KYOCERA

A **B** **C**

Service Bulletin

Ref. No. **2ZS-0034(P102)**

<Date> May 14, 2025

Subject:	**Firmware upgrade (Upgrade Pack Ver_V3.03)** **(Except Russia and Belarus)**			
Model:	**TASKalfa MZ4000i, TASKalfa MZ3200i**			
Classification:	*Field measures timing:*	☐ *At Set Up* ☒ *Next Visit/Service Call*	☐ *Next Periodic Maintenance* ☐ *Information only*	
	Phenomenon:	☒ *SC/Error* ☐ *Image*	☐ *Paper Feeding/Conveying* ☒ *Machine operation*	☒ *Other*
	Type of change:	☐ *Hardware*	☒ *Firmware and Software*	☐ *Information*
Remarks:	*Supplement for KDEM:*	Delivery to Russia and Belarus is prohibited by KDC in consideration of the law.		

The software for Radio Equipment Directive Delegated Act (RED-DA) compliance is released.
Refer to the next page for details on the above and other changes.

< TASKalfa MZ4000i, TASKalfa MZ3200i >   **[Pack contains Enhancement unit firmware]**

Type	**Program No.**	**Remarks**	
Upgrade Pack Ver.	**2ZS_V3.03-S**	Other than KDCN	**New upgrade** (Note: KDEM)
	2ZS_V3.03CN-S	KDCN	**New upgrade**
USB Multi Directory	**FWUP_02ZS**		
CONTROLLER	2ZS_S000.003.210		**New upgrade** (Note: KDEM)
CONTROLLER CN	2ZS_S000.U03.210		**New upgrade**
PANEL MAIN	2XD_7200.001.011		
ENGINE	2ZS_1000.004.001		
LANGUAGE MLT	2ZS_81XM.003.103		
OCR DATA	2XC_L000.001.001		
SRGAN DATA	2XC_T100.001.003		
HWE DATA	2XC_T400.001.004		
ESPECIAL	ES_SKIP.ON		
ENHANCE			
DP-7140	2P1_9500.004.001	RADF	
DP-7150	3V3_9500.001.005	RADF	
DP-7160/DP-7170	3TC_9500.002.301	CIS	
PF-810	3PC_9000.002.004	1500x2	
PF-791	3N4_9000.004.001	500x2	
DF-791	3NB_9200.025.001	3K	
DF-7120	3RW_9200.006.002	1K	
PH-7A/7B/7C/7D	3NK_9A00.006.001		
MT-730(B)	3N0_9800.004.001		

(Note: KDEM) Do not distribute to Russia and Belarus.

(Standalone firmware details continue on the next page)

Field Measure:
[All destinations]
When upgrading firmware or replacing PWB, etc., please upgrade each firmware (MAIN, ENGINE, etc.) to the latest version at the same time.

[Only for European specification]
From August 1, 2025, only products that comply with the Radio Equipment Directive Delegated Act (RED-DA) will be allowed to clear customs in Europe.
Compliant products are marked with "R" in the REMARK section of the outer box label of the main unit.
Refer to the next page for details.

*Compliance with the Radio Equipment Directive Delegated Act (RED-DA) does not affect machines already in operation in the field.

First implemented timing at factory:
Planned in April 2025 production

KYOCERA Document Solutions Inc.

KYOCERA

A **B** C

Service Bulletin

The following FW is supplied individually not as in pack.

*For details of FAX System 14 support, refer to Service bulletin No.2ZS-0023(N316).

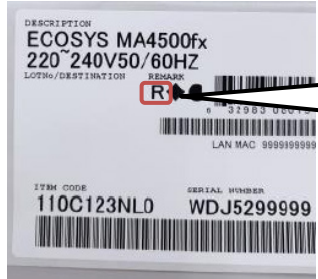| ENHANCE			
FAX System 14	3WN_5100.001.010		
FAX System 12	3R2_5400.003.012	Other than KDCN *1	(Note: KDEM)
FAX System 12 CHN	3R2_5600.Z03.012	KDCN *2	

(Note: KDEM) Do not distribute to Russia and Belarus.

*Firmware configuration   *1: BOOT:3R2_5000.001.009 / APL:3R2_5100.003.012 / IPL:3R2_5600.002.002
   *2: BOOT:3R2_5000.001.009 / APL:3R2_5100.Z03.012 / IPL:3R2_5600.002.002

[Content of Change]

No	Items	Contents	CTL	FW

1	Compliance with the Radio Equipment Directive Delegated Act (RED-DA)
	
	(Only for European specification)
		The Radio Equipment Directive Delegated Act (RED-DA*) will be enforced on August 1, 2025.
		With the enforcement mentioned above, the activation of user account lockout settings in wireless devices (WiFi-equipped machines) is mandated, and non-compliant machines will no longer be able to clear customs. Therefore, the following changes are made.
		 *EU Radio Equipment Directive - Delegated Act
		[Content of Change]
		1. The factory default settings for user account lockout are changed as follows.
		
