Business imaging security solutions

WorkForce Enterprise 2
and AM-C series

EPSON®

Protect network security wherever printing happens

It's easy to overlook important security measures with any networked devices in your business. And while you may not have considered it, multifunction printers (MFPs), scanners and any other connected or networked device can be open to security weaknesses.

The rise of home and hybrid working has amplified this risk. A study by Quocirca[1] found that while 70% of IT decision-makers believe printing is critical or very important to their business, 31% are concerned about the security risks associated with remote/home printing and just 19% feel completely confident that their print infrastructure is secure.

With the average cost of a print-related data breach standing at €865k*, it isn't something you can afford to take lightly.

Thanks to Epson's approach to printer security, however, it is a risk you can mitigate, no matter where your business printing happens.

70%

of IT decision-makers believe printing is critical or very important to their business

31%

are concerned about the security risks associated with remote/home printing

19%

feel completely confident that their print infrastructure is secure

*Based on £743k as quoted by Quocirca and converted to €865k using FX rate from xe.com as of 09/01/2024.

Epson's security approach

Strengthening the network capabilities of your devices is key to our security approach. To ensure the security of Epson devices throughout their lifecycle, every Epson WorkForce printer is built on three core principles:

1. Product security is the basis for quality
2. Information and knowledge about security is actively shared, so you're always up to date
3. Vulnerabilities are constantly reviewed to maximise device protection

Security features designed around you

Protected data and secure networks come as standard with Epson's MFPs, using features that can help with your General Data Protection Regulation (GDPR) and Corporate Social Responsibility (CSR). These security measures, integrated directly into our products, gives you the assurance that your business meets your security requirements.

Secure printing and scanning

You can ensure document privacy and prevent unauthorised people from viewing unattended output at the device, by submitting your documents as a 'Confidential Job' from the print driver.

Restricting access to functions on the device can be done using the front panel lock.

Secure communication

Filter IP addresses, services, reception and transmission port numbers that have access to Epson devices. You can also encrypt all network communication using the IPSec function.

On device

With Epson Device Admin, on-device security becomes easier to manage. Compatible with a wide range of our networked printers, it allows users to control everything via a smart and intuitive interface.

PDF protection

Add password protection functionality[3] to scanned PDF files to protect against unauthorised viewers and prevent document editing and printing.

Document processing and data management

Manage multiple tasks centrally,from scan job profiles to user access rights. Administrators can manage a variety of tasks centrally from scan job profiles to user access rights. IT administrators have the ability to control access rights to jobs in a number of ways including ID cards, logins/passwords and PIN Codes.

Seamless integration into IT infrastructure with the local user database or Directory Services such as Microsoft EntraID and Google Cloud Directory.

Epson Solutions Suite

For more about Epson solutions please visit
https://support.epson.net/stories/en/

Security recognised around the world

At Epson, we benchmark our security on a global scale. We meet ISO/IEC 15408[3], also called Common Criteria (CC), which is an international standard for security measures in IT products and systems, and CCRA certification, which demonstrates that the product has been certified in accordance with the Japan Information Technology Security Evaluation and Certification Scheme (JISEC).

④

Network security
With network security a major priority, administrators can set up individual permissions and restrictions on a wide range of network tasks. With our WorkForce Enterprise 2 printers, administrators can also filter IP addresses, types of service,reception and transmission port numbers using the IP Sec/IP Filtering function. While deciding whether to accept or block specific IP addresses. We also support SNMPv3 email encryption and TLS1.3.

Protecting your all-in-one printer
For additional protection for your printers, you can choose to block access from a computer via USB, and disable the memory card and USB memory interfaces. You can also use anti-copy watermarking[2] to prevent unauthorised duplication of original documents and PDF encryption[2] to ensure digital documents remain safe.

Secure print/scan
The ‘confidential job’ option means you can protect document privacy and prevent any unwanted viewing of unattended output.

WPA3
Epson’s lastest MFPs support WPA3[2], which is the latest authentication and encryption technology for WiFi (wireless LAN), giving businesses more robust and stronger protection for their data over the wireless network.

Document protection
Boost productivity and monitor usage with secure printing, scanning and copying, through user-authentication.

Access control
User authentication and function restrictions.

Device protection
Firmware signature verification, secure boot and new malware runtime intrusion detection.

