

# Řešení zabezpečení firemního tisku

Řada WorkForce  
Enterprise 2 a AM-C



# Chraňte zabezpečení sítě bez ohledu na to, kde se tiskne

Je snadné přehlédnout důležitá bezpečnostní opatření na síťových zařízeních ve vaší firmě. A ačkoli jste o tom možná ještě neuvažovali, mohou být multifunkční tiskárny (MFP), skenery a jiná připojená nebo síťová zařízení náchylná na ohrožení zabezpečení.

Rozšiřování práce z domova a hybridní práce toto riziko ještě více zvýšilo. Studie společnosti Quocirca<sup>1</sup> zjistila, že zatímco 70 % osob s rozhodovací pravomocí v oblasti IT věří, že tisk je pro jejich podnikání zásadní nebo velmi důležitý, 31 % se obává bezpečnostních rizik spojených s tiskem na dálku / doma a jen 19 % si je zcela jistá, že jejich infrastruktura je bezpečná.

Průměrné náklady za únik dat v souvislosti s tiskem představují 21 209 000 CZK\*, což nelze brát na lehkou váhu.

Díky přístupu společnosti Epson k zabezpečení tiskáren však lze toto riziko zmírnit, bez ohledu na to, kde tisk ve vaší firmě probíhá.



## 70 %

osob s rozhodovací pravomocí v oblasti IT věří, že tisk je pro jejich podnikání zásadní nebo velmi důležitý.

## 31 %

z nich se zabývá bezpečnostními riziky spojenými se vzdáleným/domácím tiskem.

## 19 %

respondentů si je zcela jistá, že jejich infrastruktura tisku je bezpečná.

\*Založeno na hodnotě 743 000 liber podle citace společnosti Quocirca a po převodu na 21 209 000 CZK s použitím kurzu FX z xe.com k 9. 1. 2024.

# Přístup společnosti Epson k zabezpečení

Pro náš přístup k zabezpečení je důležité posílení síťových schopností vašich zařízení. Každá tiskárna Epson WorkForce je postavena na třech základních principech, které zajišťují bezpečnost zařízení Epson po celou dobu jejich životnosti:

1. Zabezpečení produktů je základem pro kvalitu.
2. Informace a znalosti o bezpečnosti jsou aktivně sdíleny, takže máte vždy aktuální informace.
3. Zranitelná místa jsou neustále kontrolována, aby se maximalizovala ochrana zařízení.

## Funkce zabezpečení navržené kolem vás

Chráněná data a zabezpečené sítě jsou standardně dodávány s multifunkčními zařízeními Epson využívajícími funkce, které mohou pomoci s obecným nařízením o ochraně osobních údajů (GDPR) a společenskou odpovědností firem (CSR). Tato bezpečnostní opatření, která jsou integrována přímo do našich produktů, vám dávají jistotu, že vaše firma splňuje vaše bezpečnostní požadavky.

### Bezpečný tisk a skenování

Chcete-li zajistit ochranu osobních údajů dokumentů a zabránit neoprávněným osobám v prohlížení výstupu bez dozoru na zařízení, odešlete vaše dokumenty jako „důvěrnou práci“ z ovladače tisku/skenování.

Přístup k funkcím zařízení lze omezit pomocí zámku předního panelu.

### Na zařízení

Se správcem zařízení Epson se zabezpečení zařízení spravuje jednodušeji. Jelikož je kompatibilní se širokou řadou našich síťových tiskáren, uživatelé mohou vše ovládat prostřednictvím chytrého a intuitivního rozhraní. Pomocí jednoho jednotného nástroje mohou správci zabezpečit tisk a zobrazování, včetně vzdáleného zamykání obrazovek, aby se zabránilo neoprávněným úpravám profilu.

### Zabezpečená komunikace

Můžete filtrovat IP adresy, služby, čísla příjmových a přenosových portů, které mají přístup k zařízením Epson. Pomocí funkce IPSec můžete také šifrovat veškerou síťovou komunikaci.

### Ochrana PDF

Přidejte do naskenovaných souborů PDF funkci ochrany heslem<sup>3</sup>, abyste je ochránili před neoprávněným prohlížením a zabránili úpravám a tisku dokumentů.

