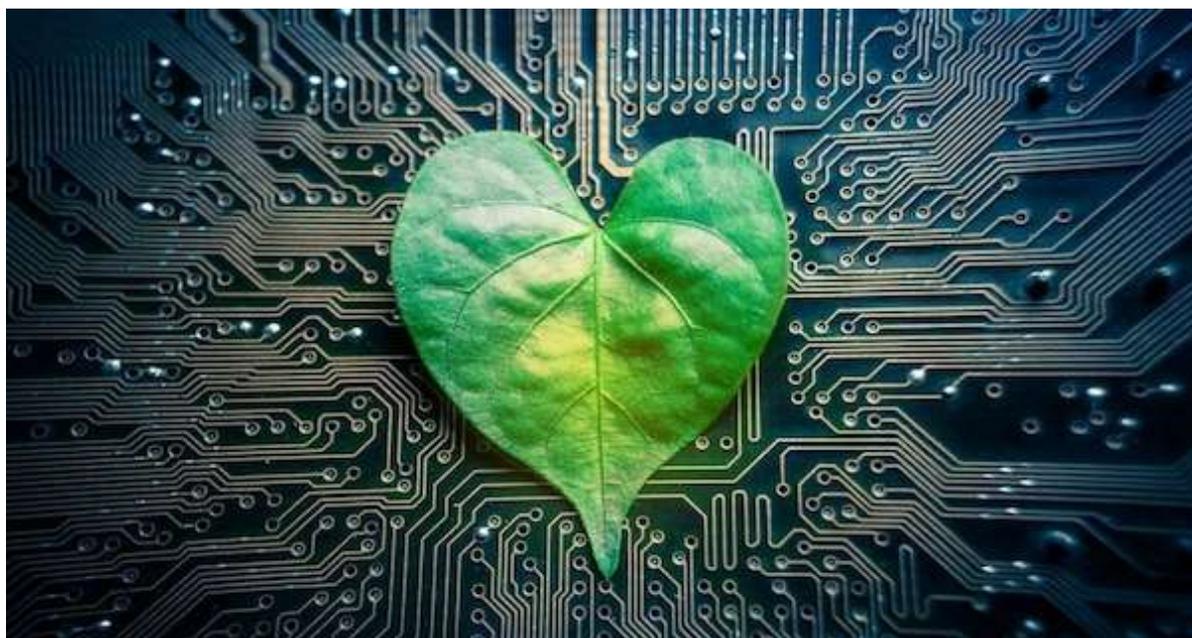




SERVICE NEWS

Ottobre 2022

Service Department | Ottobre 2022 | Milano



Gentile Business Partner,

Abbiamo il piacere di inviarLe la nostra Service News, con novità e aggiornamenti su tematiche tecniche.

Siamo a proporvi alcune novità in merito alla parte tecnica.



Disponibili corsi eLearning – Kyocera Cloud Print and Scan.

Kyocera Cloud Print and Scan migliora la visibilità dei costi relativi alla stampa sui dispositivi Kyocera e si rivolge alle aziende che desiderano installare e configurare facilmente una soluzione di gestione della stampa, senza aggiungere gli svantaggi dei costi relativi al server. Con Kyocera Cloud Print and Scan, i documenti vengono scansati direttamente nel cloud e vengono rimosse le spese in conto capitale per avere un server di stampa dedicato in loco, fornendo alle piccole e medie imprese la soluzione perfetta quando si tratta di una maggiore sicurezza e gestione dei documenti dei costi di stampa.

La gestione elettronica dei documenti consente infatti di:

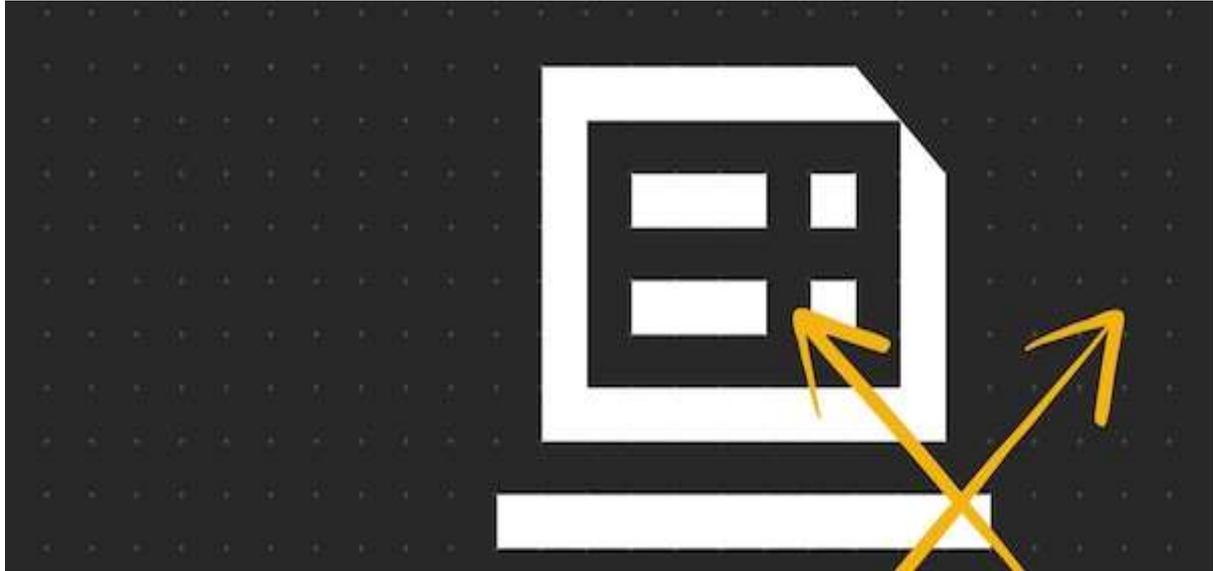
- ridurre gli spazi di archiviazione;
- ridurre i costi di gestione e snellire i processi interni;
- supporta la mobilità tra più sedi di lavoro differenzi struttando una infrastruttura Ibrida (sfuttando il Cloud);
- rilascio del lavoro con sicurezza (rilascio del lavoro con PIN, autenticazione, badge)
- compatibili con piattaforme Cloud come Google Drive, One Drive, Sharepoint, Box.

Accedendo ai corsi di formazione sul portale KYOCERA Academy:

Corsi eLearning:

- [Kyocera Cloud Print and Scan \(V1.0\) for Customer Admins E-Learning Ita](#)
- [Kyocera Cloud Print and Scan \(V1.2\) for Provider Admins](#)
- [Kyocera Cloud Print and Scan \(V1.2\) for Users](#)

[Accedi subito](#)



Problemi di autenticazione con SMTP Gmail / Office365

Errore di comunicazione SMTP Gmail/Office365 – Autenticazione a 2 fattori.

Recentemente Gmail e Office365 hanno elevato i criteri di sicurezza, quindi alcuni clienti che hanno abilitato la scansione tramite posta – “SCAN TO SMTP” stanno riscontrando problemi. La macchina rilascia l’errore di comunicazione 1102 (Errore di mancata comunicazione).

Tale problematica non è legata a Kyocera, ma all’account usato dal cliente che richiede l’autenticazione a due fattori.

Il metodo per risolvere tale problematica SMTP è data dall’imminente disattivazione da parte di Google e di Microsoft dell’autenticazione semplice, ma all’utilizzo della **PASSWORD PER L’APP**.

Sotto trovate i link ove vengono forniti le indicazioni step-by-step e tutti i dettagli del caso:

- **CREARE PASSWORD PER L’APP GMAIL:** [clicca qui](#)
- **CREARE PASSWORD PER L’APP OFFICE365:** [clicca qui](#)

Al seguente link troverete degli screen: (scarica la guida)

[Configurazione_SMTP – Password_per_APP – GMAIL_e_OFFICE365_pdf](#)

Una volta generata la “Password per app” bisogna inserirla all’interno della configurazione SMTP nel Command Center RX nella sezione “Password di acc.”:

SMTP

Protocollo SMTP :	On
	N.B. : Le impostazioni devono essere eseguite in SMTP (invio e-mail). Protocollo
Nome server SMTP :	<input type="text" value="smtp.office365.com"/> 
	N.B. : Per specificare il nome server dal nome del dominio, impostare il server DNS. TCP/IP
Numero porta SMTP :	<input type="text" value="587"/> (1- 65535)
Timeout server SMTP :	<input type="text" value="60"/> secondi
Protocollo autenticazione :	<input type="text" value="On"/> ▼
Autentica come :	<input type="text" value="Altro"/> ▼
Nome utente acc. :	<input type="text" value="l@dit.kyocera.com"/>
Password di acc. :	<input type="password" value="..... <<PASSWORD PER L'APP"/> 



IMPORTANTE: Modifiche su TASKalfa 2554ci/3554ci

Modifiche Hardware su alcune schede.