User data protection

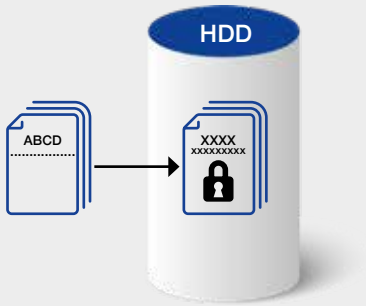
You can also set unique passwords for shared boxes[2], documents, and address books on your Epson printers. For complete security, data is cleared from the printer once jobs are completed or the power is switched off. If the device has a hard disk, all data is encrypted and data is erased after every print job. For added protection the administrator can also overwrite the hard drive.
Read more in our security guide book at epson.eu/bi-security-solutions

Data protection

HDD encryption, HDD safe data erasure, Trusted Platform Module (TPM) and password encryption.

Encryption of Saved Data in HDD

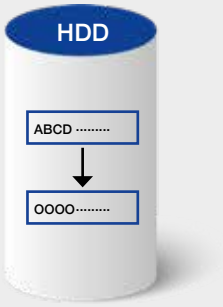
We always protect customer data with encryption when saving data onto an internal HDD on an all-in-one printer. Encrypting the data prevents unauthorized access or malicious attack to personal data if the HDD is stolen. The HDD comes with a self-encrypting drive, and the document data is encrypted with AES-256.



Sequential Deletion of Job Data

When enabled, the deleted data in the hard disk[2] is overwritten in the following ways to prevent from restoration. There are several options:

1. Quick deletion: The encryption key is changed to prevent deleted data from restoration.
2. Secure sequential deletion: The encryption key is changed, and the deleted data on hard drive are overwritten with “0’s” to further ensure the deleted data cannot be recovered.



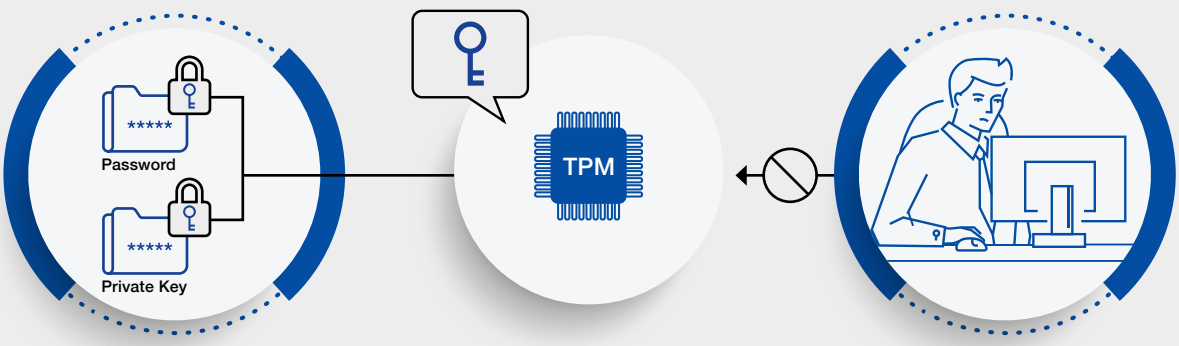
Please refer to the user manual of your product for a detailed explanation on job data deletion.

TPM

In models with TPM (Trusted Platform Module), the security level improves as follows:

- The encryption keys for restoring encrypted passwords and private key information are stored on the TPM chip.
- The TPM chip can be protected from unauthorized analysis at the hardware level, since the TPM chip cannot be accessed from outside the printer.
- TPMs true random numbers are used as session keys for communication with the browser (Web Config).
- TPMs true random numbers are used in generating authentication keys for the encrypted HDD.

The all-in-one printer has a TPM 2.0 chip.



