

Soluții de securitate de la Epson

Soluții de securitate pentru imagistică de afaceri

Gamele WorkForce
Enterprise 2 și AM-C



EPSON®

Asigurați securitatea rețelei oriunde se utilizează echipamentul de imprimare

Este ușor să treceți cu vederea unele măsuri de securitate importante pentru orice dispozitiv conectat în rețea în cadrul companiei dvs. Și, deși poate că nu v-ați gândit la acest lucru, multifuncționalele (MFP), scanerile și orice alt echipament conectat direct sau în rețea, pot fi expuse problemelor de securitate.

Evoluția înregistrată în domeniul muncii de la domiciliu și în sistem hibrid a sporit acest risc. Un studiu realizat de Quocirca¹ a arătat că, deși 70% dintre factorii de decizie din domeniul IT consideră că imprimarea este esențială sau foarte importantă pentru afacerea lor, 31% dintre aceștia sunt îngrijorați de riscurile de securitate asociate cu utilizarea echipamentelor de imprimare de la distanță sau la domiciliu și doar 19% sunt complet încrezători că infrastructura lor de imprimare este sigură.

În condițiile în care costul mediu al problemelor datorate unei deficiențe de securitate a datelor legate de componenta de imprimare se ridică la 865.000 €, subiectul asigurării securității nu trebuie tratat cu superficialitate.

Cu toate acestea, datorită abordării Epson în ceea ce privește securitatea imprimantelor, acesta este un risc pe care îl puteți reduce, indiferent de locul în care se utilizează imprimantele pentru afaceri.



70%

dintre factorii de decizie din domeniul IT consideră că imprimarea este esențială sau foarte importantă pentru compania lor

31%

sunt îngrijorați de riscurile de securitate asociate cu imprimarea la distanță sau la domiciliu

19%

se simt complet încrezători că infrastructura lor de imprimare este sigură

*Pe baza valorii de 743.000 £ stabilită de Quocirca și convertită în 865.000 € utilizând rata de schimb valutar de pe xe.com la data de 09.01.2024.

Abordarea Epson în materie de securitate

Consolidarea capacităților de rețea ale echipamentelor dvs. este esențială pentru abordarea noastră în materie de securitate. Pentru a asigura securitatea dispozitivelor Epson pe tot parcursul ciclului de viață al acestora, fiecare imprimantă Epson WorkForce este construită pe trei principii de bază:

1. Securitatea produselor reprezintă baza pentru calitate
2. Informațiile și cunoștințele despre securitate sunt partajate în mod activ, astfel încât să fiți mereu la curent cu noutățile
3. Vulnerabilitățile sunt evaluate în mod constant pentru a asigura nivelul maxim de protecție al echipamentelor

Caracteristici de securitate concepute pentru a vi se potrivi

Datele protejate și rețelele securizate fac parte din dotarea standard a multifuncționalelor Epson, folosind funcții care vă pot ajuta în ceea ce privește Regulamentul general privind protecția datelor (GDPR) și responsabilitatea socială a întreprinderilor (CSR). Aceste măsuri de securitate, integrate direct în produsele noastre, vă oferă garanția că afacerea dvs. îndeplinește cerințele de securitate.

Imprimare și scanare securizată

Puteți să asigurați confidențialitatea documentelor și să împiedicați persoanele neautorizate să vizualizeze documentele rezultate nesupravegheate, trimițând documentele dvs. ca „Lucrare confidențială” din driverul imprimantei.

Restricționarea accesului la funcțiile echipamentului se poate realiza prin blocarea panoului frontal.

Comunicare securizată

Filtrați adresele IP, serviciile, numerele de port de recepție și de transmisie care au acces la dispozitivele Epson. Puteți, de asemenea, cripta toate comunicările în rețea cu ajutorul funcției IPsec.

Pe echipament

Cu funcția Epson Device Admin, securitatea la nivel de echipament devine mai ușor de gestionat. Compatibilă cu o gamă largă de imprimante conectate în rețea, aceasta permite utilizatorilor să controleze totul prin intermediul unei interfețe inteligente și intuitive.

