

WorkForce Enterprise 2 und AM-Produktreihe

Business-Drucker

Sichere Lösungen



EPSON®

Netzwerksicherheit überall dort gewährleisten, wo gedruckt wird

Wichtige Sicherheitsmaßnahmen bei vernetzten Geräten in Ihrem Unternehmen sind leicht zu übersehen. Auch wenn Sie vielleicht noch nicht darüber nachgedacht haben: Multifunktionsdrucker (MFD), Scanner und andere angeschlossene oder vernetzte Geräte können Sicherheitslücken aufweisen.

Durch die zunehmende Verbreitung von Homeoffice und Hybridarbeit hat sich dieses Risiko noch verstärkt. Eine Studie von Quocirca¹ ergab, dass 56 % der Unternehmen mindestens einen Vorfall von Datenverlust aufgrund einer Sicherheitsverletzung im Zusammenhang mit Druckern erlitten haben. 83 % werden ihre Ausgaben für Drucksicherheit im kommenden Jahr erhöhen. Die größten Bedenken für Unternehmen sind die Sicherung des Druckens zu Hause (28 %), der Schutz

vertraulicher oder sensibler Dokumente vor dem Ausdrucken (28 %) und das Verständnis der Art der Bedrohungen und Schwachstellen ihrer Druckinfrastruktur (25 %).

Da die durchschnittlichen Kosten einer datenschutzrechtlichen Verletzung im Zusammenhang mit dem Drucken bei 953.000 €* liegen, ist dies keine Angelegenheit, die man auf die leichte Schulter nehmen kann.

Dank Epsons Ansatz für die Druckersicherheit können Sie jedoch Risiken minimieren, egal wo Ihr Unternehmen druckt.

Die drei größten Herausforderungen im Bereich Drucksicherheit

28%

Sicheres Drucken in einer Remote-/Home-Umgebung

28%

Schutz sensibler oder vertraulicher Dokumente vor dem Ausdrucken

25%

Die unterschiedlichen Bedrohungen und Schwachstellen unserer Druckinfrastruktur verstehen



* Basierend auf der Umrechnung der von Quocirca angegebenen 820.000 £ in 953.000 € unter Verwendung des Wechselkurses von xe.com zum 07.07.2025.

Sicherheitserklärung von Epson

Die Stärkung der Netzwerkfunktionen Ihrer Geräte ist ein wesentlicher Bestandteil unseres Sicherheitsansatzes. Um die Sicherheit von Epson Geräten während ihres gesamten Lebenszyklus zu gewährleisten, basiert jeder Epson WorkForce-Drucker auf drei Grundprinzipien:

1. Produktsicherheit ist die Grundlage für Qualität.
2. Informationen und Wissen zum Thema Sicherheit werden aktiv ausgetauscht, sodass Sie immer auf dem neuesten Stand sind.
3. Schwachstellen werden ständig überprüft, um den Geräteschutz zu maximieren.

Sicherheit durch Design
Multifunktionsgeräte von Epson sind standardmäßig darauf ausgelegt, Daten zu schützen und sich sicher in Netzwerke zu integrieren. Dafür verwenden sie Funktionen, die helfen, die Richtlinien der EU-Datenschutz-Grundverordnung (DSGVO) und die soziale Verantwortung von Unternehmen (CSR) einzuhalten. Diese Sicherheitsmaßnahmen, die direkt in unsere Produkte integriert sind, geben Ihnen die Gewissheit, dass Ihr Unternehmen Ihre Sicherheitsanforderungen erfüllt.

Unsere Geräte werden unabhängig getestet und die Sicherheit wird von Keypoint Intelligence validiert. Die proprietäre Drucker-/Scanner-SoC- und Firmware-Plattformtechnologie von Epson schützt Kundeninformationen und -produkte vor Sicherheitsbedrohungen.



Sicheres Drucken und Scannen
Stellen Sie die Vertraulichkeit von Dokumenten sicher und verhindern Sie, dass nicht autorisierte Personen die unbeaufsichtigten Druckausgaben am Gerät einsehen, indem Sie Ihre Dokumente über den Druckertreiber als „vertrauliche Aufträge“ senden.

Der Zugriff auf Funktionen des Geräts kann über die Frontblendenverriegelung eingeschränkt werden.

Sichere Kommunikation
Filtern Sie IP-Adressen, Services sowie Portnummern für Empfang und Übertragung, die Zugriff auf Epson Geräte haben. Mit der IPSec-Funktion können Sie die gesamte Netzwerkkommunikation verschlüsseln.