### Zpracování dokumentů a správa dat

Spravujte centrálně více úloh, od profilů úloh skenování po přístupová práva uživatelů. Správci mohou centrálně spravovat různé úkoly, od profilů úloh skenování po přístupová práva uživatelů. Správci IT mají mnoho způsobů, jak kontrolovat přístupová práva k pracovním pozicím, včetně ID uživatele a hesla, aktivního adresáře LDAP, ID přihlašovací karty a kódu PIN.

# Zabezpečení uznávané po celém světě

Ve společnosti Epson udáváme kritéria našeho zabezpečení v globálním měřítku. Splňujeme normu ISO/IEC 15408<sup>3</sup>, která se také nazývá Společná kritéria (CC), což je mezinárodní standard pro bezpečnostní opatření v IT produktech a systémech, a certifikaci CCRA, která prokazuje, že produkt byl certifikován v souladu s japonským plánem hodnocení a certifikace bezpečnosti informačních technologií (JISEC).



## Zabezpečení sítě

Hlavní prioritou zabezpečení sítě je, že správci mohou nastavit individuální oprávnění a omezení pro širokou škálu síťových úkolů. S našimi tiskárnami WorkForce Enterprise 2 mohou správci filtrovat také IP adresy, typy služeb, čísla přijímacích a přenosových portů pomocí funkce filtrování IP Sec / IP. Při rozhodování, zda přijmout nebo zablokovat konkrétní IP adresy. Podporujeme také šifrování e-mailů SNMPv3 a TLS1.3.



## Ochrana all-in-one tiskárny

Pro další ochranu vašich tiskáren můžete zablokovat přístup z počítače prostřednictvím USB a deaktivovat paměťovou kartu a paměťová rozhraní USB. Můžete také použít vodoznak proti kopírování<sup>2</sup>, abyste zabránili neoprávněnému duplikování původních dokumentů, a šifrování PDF<sup>2</sup>, abyste zajistili, že digitální dokumenty zůstanou v bezpečí.



## Zabezpečený tisk/skenování

Možnost „důvěrná úloha“ znamená, že můžete chránit soukromí dokumentů a zabránit nechtěnému zobrazení výstupu bez dozoru.



## WPA3

Nejnovější multifunkční zařízení Epson podporují technologii WPA3<sup>2</sup>, což je nejnovější ověřovací a šifrovací technologie pro Wi-Fi (bezdrátová síť LAN), která firmám poskytuje robustnější a silnější ochranu jejich dat prostřednictvím bezdrátové sítě.



## Ochrana dokumentů

Autentizační tisk, skenování autentizace a protokolování úloh.



## Kontrola přístupu

Ověřování uživatele a omezení funkcí.



## Ochrana zařízení

Ověřování podpisů firmwaru, zabezpečené spuštění a nová detekce napadení malwarem po spuštění.





## Ochrana údajů uživatelů

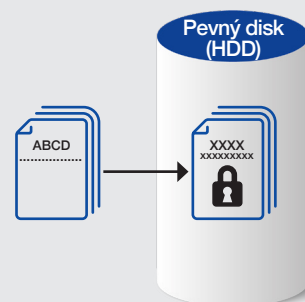
Na svých tiskárnách Epson můžete také nastavit jedinečná hesla pro sdílená pole<sup>2</sup>, dokumenty a adresáře. Pro úplné zabezpečení jsou data vymazána z tiskárny, jakmile jsou úlohy dokončeny nebo je vypnuto napájení. Pokud má zařízení pevný disk, všechna data jsou šifrována a po každé tiskové úloze jsou vymazána. Pro zvýšenou ochranu může správce také přepsat pevný disk. Další informace naleznete v našem průvodci zabezpečením na adrese [epson.eu/bi-security-solutions](http://epson.eu/bi-security-solutions).

## Ochrana údajů

Šifrování pevného disku, bezpečné vymazání dat na pevném disku, čip Trusted Platform Module (TPM) a šifrování hesel.

