Solutions d’impression professionnelles sécurisées

Gammes WorkForce Enterprise 2
et AM-C

EPSON®

Protégez la sécurité du réseau partout où des impressions sont effectuées

En ce qui concerne les périphériques professionnels en réseau, d'importantes mesures de sécurité sont souvent négligées. Les utilisateurs n'y pensent peut-être pas, mais les solutions d'impression, les scanners et tout autre type de périphérique connecté ou en réseau peuvent présenter des failles de sécurité.

L'essor du télétravail et du travail hybride n'a fait qu'amplifier ce risque. Une étude menée par Quocirca[1] a révélé que, bien que 70 % des décideurs informatiques considèrent l'impression comme essentielle ou très importante pour leur entreprise, 31 % d'entre eux sont préoccupés par les risques de sécurité associés à l'impression à distance ou à domicile et seulement 19 % font totalement confiance à la sécurité de leur infrastructure d'impression.

Le coût moyen d'une violation de données liée à l'impression s'élevant à 865 000 €*, c'est là un problème qui ne peut être ignoré.

Grâce à l'approche d'Epson en matière de sécurité des solutions d'impression, vous pouvez cependant atténuer ce risque, où que vous réalisiez vos impressions professionnelles.

70 %

des décideurs informatiques considèrent l'impression comme essentielle ou très importante pour leur entreprise

31 %

sont préoccupés par les risques de sécurité associés à l'impression à distance ou à domicile

19 %

font totalement confiance à la sécurité de leur infrastructure d'impression

*Sur la base d'un montant de 743 000 £, tel qu'indiqué par Quocirca et converti en 865 000 € en utilisant le taux de change de xe.com au 09/01/2024.

L’approche sécurité selon Epson

Renforcer les capacités réseau de vos périphériques est l’élément clé de notre approche sécurité. Pour garantir la sécurité des solutions d’impression Epson tout au long de leur cycle de vie, chaque modèle Epson WorkForce est construite en fonction de trois principes fondamentaux :

1. La qualité repose sur la sécurité des produits.
2. Les informations et les connaissances sur la sécurité sont activement partagées afin que vous disposiez toujours des dernières mises à jour.
3. Les vulnérabilités sont constamment examinées pour optimiser la protection des périphériques.

Des fonctions de sécurité conçues pour vous

La protection des données et la sécurisation des réseaux sont disponibles en standard sur les multifonctions Epson, avec des fonctionnalités qui favorisent la conformité au règlement général sur la protection des données (RGPD) et à votre politique de Responsabilité Sociétale des Entreprises. Ces mesures de sécurité, intégrées directement à nos produits, garantissent le respect des exigences de sécurité de votre entreprise.

Impression et numérisation sécurisées

Vous pouvez garantir la confidentialité des documents et empêcher les personnes non autorisées de consulter des impressions réalisées et non récupérées sur la solution d’impression en soumettant vos documents en tant que « travaux confidentiels » à partir du pilote d’impression.

La restriction de l’accès aux fonctions de la solution d’impression peut être appliquée à l’aide du système de verrouillage du panneau de commandes.

Communication sécurisée

Filtrez les adresses IP, les services et les numéros des ports de réception et de transmission qui ont accès aux solutions d’impression Epson. Vous pouvez également crypter toutes les communications réseau à l’aide de la fonction IPSec.

Sur le périphérique

Epson Device Admin facilite la gestion de la sécurité sur les matériels. Compatible avec notre large gamme de solutions d’impression en réseau, il permet aux administrateurs de tout contrôler via une interface intelligente et intuitive.

Protection des PDF

Ajoutez une fonctionnalité de protection par mot de passe[3] aux fichiers PDF numérisés pour les protéger contre les consultations non autorisées et prévenir les modifications et l’impression de ces documents.

Traitement des documents et gestion des données

Les administrateurs peuvent gérer de nombreuses tâches de façon centralisée, des profils de numérisation aux droits d’accès des utilisateurs. Les administrateurs informatiques ont la possibilité de contrôler les droits d’accès aux tâches de plusieurs façons, notamment à l’aide de badges, de noms d’utilisateur et mots de passe, et de codes.

Intégration simple dans l’infrastructure informatique avec la base de données d’utilisateurs locale ou les services d’annuaires tels que Microsoft EntraID et Google Cloud Directory.

Epson Solutions Suite

Pour en savoir plus sur les solutions Epson, consultez https://support.epson.net/stories/en/

Un niveau de sécurité reconnu dans le monde entier

Chez Epson, nous définissons nos mesures de sécurité conformément à des exigences mondiales. Nous respectons la norme ISO/IEC 15408[3], également appelée Common Criteria (CC, critères communs), une norme internationale s'appliquant aux mesures de sécurité pour les produits et systèmes d'information, et la certification CCRA qui atteste que le produit a été certifié conformément au Japan Information Technology Security Evaluation and Certification Scheme (JISEC).