Protecție PDF

Adăugați posibilitatea de a proteja prin parolă³ fișierele PDF scanate pentru a preveni vizualizările neautorizate, editarea și imprimarea documentelor.

Prelucrare documente și gestionare date

Gestionați mai multe sarcini în mod centralizat, de la profilurile sarcinilor de scanare la drepturile de acces ale utilizatorilor. Administratorii pot gestiona în mod centralizat o diversitate de sarcini, de la profiluri de lucrări de scanare până la drepturi de acces pentru utilizatori. Administratorii IT au posibilitatea de a controla drepturile de acces pentru lucrări în diverse moduri, incluzând carduri de identitate, date de autentificare, parole și coduri PIN.

Integrare perfectă în infrastructura IT cu baza de date locală a utilizatorilor sau servicii de directoare, precum Microsoft EntraID și Google Cloud Directory.



Epson
Solutions Suite

Pentru mai multe informații despre soluțiile Epson accesați <https://support.epson.net/stories/en/>

Securitate recunoscută la nivel mondial

În cadrul Epson, ne evaluăm securitatea la scară globală. Respectăm standardul ISO/IEC 15408³, denumit și Criterii comune (Common Criteria, CC), care este un standard internațional pentru măsurile de securitate care vizează produsele și sistemele IT, și dispunem de certificarea CCRA, care demonstrează că produsul este certificat în conformitate cu Sistemul japonez de evaluare și certificare a securității tehnologiei informației (Japan Information Technology Security Evaluation and Certification Scheme, JISEC).



Securitate rețea

Având în vedere că securitatea rețelei reprezintă o prioritate majoră, administratorii pot stabili permisiuni și restricții individuale pentru o gamă largă de sarcini de rețea. Cu imprimantele noastre WorkForce Enterprise 2, administratorii pot, de asemenea, să filtreze adresele IP, tipurile de servicii, porturile de recepție și transmisie, utilizând funcția IP Sec/Filtrare IP. Și aceasta în timp ce ei decid dacă să accepte sau să blocheze anumite adrese IP. De asemenea, dispozitivele noastre acceptă criptarea e-mailurilor SNMPv3 și TLS1.3.



Protejarea multifuncționalului dvs.

Pentru o protecție suplimentară a echipamentelor dvs., puteți alege să blocați accesul de la un computer prin USB și să dezactivați interfețele pentru carduri de memorie și memorii USB. De asemenea, puteți utiliza marcajul anti-copiere² pentru a preveni duplicarea neautorizată a documentelor originale și criptarea fișierului PDF² pentru a vă asigura că documentele digitale sunt protejate.



Imprimare/scanare securizată

Opțiunea „Lucrare confidențială” vă permite să asigurați confidențialitatea documentelor și să împiedicați orice vizualizare nedorită atunci când acestea sunt nesupravegheate.



WPA3

Cele mai recente multifuncționale Epson sunt compatibile cu WPA3², care reprezintă cea mai recentă tehnologie de autentificare și criptare pentru WiFi (LAN wireless), oferind companiilor o protecție avansată pentru datele transmise prin intermediul rețelei wireless.



Protecție documente

Sporiți productivitatea și monitorizați modul utilizare la tipărire, scanare și copiere în mod securizat, prin autentificarea utilizatorilor.



Control acces

Autentificare utilizator și restricții funcționale.



Protecție echipament

Verificarea semnăturii de firmware, inițializare securizată și detecție malware.