Am Gerät
Mit Epson Device Admin (EDA) ist die Gerätesicherheit einfacher zu verwalten. Diese Lösung ist mit vielen unserer Netzwerkdrucker kompatibel und ermöglicht die Steuerung der Geräte mittels einer durchdachten und intuitiven Oberfläche.

PDF-Schutz
Fügen Sie gescannten PDF-Dateien einen Kennwortschutz² hinzu, um sie vor unbefugten Benutzern zu schützen sowie das Bearbeiten und Drucken von Dokumenten zu verhindern.

Dokumentenverarbeitung und Datenverwaltung
Verwalten Sie vielfältige Aufgaben zentral, von Scanauftragsprofilen bis hin zu Benutzerzugriffsrechten. Administratoren können eine Vielzahl von Aufgaben zentral verwalten, von Scanauftragsprofilen bis hin zu Zugriffsrechten. IT-Administratoren können die Zugriffsrechte für Aufträge über verschiedene Möglichkeiten steuern, z. B. ID-Karten, Login-Daten/Kennwörter und PIN-Codes.

Sie können Geräte nahtlos in ihre IT-Infrastruktur mit der lokalen Benutzerdatenbank oder Verzeichnisdiensten wie Microsoft EntraID und Google Cloud Directory integrieren.

Weitere Informationen zu den Sicherheitslösungen von Epson finden Sie unter den folgenden Codes oder Links.

Epson Solutions Suite



[Epson Solutions Suite](#)



[Produktsicherheit](#)

Weltweit anerkannte Sicherheit

Bei Epson bewerten wir unsere Sicherheit auf globaler Ebene. Wir erfüllen ISO/IEC 15408³, auch Common Criteria (CC) genannt, eine internationale Norm für Sicherheitsmaßnahmen bei IT-Produkten und -Systemen, und die CCRA-Zertifizierung, die belegt, dass das Produkt gemäß dem Japan Information Technology Security Evaluation and Certification Scheme (JISEC) zertifiziert wurde.



Netzwerksicherheit

Da die Netzwerksicherheit eine große Priorität hat, können Administratoren individuelle Berechtigungen und Einschränkungen für eine Vielzahl von Netzwerkaufgaben festlegen. Mit unseren WorkForce Enterprise 2-Druckern können Administratoren auch IP-Adressen, Art des Services sowie Empfangs- und Übertragungsportnummern mithilfe der IP Sec/IP-Filterfunktion filtern. Dabei entscheiden sie, ob bestimmte IP-Adressen akzeptiert oder blockiert werden sollen. Wir unterstützen auch die SNMPv3-E-Mail-Verschlüsselung und TLS1.3.



Sicheres Drucken/Scannen

Mit der Option „Vertraulicher Auftrag“ können Sie die Vertraulichkeit von Dokumenten schützen und verhindern, dass unbeaufsichtigte Ausdrucke ungewollt eingesehen werden.



Dokumentenschutz

Steigern Sie die Produktivität und überwachen Sie die Nutzung durch sicheres Drucken, Scannen und Kopieren mittels Benutzerauthentifizierung.



Geräteschutz

Überprüfung der Firmware-Signatur, sicheres Booten und Erkennung von Malware-Bedrohungen.



Schutz Ihres Multifunktionsdruckers

Um Ihre Drucker zusätzlich zu schützen, können Sie den Zugriff von einem Computer über USB blockieren und die Speicherkarte und USB-Speicherschnittstellen deaktivieren. Sie können auch Anti-Copy-Wasserzeichen⁵ verwenden, um eine unbefugte Vervielfältigung von Originaldokumenten zu verhindern, und PDF-Verschlüsselung⁵, um die Sicherheit digitaler Dokumente zu gewährleisten.



WPA3

Die neuesten Multifunktionsgeräte von Epson unterstützen WPA3⁵, die neueste Authentifizierungs- und Verschlüsselungstechnologie für WLAN und bieten Unternehmen einen robusteren und stärkeren Schutz für ihre Daten über das drahtlose Netzwerk.



Zugriffskontrolle

Benutzerauthentifizierung und Funktionseinschränkungen.



Manipulationssichere Tinte

Unsere DURABrite™ Pro-Tinte dringt tief in die Fasern des Papiers ein, wodurch wichtige Dokumente vor Manipulationen geschützt sind und die Norm ISO 11798:2023 erfüllt wird.