Sono state apportate modifiche sui modelli TASKalfa 2554ci/3554ci, si riconosce dalla matricola con fondo giallo. Questo implica che in caso di problemi su MAIN PWB o LASER (LK) bisogna ordinare il codice corretto e aggiornare il FW all'ultima release

Identification			
Month, Year	June 2021 and before	From July to October 2021	November 2021 and after
LSU, main PWB	Before change	After change	
Main unit serial number color	White		Yellow

(1) Identify with serial number

(2) Identify with label color (November 2021 and after)

Se ordinata la parte non corretta potrebbe generare i seguenti errori:

- C7941: LSU EEPROM error
- C4801: LSU type mismatch error
- C4101: BD initialization error
- C3800: AFE error

Tutti i dettagli sono presenti nei technical **SB**:

- **2XD-0010 (L072)**
- **2XD-0025 (L198)**
- **2XD-0048 (M059)**

No.	Old Part No.	New Part No.	Description	Q'ty		Compati bi lity		Remarks
				Old	New	Old	New	
LSU								
1	302L793112	302XD93090	LK-8351	1	1	X	X	Old name: LK-8350 *1, *2
ISU								
2	302XD93030	302XD93031	PARTS ISU ASSY SP	1	1	O	*4	*3
Main PWB								
3	302XD94080	302XD94220	PARTS PWB MAIN ASSY SP	1	1	X	X	KDAU, *2
4	302XD94070	302XD94210	PARTS PWB MAIN ASSY EU SP	1	1	X	X	KDE, TA/UTAX, OLIVETTI, *2
5	302XD94110	302XD94230	PARTS PWB MAIN ASSY US SP	1	1	X	X	KDA territory (KDA120V, KDA220V, CopyStar, KDBR) *2
6	302XD94200	302XD94240	PARTS PWB MAIN ASSY CN SP	1	1	X	X	KDCN, *2
Engine PWB								
7	302XD94090	302XD94091	PARTS PWB ENGINE ASSY SP	1	1	*4	O	
SHD PWB(DP)								
8	303TC94010	303TC94011	PARTS PWB SHD ASSY SP	1	1	O	*5	*3
DP PWB								
9	303TC94090	303TC94091	PARTS PWB DRIVER ASSY SP	1	1	*5	O	
10	303TD94030	303TD94031	PARTS PWB DRIVER ASSY SP	1	1	*5	O	



Mancato accesso al Command Center RX.

In alcuni casi a causa di versioni differenti del TLS manca la comunicazione tra il Browser e il dispositivo (MFP) – Soprattutto dispositivi meno recenti.
Tale integrazione è vincolata al fatto di sicurezza di rete ad connessione ad alcuni siti/pagine web.
Se si sta parlando dell'impossibilità da browser della connessione ad alcuni siti/pagine web, le modalità di accesso possono essere 3:

1. Command Center RX;
2. Kyocera Net Viewer;
3. Abilitazione del TLS1.2 lato browser (non tutti i browser).

02. Command Ceter RX:

The screenshot displays the 'Network Security Settings' page. The left sidebar contains a navigation menu with 'Security Settings' and 'Network Security' highlighted. The main content area is titled 'Secure Protocol Settings' and includes the following sections:

- SSL :** On Off. A note states: 'If you select Off, SSL cannot be used for communication.' A box labeled 'Check in TLS1.2' has an arrow pointing to the 'SSL3.0/TLS1.0' and 'TLS1.2' checkboxes.
- Serverside Settings :** ***TLS Version :** SSL3.0/TLS1.0 TLS1.1 TLS1.2
- Effective Encryption :** ARCFOUR DES AES 3DES AES-GCM. A box labeled 'Check in SHA2 (256/384)' has an arrow pointing to the 'SHA2(256/384)' checkbox.
- *Hash :** SHA1 SHA2(256/384)
- *HTTP Security :** Secure Only (HTTPS) Not Secure (HTTPS & HTTP)
- *IPP Security :** Secure Only (IPPS) Not Secure (IPPS & IPP)
- *Enhanced WSD Security :** Secure Only (Enhanced WSD over SSL) Not Secure (Enhanced WSD over SSL & Enhanced WSD)
- *eSCL Security :** Secure Only (eSCL over SSL) Not Secure (eSCL over SSL & eSCL)
- *RFST Security :** Secure Only (REST over SSL)

Se si sta parlando dell'impossibilità da browser della connessione ad alcuni siti/pagine web con livello sicurezza SSL/TLS inferiore a TLS1.2.

