WorkForce Enterprise Series

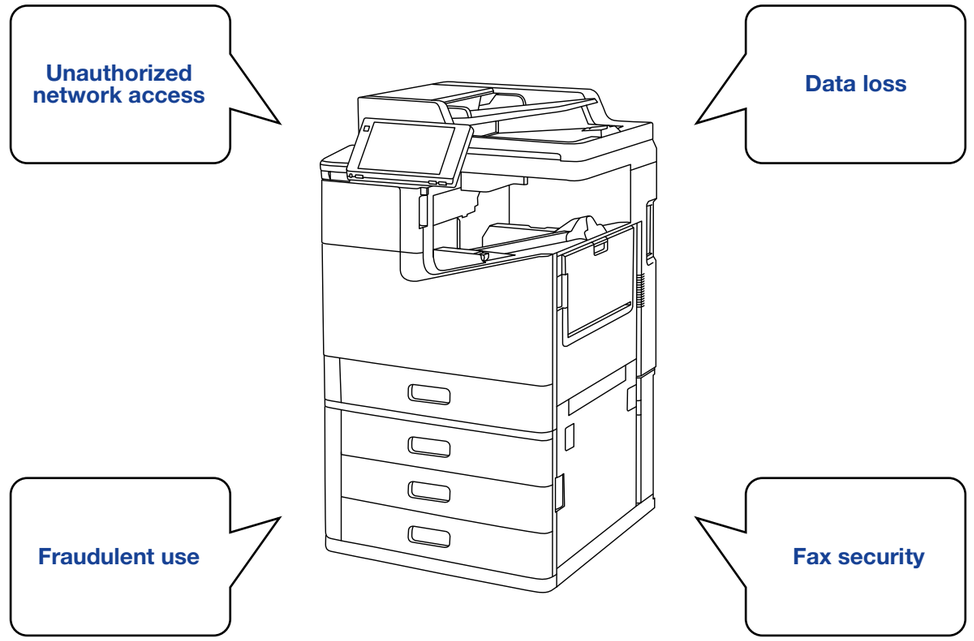
Security white paper

EPSON
EXCEED YOUR VISION

Contents

Introduction

Epson takes customers' security very seriously and builds security features into all of its business inkjet products. Whether it be user, network or data security, you can trust Epson to have a solution to meet your security requirements.



Epson’s approach to security

Epson understands the importance of security in its business inkjet printers and MFP’s – and makes every effort to ensure that high levels of security are maintained:

We regard product security as the basis of product quality.
From the planning stage to use by customers, we design security into the products

We actively provide information on security to customers

We continue to respond to vulnerabilities

Conducting vulnerability testing with industry standard tools and striving to ship non-vulnerable products

Steady monitoring of vulnerability information around open source software used in firmware for multifunction peripherals

If new vulnerabilities are found, analyse promptly and provide both information and countermeasures

Correspond to security standards

ISO15408/IEEE2600

ISO15408 is an international evaluation and certification system on security

Conforms to IEEE2600.2 which is a profile for multifunction devices, shows that they have been evaluated and certified by a third party and have a security function

FASEC1

FASEC1, is a standards guideline for security for Fax transmission for business created by the Information and Telecommunications Network Industry Association Japan (CIAJ)

The function is to prevent erroneous transmission and connection, the standing of the received paper and to check that it was actually transmitted in order to improve security

General security

Tamper-proof packaging

Our WorkForce Enterprise range is shipped from the factory in packaging with tamper-proof seals, which show if the package has been interfered with.

Ink access & paper cassette locks

The Workforce Enterprise ink access panel can be locked using a small padlock to prevent access to the ink cartridges.

Optional cassette draw locks can be purchased to protect the standard paper tray cassettes.

Front panel lock

All our MPFs and printers have the ability to have the front panel locked to avoid access and unauthorised use.

More advanced access control can be achieved by adding users to an access control list or by using Epson open platform applications to provide user level or card access.

User access control

The administrator can set access rights for users. Functions such as copy, scan and fax can be enabled or disabled for individual users (up to 10 users).