④

Sécurité réseau

La sécurité du réseau étant une priorité majeure, les administrateurs peuvent configurer des autorisations et des restrictions individuelles à de nombreuses actions sur le réseau. Sur nos multifonctions WorkForce Enterprise 2, les administrateurs peuvent également filtrer les adresses IP, les types de service et les numéros des ports de réception et de transmission à l'aide de la fonction de filtrage IP Sec/IP. Ils déterminent ainsi s'il faut accepter ou bloquer des adresses IP spécifiques. Nous prenons également en charge le chiffrement SNMPv3, des e-mails et le TLS1.3.

Impression/numérisation sécurisée

L'option « travail confidentiel » vous permet de protéger la confidentialité des documents et d'empêcher toute consultation non souhaitée des documents imprimés laissés sans surveillance.

Protection des documents

Augmentez la productivité et surveillez l'usage du matériel grâce à un environnement d'impression, de numérisation et de copie sécurisé par authentification de l'utilisateur.

Protection du multifonction

Vérification de la signature du micrologiciel, démarrage sécurisé et détection d'intrusion et d'exécution de nouveaux logiciels malveillants.

Protection de votre solution d'impression

Pour une protection supplémentaire de vos matériels, vous pouvez choisir de bloquer l'accès à partir d'un ordinateur par le port USB et désactiver le port USB en façade. Vous pouvez également utiliser le système de motif anti-copie[2] pour empêcher la duplication non autorisée des documents originaux et le chiffrement des documents PDF[2] pour garantir la sécurité des documents numériques.

WPA3

Les dernières solutions d'impression Epson prennent en charge le chiffrement WPA3[2], la technologie d'authentification et de chiffrement pour le Wi-Fi (réseau local sans fil) la plus récente, offrant ainsi aux entreprises une protection Wi-Fi renforcée de leurs données.

Contrôle d'accès

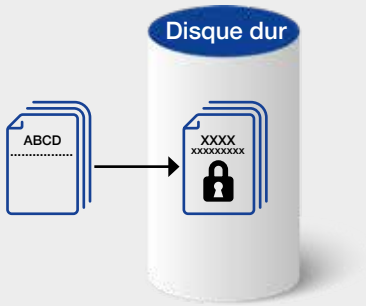
Authentification de l'utilisateur et restrictions de certaines fonctions.

Protection des données utilisateur

Vous pouvez également définir des mots de passe uniques pour les boîtes[2], les documents et les carnets d'adresses partagés sur vos solutions d'impression Epson. Pour une sécurité totale, les données sont effacées du multifonction une fois les travaux terminés ou l'alimentation coupée. S'il dispose d'un disque dur, toutes les données sont chiffrées et effacées après chaque travail d'impression. Pour une protection accrue, l'administrateur peut également effacer le disque dur. Pour en savoir plus, consultez notre guide de sécurité sur la page epson.fr/bi-security-solutions.

Protection des données

Disque dur crypté, effacement sécurisé des données sur le disque dur, technologie de module de plateforme sécurisée (TPM) et chiffrement des mots de passe.



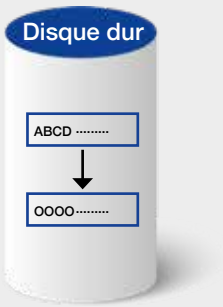
Chiffrement des données enregistrées sur le disque dur

Nous protégeons toujours les données des clients par chiffrement lors de l'enregistrement des données sur le disque dur interne à la solution d'impression. Le chiffrement des données empêche les accès non autorisés ou les attaques visant les données personnelles en cas de vol du disque dur. Le disque dur embarque un processus de chiffrement automatique et les données des documents sont chiffrées avec l'algorithme AES-256.

Suppression séquentielle des données des travaux

En cas d'activation, les données supprimées du disque dur[2] sont écrasées comme suit pour éviter leur restauration. Il existe plusieurs options :

1. Suppression rapide : la clé de chiffrement est modifiée pour empêcher les données supprimées d'être restaurées.
2. Suppression séquentielle sécurisée : la clé de chiffrement est modifiée et les données supprimées du disque dur sont remplacées par des « 0 » pour garantir que les données supprimées ne pourront pas être récupérées.