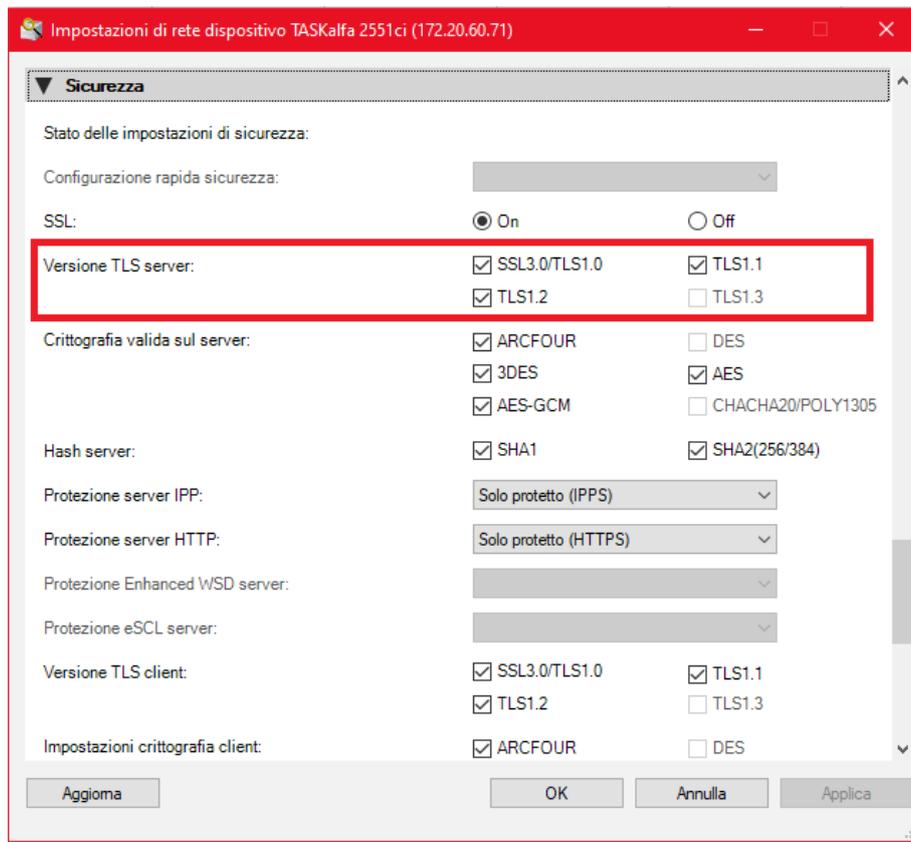
Questo tipo di gestione è stata attuata recentemente per un discorso di sicurezza (disabilitati i vecchi livelli SSL/TLS es. TLS1.0 / TLS1.1) su molti browser/PC (in generale anche lo stesso Windows può gestire questo tipo di comunicazione agendo in "Opzioni Internet" oppure in chiavi di registro che dipendono dallo stato del sistema operativo).

2. KYOCERA Net Viewer

Quindi se si ritiene una pagina poco sicura potrebbe mancare la comunicazione con la macchina (soprattutto con i vecchi modelli es.TA-2551ci), un modo per abilitare le versioni TLS è quello di passare da **KYOCERA Net Viewer**.

Andando sul modello in oggetto – [Fondamentale aggiornare il FW all'ultima release indipendentemente alla macchina in oggetto].

<Tasto destro sulla macchina> -> *Avanzate* -> *Impostazione di rete dispositivo* -> **Sicurezza**->





La Sicurezza è importante sulla tua MFP.

Protocollo Enhanced WSD > OFF

Usando il protocollo Enhanced WSD basato su SOAP c'è la possibilità che alcuni dispositivi rispondano senza l'autenticazione dell'utente e consentano l'acquisizione dei dati della rubrica registrata nonostante le impostazioni precedenti per richiedere l'autenticazione dell'utente.

Sono state implementati aggiornamento Firmware in merito. Se nel caso non fosse possibile è consigliato disattivare il protocollo Enhanced WSD e attivare il protocollo Enhanced WSD over SSL.