Operation timeout

An operation timeout can be set for the control panel from between 10 seconds to 240 minutes. If the set time is reached, then the panel will automatically lock.

Administrator password

The business inkjet range allows administrators to set a password between 1 and 20 characters. Access to certain features can then be enabled or disabled by admin access only.

Access and security

Log and report print – audit report

Job history logs can be configured to show job logs, fax access, sent history of email and scan.

Print logs and reports provide information such as save history, scan to network folder/FTP and fax reports.

Access control / User authentication

By default, the device can be set to have access control for 10 users. The user can be configured for print, copy scan and fax functions.

More advanced access control can be achieved by using an open platform application such as Epson Print Admin.

Card authentication printing

Card authentication and advanced user authentication can be achieved by using the optional Epson Print Admin open platform application or third-party compatible open platform applications.

Password policy

A password policy can be set for the administrator password, user limit password and fax box password. Setting conditions such as the number of characters and combination of character types can reduce the risk of password leakage.

Address book protection

The address book is protected against export or editing by access control. Only the administrator password can unlock these features, preventing export or unauthorised tampering.

Personal data display

Set to a level where the end user can see paths for network drives and scan locations.

Block USB ports

Using the setup options, the administrator can block both the front USB port for memory devices and the USB ports which connect to a PC.

Physical USB port blockers

Epson does not supply physical USB blockers.
However, these can be purchased from various sources.

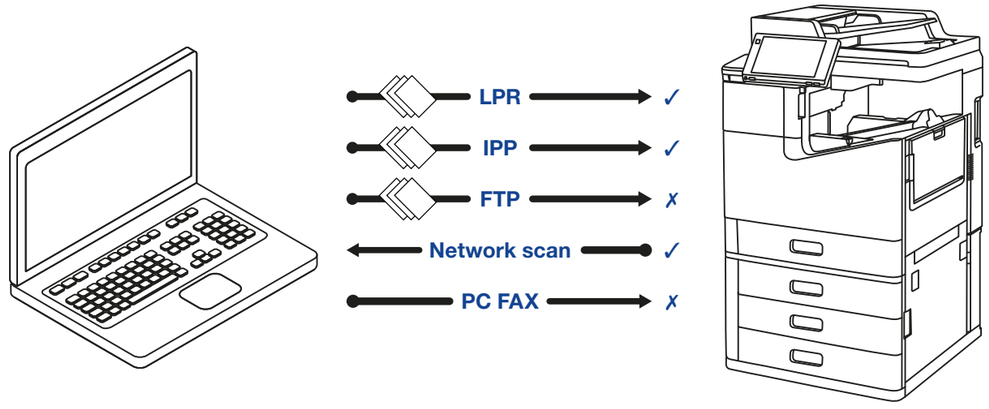
Network security

The WorkForce Enterprise series has a large range of security network features covering both local area and wireless networks.

Enable or disable network protocols

The following network protocols can be enabled or disabled by system admin.

Protocol	Description
Bonjour	A protocol used to discover Apple devices.
SLP	Used for push scanning and network searches by Epson Netconfig.
WSD	Microsoft API that enables easy access to web services.
LLTD	Allows Windows to display the device on the network map.
LLMNR	Enables name resolution without NetBIOS or DNS.
LPR	Enable or disable printing to the LPR port.
Port 9100	Enable or disable RAW Port 9100 printing.
IPP	Enable or disable IPP printing.
FTP	Enable or disable FTP
SNMP v1/v2c	Used to setup device monitoring.
SNMP v3	Used to monitor devices with encryption.