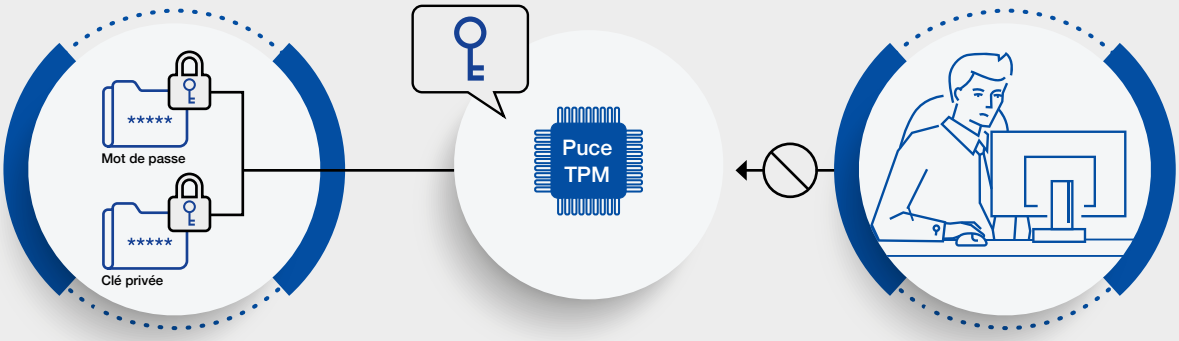
Veuillez vous reporter au manuel d'utilisation de votre modèle pour une explication détaillée de la suppression des données de travaux.

Puce TPM

Pour les modèles dotés d'une puce TPM (Trusted Platform Module), le niveau de sécurité est amélioré de la façon suivante :

- Les clés de chiffrement pour la restauration des mots de passe chiffrés et les informations de clés privées sont stockées sur la puce TPM.
- La puce TPM peut être protégée d'une analyse non autorisée au niveau du matériel, car elle n'est pas accessible depuis l'extérieur de la solution d'impression.
- Les vrais nombres aléatoires de la puce TPM sont utilisés comme clés de session pour la communication avec le navigateur (page Web du multifonction).
- Les vrais nombres aléatoires de la puce TPM sont utilisés dans la génération de clés d'authentification pour le disque dur chiffré.

Les modèles multifonction intègrent une puce TPM 2.0.



	WorkForce Enterprise	AM-C	
Nom du produit	**WF-C21000/C20600/C20750**	**AM-C4000/C5000/ C6000**	**AM-C400/C550**
Type	A3	A3	A4
Sécurité réseau			
Communication TLS	✔	✔	✔
TLS1.1, TLS1.2, TLS1.3	✔	✔	✔
Contrôle des autorisations et exclusions de protocoles	✔	✔	✔
Filtrage IPsec/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	✔	✔	✔
Authentification IEEE802.1X	✔	✔	✔
EAP-TLS, PEAP-TLS	✔	✔	✔
PEAP/MSCHAPv2	✔	✔	✔
EAP-TTLS	✔	✔	✔
AES128/AES256/3DES/RC4	✔	✔	✔
SNMPv3	✔	✔	✔
WPA3	✔	✔	✔
Séparation entre les interfaces réseau	✔	✔	✔
Protection de votre solution d'impression			
Blocage de la connexion USB à partir d'un ordinateur	✔	✔	✔
Désactivation de l'interface externe	✔	✔	✔
Gestion des virus introduits par une clé USB	✔	✔	✔
Sécurité d'impression / de numérisation			
Travaux confidentiels	✔*2	✔	✔
Motif anti-copie [2]	✔	✔	✔
Filigrane [2]	✔	✔	✔
Chiffrement des documents PDF	✔	✔	✔
S/MIME	✔	✔	✔
AES-128/AES-192/AES-256/3DES	✔	✔	✔
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✔	✔	✔
Restrictions de domaine	✔*1	✔	✔
Mot de passe d'autorisation pour la numérisation vers dossier réseau/ FTP, la numérisation vers e-mail et la notification par e-mail	–	✔ *1	✔
Désactivation par défaut de l'accès aux fichiers à partir de PDL	✔*1	✔	✔
Impression sécurisée	✔	✔	✔
Sécurité du fax[3]			
Restrictions de numérotation directe	✔	✔	✔
Confirmation de la liste d'adresses	✔	✔	✔
Détection de la tonalité	✔	✔	✔
Mesures contre les fax abandonnés	✔	✔	✔
Rapport de confirmation de transmission	✔	✔	✔
Suppression des données de sauvegarde pour les fax reçus	✔	✔	✔
Limite d'envoi à plusieurs destinataires	✔	✔	✔
Sécurité du multifonction			
Mises à jour automatiques du micrologiciel	✔	✔	✔
Protection contre les mises à jour illégales du micrologiciel	–	✔	✔
Démarrage sécurisé	–	✔	✔
Détection d'intrusion de logiciels malveillants	✔*1	✔	✔
Mesures de sécurité pour la mise au rebut du multifonction			
Rétablissement des paramètres d'usine	✔	✔	✔
Certification et normes de sécurité			
ISO15408/IEEE2600.2™	✔	✔	–

