

Rendszergazdai kézikönyv

Tartalomjegyzék

Szerzői jog

Védjegyek

Tájékoztató a kézikönyvről

Jelölések és ábrák.	6
A kézikönyvben szereplő leírások.	6
Operációs rendszerre vonatkozó hivatkozások.	6

Bevezetés

Manuális komponens.	8
Az ebben az Útmutatóban használt kifejezések meghatározása.	8

Előkészítés

A lapolvasó beállításának és kezelésének folyamata.	10
Példa hálózati környezetre.	11
A lapolvasó csatlakozási beállításainak bemutatása — példa.	11
Hálózathoz történő csatlakozás előkészítése.	12
Információszerzés a Kapcsolat beállításairól.	12
A lapolvasó műszaki adatai.	12
A portszám használata.	13
Az IP-cím hozzárendelésének a típusa.	13
DNS-kiszolgáló és Proxy-kiszolgáló.	13
A hálózati kapcsolat beállításának módja.	13

Kapcsolat

Csatlakoztatás a hálózathoz.	15
Csatlakozás a hálózathoz a kezelőpanelről.	15
Csatlakozás a hálózathoz a telepítő segítségével.	19

A funkciók beállításai

Szoftverek a beállításhoz.	22
Web Config (Weboldal az eszközhez).	22
A beolvasási funkciók használata.	24
Beolvasás számítógépről.	24
Lapolvasás a kezelőpanel használatával.	26
Rendszerbeállítások elvégzése.	28
Rendszerbeállítások elvégzése a kezelőpanelről.	28

Rendszerbeállítások elvégzése a Web Config alkalmazás segítségével.	30
---	----

Alapvető biztonsági beállítások

Az alap biztonsági funkciók bemutatása.	32
A rendszergazdai jelszó beállítása.	33
A rendszergazdai jelszó konfigurálása a kezelőpanelről.	33
A rendszergazdai jelszó konfigurálása Web Config alkalmazással.	33
A rendszergazdai jelszóval zárolandó elemek.	34
Protokollok vezérlése.	35
Engedélyezhető és letiltható protokollok.	36
Protokollbeállítások.	37

Működési és kezelési beállítások

Egy eszköz adatainak a megerősítése.	40
Eszközök kezelése (Epson Device Admin).	40
E-mail értesítések fogadása bizonyos események bekövetkeztekor.	41
Az e-mailes értesítésekről.	41
Az e-mailes értesítések konfigurálása.	41
Levelezőkiszolgáló beállítása.	42
A levelezőkiszolgáló kapcsolódásának ellenőrzése.	44
Firmware frissítése.	46
Firmware frissítése Web Config használatával.	46
Firmware frissítése az Epson Firmware Updater használatával.	46
Biztonsági mentés készítése a beállításokról.	47
A beállítások exportálása.	47
A beállítások importálása.	47

Problémák megoldása

Problémamegoldási tippek.	49
A Kiszolgálónapló és a Hálózati eszköz naplójának ellenőrzése.	49
Hálózati beállítások inicializálása.	49
Hálózati beállítások visszaállítása a nyomtató kezelőpaneljén.	49
Az eszközök és a számítógépek közötti kommunikáció ellenőrzése.	49
Csatlakozás ellenőrzése Ping paranccsal — Windows.	49

Tartalomjegyzék

Csatlakozás ellenőrzése Ping paranccsal — Mac OS.	51	Problémák megoldása a fokozott biztonság érdekében.	88
Problémák a hálózati szoftver használatával.	52	A biztonsági beállítások visszaállítása.	88
Nem sikerül elérni a Web Config alkalmazást.	52	A hálózati biztonsági funkciókkal kapcsolatos problémák.	89
A modell neve és/vagy IP-címe nem jelenik meg az EpsonNet Config alkalmazásban.	53	A digitális tanúsítvány használatával kapcsolatos problémák.	91
Melléklet			
A hálózati szoftver bemutatása.	55		
Epson Device Admin.	55		
EpsonNet Config.	55		
EpsonNet SetupManager.	56		
IP-cím hozzárendelése EpsonNet Config alkalmazással.	56		
IP-cím hozzárendelése csoportos beállítások alkalmazásával.	56		
IP-cím hozzárendelése az egyes eszközökhöz.	59		
Port használata a lapolvasóhoz.	60		
Speciális biztonsági beállítások vállalatok számára			
Biztonsági beállítások, és a veszélyek megelőzése.	62		
A biztonsági funkciók beállításai.	63		
SSL/TLS kommunikáció a lapolvasóval.	63		
Tudnivalók a digitális tanúsítványról.	63		
CA által aláírt tanúsítvány beszerzése és importálása.	64		
Hitelesítésszolgáltató által aláírt tanúsítvány törlése.	68		
Saját aláírt tanúsítvány frissítése.	68		
A CA Certificate konfigurálása.	69		
Titkosított kommunikáció IPsec-/IP-szűrés funkcióval.	71		
Tudnivalók az IPsec/IP Filtering alkalmazásról.	71		
A(z) Default Policy beállítása.	72		
A(z) Group Policy beállítása.	75		
IPsec/IP Filtering konfigurációs példák.	81		
Tanúsítvány beállítása az IPsec/IP Filtering hálózathoz.	82		
Az SNMPv3 protokoll használata.	83		
Tudnivalók az SNMPv3 protokollról.	83		
Az SNMPv3 konfigurálása.	83		
A lapolvasó csatlakoztatása IEEE802.1X hálózathoz.	85		
IEEE802.1X hálózat beállítása.	85		
Tanúsítvány beállítása az IEEE802.1X hálózathoz.	87		

Szerzői jog

A jelen kiadvány semelyik része sem reprodukálható, tárolható visszakereső-rendszerben vagy vihető át bármiféle eszközzel, elektronikusan, mechanikusan, fénymásolással, felvétellel vagy bármilyen más módszerrel a Seiko Epson Corporation előzetes írásbeli engedélye nélkül. A dokumentum tartalmának felhasználására vonatkozóan nem vállalunk felelősséget. A dokumentum tartalmának felhasználásából származó károkért sem vállalunk semmiféle felelősséget. A jelen dokumentumban lévő információk csak az ezzel az Epson termékkel történő felhasználásra vonatkoznak. Az Epson nem felelős az olyan esetekért, amikor ezeket az információkat más termékekre alkalmazzák.

Sem a Seiko Epson Corporation, sem bármely leányvállalata nem vállal felelősséget a termék megvásárlójának vagy harmadik félnek olyan karáért, veszteségéért, költségéért vagy kiadásáért, amely a következőkből származik: baleset, a termék nem rendeltetésszerű vagy helytelen használata, a termék jogosulatlan módosítása, javítása vagy megváltoztatása, illetve (az Egyesült Államok kivételével) a Seiko Epson Corporation üzemeltetési és karbantartási utasításainak nem pontos betartása.

A Seiko Epson Corporation nem vállal felelősséget az olyan károkért és problémákért, amelyek a Seiko Epson Corporation által Eredeti Epson terméknek, vagy az Epson által jóváhagyott terméknek nem minősített kiegészítők vagy fogyóeszközök használatából származnak.

A Seiko Epson Corporation nem tehető felelőssé az olyan károkért, amelyek a Seiko Epson Corporation által Epson jóváhagyott terméknek nem minősített bármely csatlakozókábel használatából következő elektromágneses interferenciából származnak.

©Seiko Epson Corporation 2016.

A kézikönyv tartalma és a termékspecifikációk minden külön figyelmeztetés nélkül módosulhatnak.

Védjegyek

- ❑ Az EPSON® bejegyzett védjegy, az EPSON EXCEED YOUR VISION és az EXCEED YOUR VISION pedig a Seiko Epson Corporation védjegye.
- ❑ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❑ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❑ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❑ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❑ Általános megjegyzés: az itt használt egyéb terméknevek kizárólag az azonosítás célját szolgálják, és előfordulhat, hogy tulajdonosaik védjeggyel védték azokat. Az Epson ezekkel a védjegyekkel kapcsolatban semmiféle jogra nem tart igényt.

Tájékoztató a kézikönyvről

Jelölések és ábrák

**Figyelem!**

Az ilyen utasításokat a testi sérülések elkerülése érdekében gondosan be kell tartani.

**Fontos:**

Az ilyen utasításokat a berendezés megsérülésének elkerülése végett kell betartani.

Megjegyzés:

A lapolvasó működésével kapcsolatos hasznos tanácsokat és korlátozásokat tartalmazó utasítások.

Kapcsolódó információ

➔ Az ikonra kattintva kapcsolódó tájékoztatások nyílnak meg.