IRIS2020 Licenza velocità



License Speed

Licenza UG-36/UG-37/UG-38/UG-40/UG-41 per IRIS2020 solo licenza per l'upgrade della velocità delle macchine.

Utilizzando una licenza software (UG-XX) i modelli base possono essere aggiornati ad una velocità più elevata.

Modelli B/W

Modello Base	Velocità	Licenza	Nuovo Modello	Nuova Velocità
TASKalfa-5004i	50ppm	UG-41	TASKalfa- 7004i	70ppm BN
TASKalfa-5004i	50ppm	UG-40	TASKalfa- 6004i	60ppm BN

Modelli Colore

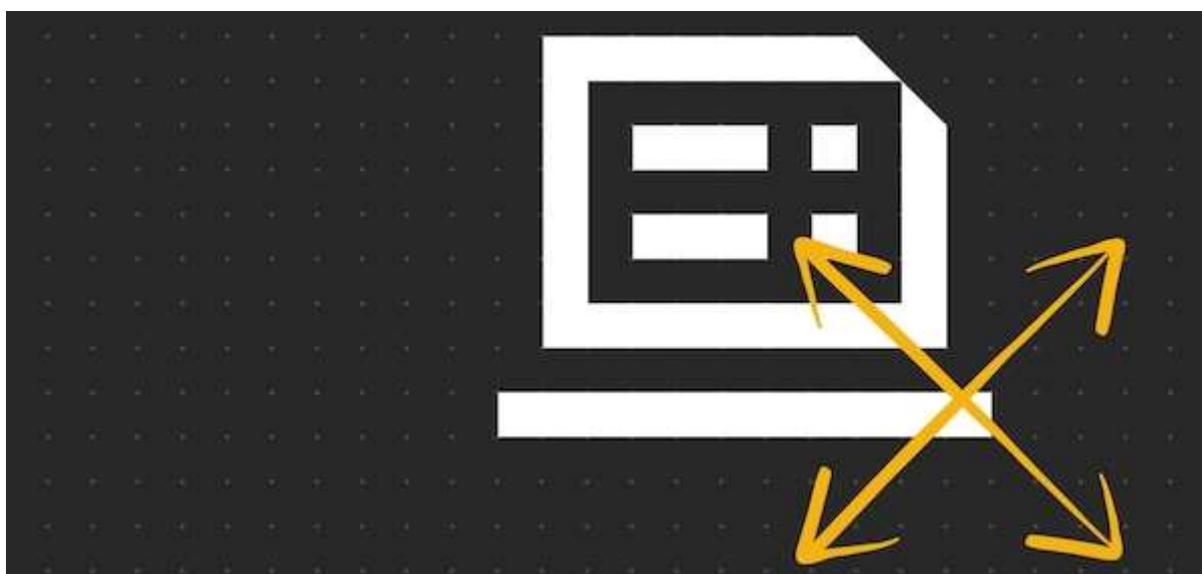
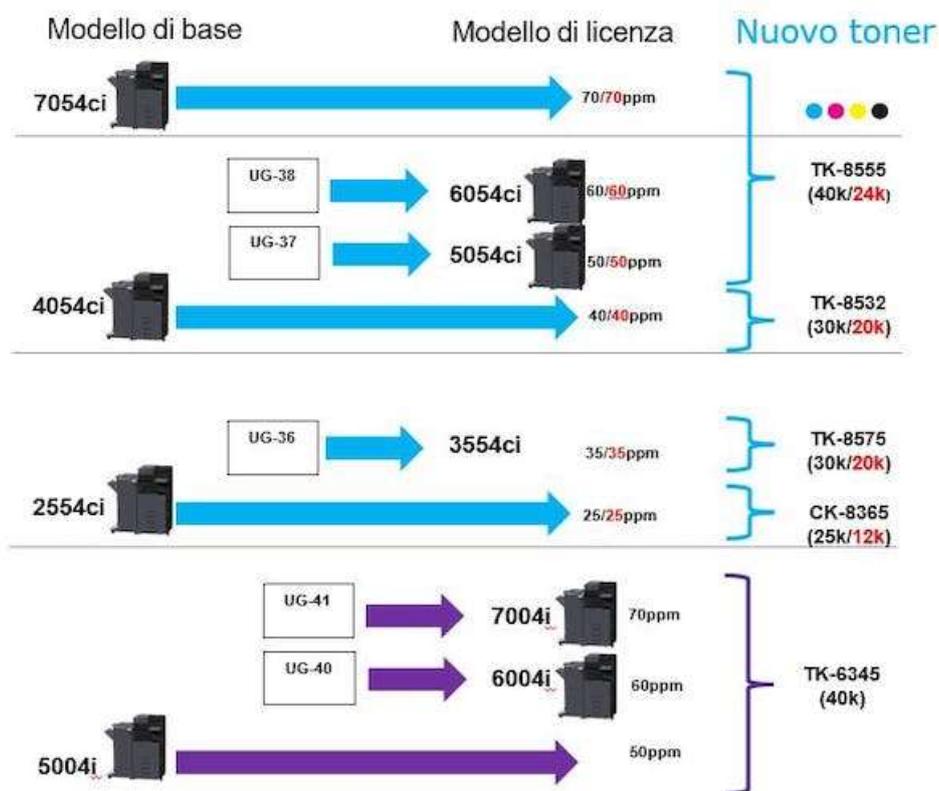
Modello Base	Velocità	Licenza	Nuovo Modello	Nuova Velocità
TASKalfa-4054ci	40ppm BN/COL	UG-38	TASKalfa- 6054ci	60ppm BN/COL
TASKalfa-4054ci	40ppm BN/COL	UG-37	TASKalfa- 5054ci	50ppm BN/COL
TASKalfa-2554ci	25ppm BN/COL	UG-36	TASKalfa- 3554ci	35ppm BN/COL