	WorkForce Enterprise	AM-C	
Nom du produit	**WF-C21000/C20600/C20750**	**AM-C4000/C5000/ C6000**	**AM-C400/C550**
Type	A3	A3	A4
Fonctions de sécurité grâce à la compatibilité avec des logiciels tiers			
Modèle conforme à Epson Open Platform	✔	✔	✔
Epson Print Admin (EPA) / EPA Serverless			
Authentification de l'utilisateur par badge, mon d'utilisateur/mot de passe ou code	✔	✔	✔
Contrôle total des actions sur le multifonction par personne	✔	✔	✔
Personnalisation du menu de la solution d'impression	✔	✔	✔
Impression en mode Pull et impression directe	✔	✔	✔
Numérisation et envoi vers mon adresse (e-mail, dossier)	✔	✔	✔
Services de numérisation vers le Cloud (OneDrive for Business, SharePoint Online, Teams et Google Drive) [8]	✔	✔	✔
Numérisation vers des fichiers PDF protégés par mot de passe	✔	✔	✔
Paramètres avancés de flux de travaux de numérisation [6]	✔	✔	✔
Impression sans pilote à partir de services Cloud (OneDrive for Business, SharePoint Online et Teams) [8]	✔	✔	✔
Synchronisation avec les services d'annuaires (LDAP, Open LDAP, Microsoft EntraID, Microsoft Entra DS, Google Secure LDAP et Google Cloud Directory) [8]	✔	✔	✔
Rapports - Paramètre de protection de l'utilisateur - Masquage du nom du fichier	✔	✔	✔
Politique relative aux mots de passe, verrouillage de compte [6]	✔	✔	✔
Règles et politiques d'impression [6]	✔	✔	✔
Suivi et rapports	✔	✔	✔
Quotas [8]	✔	✔	✔
Impression mobile sécurisée (AirPrint et Mopria) [7]	–	✔	✔
Protection des données utilisateur			
Sécurité des boîtes	✔	✔	✔
Protection de votre carnet d'adresses	✔	✔	✔
Gestion des données traitées par un multifonction	✔	✔	✔
Chiffrement des données enregistrées sur le disque dur	✔	✔	✔
Suppression séquentielle des données des travaux	✔	✔	✔
Chiffrement des mots de passe	✔	✔	✔
Puce TPM	✔*4	✔	✔
Mise en miroir du disque dur	–	✔	–
Limitation du fonctionnement			
Verrouillage du panneau de commandes	✔	✔	✔
Contrôle d'accès	✔	✔	✔
Impression / numérisation authentifiée [5]	✔	✔	✔
Politique relative aux mots de passe	✔	✔	✔
Journal d'audit	✔	✔	✔

1. Pour utiliser cette fonction, mettez le micrologiciel de de votre solution d'impression à jour vers la version la plus récente.
2. Seul le pilote d'imprimante Windows est pris en charge.
3. Uniquement disponible lorsque la carte fax en option est installée.
4. Peut ne pas être pris en charge selon la région. Veuillez contacter votre bureau de vente Epson local pour connaître la disponibilité sur ce marché.
5. Nécessite une méthode d'impression authentifiée.
6. S'applique uniquement à Epson Print Admin.
7. S'applique uniquement à Epson Print Admin Serverless.
8. S'applique à Epson Print Admin et uniquement à des modèles spécifiques sur Epson Print Admin Serverless

Pour en savoir plus, contactez votre représentant commercial Epson.

Nom :

Téléphone :

E-mail :

1. « The Print Security Landscape, 2023 - Securing the print infrastructure amidst a growing threat landscape » (Le paysage de la sécurité de l'impression, 2023 - Sécuriser l'infrastructure d'impression dans un paysage de menaces croissant), Quocirca, mai 2023.
2. Pour obtenir la liste complète des caractéristiques techniques du motif, rendez-vous sur la page www.epson.fr/bi-security-solutions.
3. La norme ISO/IEC 15408 n'est pas fournie avec une configuration standard. Micrologiciel et processus de configuration spéciaux requis. À l'exception de l'AM-C400/550.
4. Applicable à la gamme AM-C

Veuillez recycler
de manière responsable

Epson France
Batiment HARMONY
22 rue Dora Maar
93400 SAINT OUEN SUR SEINE
Pour plus d'informations, visitez www.epson.fr/contactus

EpsonFrance
@Epson_FR
@EpsonFrance
epson-france

A19399-fr-FR

EPSON®