Schutz von Benutzerdaten

Sie können auch eindeutige Passwörter für gemeinsam genutzte Boxen⁵, Dokumente und Adressbücher auf Ihren Epson Druckern festlegen. Für eine vollständige Sicherheit werden die Daten vom Drucker gelöscht, sobald die Aufträge abgeschlossen sind oder die Stromversorgung ausgeschaltet ist. Wenn das Gerät über eine Festplatte verfügt, werden alle Daten verschlüsselt und nach jedem Druckauftrag gelöscht. Für zusätzlichen Schutz kann der Administrator auch die Festplatte überschreiben. Weitere Informationen finden Sie in unserem [Sicherheitshandbuch](#).

Datenschutz

HDD-Verschlüsselung, sichere Datenlöschung auf der Festplatte, Trusted Platform Module (TPM) und Passwortverschlüsselung

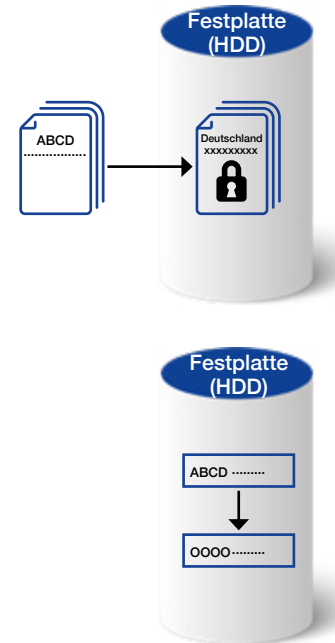
Verschlüsselung von auf HDD gespeicherten Daten

Die Kundendaten werden stets durch Verschlüsselung geschützt, wenn sie auf einer internen HDD eines Multifunktionsdruckers gespeichert werden. Die Verschlüsselung der Daten verhindert den unbefugten Zugriff oder einen Angriff auf persönliche Daten, sollte die HDD gestohlen werden. Die HDD verfügt über ein selbstverschlüsselndes Laufwerk, und die Dokumentdaten werden mittels AES-256 verschlüsselt.

Löschen von Auftragsdaten

Wenn die Funktion aktiviert ist, werden die Daten auf der Festplatte⁵ wie nachfolgend beschrieben überschrieben, um eine Wiederherstellung der Daten zu verhindern. Es gibt mehrere Optionen:

1. Schnelles Löschen: Der Verschlüsselungsschlüssel wird geändert, damit gelöschte Daten nicht wiederhergestellt werden können.
2. Sichere sequenzielle Löschung: Der Verschlüsselungsschlüssel wird geändert, und die gelöschten Daten auf der Festplatte werden mit Nullen (0) überschrieben, um sicherzustellen, dass die gelöschten Daten nicht wiederhergestellt werden können.



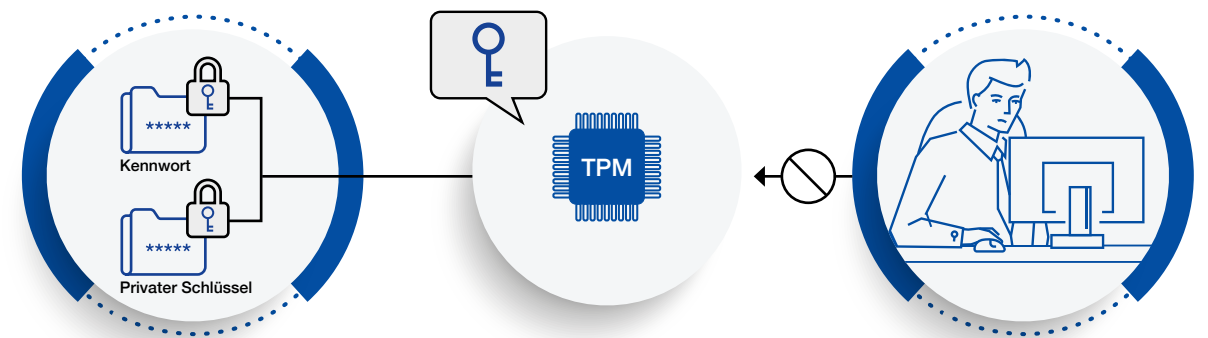
Ausführliche Informationen zur Löschung von Auftragsdaten finden Sie in der Bedienungsanleitung zu Ihrem Produkt.