Protecție date utilizator

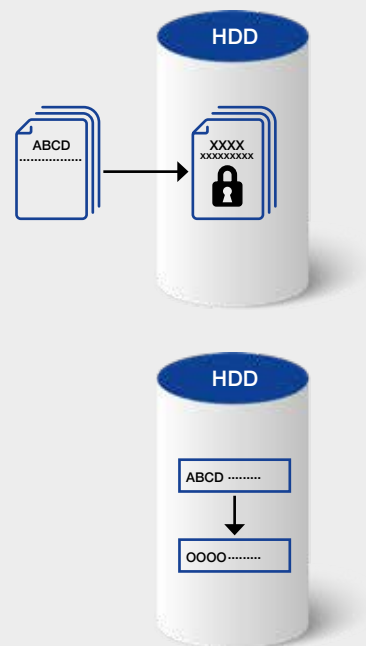
De asemenea, puteți seta parole unice pentru cutiile², documentele și agendele partajate de pe imprimantele Epson. Pentru o securitate completă, datele sunt șterse din imprimantă imediat ce lucrările s-au finalizat și atunci când alimentarea este oprită. În cazul în care dispozitivul dispune de un hard-disk, toate datele sunt criptate; de asemenea, informațiile sunt șterse după fiecare activitate de imprimare. Pentru o protecție suplimentară, administratorul are posibilitatea de a suprascrise hard-disk-ul. Aflați mai multe informații din ghidul nostru de securitate disponibil pe adresa epson.ro/bi-security-solutions

Protecția datelor

Criptarea HDD, ștergerea în siguranță a datelor de pe HDD, modulul Trusted Platform Module (TPM) și criptarea parolelor.

Criptarea datelor salvate pe HDD

Protejăm întotdeauna informațiile clienților prin criptare, atunci când salvăm date pe o unitate HDD internă a unui multifuncțional. Criptarea informațiilor previne accesul neautorizat și atacurile rău intenționate la datele personale, în cazul în care unitatea HDD este pierdută sau furată. Unitatea HDD este prevăzută cu o unitate de auto-criptare, iar informațiile din documente sunt criptate prin intermediul tehnologiei AES-256.



Ștergere secvențială date privind lucrarea

Atunci când această funcție este activată, datele șterse de pe hard-disk² sunt suprascrise în diverse moduri, pentru a preveni restaurarea. Există mai multe opțiuni:

1. Ștergere rapidă: Cheia de criptare este modificată pentru a împiedica restaurarea datelor șterse.
2. Ștergere secvențială securizată: Cheia de criptare este modificată iar datele șterse de pe hard-disk sunt suprascrise cu „0” pentru a se asigura că acestea nu pot fi recuperate.

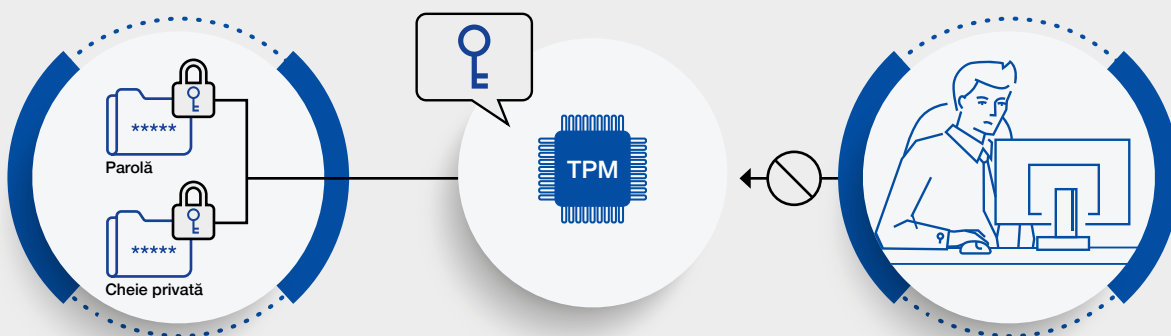
Vă rugăm să consultați manualul de utilizare al produsului dvs. pentru o explicație detaliată privind ștergerea datelor de lucru.

TPM

În cazul modelelor cu TPM (Trusted Platform Module), nivelul de securitate se îmbunătățește după cum urmează:

- Cheile de criptare pentru restabilirea parolelor criptate și a informațiilor privind cheia privată sunt stocate pe cipul TPM.
- Cipul TPM poate fi protejat împotriva analizelor neautorizate la nivel hardware, fiind imposibil ca acesta să fie accesat din exteriorul imprimantei.
- Pentru comunicarea cu browser-ul (Web Config.) sunt utilizate, ca și chei de sesiune, numere aleatorii reale ale cipurilor TPM.
- Pentru generarea cheilor de autentificare pentru unitatea HDD criptată sunt utilizate numere aleatorii reale ale cipurilor TPM.