A kézikönyvben szereplő leírások

- A szkennermeghajtó képernyőfelvételei és a(z) Epson Scan 2 (lapolvasó illesztőprogram) képernyői Windows 10 vagy OS X El Capitan rendszeren készültek. A képernyőkön megjelenő tartalom a készülék típusától és az adott helyzettől függően változik.
- A kézikönyvben szereplő képek csak példaként szolgálnak. Ugyan az egyes modellek esetében lehetnek különbségek, de a készüléket ugyanúgy kell működtetni.
- Az LCD képernyőn megjelenő menük a modelltől és a beállításoktól függően eltérő elemeket tartalmazhatnak.

Operációs rendszerre vonatkozó hivatkozások

Windows

Ebben a kézikönyvben a(z) „Windows 10”, „Windows 8.1”, „Windows 8”, „Windows 7”, „Windows Vista”, „Windows XP”, „Windows Server 2016”, „Windows Server 2012 R2”, „Windows Server 2012”, „Windows Server 2008 R2”, „Windows Server 2008”, „Windows Server 2003 R2” és „Windows Server 2003” kifejezések az alábbi operációs rendszerekre vonatkoznak. Továbbá, a „Windows” kifejezés valamennyi verzióra vonatkozik.

- Microsoft® Windows® 10 operációs rendszer
- Microsoft® Windows® 8.1 operációs rendszer
- Microsoft® Windows® 8 operációs rendszer
- Microsoft® Windows® 7 operációs rendszer
- Microsoft® Windows Vista® operációs rendszer
- Microsoft® Windows® XP operációs rendszer

Tájékoztató a kézikönyvről

- Microsoft® Windows® XP Professional x64 Edition operációs rendszer
- Microsoft® Windows Server® 2016 operációs rendszer
- Microsoft® Windows Server® 2012 R2 operációs rendszer
- Microsoft® Windows Server® 2012 operációs rendszer
- Microsoft® Windows Server® 2008 R2 operációs rendszer
- Microsoft® Windows Server® 2008 operációs rendszer
- Microsoft® Windows Server® 2003 R2 operációs rendszer
- Microsoft® Windows Server® 2003 operációs rendszer

Mac OS

Ebben a kézikönyvben a(z) „Mac OS” a(z) macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x és Mac OS X v10.6.8 operációs rendszerekre vonatkozik.

Bevezetés

Manuális komponens

A jelen útmutató azon eszköz-rendszergazda részére szól, aki a nyomtató, illetve lapolvasó hálózathoz történő csatlakozását végzi. Az útmutató a funkciók használatához szükséges beállítások elvégzésével kapcsolatos információkat ismerteti.

A funkciók használatával kapcsolatos információkért lásd: *Használati útmutató*.

Előkészítés

Ismerteti a rendszergazda feladatait, az eszközök beállításának folyamatát, valamint a rendszerfelügyelethez szükséges szoftvert.

Kapcsolat

Ismerteti, hogyan lehet egy eszközt a hálózathoz, illetve a telefonvonalhoz csatlakoztatni. Ezen kívül ismerteti a hálózati környezetet is, például egy port használatát az eszközhöz, valamint a(z) DNS kiszolgálóval és a proxykiszolgálóval kapcsolatos információkat.

A funkciók beállításai

Ismerteti az eszköz egyes funkcióihoz tartozó beállításokat.

Alapvető biztonsági beállítások

Ismerteti az egyes funkciókhoz (pl. nyomtatás, beolvasás és faxolás) tartozó beállításokat.

Működési és kezelési beállítások

Ismerteti az eszközök használatának megkezdése utáni műveleteket, például az információk ellenőrzését és a karbantartást.

Problémamegoldás

Ismerteti a beállítások inicializálását és a hálózat hibaelhárítását.

Speciális biztonsági beállítások vállalatok számára

Ismerteti az eszköz biztonságosságának fokozására vonatkozó beállítási módszereket, például egy hitelesítésszolgáltató által kiállított tanúsítvány, az SSL/TLS kommunikáció és az IPsec protokollcsomag/IP-szűrés funkció használatát.

Típustól függően elképzelhető, hogy a jelen fejezetben szereplő néhány funkció nem támogatott.

Az ebben az Útmutatóban használt kifejezések meghatározása

Ebben az útmutatóban a következő kifejezések fordulnak elő.

Bevezetés

Rendszergazda

Olyan személy, aki felelős az eszköz vagy a hálózat telepítéséért és beállításáért egy irodában vagy szervezetben. Kis szervezeteknél előfordulhat, hogy ez a személy felel mind az eszköz, mind a hálózat felügyeletéért. Nagyobb szervezetek esetében a rendszergazdák rendelkeznek jogosultsággal a hálózathoz vagy egy részleg, illetve divízió csoportos egységének eszközeihez, illetve a hálózati rendszergazdák felelősek a szervezeten kívüli (pl.: internet) kommunikációs beállításokért.

Hálózati rendszergazda

A hálózati kommunikáció vezérléséért felelős személy. Az a személy, aki a kommunikáció interneten vagy hálózaton keresztül történő vezérléséhez elvégzi az útválasztó, a proxy-kiszolgáló és a DNS-kiszolgáló beállításait.

Felhasználó

Eszközöket — pl.: nyomtatókat vagy lapolvasókat — használó személy.

Web Config (eszköz weboldal)

Az eszközbe beépített webkiszolgáló. A neve Web Config. A böngésző segítségével az eszköz állapotát ellenőrizheti és módosíthatja.

Eszköz

Általános kifejezés az eszköz beállításához vagy kezeléséhez használt szoftverre, pl.: Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, stb.

Push scan

Általános kifejezés az eszköz kezelőpaneljéről történő lapolvasásra.

ASCII (az „American Standard Code for Information Interchange” amerikai szabványos információátviteli kód)

Egyike a normál karakterkódoknak. 128 karakter van meghatározva, beleértve az olyan karaktereket, mint az ABC betűi (a–z, A–Z), az arab számok (0–9), szimbólumok, üres karakterek és vezérlőkarakterek. Ha az útmutatóban az „ASCII” kifejezés szerepel, akkor az az alább felsorolt 0x20–0x7E közötti kódtartományra (hex számjegyekre) utal, és nem igényel vezérlőkaraktereket.

SP*	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{		}	~	

* Szóköz karakter.

Unicode (UTF-8)

A legtöbb fontosabb, globálisan használt nyelvet lefedő nemzetközi szabványos kód. Ha az útmutatóban az „UTF-8” kifejezés szerepel, akkor az a karakterek UTF-8 formátumban történő kódolását jelzi.

Előkészítés

A jelen fejezet a rendszergazda szerepkörét, valamint a beállítások elvégzése előtti előkészítő folyamatot ismerteti.

A lapolvasó beállításának és kezelésének folyamata

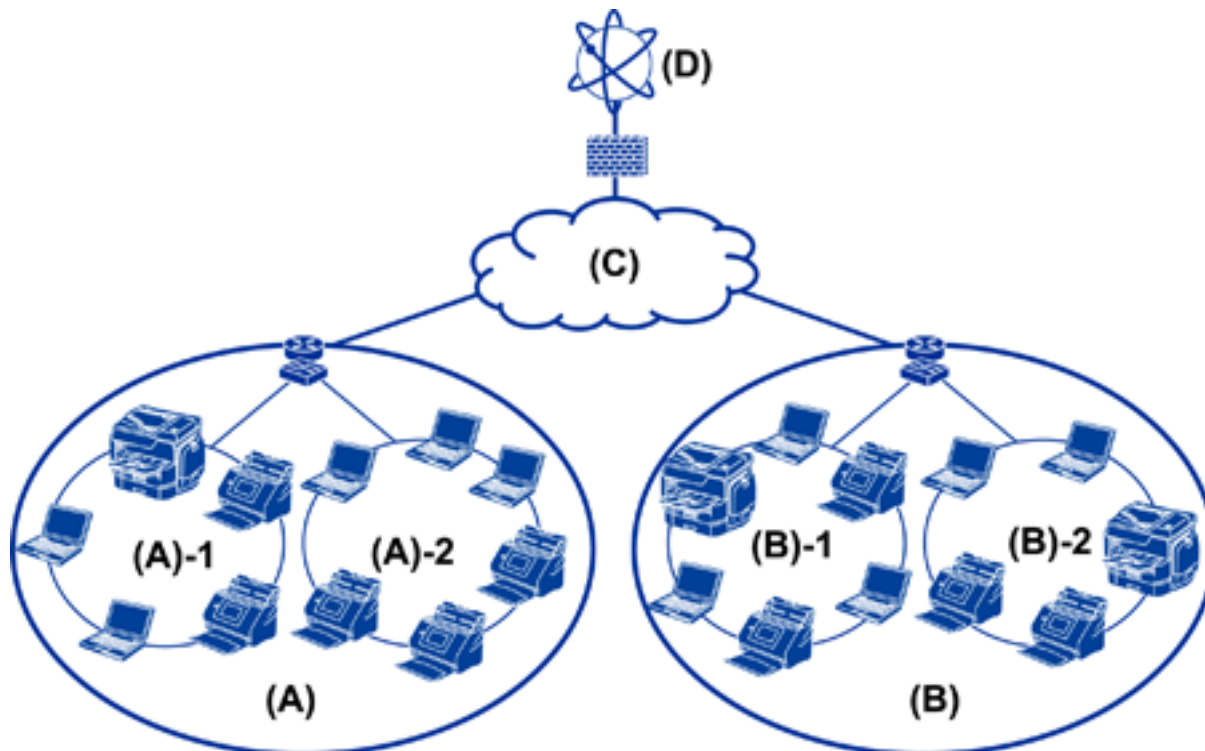
A rendszergazda elvégzi a lapolvasó hálózati kapcsolatának beállításait, kezdeti beállítását és karbantartását, hogy a felhasználók használni tudják az eszközt.