TPM

Bei Modellen mit TPM (Trusted Platform Module) erhöht sich die Sicherheitsstufe wie folgt:

- Die Verschlüsselungsschlüssel zum Wiederherstellen von verschlüsselten Kennwörtern und Daten zu privaten Schlüsseln werden auf dem TPM-Chip gespeichert.
- Der TPM-Chip kann auf Hardware-Ebene vor nicht autorisierter Analyse geschützt werden, da kein Zugriff auf den TPM-Chip von außen möglich ist.
- Die Zufallszahlen von TPM werden als Sitzungsschlüssel für die Kommunikation mit dem Browser (Web Config) verwendet.
- Die echten Zufallszahlen von TPM werden zum Generieren von Authentifizierungsschlüsseln für die verschlüsselte HDD verwendet.

Die Multifunktionsdrucker verfügen über einen TPM 2.0-Chip.



	WorkForce Enterprise	WorkForce Enterprise AM	
Produktname	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 und AM-M5500	AM-C400/C550/C550z
Typ	DIN A3	DIN A3	DIN A4
Netzwerksicherheit			
TLS-Kommunikation	✓	✓	✓
TLS1.1, TLS1.2, TLS1.3	✓	✓	✓
Steuern von Protokollberechtigungen und -ausschlüssen	✓	✓	✓
IPsec/IP-Filterung	✓	✓	✓
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-Authentifizierung	✓	✓	✓
EAP-TLS, PEAP-TLS	✓	✓	✓
PEAP/MSCHAPv2	✓	✓	✓
EAP-TTLS	✓	✓	✓
AES128/AES256/3DES/RC4□	✓	✓	✓
SNMPv3	✓	✓	✓
WPA3	✓	✓	✓
Trennung der Schnittstellen	✓	✓	✓
Schutz Ihres Multifunktionsdruckers			
Abschalten der USB-Verbindung zum Computer	✓	✓	✓
Deaktivieren der externen Schnittstellen	✓	✓	✓
Schutz vor Viren auf USB-Speichersticks	✓	✓	✓
Sicherheit beim Drucken/Scannen			
Vertrauliche Aufträge	✓*6	✓	✓
Kopierschutzmuster ⁶	✓	✓	✓
Wasserzeichen ⁶	✓	✓	✓
PDF-Verschlüsselung	✓	✓	✓
S/MIME	✓	✓	✓
AES-128/AES-192/AES-256/3DES	✓	✓	✓
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✓	✓	✓
Domain-Einschränkungen	✓*7	✓	✓
Autorisierungspasswort für Scan zu Netzwerkordner/FTP, Scan zu E-Mail und E-Mail-Benachrichtigung	–	✓*7	✓
Unterstützung langer Authentifizierungspasswörter	–	–	✓*8
Standarddeaktivierung des Dateizugriffs von PDL	✓*7	✓	
Sicheres Drucken	✓	✓	✓
Fax-Sicherheit ⁹			
Einschränkungen der Direktwahl	✓	✓	✓
Prüfen der Adressenliste	✓	✓	✓
Ruftonerkennung	✓	✓	✓
Maßnahmen bei zurückgelassenen Faxen	✓	✓	✓
Übermittlungsbestätigungsbericht	✓	✓	✓
Löschen der Sicherungskopie von empfangenen Faxen	✓	✓	✓
Einschränken des Sendens an mehrere Empfänger	✓	✓	✓
Druckersicherheit			
Automatische Firmware-Updates	✓	✓	✓
Schutz vor illegalen Firmware-Updates	–	✓	✓
Sicheres Booten	–	✓	✓
Erkennung von Malware-Infiltration	✓*7	✓	✓
Sicherheitsmaßnahmen beim Entsorgen des Druckers			
Zurücksetzen auf Werkseinstellungen	✓	✓	✓
Sicherheitszertifizierung und -standards			
ISO15408/IEEE2600.2™	✓	✓	✓