Multifuncționalul dispune de un cip TPM 2.0.



	WorkForce Enterprise	AM-C	
Denumire produs	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000	AM-C400/C550
Tip	A3	A3	A4
Securitate rețea			
Comunicare TLS	✓	✓	✓
TLS1.1, TLS1.2, TLS1.3	✓	✓	✓
Controlul permisiunilor și excluderilor de protocol	✓	✓	✓
IPsec/Filtrare IP	✓	✓	✓
IKEv1, IKEv2	✓	✓	✓
ESP:AES-CBC-128/AES-CBC-192/AES-CBC-256/3DES	✓	✓	✓
ESP:AES-GCM-128/AES-GCM-192/AES-GCM-256	✓	✓	✓
ESP/AH:SHA-1/MD5	✓	✓	✓
ESP/AH:SHA-256/SHA-384/SHA-512	✓	✓	✓
Autentificare IEEE802.1X	✓	✓	✓
EAP-TLS, PEAP-TLS	✓	✓	✓
PEAP/MSCHAPv2	✓	✓	✓
EAP-TTLS	✓	✓	✓
AES128/AES256/3DES/RC4	✓	✓	✓
SNMPv3	✓	✓	✓
WPA3	✓	✓	✓
Separare între interfețe	✓	✓	✓
Protejarea multifuncționalului dvs.			
Blocare conexiune USB de la computer	✓	✓	✓
Dezactivare interfață externă	✓	✓	✓
Mod tratare viruși introduși prin memoria USB	✓	✓	✓
Securitate imprimare/scanare			
Lucrări confidențiale	✓*2	✓	✓
Model anti-copiere ²	✓	✓	✓
Watermark ²	✓	✓	✓
Criptare PDF	✓	✓	✓
S/MIME	✓	✓	✓
AES-128/AES-192/AES-256/3DES	✓	✓	✓
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✓	✓	✓
Restricții domeniu	✓*1	✓	✓
Parolă de autorizare pentru opțiunile scanare în fișierul de rețea/FTP, scanare către e-mail și notificare prin e-mail	-	✓*1	✓
Dezactivare implicită a accesului la fișiere din PDL	✓*1	✓	✓
Imprimare securizată	✓	✓	✓
Securitate fax³			
Restricții apelare directă	✓	✓	✓
Confirmare listă de adrese	✓	✓	✓
Detectare ton de apel	✓	✓	✓
Măsuri împotriva faxurilor abandonate	✓	✓	✓
Raport confirmare transmitere	✓	✓	✓
Ștergere date de backup pentru faxurile recepționate	✓	✓	✓
Limitare transmitere către mai mulți destinatari	✓	✓	✓
Securitate imprimantă			
Actualizări automate de firmware	✓	✓	✓
Protecție împotriva actualizărilor ilegale de firmware	-	✓	✓
Inițializare securizată	-	✓	✓
Detectare infiltrare malware	✓*1	✓	✓
Măsuri de securitate atunci când se renunță la o imprimantă			
Revenire la setările implicite din fabrică	✓	✓	✓
Certificare și standarde de securitate			
ISO15408/IEEE2600.2™	✓	✓	-