1. Előkészítés folyamatban
 - A csatlakozási beállítás adatainak összegyűjtése
 - A csatlakozási mód kiválasztása
2. Csatlakozás
 - Hálózati kapcsolat létrehozása a lapolvasó kezelőpaneljéről
3. A funkciók beállítása
 - Lapolvasó-illesztőprogram beállításai
 - Egyéb speciális beállítások
4. Biztonsági beállítások
 - Rendszergazda beállítások
 - SSL/TLS
 - Protokollvezérlés
 - Speciális biztonsági beállítások (opcionális)
5. Működtetés és kezelés
 - Az eszköz állapotának ellenőrzése
 - Vészhelyzetek kezelése
 - Biztonsági másolat készítése az eszközbeállításokról

Kapcsolódó információ

- ➔ [„Előkészítés“ 10. oldal](#)
- ➔ [„Kapcsolat“ 15. oldal](#)
- ➔ [„A funkciók beállításai“ 22. oldal](#)
- ➔ [„Alapvető biztonsági beállítások“ 32. oldal](#)
- ➔ [„Működési és kezelési beállítások“ 40. oldal](#)

Példa hálózati környezetre



(A): Office 1

(A) – 1: LAN 1

(A) – 2: LAN 2

(B): Office 2

(B) – 1: LAN 1

(B) – 2: LAN 2

(C): WAN

(D): Internet

A lapolvasó csatlakozási beállításainak bemutatása — példa

Attól függően, hogy hogyan szeretné használni a lapolvasót, alapvetően két csatlakozástípus áll rendelkezésre. Mindkettő a hubon keresztül csatlakoztatja a lapolvasót a számítógéppel a hálózathoz.

- Kiszolgáló/ügyfél kapcsolat (Windows-kiszolgálón futó lapolvasó feladatkezelése esetén)
- Társközi csatlakozás (az ügyfélszámítógép által létrehozott közvetlen kapcsolat)

Kapcsolódó információ

- ➔ „Kiszolgálói/ügyfélkapcsolat“ 12. oldal
- ➔ „Társközi csatlakozás“ 12. oldal

Kiszolgálói/ügyfélkapcsolat

A lapolvasó és feladatkezelés központosítása a kiszolgálóra telepített Document Capture Pro Server alkalmazással. Olyan munkákhoz a legmegfelelőbb, amik során több lapolvasót használnak nagyszámú dokumentum meghatározott formátumban történő beolvasásához.

Kapcsolódó információ

➔ „Az ebben az Útmutatóban használt kifejezések meghatározása“ 8. oldal

Társközi csatlakozás

Használjon egy külön lapolvasót az ügyfélszámítógépre telepített olyan lapolvasó-illesztőprogrammal, mint például a(z) Epson Scan 2. Ha telepíti a(z) Document Capture Pro (Document Capture) alkalmazást az ügyfélszámítógépre, akkor feladatokat futtathat a lapolvasóhoz tartozó külön ügyfélszámítógépeken.

Kapcsolódó információ

➔ „Az ebben az Útmutatóban használt kifejezések meghatározása“ 8. oldal

Hálózathoz történő csatlakozás előkészítése

Információszerzés a Kapcsolat beállításairól

A hálózati kapcsolathoz szükség van egy IP-címre, egy átjáró címre, stb. Előzetesen ellenőrizze a következőket.

Részlegek	Elemek	Megjegyzés
Eszközcsatlakozások módja	<input type="checkbox"/> Ethernet	Ethernet kapcsolathoz legalább 5e kategóriájú STP- (árnyékolt, csavart érpáras) kábelt használjon.
LAN-kapcsolati adatok	<input type="checkbox"/> IP-cím <input type="checkbox"/> Alhálózati maszk <input type="checkbox"/> Alapértelmezett átjáró	Ha az útválasztó DHCP funkciójával állítja be automatikusan az IP-címet, akkor nincs rá szükség.
DNS-kiszolgálói adatok	<input type="checkbox"/> Elsődleges DNS IP-címe <input type="checkbox"/> Másodlagos DNS IP-címe	Statikus IP-cím használatakor konfigurálja a DNS-kiszolgálót. Konfigurálja, ha a DHCP-funkcióval automatikus hozzárendelést végez, illetve, ha a DNS-kiszolgáló nem rendelhető hozzá automatikusan.
Proxy-kiszolgálói adatok	<input type="checkbox"/> Proxy-kiszolgáló neve <input type="checkbox"/> Portszám	Konfigurálja, ha proxy-kiszolgálót használ internetkapcsolathoz, illetve, ha a(z) Epson Connect szolgáltatást vagy a firmware automatikus frissítése funkciót használja.

A lapolvasó műszaki adatai

A lapolvasó által alapkitételben támogatott specifikációval, valamint a csatlakoztatási móddal kapcsolatban lásd a(z) *Használati útmutató* dokumentumot.

A portszám használata

A lapolvasó által használt portszámot lásd a „Függelék” című részben.

Kapcsolódó információ

➔ [„Port használata a lapolvasóhoz” 60. oldal](#)

Az IP-cím hozzárendelésének a típusa

Egy IP-címet kétféleképpen lehet hozzárendelni a lapolvasóhoz.

Statikus IP-cím:

Az előre definiált, egyedi IP-cím hozzárendelése a lapolvasóhoz.

Az IP-cím még a lapolvasó, illetve az útválasztó kikapcsolása esetén sem változik, így az eszköz IP cím alapján kezelhető.

Ez a típus olyan hálózatokhoz alkalmas, ahol több lapolvasót kezelnek, például nagy irodákban vagy iskolákban.

Automatikus hozzárendelés DHCP funkció révén:

Amikor a lapolvasó és a DHCP funkciót támogató útválasztó közötti kommunikáció sikeresen létrejön, a rendszer automatikusan hozzárendeli a megfelelő IP-címet.

Amennyiben egy adott eszköz esetében nem szerencsés megváltoztatni az IP-címet, őrizze meg előre az IP-címet, majd azután rendelje hozzá.

DNS-kiszolgáló és Proxy-kiszolgáló

Ha internetszolgáltatást használ, konfigurálja a DNS-kiszolgálót. Ha ezt nem teszi meg, akkor a hozzáféréshez meg kell adnia az IP-címet, mert előfordulhat, hogy a névfeloldás nem fog sikerülni.

A proxy-kiszolgáló a hálózat és az internet közötti átjárónál található, és azok nevében kommunikál a számítógéppel, a lapolvasóval és az internettel (ellenkező oldali kiszolgálóval). Az ellenkező oldali kiszolgáló csak a proxy-kiszolgálóval kommunikál. Ezért az olyan lapolvasóadatok, mint az IP-cím és a portszám nem olvasható le, így várhatóan fokozódik a biztonság szintje.

A szűrőfunkció segítségével letilthatja a hozzáférést egy bizonyos URL-hez, mivel a proxy-kiszolgáló képes ellenőrizni a kommunikáció tartalmát.

A hálózati kapcsolat beállításának módja

A lapolvasó IP-címéhez, alhálózati maszkjához és alapértelmezett átjárójához tartozó csatlakozási beállításokhoz kövesse az alábbi lépéseket.

A kezelőpanel használata:

A beállítások az egyes lapolvasóknál az adott lapolvasó kezelőpanelén konfigurálhatók. A lapolvasó csatlakozási beállításainak konfigurálása után csatlakozzon a hálózathoz.

Előkészítés

A telepítőprogram használata:

Ha telepítőprogramot használ, a lapolvasó hálózatát és az ügyfélszámítógépet a rendszer automatikusan beállítja. A beállítás a telepítőprogram által közölt utasítások követésével akkor is megvalósítható, ha nem ismeri tüzetesen a hálózatot.

Eszköz használata:

Használjon eszközt a rendszergazda számítógépéről. A lapolvasót megkeresheti és beállíthatja, vagy SYLK-fájl létrehozásával köteges beállításokat adhat meg a lapolvasókhoz. Több lapolvasót is beállíthat, azonban a beállítás előtt azokat fizikailag — Ethernet-kábellel — csatlakoztatni kell. Emiatt ajánlott Ethernet-rendszert kiépíteni a beállításhoz.