### Šifrování dat uložených na pevném disku

Při ukládání dat na interní pevný disk v all-in-one tiskárně vždy chráníme data zákazníků šifrováním. Šifrování dat brání neoprávněnému přístupu nebo škodlivému útoku na osobní údaje v případě odcizení pevného disku. Pevný disk se dodává se samošifrovací jednotkou a dokumentová data jsou šifrována pomocí AES-256.

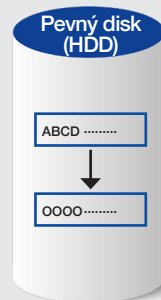


### Sekvenční odstranění dat úlohy

Pokud je tato funkce povolena, odstraněná data na pevném disku<sup>2</sup> se přepíše následujícími způsoby, aby se zabránilo obnovení.

Existuje několik možností:

1. Rychlé odstranění: Šifrovací klíč se změní, aby se zabránilo obnovení odstraněných dat.
2. Bezpečné sekvenční odstranění: Šifrovací klíč se změní a odstraněná data na pevném disku budou přepsána nulami, aby se dále zajistilo, že odstraněná data nebude možné obnovit.



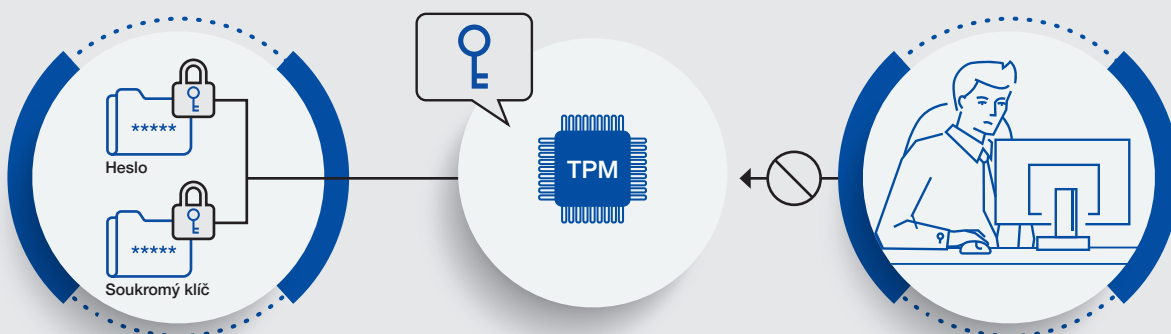
Podrobné pokyny pro vymazání dat úlohy naleznete v uživatelské příručce k produktu.

## TPM

U modelů Trusted Platform Module (TPM) se úroveň zabezpečení zvyšuje následovně:

- Šifrovací klíče pro obnovení šifrovaných hesel a soukromých klíčových informací jsou uloženy na čipu TPM.
- Čip TPM lze chránit před neautorizovanou analýzou na úrovni hardwaru, protože k čipu TPM nelze přistupovat zvenčí tiskárny.
- Skutečná náhodná čísla TPM se používají jako klíče relace pro komunikaci s prohlížečem (konfigurace webu).
- Skutečná náhodná čísla TPM se používají při generování ověřovacích klíčů pro šifrovaný pevný disk.

All-in-one tiskárna má čip TPM 2.0.