	WorkForce Enterprise	AM-C	
Denumire produs	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000	AM-C400/C550
Tip	A3	A3	A4
Funcții de securitate prin compatibilitate cu un program software terț			
Model compatibil cu Open Platform	✓	✓	✓
Epson Print Admin (EPA)/EPA Serverless			
Autentificare utilizatori prin carduri de identitate/credențiale de autentificare/cod PIN	✓	✓	✓
Control complet al acțiunilor dispozitivelor pentru fiecare persoană	✓	✓	✓
Personalizare meniu MFP	✓	✓	✓
Imprimare distribuită în rețea și imprimare directă	✓	✓	✓
Scanare și trimitere către mine (e-mail, folder)	✓	✓	✓
Scanare către servicii cloud (OneDrive for Business, SharePoint online, Teams și Google Drive) ⁸	✓	✓	✓
Scanare în fișiere PDF protejate prin parolă	✓	✓	✓
Setări avansate flux de lucru pentru scanare ⁶	✓	✓	✓
Imprimare fără drivere prin servicii cloud (OneDrive for Business, SharePoint Online și Teams) ⁸	✓	✓	✓
Sincronizare cu serviciul de directoare (LDAP, Open LDAP, Microsoft EntraID, Microsoft Entra DS, Google secure LDAP & Google cloud directory) ⁸	✓	✓	✓
Rapoarte - Setare protecție utilizator - Ascundere denumire fișier	✓	✓	✓
Politică privind parolele, blocare cont ⁶	✓	✓	✓
Reguli și politici privind imprimarea ⁶	✓	✓	✓
Monitorizare și raportare	✓	✓	✓
Cotă ⁸	✓	✓	✓
Imprimare mobilă securizată (AirPrint și Mopria) ⁷	-	✓	✓
Protecție date utilizator			
Securitate casetă	✓	✓	✓
Protejare agendă de contacte	✓	✓	✓
Gestionare date procesată de un multifuncțional	✓	✓	✓
Criptare date salvate pe hard-disk	✓	✓	✓
Ștergere secvențială date privind lucrarea	✓	✓	✓
Criptare parolă	✓	✓	✓
TPM	✓*4	✓	✓
Hard-disk în oglindă	-	✓	-
Limitare operațională			
Blocare panou	✓	✓	✓
Control acces	✓	✓	✓
Imprimare/scanare pe bază de autentificare ⁵	✓	✓	✓
Politică privind parolele	✓	✓	✓
Jurnal de audit	✓	✓	✓

1. Pentru a utiliza această funcție, actualizați firmware-ul imprimantei la cea mai recentă versiune.

2. Acceptă doar driver-ul de imprimare pentru Windows.

3. Funcție disponibilă doar atunci când este instalată placa de fax opțională.

4. În funcție de regiune, este posibil ca funcția respectivă să nu fie disponibilă. Vă rugăm să contactați biroul local de vânzări pentru a verifica disponibilitatea în țara dvs.

5. Necesită o metodă de imprimare pe bază de autentificare.

6. Valabil exclusiv pentru Epson Print Admin.

7. Valabil exclusiv pentru Epson Print Admin Serverless.

8. Se aplică pentru Epson Print Admin și exclusiv pentru anumite produse pe Epson Print Admin Serverless

**Pentru informații suplimentare, contactați reprezentantul
dvs. de vânzări Epson.**

Nume:

Telefon:

E-mail:

EPSON și WorkForce sunt mărci comerciale înregistrate, iar EPSON Exceed Your Vision este o marcă grafică înregistrată a Seiko Epson Corporation. Toate celelalte produse și mărci sunt denumiri comerciale de mărci și/sau denumiri comerciale de mărci înregistrate ale companiilor care le dețin. Epson nu își asumă niciunul dintre drepturile asupra acestor mărci.

1. „Peisajul securității imprimării, 2023 - securizarea infrastructurii de imprimare în contextul unor amenințări în creștere”, Quocirca, mai 2023.
2. Pentru o listă completă a specificațiilor produselor, vizitați www.epson.ro/bi-security-solutions.
3. ISO/IEC 15408 nu vine cu o configurație standard. Sunt necesare un firmware special și un proces de configurare special. Cu excepția AM-C400/550.
4. Aplicabilitate pentru gama AM-C



Vă rugăm să reciclați
responsabil

EPSON Europe BV, Sucursala România
AFI TECH PARK 1
Bulevardul Tudor Vladimirescu, nr. 29A, etaj 4
Sector 5, 050881, București
Telefon: +40 21 402 5024
Fax: +40 21 402 5020
www.epson.ro

Call Center Epson
Telefon: +40 21 794 0809
Luni – Vineri, 09:00 – 18:00



Mărcile comerciale și mărcile înregistrate sunt proprietatea companiei Seiko Epson Corporation sau a deținătorilor respectivi. Informațiile privind produsul se pot modifica fără anunț prealabil.