Kapcsolódó információ

- ➔ [„Csatlakozás a hálózathoz a kezelőpanelről“ 15. oldal](#)
- ➔ [„Csatlakozás a hálózathoz a telepítő segítségével“ 19. oldal](#)
- ➔ [„IP-cím hozzárendelése EpsonNet Config alkalmazással“ 56. oldal](#)

Kapcsolat

Ez a fejezet a lapolvasó hálózathoz való csatlakoztatásához szükséges környezetet és eljárást ismerteti.

Csatlakoztatás a hálózathoz

Csatlakozás a hálózathoz a kezelőpanelről

Csatlakoztassa a lapolvasót a hálózathoz a lapolvasó kezelőpaneljén keresztül.

A lapolvasó kezelőpaneljéről a *Használati útmutató* dokumentumában talál részletes leírást.

Az IP-cím hozzárendelése

Állítsa be az olyan alapelemeket, mint a(z) IP-cím, Alhálózatmaszk, és a(z) Alapértelmezett átjáró.

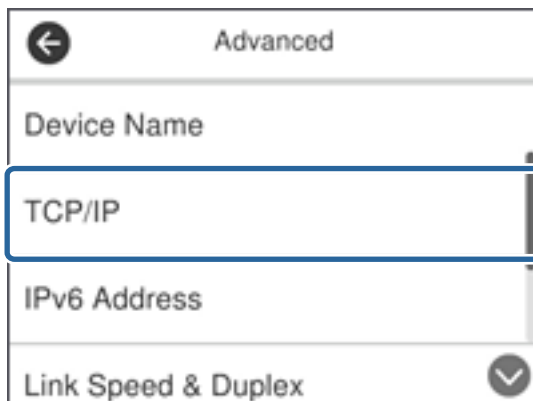
1. Kapcsolja be a lapolvasót.
2. Pöccintse balra a képernyőt a lapolvasó kezelőpaneljén, majd koppintson a(z) **Beáll.** elemre.



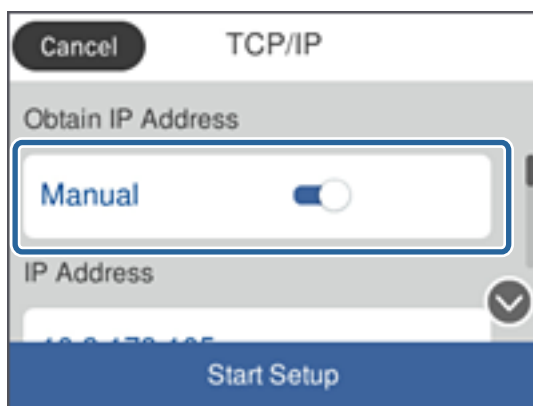
3. Koppintson a(z) **Hálózati beállítások > Beállítások módosítása** elemre.
Ha nem jelenik meg az elem, a képernyő felfelé pöccintésével hívhatja elő azt.

Kapcsolat

4. Koppintson a(z) **TCP/IP** elemre.

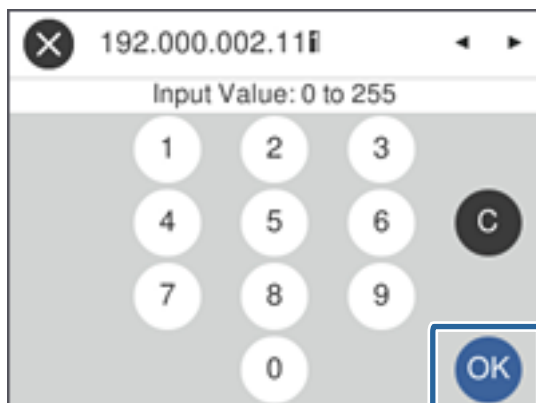


5. Válassza ki a(z) **Manuális** lehetőséget a(z) **IP-cím lekérése** paraméterhez.

**Megjegyzés:**

Ha az útválasztó DHCP funkciójával állítja be automatikusan az IP-címet, akkor válassza az **Auto** opciót. Ebben az esetben a(z) **IP-cím**, a(z) **Alhálózat maszk**, és a(z) **Alapértelmezett átjáró** beállítása a 6-7. lépésben automatikusan megtörténik, ezért menjen a 8. lépésre.

6. Koppintson a(z) **IP-cím** mezőre, írja be az IP-címet a képernyőn megjelenő billentyűzet segítségével, majd koppintson a(z) **OK** gombra.



Erősítse meg az előző képernyőn megjelenített értéket.

Kapcsolat

7. Állítsa be a(z) **Alhálózat maszk** és a(z) **Alapértelmezett átjáró** lehetőségeket.

Erősítse meg az előző képernyőn megjelenített értéket.

Megjegyzés:

Ha nem megfelelő az IP-cím, az Alhálózat maszk és az Alapértelmezett átjáró kombinációja, akkor a(z) **Beállítás indítása** inaktív és nem folytatható a beállítások elvégzése. Ellenőrizze, hogy nem hibás-e a bejegyzés.

8. Koppintson a(z) **DNS-szerver Elsődleges DNS** mezőjére, írja be az elsődleges DNS-kiszolgáló IP-címét a képernyőn megjelenő billentyűzet segítségével, majd koppintson a(z) **OK** gombra.

Erősítse meg az előző képernyőn megjelenített értéket.

Megjegyzés:

Ha az IP-cím hozzárendelés beállításainál a **Manuális** opciót választja, akkor a DNS-kiszolgáló beállításaként a **Auto** vagy az **Auto** opciót választhatja. Ha nem tudja automatikusan beszerezni a DNS-kiszolgáló címét, akkor válassza a **Manuális** opciót, és adja meg a DNS-kiszolgáló címét. Azután adja meg közvetlenül a másodlagos DNS-kiszolgáló címét. Ha a(z) **Auto** opciót választja, menjen a 10. lépésre.

9. Koppintson a(z) **Másodlagos DNS** mezőre, írja be a másodlagos DNS-kiszolgáló IP-címét a képernyőn megjelenő billentyűzet segítségével, majd koppintson a(z) **OK** gombra.

Erősítse meg az előző képernyőn megjelenített értéket.

10. Koppintson a(z) **Beállítás indítása** elemre.


11. Koppintson a(z) **Bezár** opcióra a megerősítés képernyőn.

A képernyő automatikusan bezáródik meghatározott idő elteltével, ha nem koppint a(z) **Bezár** gombra.

Csatlakozás Ethernet-hálózathoz

Csatlakoztassa a szkennert a hálózathoz az Ethernet-kábellel, majd ellenőrizze a kapcsolatot.

1. Csatlakoztassa a szkennert és a hubot (L2-kapcsolót) egy Ethernet-kábellel.

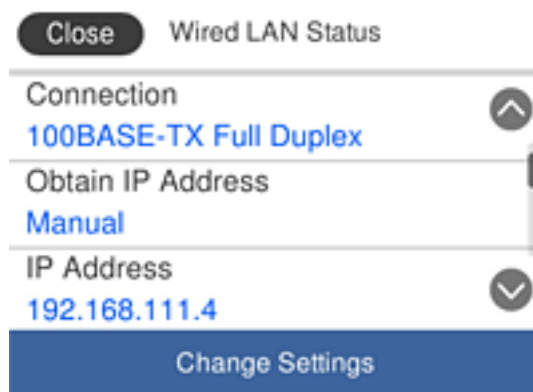
A kezdőképernyőn az alábbi ikon lesz látható: .

2. Koppintson a(z)  elemre a kezdőképernyőn.



Kapcsolat

3. Pöccintse a képernyőt felfelé, majd ellenőrizze, hogy megfelelő-e a kapcsolat állapota és az IP-cím.



A proxykiszolgáló beállítása

A proxykiszolgáló nem állítható be a panelen. A konfigurálást a(z) Web Config alkalmazással végezze.

1. Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **Network Settings** > **Basic** menüpontot.
2. Jelölje ki a(z) **Use** elemet a(z) **Proxy Server Setting** menüben.
3. Írja be a proxykiszolgáló címét IPv4 vagy FQDN formátumban a(z) **Proxy szerver** elemnél, majd írja be a portszámot a(z) **Proxy Server Port Number** elemnél.

A hitelesítést igénylő proxykiszolgálóknál írja be a proxykiszolgáló hitelesítési adatait (a felhasználónevet és jelszót).