	WorkForce Enterprise			AM-C		
Název produktu	WF-C21000	WF-C20600	WF-C20750	AM-C6000	AM-C5000	AM-C4000
Typ	A3	A3	A3	A3	A3	A3
<b>Zabezpečení sítě</b>						
Komunikace TLS	✓	✓	✓	✓	✓	✓
TLS1.1	✓	✓	✓	✓	✓	✓
TLS1.2	✓	✓	✓	✓	✓	✓
TLS1.3	✓*1	✓*1	✓*1	✓	✓	✓
Kontrola oprávnění a vyloučení protokolu	✓	✓	✓	✓	✓	✓
Filtrování 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	✓	✓	✓	✓	✓	✓
Ověření IEEE802.1X	✓	✓	✓	✓	✓	✓
EAP-TLS	✓	✓	✓	✓	✓	✓
PEAP-TLS	✓	✓	✓	✓	✓	✓
PEAP/MSCHAPv2	✓	✓	✓	✓	✓	✓
EAP-TTLS	✓	✓	✓	✓	✓	✓
AES128/AES256/3DES/RC4	✓	✓	✓	✓	✓	✓
SNMPv3	✓	✓	✓	✓	✓	✓
WPA3	✓	✓	✓	✓	✓	✓
Separace mezi rozhraními	✓	✓	✓	✓	✓	✓
<b>Ochrana all-in-one tiskárny</b>						
Blokování připojení USB z počítače	✓	✓	✓	✓	✓	✓
Vypnutí externího rozhraní	✓	✓	✓	✓	✓	✓
Manipulace s viry zaváděnými pamětí USB	✓	✓	✓	✓	✓	✓
<b>Zabezpečení tisku/skenování</b>						
Důvěrné pracovní pozice	✓*2	✓*2	✓*2	✓	✓	✓
Ochranný vzorek proti kopírování	✓*2	✓*2	✓*2	✓*2	✓*2	✓*2
Vodoznak	✓*2	✓*2	✓*2	✓*2	✓*2	✓*2
Šifrování PDF	✓	✓	✓	✓	✓	✓
S/MIME	✓	✓	✓	✓	✓	✓
AES-128/AES-192/AES-256/3DES	✓	✓	✓	✓	✓	✓
SHA-1/SHA-256/SHA-384/SHA-512/MD5	✓	✓	✓	✓	✓	✓
Zabezpečení faxu	✓	✓	✓	✓	✓	✓
<b>Zabezpečení faxu</b>						
Omezení domény	✓*1	✓*1	✓*1	✓	✓	✓
Autorizační heslo pro skenování do síťové složky / FTP, skenování do e-mailu a e-mailové oznámení	-	-	-	✓*1	✓*1	✓*1
Bezpečný tisk	✓	✓	✓	✓	✓	✓
Výchozí deaktivace přístupu k souborům z PDL	✓*1	✓*1	✓*1	✓	✓	✓
Omezení přímého vytáčení	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Potvrzení seznamu adres	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Detekce tónů vytáčení	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Opatření proti opuštěným faxům	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Zpráva o potvrzení přenosu	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Odstranění záložních dat pro přijaté faxy	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3
Omezení odesílání více příjemcům	✓*3	✓*3	✓*3	✓*3	✓*3	✓*3

\*1. Chcete-li tuto funkci použít, aktualizujte firmware tiskárny na nejnovější verzi.

\*2. Podporován je pouze ovladač tiskárny Windows.

\*3. K dispozici pouze při instalaci volitelné faxové desky.