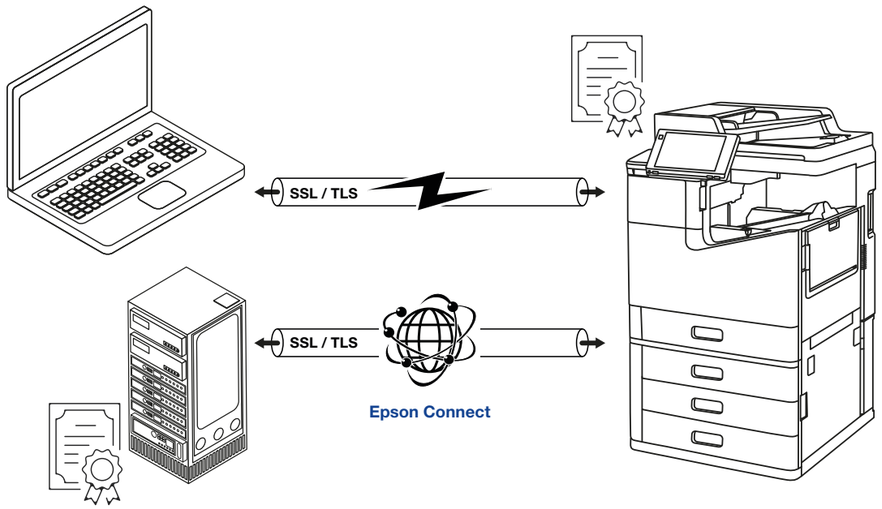
Network security

SSL/TLS communication

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are protocols that provide data encryption and authentication for secure transmission of sensitive data over a network.

Epson devices can use both Certificate Authority (CA) or self-certification.
The former is more secure as the certificate is dedicated to the organisation that applied for it.

SSL/TLS are used when setting up multifunction devices via a browser or by printing with the IPPS protocol. Communication contents are maintained by SSL /TLS.



IP filtering

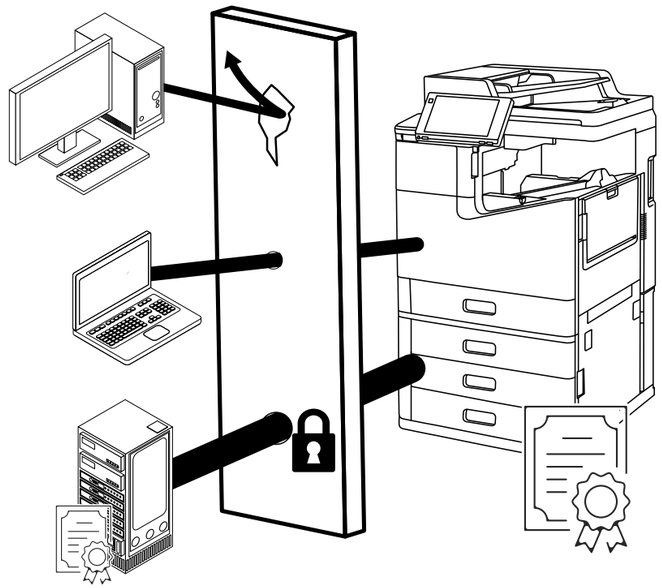
Epson business inkjet printers can filter network traffic based on the IP address, port and services.

Encrypted security using IPsec

The Workforce Enterprise supports IPsec and IP filtering.

IPsec enables secure transportation of data over a network. Epson business inkjet products can also filter traffic based on the IP address, port and services.

Epson devices support both IKEv1 and IKEv2 functions (Internet Key Exchange).



Network security

Epson printers support the following algorithms.

Security Methods	Algorithms
IKE encryption algorithm	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
IKE authentication algorithm	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE key exchange algorithm	DHGroup1, DHGroup2, DHGroup5, DHGroup14, DHGroup15, DHGroup16, DHGroup17, DHGroup18, DHGroup19, DHGroup20, DHGroup21, DHGroup22, DHGroup23, DHGroup24, DHGroup25, DHGroup26, DHGroup27, DHGroup28, DHGroup29, DHGroup30
ESP encryption algorithm	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP authentication algorithm	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH authentication algorithm	SHA-1, SHA-256, SHA-384, SHA-512, MD5

SNMP v1/v2c/v3

Epson devices support SNMP versions 1, 2 and 3. SNMP is a protocol that carries out monitoring and control to collect information from print devices. SNMP v3 is the most secure version.

IEEE802.1X

IEEE802.1X defines a secure authentication method for peripherals connecting to a wired or wireless network. The protocol in 802.1X is called EAP encapsulation over LAN (EAPOL).

Epson devices support the following EAP types.