Kapcsolat

4. Kattintson a(z) **Next** gombra.

The screenshot shows the EPSON Web Config interface for a printer. The left sidebar contains navigation options like 'Administrator Logout', 'Status', 'Scanner Settings', 'Network Settings', 'Wired LAN', 'Basic', 'Email Server', 'Network Security Settings', 'Services', 'System Settings', 'Export and Import Setting Value', and 'Administrator Settings'. Under 'Basic Settings', 'DNS/Proxy Setup' is selected. The main content area displays various network configuration fields:

- Primary DNS Server : [text box]
- Secondary DNS Server : [text box]
- DNS Host Name Setting : Auto Manual
- DNS Host Name Status : Failed
- DNS Host Name : EPSON884045
- DNS Domain Name Setting : Auto Manual
- DNS Domain Name Status : Failed
- DNS Domain Name : [text box]
- Register the network interface address to DNS : Enable Disable
- Proxy Server Setting** : Do Not Use Use
- Proxy Server : www.sample.proxy
- Proxy Server Port Number : 80
- Proxy Server User Name : XXXXXXXX
- Proxy Server Password : [password field]
- IPv6 Setting : Enable Disable
- IPv6 Privacy Extension : Enable Disable
- IPv6 DHCP Server Setting : Do Not Use Use
- IPv6 Address : [text box]
- IPv6 Address Default Gateway : [text box]
- IPv6 Link-Local Address : fe80::9eae:d3ff:fe88:4045/64
- IPv6 Stateful Address : [text box]
- IPv6 Stateless Address 1 : [text box]
- IPv6 Stateless Address 2 : [text box]
- IPv6 Stateless Address 3 : [text box]
- IPv6 Primary DNS Server : [text box]
- IPv6 Secondary DNS Server : [text box]

A blue box highlights the Proxy Server Setting section. At the bottom of the main content area, there is a 'Next' button.

5. Erősítse meg a beállításokat, majd kattintson a(z) **Beállítások** gombra.

Kapcsolódó információ

- ➔ „A Web Config elérése“ 23. oldal

Csatlakozás a hálózathoz a telepítő segítségével

Javasoljuk, hogy a lapolvasót a telepítővel csatlakoztassa számítógéphez. A telepítőt az alábbi módszerek egyikével működtetheti.

- Beállítás a webhelyről

Lépjen a következő webhelyre, majd adja meg a termék nevét. Lépjen a **Beállítás** részhez, kezdje meg a beállítást.

<http://epson.sn>

- Beállítás a szoftverlemez segítségével (csak olyan modellek esetében, amikhez szoftverlemez mellékelnek, illetve lemezmeghajtóval rendelkező felhasználók esetében)

Helyezze be a szoftverlemezt, majd kövesse a képernyőn megjelenő utasításokat.

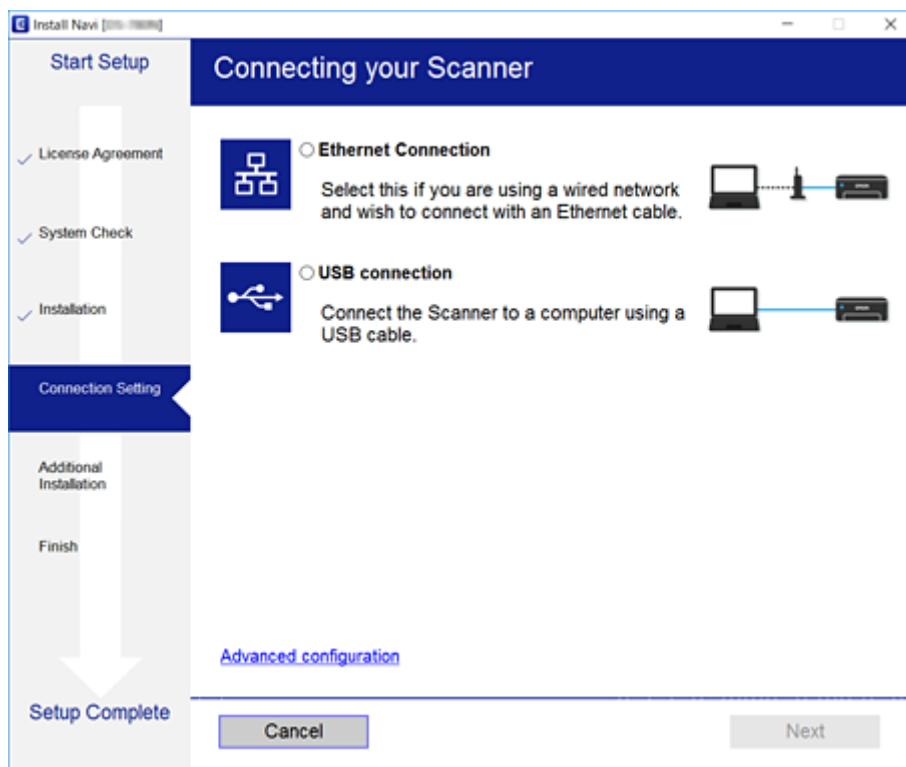
Kapcsolat

A Csatlakozási módok kiválasztása

Kövesse a képernyőn megjelenő utasításokat, amíg meg nem jelenik a következő képernyő, majd válassza ki a lapolvasó és a számítógép közötti csatlakozási módot.

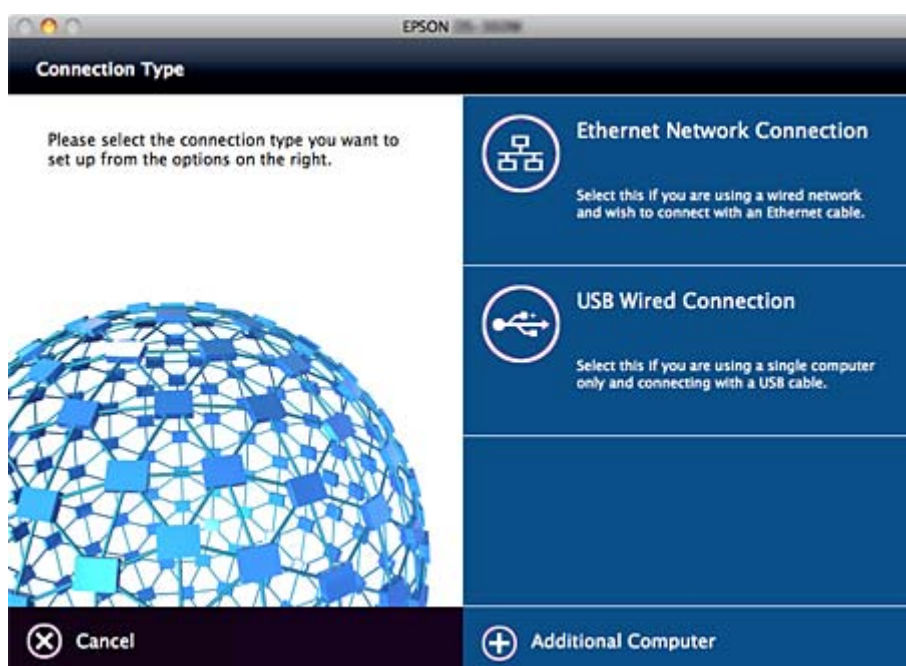
☐ Windows

Válassza ki a kapcsolat típusát, majd kattintson a(z) **Tovább** parancsra.



☐ Mac OS

A kapcsolattípus kiválasztása.



Kapcsolat

Kövesse a képernyőn megjelenő utasításokat. A szükséges szoftver telepítése megtörtént.

A funkciók beállításai

Ez a fejezet az eszköz egyes funkcióinak használatához szükséges első elvégzendő beállításokat ismerteti.

Szoftverek a beállításhoz

Ebben a témakörben a rendszergazda számítógépéről a Web Config segítségével történő beállítások elvégzésének folyamatát mutatjuk be.

Web Config (Weboldal az eszközhöz)

Tudnivalók az Web Config alkalmazásról

A Web Config egy böngészőalapú alkalmazás, amellyel megadhatók a lapolvasó beállításai.

A Web Config alkalmazás eléréséhez először a lapolvasónak ki kell osztani egy IP-címet.

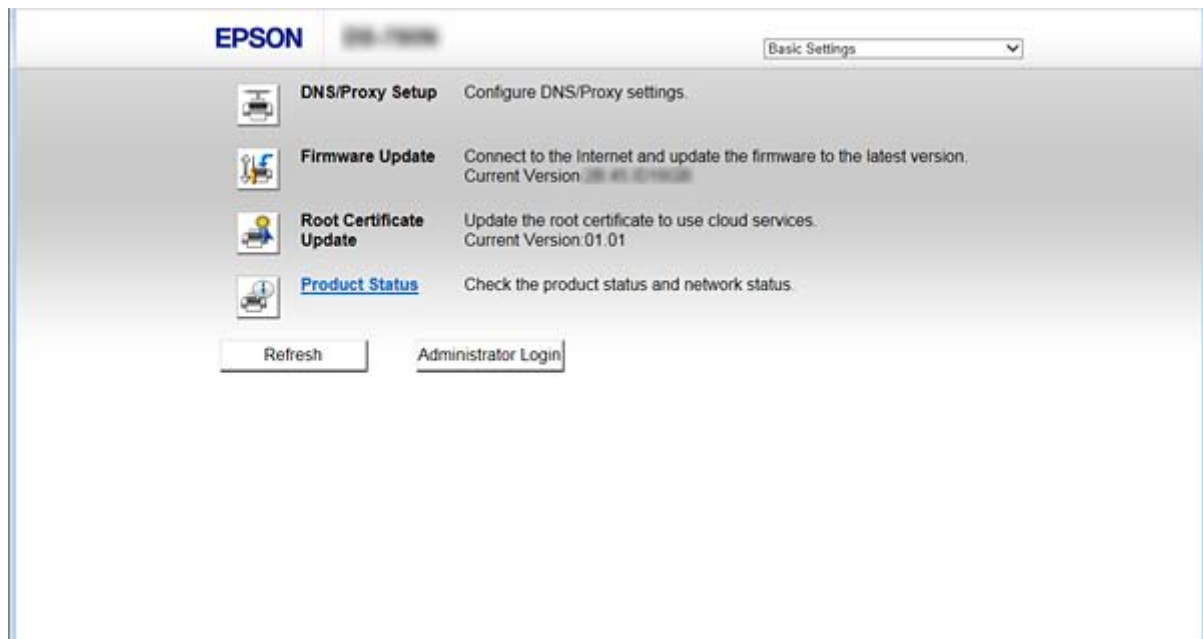
Megjegyzés:

A beállításokat a lapolvasó rendszergazdai jelszavának megadásával lehet lezárni.