	WorkForce Enterprise	WorkForce Enterprise AM	
Produktname	WF-C21000/C20600/C20750	AM-C4000/C5000/ C6000 und AM-M5500	AM-C400/C550/C550z
Typ	DIN A3	DIN A3	DIN A4
Sicherheitsfunktionen durch Kompatibilität mit Software von Drittanbietern			
Mit Open Platform kompatible Modelle	✓	✓	✓
Epson Print Admin (EPA)/EPA Serverless			
Benutzerauthentifizierung über ID-Karten/Anmeldeinformationen/PIN-Code	✓	✓	✓
Vollständige Kontrolle über Geräteaktionen pro Person	✓	✓	✓
Personalisierung des MFP-Menüs	✓	✓	✓
Pull-Druck und Direktdruck	✓	✓	✓
Scannen und an mich senden (E-Mail, Ordner)	✓	✓	✓
Scannen und an Cloud-Services senden (SharePoint Online, OneDrive for Business, Teams und Google Drive) ¹⁰	✓	✓	✓
Als passwortgeschützte PDF-Datei scannen	✓	✓	✓
Erweiterte Scan-Workflow-Einstellungen ¹¹	✓	✓	✓
Automatischer Druck aus Cloud-Services (OneDrive for Business, Share-Point Online und Teams) ¹⁰	✓	✓	✓
Synchronisation mit Verzeichnisdiensten (LDAP, Open LDAP, Microsoft EntraID, Microsoft Entra DS, Google Secure LDAP & Google Cloud Directory) ¹⁰	✓	✓	✓
Berichte – BenutzerschutzEinstellung – Dateiname ausblenden	✓	✓	✓
Passwortrichtlinie, Kontosperr ¹¹	✓	✓	✓
Druckregeln und -richtlinien ¹¹	✓	✓	✓
Nachverfolgung und Berichterstellung	✓	✓	✓
Quote ¹⁰	✓	✓	✓
Sicheres mobiles Drucken (AirPrint und Mopria) ¹²	–	✓	✓
Schutz von Benutzerdaten			
Sicherheit der Box-Funktion	✓	✓	✓
Schutz für Ihr Adressbuch	✓	✓	✓
Handhabung der vom Multifunktionsdrucker verarbeiteten Daten	✓	✓	✓
Verschlüsselung der auf der Festplatte gespeicherten Daten	✓	✓	✓
Löschen von Auftragsdaten	✓	✓	✓
Kennwortverschlüsselung	✓	✓	✓
TPM	✓*13	✓	✓
Spiegelung der Festplatte	–	✓	–
Einstellungen zur Einschränkung von Benutzerrechten			
Bedienfeldsperre	✓	✓	✓
Zugriffskontrolle	✓	✓	✓
Authentifiziertes Drucken/Scannen ⁸	✓	✓	✓
Kennwortrichtlinie	✓	✓	✓
Überwachungsprotokoll	✓	✓	✓

Weitere Informationen erhalten Sie von Ihrem Epson-Ansprechpartner vor Ort.

Name:

Tel.:

E-Mail:

1. „Print Security Landscape, 2025 – Identität, KI und Quantum: Navigation in der neuen Bedrohungslandschaft“, Quocirca, Juli 2025.
2. Keypoint Intelligence Security Validation Testing Seal 2024-2026 gilt für AM-C400 und AM-C550.
3. ISO/IEC 15408 wird nicht mit einer Standardkonfiguration geliefert. Spezielle Firmware und spezieller Einrichtungsprozess erforderlich.
4. Das Logo der CCRA-Zertifizierung zeigt, dass das Produkt in Übereinstimmung mit dem JISEC (Japan Information Technology Security Evaluation and Certification Scheme) geprüft und zertifiziert wurde. Dies stellt keine Garantie dar, dass das Produkt vollständig frei von Schwachstellen ist. Es bedeutet ebenfalls nicht, dass das Produkt mit allen notwendigen Sicherheitsfunktionen für alle Betriebsbedingungen ausgestattet ist.
5. Eine vollständige Liste der Modellspezifikationen finden Sie unter support.epson.net/security/de
6. Es wird nur der Windows-Drucktreiber unterstützt.
7. Um diese Funktion zu verwenden, aktualisieren Sie die Druckerfirmware auf die neueste Version.
8. Erfordert eine authentifizierte Druckmethode.
9. Nur verfügbar, wenn die Option Faxkarte installiert ist.
10. Gilt für Epson Print Admin und nur für bestimmte Produkte auf Epson Print Admin Serverless.
11. Gilt nur für Epson Print Admin.
12. Gilt nur für Epson Print Admin Serverless.
13. Wird je nach Region möglicherweise nicht unterstützt. Genauere Einzelheiten zur Verfügbarkeit in Ihrem Land erhalten Sie von Ihrer lokalen Vertriebsniederlassung.



Bitte verantwortungsvoll recyceln

Epson Deutschland GmbH
Schiessstraße 49
D-40549 Düsseldorf
www.epson.de/contactus

Epson in Österreich
www.epson.at/contactus
Epson in der Schweiz
www.epson.ch/contactus

EpsonDE
 [epson-deutschland-gmbh](https://www.linkedin.com/company/epson-deutschland-gmbh)
 @epsondeutschland