EAP type	EAP-TLS	You need to obtain and import a CA certificate
	PEAP-TLS	You need to obtain and import a CA certificate
	PEAP-MSCHPv2	You need to configure a password

Wireless security

Wireless can be turned on and off by the administrator. If Wi-Fi is enabled then the Ethernet connection is dropped to avoid bridging the network.

The following Wi-Fi security is supported:

WEP-64 bit (40 bit)

WEP-128 bit (104 bit)

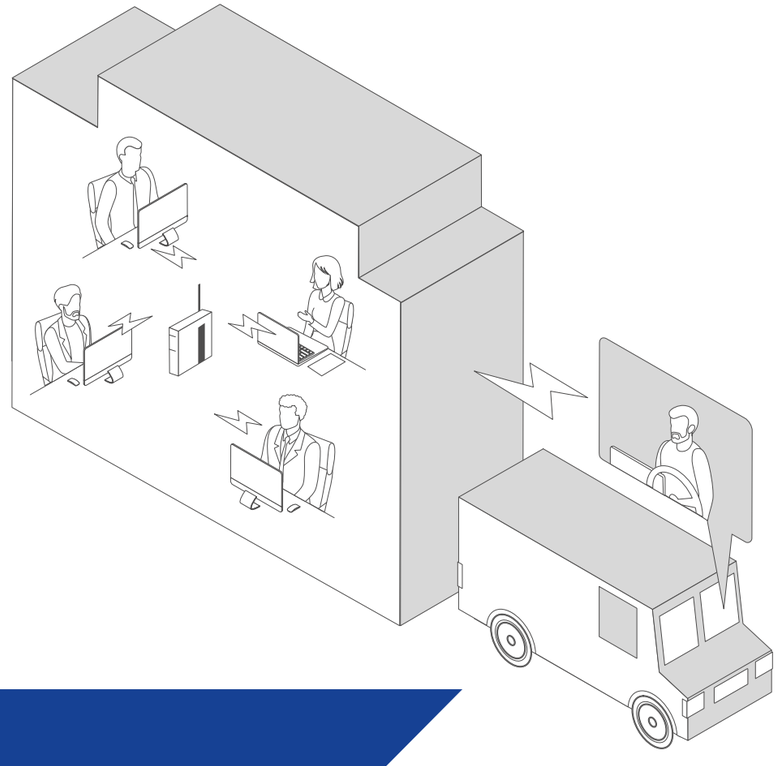
WPA PSK (TKIP/AES)

WPA 2 PSK (TKIP/AES)

WPA (TKIP/AES)

WPA 2 (TKIP/AES)

You can use WPS (Wi-Fi Protected Setup)
for wireless LAN setup to easily connect to your wireless network.



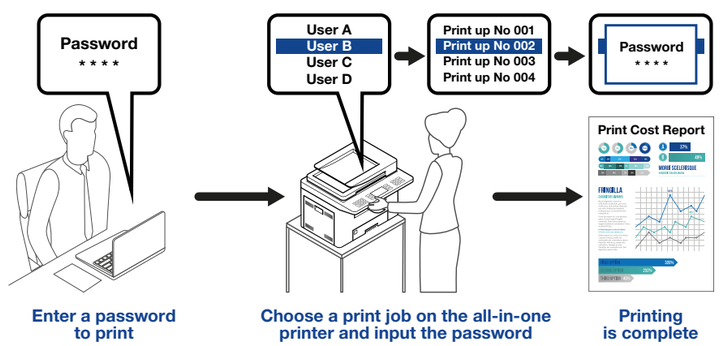
Tip

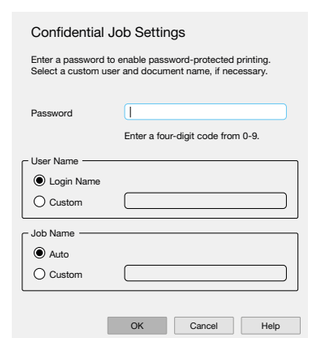
Always set up a high security level on your router when implementing and using wireless devices.