	WorkForce Enterprise	AM-C	
Product name	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000	AM-C400/C550
Type	A3	A3	A4
Network security			
TLS Communication	✔	✔	✔
TLS1.1, TLS1.2, TLS1.3	✔	✔	✔
Controlling protocol permissions and exclusions	✔	✔	✔
IPsec/IP Filtering	✔	✔	✔
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	✔	✔	✔
IEEE802.1X Authentication	✔	✔	✔
EAP-TLS, PEAP-TLS	✔	✔	✔
PEAP/MSCHAPv2	✔	✔	✔
EAP-TTLS	✔	✔	✔
AES128/AES256/3DES/RC4	✔	✔	✔
SNMPv3	✔	✔	✔
WPA3	✔	✔	✔
Separation between interfaces	✔	✔	✔
Protecting your all-in-one printer			
Block USB connection from computer	✔	✔	✔
Disabling the external interface	✔	✔	✔
Handling viruses introduced by USB memory	✔	✔	✔
Print / scan security			
Confidential jobs	✔*2	✔	✔
Anti-copy pattern [2]	✔	✔	✔
Watermark [2]	✔	✔	✔
PDF encryption	✔	✔	✔
S/MIME	✔	✔	✔
AES-128/AES-192/AES-256/3DES	✔	✔	✔
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✔	✔	✔
Domain restrictions	✔*1	✔	✔
Authorisation password for scan to network folder/FTP, scan to email, and email notification	–	✔ *1	✔
Default Disabling of File Access from PDL	✔*1	✔	✔
Secure printing	✔	✔	✔
Fax security[3]			
Direct dialing restrictions	✔	✔	✔
Confirmation of address list	✔	✔	✔
Dial tone detection	✔	✔	✔
Measures against abandoned faxes	✔	✔	✔
Transmission confirmation report	✔	✔	✔
Deleting the backup data for received faxes	✔	✔	✔
Limit sending to multiple recipients	✔	✔	✔
Printer security			
Automatic firmware updates	✔	✔	✔
Protection against Illegal Firmware Updates	–	✔	✔
Secure Boot	–	✔	✔
Malware Infiltration Detection	✔*1	✔	✔
Security measures when you dispose of printer			
Restore factory default	✔	✔	✔
Security certification and standards			
ISO15408/IEEE2600.2™	✔	✔	–

	WorkForce Enterprise	AM-C	
Product name	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000	AM-C400/C550
Type	A3	A3	A4
Security features through compatibility with 3rd party software			
Open Platform compliant model	✔	✔	✔
Epson Print Admin (EPA) / EPA Serverless			
User authentication via ID cards/login credentials/PIN code	✔	✔	✔
Complete control of devices actions per individual	✔	✔	✔
Personalisation of MFP menu	✔	✔	✔
Pull printing & Direct printing	✔	✔	✔
Scan and send-to-me (email, folder)	✔	✔	✔
Scan to Cloud Services (OneDrive for Business, SharePoint Online, Teams and Google Drive) [8]	✔	✔	✔
Scan to password protected PDF files	✔	✔	✔
Advanced scan workflow settings [6]	✔	✔	✔
Driverless Print from Cloud Services (OneDrive for Business, SharePoint Online and Teams) [8]	✔	✔	✔
Synchronisation with directory service (LDAP, Open LDAP, Microsoft EntraID, Microsoft Entra DS, Google secure LDAP & Google cloud directory) [8]	✔	✔	✔
Reports - User protection setting - Hide file Name	✔	✔	✔
Password Policy, Account Lockout [6]	✔	✔	✔
Print rules and policies [6]	✔	✔	✔
Tracking and reporting	✔	✔	✔
Quota [8]	✔	✔	✔
Secure Mobile Printing (AirPrint and Mopria) [7]	–	✔	✔
User data protection			
Box security	✔	✔	✔
Protecting your address book	✔	✔	✔
Data handling processed by an all-in-one printer	✔	✔	✔
Encryption of saved data in hard disk	✔	✔	✔
Sequential deletion of job data	✔	✔	✔
Password encryption	✔	✔	✔
TPM	✔*4	✔	✔
Mirroring of the Hard Disk	–	✔	–
Operational limitation			
Panel lock	✔	✔	✔
Access control	✔	✔	✔
Authenticated printing / scanning [5]	✔	✔	✔
Password policy	✔	✔	✔
Audit log	✔	✔	✔

1. To use this function, update the printer firmware to the latest version.
2. Only supported the windows printer driver.
3. Only available when the option fax board is installed.
4. May not be supported depending on the region. Please contact the local sales office for availability in your country.
5. Requires authenticated printing method.
6. Applies to Epson Print Admin only.
7. Applies to Epson Print Admin Serverless only.
8. Applies to Epson Print Admin and only on specific products on Epson Print Admin Serverless

Contact your Epson Sales Representative for more information.

Name:

Phone:

Email:

1. 'The Print Security Landscape, 2023 - Securing the print infrastructure amidst a growing threat landscape', Quocirca, May 2023.
2. For a full list of model specifications visit www.epson.eu/bi-security-solutions.
3. ISO/IEC 15408 does not come with standard configuration. Special firmware and special setup process required. Excludes AM-C400/550.
4. Applicable for AM-C series

Please recycle responsibly

For more information please contact:

Home users: 0343 90 37766
Business users*: 0871 42 37766
Republic of Ireland: 01 436 7742

Or visit us at www.epson.co.uk/contactus

*10p per minute plus network extras.

@EpsonUK
@EpsonUK
@EpsonUK
@Epson UK Ltd

A19339-en-GB

EPSON®