Název produktu	WorkForce Enterprise			AM-C		
	WF-C21000	WF-C20600	WF-C20750	AM-C6000	AM-C5000	AM-C4000
Typ	A3	A3	A3	A3	A3	A3
<b>Bezpečnostní funkce díky kompatibilitě se softwarem třetích stran</b>						
Model kompatibilní s otevřenou platformou	✓	✓	✓	✓	✓	✓
<b>Epson Print Admin</b>						
Kvóta, tisková pravidla a zásady	✓	✓	✓	✓	✓	✓
Ověřování uživatelů pomocí identifikačních karet / přihlašovacích údajů / kódu PIN	✓	✓	✓	✓	✓	✓
Přístup k funkcím přiřazeným roli nebo oddělení	✓	✓	✓	✓	✓	✓
Prizpůsobení nabídky multifunkčních zařízení podle skupiny nebo jednotlivce	✓	✓	✓	✓	✓	✓
Tisk s ověřením	✓	✓	✓	✓	✓	✓
Přímý tisk	✓	✓	✓	✓	✓	✓
Skenování a odeslání mně (e-mail, složka)	✓	✓	✓	✓	✓	✓
Skenování do cloudových služeb (OneDrive for Business, SharePoint online, Google Drive)	✓	✓	✓	✓	✓	✓
Pokročilá nastavení pracovního postupu skenování	✓	✓	✓	✓	✓	✓
Synchronizace s adresářovou službou (LDAP, Open LDAP, Azure AD, Azure AD DS, Google Secure LDAP a Google Cloud Directory)	✓	✓	✓	✓	✓	✓
Skenování souborů PDF chráněných heslem	✓	✓	✓	✓	✓	✓
<b>Epson Print Admin Serverless</b>						
Ověřování uživatelů pomocí identifikačních karet / přihlašovacích údajů / kódu PIN	✓	✓	✓	✓	✓	✓
Úplná kontrola akcí zařízení na jednotlivce	✓	✓	✓	✓	✓	✓
Tisk s ověřením	✓	✓	✓	✓	✓	✓
Přímý tisk	✓	✓	✓	✓	✓	✓
Skenování a odeslání mně (e-mail, složka)	✓	✓	✓	✓	✓	✓
Sledování a vykazování	✓	✓	✓	✓	✓	✓
Synchronizace s adresářovou službou (LDAP a Open LDAP)	✓	✓	✓	✓	✓	✓
Podpora tiskové kvóty	✓	✓	✓	✓	✓	✓
<b>Ochrana údajů uživatelů</b>						
Zabezpečení boxu	✓	✓	✓	✓	✓	✓
Ochrana vašeho adresáře	✓	✓	✓	✓	✓	✓
Zpracování dat pomocí all-in-one tiskárny	✓	✓	✓	✓	✓	✓
Šifrování uložených dat na pevném disku	✓	✓	✓	✓	✓	✓
Sekvenční odstranění dat úlohy	✓	✓	✓	✓	✓	✓
Šifrování heslem	✓	✓	✓	✓	✓	✓
TPM	✓*4	✓*4	✓*4	✓	✓	✓
<b>Provozní omezení</b>						
Zámek panelu	✓	✓	✓	✓	✓	✓
Kontrola přístupu	✓	✓	✓	✓	✓	✓
Tisk s ověřením	✓*5	✓*5	✓*5	✓*5	✓*5	✓*5
Zásady pro hesla	✓	✓	✓	✓	✓	✓
Protokol auditu	✓	✓	✓	✓	✓	✓
<b>Bezpečnost tiskárny</b>						
Automatické aktualizace firmwaru	✓	✓	✓	✓	✓	✓
<b>Bezpečnostní opatření při likvidaci tiskárny</b>						
Obnovit výchozí tovární nastavení	✓	✓	✓	✓	✓	✓
<b>Bezpečnostní certifikace a normy</b>						
ISO15408/IEEE2600.2™	✓	✓	✓	✓*6	✓*6	✓*6

\*4. V závislosti na regionu nemusí být podporováno. Ohledně dostupnosti ve vaší zemi kontaktujte místní prodejní kancelář.

\*5. Vyžaduje ověřenou metodu tisku.

\*6. K dispozici ve 4. čtvrtletí 2023.

## Další informace vám poskytne obchodní zástupce společnosti Epson.

Jméno:

Tel.:

E-mail:

EPSON a WorkForce jsou registrované ochranné známky a EPSON Exceed Your Vision je registrované logo společnosti Seiko Epson Corporation. Názvy a značky všech ostatních produktů jsou ochrannými známkami a/nebo registrovanými ochrannými známkami příslušných vlastníků. Společnost Epson se zřiká veškerých práv na tyto značky.

1. „The Print Security Landscape, 2023 – Zabezpečení tiskové infrastruktury v prostředí rostoucích hrozeb“, Quocirca, květen 2023.
2. Úplný seznam specifikací modelů naleznete na adrese [www.epson.eu/bi-security-solutions](http://www.epson.eu/bi-security-solutions).
3. Norma ISO/IEC 15408 se nedodává se standardní konfigurací. Je vyžadován speciální firmware a speciální proces nastavení.
4. Platí pro WorkForce Enterprise 2.
5. Platí pro řadu AM-C.



Recyklujte, prosím,  
zodpovědně

EPSON EUROPE B.V.  
Organizační složka  
Greenline Kačerov, Jihlavská 1558/21  
140 00 Praha - Michle  
Česká republika

Infolinka: +420 246 037 281  
[www.epson.cz](http://www.epson.cz)



@epsonczsk  
epson-cesko-a-slovensko

Ochranné známky a registrované ochranné známky jsou vlastnictvím společnosti Seiko Epson Corporation nebo příslušných vlastníků. Informace o produktu mohou být změněny bez předchozího upozornění.