		  - The user account lockout setting [Lockout Policy]:
		      OFF to ON **(changed this time)**
		  - Number of Retries until Locked: 3 times (not changed)
		  - Lockout Duration: 1 minute (not changed)
		  - Lockout Target: All **(changed this time)**
		
		 *When updating the machines in the field to this version, the settings are not automatically changed from those before the firmware update.
		
		2. The machine administrator and administrator password are changed from the common device password to the serial number.
		 *Regarding the administrator password, it has already been changed to the serial number.
		
		3. The mark is added to the label (REMARK section) on the outer box of the main unit for the identification of the old and new.
		
		(Identification of the old and new - Sample)
		
		Adding "**R**" to the REMARK field of the barcode label affixed on the outer box of the main unit.
		
		[Additional Information]
		- Compliance with the Radio Equipment Directive Delegated Act (RED-DA) does not affect machines already in operation in the field.
		- Change [2.] and [3.] apply only to the European specifications, with no changes to other specifications.
			2ZS-7263
			2ZS-7264
			2ZS-7196
			2ZS-7805
			2ZS-7729
			2ZS-7178
			2ZS-7170
			2ZS-7150
			2ZS-7285
			2ZS-7286
			2ZS-7132
			2ZS-7183
			2ZS-7154
			2ZS-7146
			2ZS-7187
			2ZS-7219
			2ZS-7210
			2ZS-7172
			2ZS-7204
			2ZS-7180
			2ZS-7141
			2ZS-7216
			2ZS-7155
			2ZS-7190
			2ZS-7162
			2ZS-7160
			2ZS-7287
			2ZS-7284
			2ZS-7130
			2ZS-7208
			2ZS-7173
			2ZS-7203
			2ZS-7211
			2ZS-7136
			2ZS-7145
			2ZS-7182
			2ZS-7131
			2ZS-7188
			2ZS-7159
			2ZS-7152
			2ZS-7138
			2ZS-7184
			2ZS-7193
			2ZS-7189
			2ZS-7165
			2ZS-7144
			2ZS-7199
			2ZS-7195
			2ZS-7158
			2ZS-7156
			2ZS-7161
			2ZS-7212
			2ZS-7185
			2ZS-7194
			2ZS-7133
			2ZS-7217
			2ZS-7200
			2ZS-7209
			2ZS-7129
			2ZS-7137
			2ZS-7218
			2ZS-7143
			2ZS-7260
			2ZS-7179
			2ZS-7166
			2ZS-7153
			2ZS-7278
			2ZS-7253
			2ZS-7427
			2ZS-7430
			2ZS-7431
			2ZS-7428
			2ZS-7432
			2ZS-7433
			2ZS-7429
			2ZS-7197
			2ZS-7167
			2ZS-7259
			2ZS-7279
			2ZS-7255
			2ZS-7802
				CONT

KYOCERA Document Solutions Inc.