In-driver security features

Print password protection/Confidential print

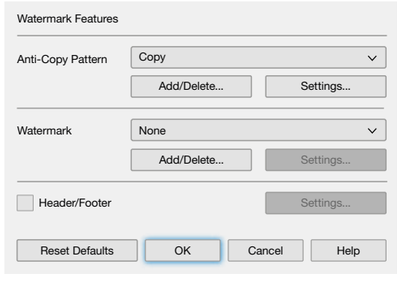
Users can add a pin at the print driver and then securely print the job. Only by adding the pin at the device will you be able to release the print job. More advanced print release can be achieved by using open platform applications such as Epson Print Admin or third-party open platform compatible applications.

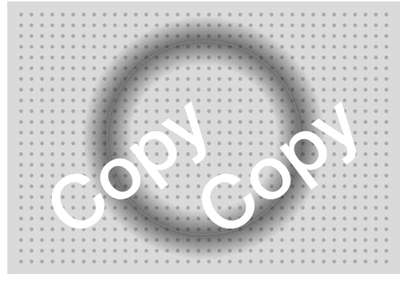




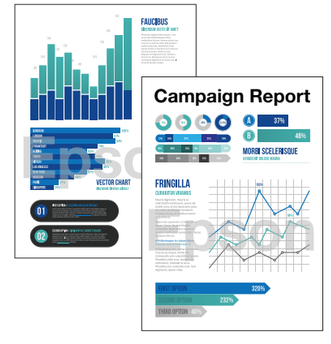
Watermark printing/Copy protection

Copy protection can be added by selecting the watermark anti-copy feature within the driver. A background dot pattern is printed on the original document and, when copied, a watermark will be created. Options include copy, reproduction, date, computer name or user name.





Watermarks can also be added to printed documents and information can be added to the footer or header when printed. There is an option to create your own watermark in either text or BMP formats.



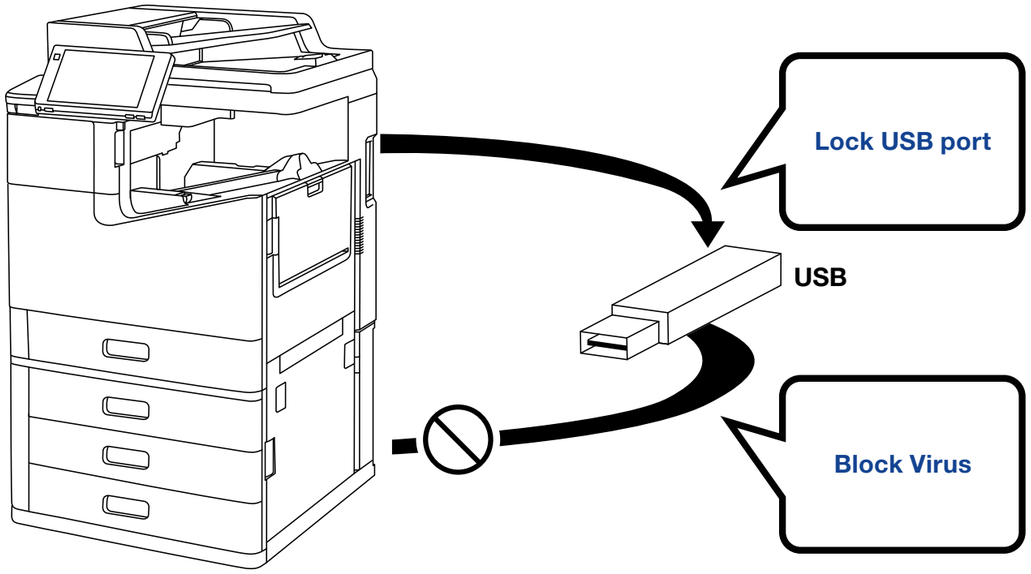
Virus security

Firmware

Our firmware is protected against viruses or changes to the code, so the device will not start up if the firmware is bad. Boot firmware is locked by the factory.

