steps are completed
9. With your Command Prompt open in the Host machine, type *“adb sideload”* command and add a space and then drag and drop the CFE_ATLAS_02-13-15.00-ON-U16-STD.zip file on to it and click enter.
 - a. Your PC screen will show files being installed and a little blue horizontal progress bar on your device will show status... and after about 6~ minutes (could be 10+ minutes if installing GMS) it should be done and you should be back at the Android Recovery screen.
10. *“Reboot system now”* is highlighted. Press the Power Key to Reboot.
11. At the Home Screen, we need to verify that the BSP upgrade took place and set the Date & Time.
 - a. Go to *“Settings”* and scroll down to *“About phone”* and look at the *“Build number”*. It should start with **“02-13-15.00-ON-U16-STD release keys”**. Now you are on the correct BSP.
12. Now you are all set to use your MC33x.

Device Compatibility

This software release has been approved for use on the following devices.

Device Part Number	Operating System	Device Part number	Operating System
--------------------	------------------	--------------------	------------------

MC330K-GE3HA3NA	Android N, O
MC330K-GE3HA3RW	Android N, O
MC330K-GE4HA3NA	Android N, O
MC330K-GE4HA3RW	Android N, O
MC330K-GE4HA4NA	Android N, O
MC330K-GE4HA4RW	Android N, O
MC330K-GI3HA3NA	Android N, O
MC330K-GI3HA3RW	Android N, O
MC330K-GI3HA4RW	Android N, O
MC330K-GI4HA3NA	Android N, O
MC330K-GI4HA3RW	Android N, O
MC330K-GI4HA4NA	Android N, O
MC330K-GI4HA4RW	Android N, O
MC330K-GI4HG3NA	Android N, O
MC330K-GI4HG3RW	Android N, O
MC330K-GI4HG4NA	Android N, O
MC330K-GI4HG4RW	Android N, O
MC330K-GL2HA3RW	Android N, O
MC330K-GL3HA3RW	Android N, O
MC330K-GL3HA4RW	Android N, O
MC330K-GL4HA3NA	Android N, O
MC330K-GL4HA3RW	Android N, O
MC330K-GL4HA4NA	Android N, O
MC330K-GL4HA4RW	Android N, O
MC330K-GL4HG3RW	Android N, O
MC330K-RC3HA4NA	Android N, O
MC330K-RC3HA4RW	Android N, O
MC330K-RC3HG4RW	Android N, O
MC330K-RC4HA4NA	Android N, O
MC330K-RC4HA4RW	Android N, O
MC330K-RL3HA3RW	Android N, O
MC330K-RL3HG3RW	Android N, O
MC330K-RL3SG3RW	Android N, O
MC330K-RL4HA3NA	Android N, O
MC330K-RL4HA3RW	Android N, O
MC330K-RL4HG3NA	Android N, O
MC330K-SB3HA4NA	Android N, O
MC330K-SB3HA4RW	Android N, O
MC330K-SB3HG4RW	Android N, O
MC330K-SB4HA4NA	Android N, O
MC330K-SB4HA4RW	Android N, O
MC330K-SB4HG4NA	Android N, O
MC330K-SE2HA3RW	Android N, O

MC330M-RL4SG2RW	Android N, O
MC330M-SI2HA2RW	Android N, O
MC330M-SI30A2RW	Android N, O
MC330M-SI3HA2NA	Android N, O
MC330M-SI3HA2RW	Android N, O
MC330M-SI40A2NA	Android N, O
MC330M-SI4HA2NA	Android N, O
MC330M-SI4HA2RW	Android N, O
MC330M-SI4HG2NA	Android N, O
MC330M-SL2HA2RW	Android N, O
MC330M-SL2HG2RW	Android N, O
MC330M-SL3HA2NA	Android N, O
MC330M-SL3HA2RW	Android N, O
MC330M-SL4HA2NA	Android N, O
MC330M-SN3HA2RW	Android N, O
MC330M-SN4HA2NA	Android N, O
MC330M-RL2SG2US	Android N, O
MC330M-SL4HG2US	Android N, O
MC330M-SL3HG2US	Android N, O
MC330M-RL4SG2US	Android N, O
MC330M-RL3HG2US	Android N, O
MC330M-SN4HG2US	Android N, O
MC330M-SI3HG2US	Android N, O
MC330M-GL4HG2US	Android N, O
MC330M-GL3HG2US	Android N, O
MC330M-GL2HG2US	Android N, O
MC330M-GI3HG2US	Android N, O
MC330M-GI2HG2US	Android N, O
MC330K-SN4HG3US	Android N, O
MC330K-SI3HG3US	Android N, O
MC330K-GL4HG3US	Android N, O
MC330K-RC4HG4US	Android N, O
MC330K-RC3HG4US	Android N, O
MC330K-GL4HG4US	Android N, O
MC330K-GI3HG3US	Android N, O
MC330K-SP4HG4US	Android N, O
MC330K-SP3HG4US	Android N, O
MC330K-SB3HG4US	Android N, O
MC330K-SE4HG3US	Android N, O
MC330K-SE3HG3US	Android N, O
MC330K-SE2HG3US	Android N, O
MC330K-GE4HG3US	Android N, O
MC330K-GE3HG3US	Android N, O