KYOCERA

A **B** **C**

Service Bulletin

Ref. No. **2ZS-0034(P102)**

<Date> May 14, 2025

No	Items	Contents	CTL	FW
2	Change in factory default settings (Other than European specifications)	In compliance with the Radio Equipment Directive Delegated Act (RED-DA), the following default values are changed for all specifications. **[Content of Change]** The factory default settings for user account lockout are changed as follows. - The user account lockout setting [Lockout Policy]: OFF to ON **(changed this time)** - Number of Retries until Locked: 3 times (not changed) - Lockout Duration: 1 minute (not changed) - Lockout Target: All **(changed this time)** *When updating the machines in the field to this version, the settings are not automatically changed from those before the firmware update.	2ZS-7140 2ZS-7164 2ZS-7292 2ZS-7293 #170 #506 #208	CONT
3	Security enhancement (Compliance with RED-DA)	The following CVE (*) vulnerability ID is addressed as part of compliance with RED-DA. *CVE: Common Vulnerabilities and Exposures [CVE reference No.] CVE-2024-42236, CVE-2022-48912, CVE-2024-43871, CVE-2024-44987, CVE-2024-46829, CVE-2024-47707, CVE-2022-48978, CVE-2022-49021, CVE-2024-50301, CVE-2024-50195, CVE-2021-47146, CVE-2024-26801, CVE-2021-47269, CVE-2021-47397, CVE-2021-47416, CVE-2021-47418, CVE-2024-56659, CVE-2021-47119, CVE-2021-47466, CVE-2023-1077, CVE-2021-47612, CVE-2024-26704, CVE-2024-27388, CVE-2024-36941, CVE-2024-57938, CVE-2023-52646, CVE-2021-47405, CVE-2024-42106, CVE-2021-47103, CVE-2021-47117, CVE-2021-47118, CVE-2023-52612, CVE-2024-26805, CVE-2025-21638, CVE-2025-21639, CVE-2025-21640, CVE-2023-30774, CVE-2024-7006, CVE-2025-27113	2ZS-7297 2ZS-7299 2ZS-7301 2ZS-7302 2ZS-6582 2ZS-7305 2ZS-7306 2ZS-7307 2ZS-7308 2ZS-7309 2ZS-7310 2ZS-7311 2ZS-7312 2ZS-7313 2ZS-7314 2ZS-7315 2ZS-7316 2ZS-7317 2ZS-7318 2ZS-7348 2ZS-7298 2ZS-7319 2ZS-7320 2ZS-7321 2ZS-7322 2ZS-7323 2ZS-7325 2ZS-7327 2ZS-7328 2ZS-7349 2ZS-7350 2ZS-7351 2ZS-7353 2ZS-7354 2ZS-7355 2ZS-7356 2ZS-9917 2ZS-9916 2ZS-9820	CONT
4	Corrective measures for F248	When a specific invalid TIFF file is sent via FTP, system error F248 occurs. Therefore, it is corrected.	2ZS-10251 2XN-9735 C30-1324	CONT
5	Corrective measures for FD4F	When printing a PDF file stored with a password using a USB memory, system error FD4F occurs. Therefore, it is corrected.	2ZT-266 2ZT-268	CONT
6	Support for common use of CIS (DP-7160/DP-7170)	Along with the standardization of CIS with the next development models, support is provided for both the old and new CIS. *When the new CIS is used in combination with the old firmware, system error F124 or abnormal images might occur. *ENGINE firmware and DP-7160/DP-7170 firmware are planned to implement this change around June 2025.	2ZS-7098 2ZS-7097 2ZS-7096 C2G-9853 C2G-9854 2ZS-6628 2ZS-6799 #177	CONT
7	Corrective measures for modifying the scanning speed of the sending feature	The control for the sending feature's [Manual feed mode (DP)] setting is modified to be independent of the scanning speed. Therefore, it is corrected.	2ZS-5013 #178	CONT

KYOCERA Document Solutions Inc.

Service Bulletin

Ref. No. **2ZS-0034(P102)**

<Date> May 14, 2025

No	Items	Contents	CTL	FW
8	Corrective measures for failures of the barcode reading using HyPAS application, and the software keyboard input	When reading a barcode using the HyPAS application or inputting characters using the software keyboard, a part of the characters cannot be read, or it takes too long time to display the characters. Therefore, it is corrected.	KDCQA-20520 KDCQA-12923 2ZS-6627 2ZS-7220	CONT
9	Corrective measures for retrieval issues of [Configuration list] in KFS Manager	[Configuration list] cannot be retrieved using snapshots in KFS Manager. Therefore, it is corrected.	2ZT-267 C2G-9641	CONT
10	Corrective measures for USB formatting issues	After formatting the USB, the preview cannot be displayed for jobs stored using the USB memory. Therefore, it is corrected.	2ZS-10254 C2G-10333	CONT
11	Corrective measures for lock-up	When specific internal processes and sleep transition occur simultaneously, taking a snapshot in KYOCERA Fleet Services (KFS) causes the device to lock up. Therefore, it is corrected.	2XN-9802 2ZS-10411	CONT

[CVE reference No.]
CVE-2024-42236, CVE-2022-48912, CVE-2024-43871, CVE-2024-44987, CVE-2024-46829,
CVE-2024-47707, CVE-2022-48978, CVE-2022-49021, CVE-2024-50301, CVE-2024-50195,
CVE-2021-47146, CVE-2024-26801, CVE-2021-47269, CVE-2021-47397, CVE-2021-47416,
CVE-2021-47418, CVE-2024-56659, CVE-2021-47119, CVE-2021-47466, CVE-2023-1077,
CVE-2021-47612, CVE-2024-26704, CVE-2024-27388, CVE-2024-36941, CVE-2024-57938,
CVE-2023-52646, CVE-2021-47405, CVE-2024-42106, CVE-2021-47103, CVE-2021-47117,
CVE-2021-47118, CVE-2023-52612, CVE-2024-26805, CVE-2025-21638, CVE-2025-21639,
CVE-2025-21640, CVE-2023-30774, CVE-2024-7006, CVE-2025-27113

N00134424(CSD)/N00135260(ESD)

KYOCERA Document Solutions Inc.