USB memory virus protection

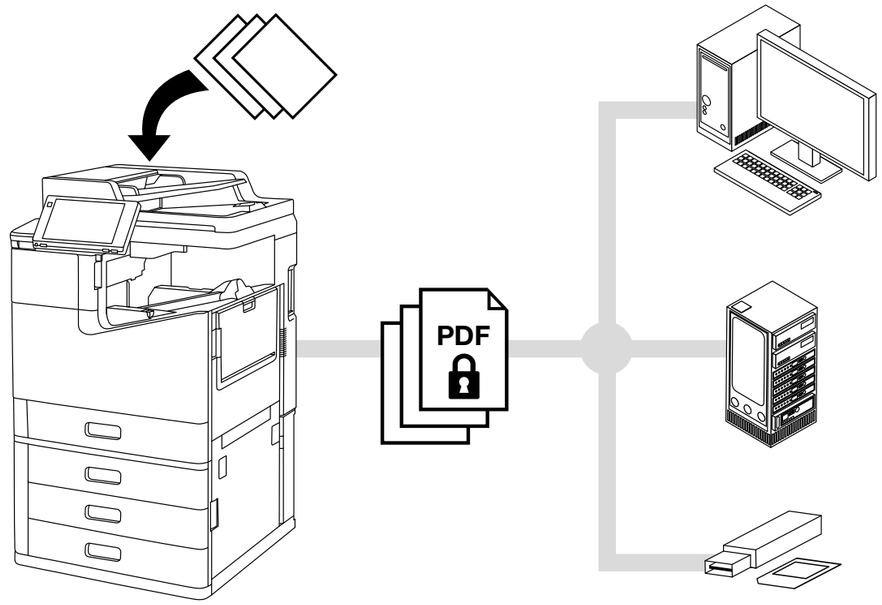
The devices are not able to run executable files, so no viruses can be executed from a USB device.



Scan security

PDF scan security

The Workforce Enterprise series allows you to add password protection and encrypt documents scanned to an email address or device.



Scan shortcuts on home page

To avoid user mistakes, scan shortcuts can be setup on the home screen of the Workforce Enterprise device.

Epson Scan 2

Scan profiles can be setup using Epson Scan 2 to avoid users making errors and to guarantee that documents are stored in the correct locations.

Scan to me/Scan to my home folder – Epson Print Admin

Epson Print Admin allows the administrator to force the user to only scan to either their home folder or email address.

Fax security **Security of telephone line and fax**

Direct link between fax and network card

There is no physical link between the fax and the network card.

Manual dial restriction - misentering telephone numbers

The administrator can set a restriction, so that manually dialled numbers need to be entered twice before a fax transmission starts. Further restrictions include locking out the use of the numeric keypad, so that faxes can only be sent by one touch dialing to addresses registered in the address book.

Destination list check

You can confirm the selected address before you send a fax, which reduces the risk of sending faxes to the wrong party.

Dial tone detection*

You can prevent wrong transmission by sending faxes after confirming the detection of a dial tone.

* Depending on your country or region, dial tone detection may not be possible.

Countermeasures against loss of printed faxes

The fax printing after viewing function allows the administrator to set up a feature which saves received faxes in the inbox (memory reception) and print it after the user has confirmed it on the printer control panel. This prevents information disclosure and the loss of printed material from received faxes that have been left unattended. In addition, if it is set to request a password when accessing the inbox, it prevents arbitrary printing by an unauthorised user and deletion.

Transmission confirmation report

You can confirm that a fax has definitely been sent to the correct address by printing out reports that confirm the transmission details, such as a sending result report, forwarding results report and sending management report.

Back up and erase fax reception data

Backup* of fax reception data can be deleted from the operation panel. This feature can be set to automatically erase, preventing illegal reprinting of fax reception data.

*Backup data for received faxes is saved in the MFP, so you can reprint faxes in case they are unclear or poor quality.

Prevention of unauthorised access via telephone line

Epson MFPs have no remote control function via a telephone line. Fax transmission/ reception processing is performed in the printer's dedicated memory. If there is an attempt to access the device via the telephone line then the printer will not operate and settings cannot be changed without authorisation.