La velocità di stampa può essere aumentata inserendo nel pannello operativo la chiave di licenza emessa dall'ID del prodotto (es.UG-XX) acquistato in anticipo al momento dell'installazione.

- Se non si inserisce una chiave di licenza: è possibile utilizzare la velocità di stampa predefinita.
- Cambio di velocità di stampa (aumentata): È possibile attivare una licenza di velocità solo durante l'installazione.
- Velocità di stampa aumentata significa: Dopo aver ottenuto la chiave di licenza, inserirla nel pannello operativo per confermare la velocità. *(Nota) La velocità non può essere cambiata una volta che la velocità è stata determinata.*

Procedura d'installazione dell'UG. [Scarica la procedura d'installazione](#)

Sotto un riepilogo delle macchine BASE + Licenza UG:



Disponibili i nuovi bollettini tecnici:

Accedi direttamente con il download del bollettini tecnici, prima di cliccare il link consigliamo sempre di loggarvi e autenticarvi:

*Come consueto consigliamo di aggiornare il firmware della macchina per migliorare le prestazioni e ovviare a diverse problematiche. All'interno trovare il file "History" un file *.txt con un resoconto delle migliorie/modifiche apportate.*

Disponibili la nuova Documentazione Tecnica.

Aggiorna sempre la tua documentazione tecnica:

Subject	Version	Affected Model
Parts List	5	TASKalfa2020_2021_2320_2321
Parts List	6	TASKalfa_7353ci_8353ci
Parts List	5	TASKalfa2554ci_3554ci
Parts List	4	TASKalfa4004i_5004i_6004i_7004i
Parts List	4	TASKalfa4054ci_5054ci_6054ci_7054ci
Service Manual	E0	SM_TASKalfa-2553ci-3253ci-3553ci-4053ci-5053ci-6053ci
Service Manual	D0	SM_TASKalfa-2554-3554-6054-7054
Service Manual	E0	SM_TASKalfa 5003i-6003i
Service Manual	9	SM_TASKalfa 5004i-6004i-7004i
Service Manual	9	SM_TASKalfa-4054ci-5054ci-6054ci-7054ci
Service Manual	6	ECOSYS M3860idn_M3860idnf
Service Manual	6	ECOSYS P8060cdn
Service Manual	6	TASKalfa MZ4000i
Service Manual	6	ECOSYS P4140dn;PF-4110;CA-3100;PT-320;

Disponibili i nuovi aggiornamenti Firmware. (necessario autenticarsi prima).