Az alábbi két beállítási oldal érhető el.

Basic Settings

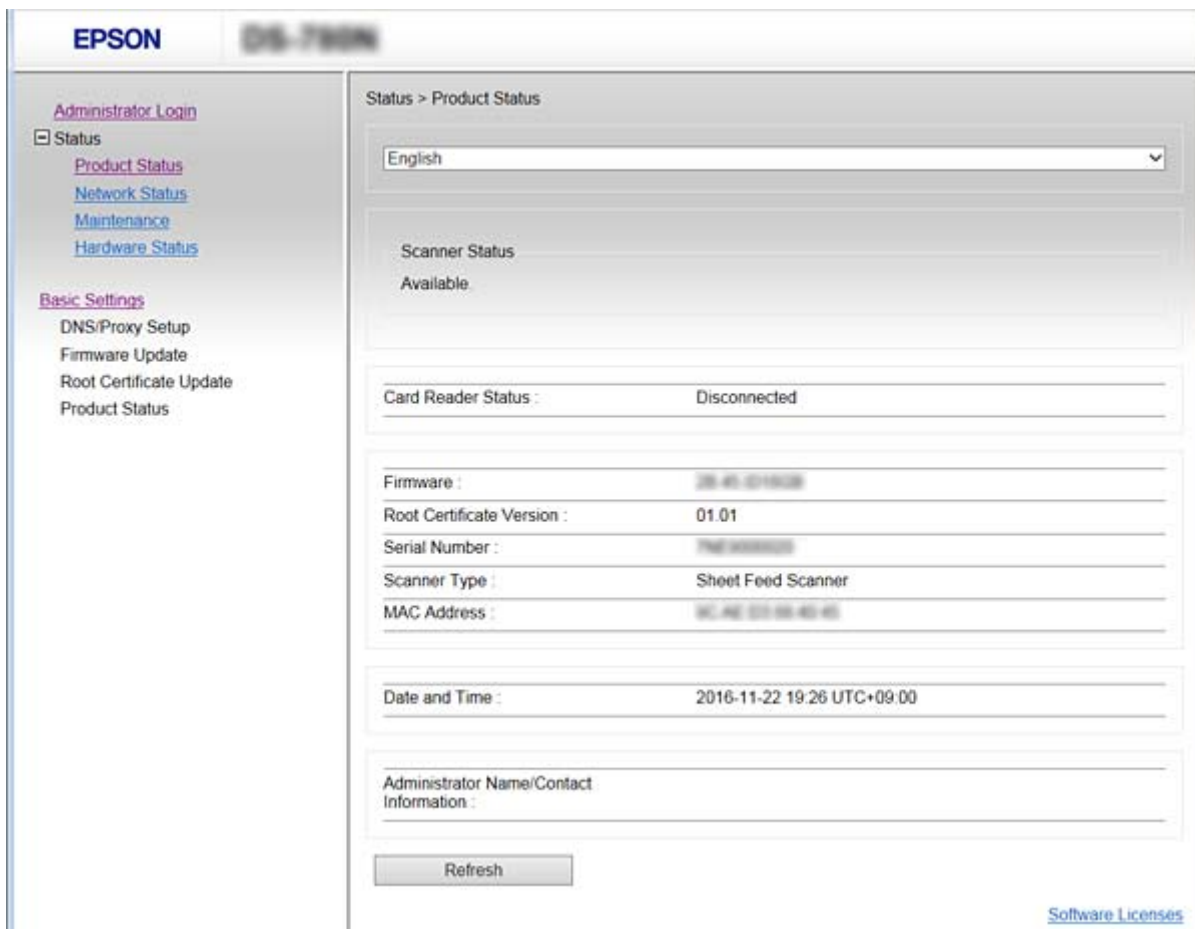
Itt a lapolvasó alapbeállításait adhatja meg.



A funkciók beállításai

❑ Advanced Settings

Itt a lapolvasó speciális beállításait adhatja meg. Ezt az oldalt főleg a rendszergazda használhatja.



A Web Config elérése

Írja be a lapolvasó IP-címét egy webböngészőbe. Engedélyezni kell a JavaScriptet. Amikor a Web Config alkalmazást HTTPS-kapcsolaton keresztül éri el, figyelmeztető üzenet jelenik meg a böngészőben, mert egy, a lapolvasóban tárolt ön aláíró tanúsítvány van használatban.

❑ HTTPS-elérés

IPv4: `https://<lapolvasó IP-címe>` (< > nélkül)

IPv6: `https://[lapolvasó IP-címe]/` ([] zárójellel)

❑ HTTP-elérés

IPv4: `http://<lapolvasó IP-címe>` (< > nélkül)

IPv6: `http://[lapolvasó IP-címe]/` ([] zárójellel)

A funkciók beállításai

Megjegyzés:

Példák

IPv4:

`https://192.0.2.111/`

`http://192.0.2.111/`

IPv6:

`https://[2001:db8::1000:1]/`

`http://[2001:db8::1000:1]/`

- Ha a DNS-kiszolgáló már tárolta a lapolvasó nevét, a lapolvasó IP-címe helyett annak nevét is használhatja.

Kapcsolódó információ

- ➔ [„SSL/TLS kommunikáció a lapolvasóval“ 63. oldal](#)
- ➔ [„Tudnivalók a digitális tanúsítványról“ 63. oldal](#)

A beolvasási funkciók használata

A lapolvasó használatától függően telepítse az alábbi szoftvert, és segítségével végezze el a beállításokat.

Lapolvasás számítógépről

- A(z) Web Config segítségével erősítse meg a hálózati lapolvasás szolgáltatás érvényességét (a gyári kiszállításkor érvényes).
- Telepítse a(z) Epson Scan 2 alkalmazást a számítógépre, majd állítsa be az IP-címet
- Ha feladatok végrehajtásával végez lapolvasást, akkor telepítse a(z) Document Capture Pro (Document Capture) alkalmazást, és végezze el a feladatbeállításokat.

Lapolvasás a kezelőpanelről

- A(z) Document Capture Pro vagy a(z) Document Capture Pro Server használatakor:
Telepítse a(z) Document Capture Pro vagy a(z) Document Capture Pro Server programot
DCP-beállítás (kiszolgáló üzemmód, ügyfél üzemmód).
- A WSD-protokoll használatakor:
Erősítse meg a WSD érvényességét a(z) Web Config alkalmazásban vagy a kezelőpanelen (a gyári kiszállításkor érvényes)
További eszközbeállítások (Windows rendszerű számítógép).

Beolvasás számítógépről

Telepítse a szoftvert, majd ellenőrizze, hogy a hálózati beolvasási szolgáltatás engedélyezve van-e, hogy beolvasást végezhesen a számítógépről hálózaton keresztül.

Kapcsolódó információ

- ➔ [„Telepítendő szoftverek“ 25. oldal](#)
- ➔ [„Hálózati lapolvasás engedélyezése“ 25. oldal](#)

A funkciók beállításai

Telepítendő szoftverek

❑ Epson Scan 2

Ez egy lapolvasó-illesztőprogram. Amennyiben az eszköz egy számítógépről látható, telepítse az illesztőprogramot minden ilyen ügyfélszámítógépre. Ha a Document Capture Pro/Document Capture programok telepítve vannak, elvégezheti az eszköz gombjaihoz társított műveleteket.

A(z) EpsonNet SetupManager alkalmazással a nyomtató-illesztőprogramok együttesen, csomagokba foglalva is terjeszthetők.

❑ Document Capture Pro (Windows)/Document Capture (Mac OS)

Telepítse az ügyfélszámítógépre. A számítógép és a lapolvasó kezelőpaneljéről hívhat elő és hajthat végre olyan, a hálózaton lévő számítógépre regisztrált feladatokat, amin telepítve van a(z) Document Capture Pro/Document Capture alkalmazás.