User data protection

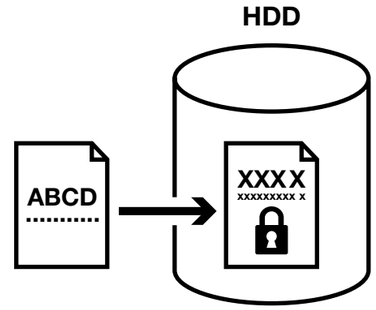
Using document data handled by the multifunction device

Printing, copying, and scanning data is temporarily held in the MFP, but when the target job is completed, the data is overwritten. Data is also erased when the device is turned off.

Fax data is deleted when transmission/reception is completed. The fax reception data is backed up by the backup function. Although it holds data based on the setting, it can be automatically deleted by changing the setting (see fax security section).

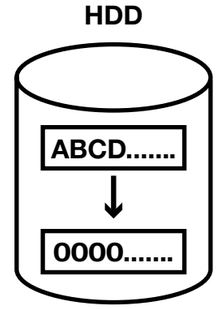
Encryption of data recorded on the hard disk

When data is recorded on the built-in hard disk, it always encrypts and protects that data. The data is encrypted to AES256 standard, making it difficult to retrieve if the hard disk is removed.



Sequential erase of job data

When this function is enabled, job data temporarily recorded on the hard disk of the main unit is overwritten with a specific pattern. This means data will be erased and you will not be able to restore it.



Disposal of device after use – return to factory default

The device can be initialised, so that when disposing of or transferring a printer, all settings and data recorded in the main body will be erased, including information on the hard disk.

Security certification and standards

IEEE Std. 2600.2™

IEEE Std. 2600.2™ is an international standard that specifies information security criteria for MFPs. MFP security can be comprehensively strengthened by providing standard-compliant security functionalities, such as user identification and authentication, access control, data overwrite, network protection, security management, self-test, and audit logs.

The Epson Workforce Enterprise series conforms with IEEE Std. 2600.2™-2009 standard.

ISO/IEC 15408 (Common Criteria)

ISO/IEC15408, also called Common Criteria (CC), is an international standard for the independent and objective evaluation of security measures in IT products and systems to determine whether those measures are properly designed and implemented.

Specified versions of firmware, manuals, and other components are evaluated for ISO/IEC15408 certification. The version of the firmware in a purchased product may differ from the certified version.

WF-C20590, WF-C17590

Certification for compliance with ISO/IEC 15408 (IEEE Std. 2600.2™)*1*2

*1 U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009).

*2 The CCRA certification logo shows that the product was evaluated and certified in accordance with the Japan Information Technology Security Evaluation and Certification Scheme (JISEC).

It does not imply a guarantee that the product is completely free from vulnerability.

It also does not imply that the product is equipped with all necessary security functions under every operational environment.

For the MFP to be ISO/IEC 15408 compliant, a strict installation and implementation process is required. This process is only available for new machines. There may be some limitations on product functionality when using a certified version.

Open platform and solutions

The WorkForce Enterprise range is open platform compliant. Epson and third-party applications can be used to add additional security features to the product, such as card readers, biometric readers, pull print, advanced auditing and cost control, and scan workflow.

Please refer to the solution pages at **Epson.eu**

Summary table

Security Function

Responding to security standards	WorkForce Enterprise WF-C20590	WorkForce Enterprise WF-C17590
15408 Common Criteria	Yes*	Yes*
P2600.2	Compliant	Compliant
FASEC1 (fax)	Yes	Yes
Network Security - Interface		
Enable/Disable network protocols	Yes Bonjour, SLP, WSD, LLTD, LLMNR, LPR, Port 9100, IPP, FTP, SNMP v1/v2c/v3	Yes Bonjour, SLP, WSD, LLTD, LLMNR, LPR, Port 9100, IPP, FTP, SNMP v1/v2c/v3
SSL/TLS	Yes	Yes
IP Filtering	Yes	Yes
IPsec	Yes	Yes
SNMPv1/v2c/v3	Yes	Yes
IEEE802.1X	Yes EAP-TLS PEAP-TLS PEAP-MSCHAP v2	Yes EAP-TLS PEAP-TLS PEAP-MSCHAP v2
Wireless security	Yes WEP-64 bit WEP-128 bit WPA PSK (TKIP/AES) WPA 2 PSK (TKIP/AES) WPA (TKIP/AES) WPA 2 (TKIP/AES)	Yes WEP-64 bit WEP-128 bit WPA PSK (TKIP/AES) WPA 2 PSK (TKIP/AES) WPA (TKIP/AES) WPA 2 (TKIP/AES)