SB	Oggetto	Modelli
M178_2V8_0057_SB	Firmware upgrade (Upgrade Pack 2VG_V2.09/2V8_V2.12/2VK_V2.12)	TASKalfa 6053ci, TASKalfa 5053ci, TASKalfa 4053ci TASKalfa 3253ci, TASKalfa 2553ci, TASKalfa 6003i, TASKalfa 5003i, TASKalfa 4003i
M200_2TA_0027_SB	Firmware upgrade (CONTROLLER VER.003.401)	M3660idn, M3655idn, M3655idn/A, M3645idn, M3145idn, M3645dn, M3145dn
M183_2XN_0027_SB	Firmware upgrade (Upgrade Pack 2XN_V2.11, 2XV/2XT_V2.09)	TASKalfa 8353ci, TASKalfa 7353ci, TASKalfa 9003i, TASKalfa 8003i, TASKalfa 7003i
M217_2V8_0058_SB	Firmware upgrade (Upgrade Pack 2VG_V2.10/2V8_V2.13/ 2VK_V2.13)	TASKalfa 6053ci, TASKalfa 5053ci, TASKalfa 4053ci, TASKalfa 3553ci, TASKalfa 3253ci, TASKalfa 2553ci, TASKalfa 6003i, TASKalfa 5003i, TASKalfa 4003i
M218_2XN_0028_SB	Firmware upgrade (Upgrade Pack 2XN_V2.12, 2XV/2XT_V2.10)	TASKalfa 8353ci, TASKalfa 7353ci, TASKalfa 9003i, TASKalfa 8003i, TASKalfa 7003i
M214_2Y8_0008_SB	Firmware upgrade (MAIN VER. 2YW_2000.001.101 etc.)	MA2000, MA2001, MA2000w, MA2001w, PA2000, PA2001, PA2000w, PA2001w

M163_2WL_0008_SB	Firmware upgrade (CONTROLLER Ver.003.504)	TASKalfa 308ci
M160_2ZS_0004_SB	Firmware upgrade (CONTROLLER Ver.002.452)	TASKalfa MZ4000i, TASKalfa MZ3200i
M145_2WF-0012_SB	Firmware upgrade (CONTROLLER VER.003.802) (Except Russia and Belarus...)	ECOSYS M3860idnf, ECOSYS M3860idn
M143_2TA_0026_SB	Firmware upgrade (CONTROLLER VER.003.302)	M3660idn, M3655idn, M3145idn, M3645idn, M3145dn, M3645dn
M106_2V6_0030_SB	Firmware upgrade (Upgrade Pack Ver. 2V6_V2.02)	TASKalfa 4012i, TASKalfa 3212i
M136_2TP_0022_SB	Firmware upgrade (CONTROLLER VER.003.802)	P3160dn, P3155dn, P3150dn, P3145dn, P3260dn
M141_2TV_0039_SB	Firmware upgrade (CONTROLLER VER003.302)	P6230cdn, P6235cdn, P7240cdn, M6230cidn, M6630cidn, M6235cidn, M6635cidn, TASKalfa 351ci, TASKalfa 352ci
M149_2P1_0021_SB	Firmware upgrade (Upgrade Pack V2.04, etc.)	M4132idn, TASKalfa 2520i, TASKalfa 2510i, M4125idn, M4230idn, M4226idn, TASKalfa 4020i
M150_2P3_0027_SB	Firmware upgrade (Upgrade Pack V2.04, etc.)	M8130cidn, M8124cidn, M8228cidn, M8224cidn, TASKalfa 3060ci
M119_2XD_0054_SB	Firmware upgrade (Upgrade Pack 2XD/2XC/2XF_V.3.01)	TASKalfa 7054ci, TASKalfa 6054ci, TASKalfa 5054ci, TASKalfa 4054ci, TASKalfa 3554ci, TASKalfa 2554ci, TASKalfa 7004i, TASKalfa 6004i, TASKalfa 5004i, TASKalfa 4004i
M138_2TA_0025_SB	Firmware upgrade (ENGINE VER.006.001)	M3660idn, M3655idn, M3145idn, M3645idn, M3145dn, M3645dn
M146_2XD__0056_SB	Firmware upgrade (Upgrade Pack 2XD/2XC/2XF_V.3.02)	TASKalfa 7054ci, TASKalfa 6054ci, TASKalfa 5054ci, TASKalfa 4054ci, TASKalfa 3554ci, TASKalfa 2554ci, TASKalfa 7004i, TASKalfa 6004i, TASKalfa 5004i, TASKalfa 4004i, DF-7140
M125_2S0_0051_SB	Firmware upgrade (Upgrade Pack MFP V2.10 / Printer V2.09)	M2135dn, M2635dn, M2635dw, M2735dw, M2040dn, M2540dn, M2540dw, M2640idw, P2235dn, P2235dw, P2040dn, P2040dw, P2230dn M2235dn, M2735dn, M2835dw, P2335dn, P2335dw, P2335d
M126_2R7_0053_SB	Firmware upgrade (Upgrade Pack MFP V2.09 / Printer V2.08)	M5526cdw, M5526cdn, M5521cdw, M5521cdn, M5525cdn, M5520cdw, M5520cdn, M5021cdn, P5026cdw, P5026cdn, P5021cdw, P5021cdn, P5025cdn, P5020cdw, P5020cdn, P5018cdn