A számítógépről lapolvasást is végezhet a hálózaton keresztül. A beolvasáshoz Epson Scan 2 szükséges.

Kapcsolódó információ

➔ „EpsonNet SetupManager“ 56. oldal

A lapolvasó IP-címéhez írja be a következőt: Epson Scan 2



Úgy adja meg a lapolvasó IP-címét, hogy használni lehessen a lapolvasót a hálózaton.

1. Indítsa el az **Epson Scan 2 Utility** segédprogramot a **Start > Minden program > EPSON > Epson Scan 2** menüből.

Ha egy másik lapolvasót már regisztráltak, akkor folytassa a 2. lépéssel.

Ha nem regisztráltak, akkor folytassa a 4. lépéssel.

2. Kattintson a(z) ▼ elemre a(z) **Lapolvasó** szakaszban.
3. Kattintson a(z) **Beállítások** elemre.
4. Kattintson a(z) **Szerkesztés engedélyezése** elemre, majd a(z) **Hozzáadás** elemre.
5. Válassza ki a lapolvasó típusnevét a(z) **Modell** menüből.
6. Válassza ki a lapolvasó használandó IP-címét a(z) **Cím** elemnél a(z) **Hálózat keresése** menüből.

Kattintson a(z)  elemre, majd a lista frissítéséhez a(z)  elemre. Ha nem találja a lapolvasó IP-címét, akkor válassza a(z) **Cím beírása** lehetőséget, majd írja be az IP-címet.

7. Kattintson a(z) **Hozzáadás** elemre.
8. Kattintson a(z) **OK** elemre.

Hálózati lapolvasás engedélyezése

Ha ügyfélszámítógépről végez lapolvasást a hálózaton keresztül, akkor beállíthatja a hálózati lapolvasás szolgáltatást. Alapértelmezett beállításként ez engedélyezve van.

A funkciók beállításai

1. Nyissa meg a Web Config alkalmazást, majd válassza a **Services > Network Scan** elemet.
2. Ellenőrizze, hogy ki van-e jelölve a(z) **Enable scanning** a(z) **EPSON Scan** menüben.
Ha ki van jelölve, akkor a feladat befejeződött. Zárja be a Web Config alkalmazást.
Ha törölve van a kijelölés, akkor jelölje ki, majd folytassa a következő lépéssel.
3. Kattintson a(z) **Next** elemre.
4. Kattintson a(z) **OK** elemre.
A hálózat újra csatlakozik, és a beállítások engedélyezve vannak.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

Lapolvasás a kezelőpanel használatával

A beolvasás mappába és a küldés e-mailben funkció használata a lapolvasó kezelőpaneljén keresztül, illetve a lapolvasás eredményének továbbítása e-mailben, mappákba, stb. a számítógépről történő feladat-végrehajtással.

A lapolvasási eredmények továbbításakor a feladat beállítását a(z) Document Capture Pro Server vagy a(z) Document Capture Pro alkalmazással végezze.

A beállításokkal és a feladat beállításával kapcsolatos bővebb információkat lásd a(z) Document Capture Pro Server vagy a(z) Document Capture Pro alkalmazás dokumentációjában, illetve súgójában.

Kapcsolódó információ

➔ „Document Capture Pro Server/Document Capture Pro beállítások“ 26. oldal

➔ „A kiszolgálók és mappák beállításai“ 27. oldal

A számítógépre telepítendő szoftver

Document Capture Pro Server

Ez a(z) Document Capture Pro kiszolgálóverziója. Telepítse Windows-kiszolgálón. A kiszolgáló képes központilag több eszközt és feladatot kezelni. Több feladat végezhető el több lapolvasóról egy időben.

A(z) Document Capture Pro Server tanúsított verziójának használatával felhasználókhöz és csoportokhoz kapcsolódó feladatokat és lapolvasási előzményeket kezelhet.

A(z) Document Capture Pro Server szoftverrel kapcsolatos további információkért vegye fel a kapcsolatot a helyi Epson irodával.

Document Capture Pro (Windows)/Document Capture (Mac OS)

Ugyanúgy, mint amikor számítógépről végez lapolvasást, a kezelőpanelről hívhatja elő és hajthatja végre a számítógépen regisztrált feladatokat. Több lapolvasóról egy időben nem futtathatók számítógép-feladatok.

Document Capture Pro Server/Document Capture Pro beállítások

Végezze el a lapolvasás funkció használatához szükséges beállításokat a lapolvasó kezelőpaneljéről.

A funkciók beállításai

1. Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **Services > Document Capture Pro** menüpontot.
2. Válassza a(z) **Üzem mód** lehetőséget.
 - Server Mode:**
Akkor válassza ezt a lehetőséget, ha a(z) Document Capture Pro Server-t használja, vagy, ha a(z) Document Capture Pro alkalmazást használja csak egy adott számítógéphez beállított feladatok végrehajtásához.
 - Client Mode:**
Ezt akkor állítsa be, ha a hálózaton lévő egyes ügyfélszámítógépekre telepített Document Capture Pro (Document Capture) alkalmazás feladatbeállítását konkrét számítógép megjelölése nélkül végzi el.
3. A kiválasztott üzemmódnak megfelelően állítsa be az alábbiakat.
 - Server Mode:**
A(z) **Server Address** elemnél írja be azt a kiszolgálót, amin a(z) Document Capture Pro Server telepítve van. 2–252 karaktert írjon be IPv4, IPv6, állomásnév, illetve FQDN-formátumban. Az FQDN-formátum esetében használhat (USA-beli billentyűzetten) ASCII betűket, számokat, az ABC betűit, illetve kötőjelet (azzal a feltétellel, hogy a karaktersorozat nem kezdődhet és/vagy nem végződhet kötőjellel).
 - Client Mode:**
Adja meg a(z) **Group Settings** értékét, ha a(z) Document Capture Pro (Document Capture) alkalmazásból meghatározott lapolvasócsoportot szeretne használni.
4. Kattintson a(z) **Beállítások** elemre.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

A kiszolgálók és mappák beállításai

A(z) Document Capture Pro és a(z) Document Capture Pro Server egyszer elmenti a beolvasott adatokat a kiszolgálóra vagy az ügyfélszámítógépre, majd a továbbítás funkció segítségével végrehajtja a beolvasás mappába, valamint a beolvasás és küldés e-mailben funkciót.

Ahhoz, hogy a számítógépre vagy felhőszolgáltatásra továbbítsa az adatokat arról a számítógépről, amin telepítve van a(z) Document Capture Pro és/vagy a(z) Document Capture Pro Server alkalmazás, jogosultságra és bizonyos adatokra lesz szüksége.

Készítse elő a használni kívánt funkcióval kapcsolatos információkat a következőkben foglaltak figyelembe vételével.

Ezeknek a funkcióknak a beállításait elvégezheti a(z) Document Capture Pro vagy a(z) Document Capture Pro Server segítségével. A beállításokkal kapcsolatos bővebb információkat lásd a(z) Document Capture Pro Server vagy a(z) Document Capture Pro alkalmazás dokumentációjában, illetve súgójában.

A funkciók beállításai

Név	Beállítások	Követelmény
Beolvasás hálózati mappába (SMB)	A mentési mappa létrehozása és megosztással kapcsolatos beállítása	A számítógéphez tartozó rendszergazdai felhasználói fiók, amely mentési mappákat hoz létre.
	A Beolvasás hálózati mappába (SMB) funkció célhelye	Ahhoz a számítógéphez tartozó bejelentkezési felhasználónév és jelszó, amelyen a mentési mappa található, és amely a mentési mappa frissítésére jogosult.
Beolvasás hálózati mappába (FTP)	FTP-kiszolgálói bejelentkezés beállítása	Az FTP-kiszolgáló bejelentkezési adatai, valamint a mentési mappa frissítési joga.
Beolvasás és küldés e-mailben	E-mail kiszolgáló beállítása	E-mail kiszolgáló beállítási adatai
Beolvasás a Document Capture Pro programba (Document Capture Pro Server használata esetén)	Beállítás felhőszolgáltatásokba történő bejelentkezéshez	Internetkapcsolat környezete A felhőszolgáltatásokhoz használt fiók regisztrációja

WSD lapolvasás használata (kizárólag Windows rendszer esetében)

A WSD lapolvasás Windows Vista vagy újabb operációs rendszereket futtató számítógépen érhető el.

Ha használható a WSD protokoll, akkor a(z) **Számítógép (WSD)** menü látható a lapolvasó kezelőpaneljén.

- Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **Services > Protocol** menüpontot.
- Ellenőrizze, hogy a(z) **Enable WSD** ki van-e választva a(z) **WSD Settings** menüben.
Ha igen, akkor Önnek nincs más dolga, és bezárhatja a(z) Web Config alkalmazást.
Ha nincs kiválasztva, akkor válassza ki, majd folytassa a következő lépéssel.
- Kattintson a(z) **Next** gombra.
- Erősítse meg a beállításokat, majd kattintson a(z) **Beállítások** gombra.