*Please contact the local sales office for availability in your country

Access security	WorkForce Enterprise WF-C20590	WorkForce Enterprise WF-C17590
Panel lock	Yes	Yes
User access control	Yes	Yes
Operation timeout	Yes	Yes
Card reader authentication	Option - EPA	Option - EPA
Audit logs	Yes	Yes
Block USB ports	Yes	Yes
Lock ink cartridge access	Yes	Yes
Lock paper trays	Option	Option
Driver security		
Confidential pin print	Yes	Yes
Watermark	Yes	Yes
Copy protection	Yes	Yes
Fax security		
Manual dial restrictions	Yes	Yes
Destination check list	Yes	Yes
Dial tone detection	Yes	Yes
Fax printing after viewing	Yes	Yes
Transmission confirmation report	Yes	Yes
Unauthorised line access protection	Yes	Yes
Backup and erase	Yes	Yes
Scan security		
Encrypted PDF	Yes	Yes
Scan shortcuts	Yes	Yes
Epson Scan 2	Yes	Yes
Scan to me email/home folder	Yes – EPA option	Yes – EPA option
User data protection - data		
Data erased when device turned off	Yes	Yes
Encrypted hard disk	Yes AES 256	Yes AES 256
Hard disk erase and overwrite	Yes	Yes
Device disposal		
Return to factory default and delete all data	Yes	Yes
Open platform		
Use compatible third-party products	Yes	Yes

Committed to corporate and social responsibility

Epson is committed to developing environmentally conscious products, which means that sustainability is considered from conception to completion. We help customers recognise the environmental gains brought on by technology, whether it is redefining manufacturing through innovative robotics, saving energy with our office printing technology or revolutionising textile printing with digital solutions.

We are committed to all 17 United Nations' sustainable development goals and to the aims of the circular economy. We offer sustainable innovations because we recognise that the choices we make as organisations, individuals or a society will be essential to our shared success.

The content of this publication has not been approved by the United Nations and does not reflect the views of the United Nations or its officials or Member States www.un.org/sustainabledevelopment

A8212_WorkForce Security Print Friendly_whitepaper_1EN-INT_10/19

For further information please contact your local Epson office or visit www.epson-europe.com
Algeria (+2213) 770 938 617 **Austria** 01 253 49 78 333 **Belgium** +32 (0)2 792 04 47 **Czech** 800/142 052 **Denmark** 44 50 85 85 **East Africa** (+254) 734 354 075
Finland 0201 552 091 **France** 09 74 75 04 04 (Cost of local call, operator charges may apply) **Germany** +49 (0) 2159/92 79 500 **Greece** (0030) 211 198 62 12
Hungary 06800 147 83 **Ireland** 01 436 7742 **Israel** (+972)-3-5751833 **Italy** 02-660321 10 (0,12 €/min) **Luxembourg** +352 27860692 **Middle East** +9714 2677638
Morocco (+212) 661 31 11 18 **Netherlands** +31 (0)20 708 5099 **Norway** +47 67 11 37 00 **Poland** 0-0-800 4911299 (0,16 zł/min) **Portugal** 707 222 111
Romania 0040 214025024 **Russia** (095) 777-03-55 **Slovakia** 0850 111 429 **Southern Africa** (+2711) 465-9621 **Spain** 93 582 15 00 **Sweden** 0771-400135
(Mobilsamtal – 0,99 kr/min, Lokala samtal – 0,30 kr/min, Utlandssamtal – 0,89 kr/min) **Switzerland** 022 592 7923 **Tunisia** (+216) 9833 3571 **Turkey** (0212) 3360303
United Kingdom 0871 42 37766 (+10p per minute plus network extras) **West Africa** (+234)8020727843