Disponibili le nuove date dei corsi tecnici.

Sono stati pubblicati le date dei corsi per il quarto trimestre 2022 in KYOCERA Academy, consultabili nel catalogo corsi, e disponibili per tutte le nostre sedi di training: **Milano** e **Roma** (per i corsi in Aula).

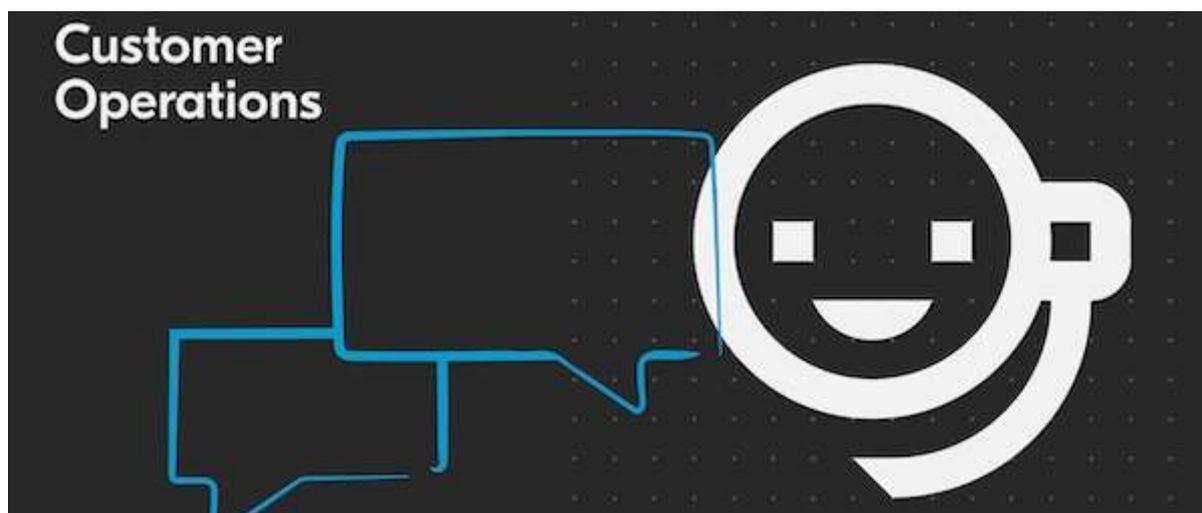
Si ricorda che per quanto concerne eventuali corsi per cui non sono state pianificate date (es. corsi a richiesta oppure corsi di Soluzioni), è comunque possibile prenotarsi nella "Lista di Attesa".

Per accedere ai calendari: [CALENDARIO CORSI*](#).

* i corsi potrebbero essere "sospesi" o "cancellati" in casi particolari per salvaguardare la salute dei partecipanti o in casi non si sia raggiunto il numero minimo di partecipanti.

NOVITA':

A Calendario sono stati integrati anche le date per i corsi WEB EX (Da remoto) sono solo su prenotazione.



Il nostro **Service Desk** è un importante riferimento per l'assistenza tecnica di primo livello ed è perciò sempre aggiornato sui prodotti e le nuove tecnologie compreso il Supporto alle Soluzioni (tasto 3).

Il numero di telefono per poter ricevere assistenza tecnica è:

02 94300085

- **Tasto 1** – Dealer, Brand Dealer e Partner
- **Tasto 2** – Macchine in Garanzia o contratti in manutenzione (End-User e Diretta Privata)
- **Tasto 3** – Soluzioni per Dealer, Brand Dealer e Partner

Per contatti via e-mail scrivere a: service.desk@dit.kyocera.com

Dario Terzoli
Senior Manager Product Support
Technical Competence Center

ISCRIVITI AI NOSTRI SOCIAL