MC330K-SE3HA3NA	Android N, O
MC330K-SE3HA3RW	Android N, O
MC330K-SE4HA3NA	Android N, O
MC330K-SE4HA3RW	Android N, O
MC330K-SG3HA4NA	Android N, O
MC330K-SG3HA4RW	Android N, O
MC330K-SG4HA4NA	Android N, O
MC330K-SI2HA3RW	Android N, O
MC330K-SI3HA3NA	Android N, O
MC330K-SI3HA3RW	Android N, O
MC330K-SI3HG3RW	Android N, O
MC330K-SI4HA3NA	Android N, O
MC330K-SI4HA3RW	Android N, O
MC330K-SI4HG3NA	Android N, O
MC330K-SL2HA3RW	Android N, O
MC330K-SL4HA3RW	Android N, O
MC330K-SN3HA3RW	Android N, O
MC330K-SN4HA3NA	Android N, O
MC330K-SN4HA3RW	Android N, O
MC330K-SP3HA4NA	Android N, O
MC330K-SP3HA4RW	Android N, O
MC330K-SP4HA4NA	Android N, O
MC330K-SP4HA4RW	Android N, O
MC330M-GI2HA2NA	Android N, O
MC330M-GI2HA2RW	Android N, O
MC330M-GI30A2RW	Android N, O
MC330M-GI3HA2IN	Android N, O
MC330M-GI3HA2NA	Android N, O
MC330M-GI3HA2RW	Android N, O
MC330M-GI3HG2RW	Android N, O
MC330M-GI40A2NA	Android N, O
MC330M-GI4HA2IN	Android N, O
MC330M-GI4HA2NA	Android N, O
MC330M-GI4HA2RW	Android N, O
MC330M-GI4HG2NA	Android N, O
MC330M-GL2HA2NA	Android N, O
MC330M-GL2HA2RW	Android N, O
MC330M-GL3HA2NA	Android N, O
MC330M-GL3HA2RW	Android N, O
MC330M-GL3HG2RW	Android N, O

MC330K-GE2HG3US	Android N, O
MC330K-SG4HG4US	Android N, O
MC330K-SG3HG4US	Android N, O
MC330K-SG2HG4US	Android N, O
MC330K-GE4HG4US	Android N, O
MC330K-GE2HG4US	Android N, O
MC330K-GI3HG3US01	Android N, O
MC330M-SN3HG2RW	Android N, O
MC330M-SL3HG2RW	Android N, O
MC330M-SI4HG2RW	Android N, O
MC330M-SI3HG2RW	Android N, O
MC330M-SI2HG2RW	Android N, O
MC330M-RL3HG2RW	Android N, O
MC330M-RL2SG2RW	Android N, O
MC330M-GL4HG2RW	Android N, O
MC330M-GL2HG2RW	Android N, O
MC330M-GI4HG2RW	Android N, O
MC330M-GI4HG2IN	Android N, O
MC330M-GI3HG2IN	Android N, O
MC330M-GI2HG2RW	Android N, O
MC330K-SP4HG4RW	Android N, O
MC330K-SP3HG4RW	Android N, O
MC330K-SN4HG3RW	Android N, O
MC330K-SN3HG3RW	Android N, O
MC330K-SL4HG3RW	Android N, O
MC330K-SL2HG3RW	Android N, O
MC330K-SI4HG3RW	Android N, O
MC330K-SI2HG3RW	Android N, O
MC330K-SG3HG4RW	Android N, O
MC330K-SG2HG4RW	Android N, O
MC330K-SE4HG3RW	Android N, O
MC330K-SE3HG3RW	Android N, O
MC330K-SE2HG3RW	Android N, O
MC330K-SB4HG4RW	Android N, O
MC330K-RL4HG3RW	Android N, O
MC330K-RC4HG4RW	Android N, O
MC330K-GL4HG3RW	Android N, O
MC330K-GL3HG4RW	Android N, O
MC330K-GL3HG3RW	Android N, O
MC330K-GL2HG3RW	Android N, O

MC330M-GL40A2NA	Android N, O	MC330K-GI3HG4RW	Android N, O
MC330M-GL40A2RW	Android N, O	MC330K-GI3HG3RW	Android N, O
MC330M-GL4HA2NA	Android N, O	MC330K-GE4HG4RW	Android N, O
MC330M-GL4HA2RW	Android N, O	MC330K-GE4HG3RW	Android N, O
MC330M-RL2SA2NA	Android N, O	MC330K-GE3HG3RW	Android N, O
MC330M-RL2SA2RW	Android N, O	MC330K-GE2HG4RW	Android N, O
MC330M-RL3HA2NA	Android N, O	MC330K-GE2HG3RW	Android N, O
MC330M-RL3HA2RW	Android N, O	MC330K-GI3HG3RW01	Android N, O
MC330M-RL3SA2NA	Android N, O	MC330K-GE2HA3US	Android N, O
MC330M-RL3SA2RW	Android N, O	MC330K-GE2HA4US	Android N, O
MC330M-RL3SG2NA	Android N, O	MC330K-SE2HA3US	Android N, O
MC330M-RL3SG2RW	Android N, O	MC330K-SG2HA4US	Android N, O
MC330M-RL40A2NA	Android N, O	MC330K-GE2HA3RW	Android N, O
MC330M-RL4SA2NA	Android N, O	MC330K-GE2HA4RW	Android N, O
MC330M-RL4SA2RW	Android N, O	MC330K-SG2HA4RW	Android N, O

Known Issues and Limitations

1. For an existing Data wedge profile which is configured for Image barcode scanning, if the user updates the profile for SimulScan data capture and reboots the device, the decoder list is shown as blank under DataWedge settings. As a workaround, user needs to use two different Data wedge profiles one for Imager barcode scanning and other profile for Simul scan data capture.
2. Velocity application stops if user use the Android Recent button to close Velocity app. As a workaround, user can close the application from the velocity application client menu.
3. Ethernet shows Connected state when device is configured with Static IP and placed in multi-slot cradle without Ethernet cable.

Last Revised: <07-08-2019>