Rendszerbeállítások elvégzése



Rendszerbeállítások elvégzése a kezelőpanelről

A képernyő fényerejének beállítása

Az LCD-képernyő fényerejének beállítása.

- Koppintson a(z) **Beáll.** elemre a kezdőképernyőn.
- Koppintson a(z) **Általános beállítások > LCD-fényerő** elemre.

A funkciók beállításai

3. A fényerő beállításához koppintson a(z)  vagy a(z)  elemre. 1 és 9 közötti értéket állíthat be.
4. Koppintson a(z) **OK** elemre.

Hang beállítása

A panel működési hangjának és a hibajelző hang beállítása.

1. Koppintson a(z) **Beáll.** elemre a kezdőképernyőn.
2. Koppintson a(z) **Általános beállítások > Hang** elemre.
3. Szükség szerint állítsa be a következő elemeket.
 - Működési hang**
Beállíthatja a kezelőpanel működési hangjának hangerejét.
 - Hibajelző hang**
Beállíthatja a hibajelző hang hangerejét.
4. Koppintson a(z) **OK** elemre.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

Az eredeti dokumentum dupla behúzásának észlelése

A funkció beállításakor a rendszer észlelni fogja, ha a beolvasandó dokumentumot duplán húzza be a készülék, illetve leállítja a lapolvasást, ha több eredeti dokumentumadagolás történik egyidejűleg.

Ha úgy gondolja, hogy előfordulhat az eredeti dokumentum (pl.: borítékok vagy matricás papírok) többszörös beadagolása, akkor a beállításuknál válassza a „ki” értéket.

Megjegyzés:

A beállítást elvégezheti a(z) *Web Config* vagy a(z) *Epson Scan 2* alkalmazásból is.

1. Koppintson a(z) **Beáll.** elemre a kezdőképernyőn.
2. Koppintson a(z) **Külső szkennelési beállítások > Ultrahangos dupla behúzás észlelése** elemre.
3. A be- vagy kikapcsoláshoz koppintson a(z) **Ultrahangos dupla behúzás észlelése** elemre.
4. Koppintson a(z) **Bezár** elemre.

Kis sebességű üzemmód beállítása

Ha beállítja, akkor a lapolvasást lassan fogja végezni a rendszer, és nem fog előfordulni papírelakadás vékony dokumentumok, (pl.: bizonylatok) beolvasásakor.

A funkciók beállításai

1. Koppintson a(z) **Beáll.** elemre a kezdőképernyőn.
2. Koppintson a(z) **Külső szkennelési beállítások** > **Lassú** elemre.
3. A be- vagy kikapcsoláshoz koppintson a(z) **Lassú** elemre.
4. Koppintson a(z) **Bezár** elemre.

Rendszerbeállítások elvégzése a Web Config alkalmazás segítségével

Energiatakarékosági beállítások inaktivitás esetén

Végezze el az energiatakarékosági beállításokat arra az esetre, ha a szkennер inaktív. A felhasználási környezettől függően állítja be az időt.

Megjegyzés:

Az energiatakarékosági beállításokat a lapolvasó kezelőpaneljén is elvégezheti.

1. Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **System Settings** > **Power Saving** menüpontot.
2. Az **Sleep Timer** mezőben adja meg azt az időtartamot, ami után a rendszer inaktivitás esetén energiatakarékos üzemmódba kapcsoljon.
A perc értékének legfeljebb 240 percet állíthat be.
3. Válassza ki a kikapcsolás idejét a **Power Off Timer** mezőben.
4. Kattintson a(z) **OK** elemre.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

A kezelőpanel beállítása

A lapolvasó kezelőpaneljének beállítása. A beállítás a következők szerint végezhető.

1. Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **System Settings** > **Control Panel** menüpontot.
2. Szükség szerint állítsa be a következő elemeket.
 - Language
Válassza ki a kezelőpanel nyelvét.
 - Panel Lock
Ha a(z) **ON** opciót választja, a rendszer rendszergazda jelszót kér, amikor olyan műveletet végez, amelyhez a rendszergazda engedélyre van szüksége. Ha nincs beállítva rendszergazda jelszó, a vezérlés zárolása funkció inaktív.

A funkciók beállításai

Operation Timeout

Ha a(z) **ON** opciót választja, akkor a rendszergazdaként történő bejelentkezéskor a rendszer automatikusan kilépteti, és a kezdőképernyőre viszi, amennyiben egy adott időszakon belül nem történik aktivitás.

A másodperc értékének 10–240 másodpercet állíthat be.

3. Kattintson a(z) **OK** elemre.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

A külső interfész korlátozásának a beállítása

Korlátozhatja az USB kapcsolatot a számítógépről. Akkor állítsa be, ha a lapolvasást nem a hálózaton keresztül szeretné korlátozni.

1. Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **System Settings > External Interface** menüpontot.
2. Válasszon a(z) **Enable** és a(z) **Disable** lehetőség közül.
A korlátozáshoz válassza a(z) **Disable** lehetőséget.
3. Koppintson a(z) **OK** elemre.

A dátum és az idő szinkronizálása az időkiszolgálóval

Amennyiben CA hitelesítést használ, idővel megspórolhatja magának a problémákat.

1. Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **System Settings > Date and Time > Time Server** menüpontot.
2. Válassza ki a(z) **Use** lehetőséget a(z) **Use Time Server** paraméterhez.
3. Írja be az időkiszolgáló címét az **Time Server Address** mezőbe.
Használhat IPv4, IPv6 vagy FQDN formátumot. Maximum 252 karakter írható be. Amennyiben nem szeretné megadni ezt az adatot, hagyja üresen a mezőt.
4. Töltse ki a **Update Interval (min)** mezőt.
A perc értékének legfeljebb 10 800 percet állíthat be.
5. Kattintson a(z) **OK** elemre.

Megjegyzés:

A kapcsolat állapotát az időkiszolgálóval az **Time Server Status** mezőben erősítheti meg.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

Alapvető biztonsági beállítások

Ez a fejezet a különleges környezetet nem igénylő, alap biztonsági beállításokat fejt ki.

Az alap biztonsági funkciók bemutatása

Az alábbiakban bemutatjuk az Epson eszközök alap biztonsági funkcióit.

A funkció neve	A funkció típusa	Beállítandó	Megelőzendő
A rendszergazdai jelszó beállítása	Zárja az olyan rendszerbeállításokat, mint a hálózat vagy az USB kapcsolatbeállítása, hogy csak a rendszergazda módosíthassa azokat.	Egy rendszergazda jelszót állít be az eszközhöz. A konfiguráció vagy frissítés bárholnan elérhető a Web Config alkalmazásban, a kezelőpanelen, valamint az Epson Device Admin és az EpsonNet Config alkalmazásban.	Védelmet nyújt az eszközön tárolt információk (pl.: azonosító, jelszó, hálózati beállítások és címtár) illetéktelen megszerzésével és módosításával szemben. Számos olyan biztonsági kockázatot is csökkent, mint például a hálózati környezetről vagy a biztonsági házirendről való információk kiszivárgása.
SSL/TLS kommunikáció	A kommunikációs tartalom titkosítása SSL/TLS-kommunikáció segítségével történik, amikor az Epson-kiszolgálót az eszközről interneten keresztül éri el, pl.: amikor a számítógéppel webböngészőn keresztül megy végbe a kommunikáció, illetve firmware frissítéskor.	Szerezzen be egy hitelesítésszolgáltató által aláírt tanúsítványt, majd importálja a lapolvasóba.	Az eszköz beazonosításának egy hitelesítésszolgáltató által aláírt tanúsítvánnyal történő törlése védelmet nyújt a megszemélyesítéssel és az illetéktelen hozzáféréssel szemben. Ezen felül az SSL/TLS kommunikációs tartalmai is védve vannak, illetve a nyomtatási és beállítási adatok kiszivárgását is megakadályozza.
A protokollokat vezérli	Az eszközök és a számítógépek közötti kommunikációhoz használandó protokollokat vezérli, illetve funkciókat engedélyez/tilt le.	Egy protokollt vagy szolgáltatást, amit külön engedélyezett vagy tiltott funkciókhoz alkalmaznak.	A nem szándékos használatból eredő biztonsági kockázatok csökkenthetőek ha megakadályozzák, hogy a felhasználók szükségtelen funkciókat használjanak.

Kapcsolódó információ

- ➔ „Tudnivalók az Web Config alkalmazásról“ 22. oldal
- ➔ „EpsonNet Config“ 55. oldal
- ➔ „Epson Device Admin“ 55. oldal
- ➔ „A rendszergazdai jelszó beállítása“ 33. oldal
- ➔ „Protokollok vezérlése“ 35. oldal

A rendszergazdai jelszó beállítása

Ha beállítja a rendszergazdai jelszót, akkor más, nem rendszergazda felhasználók nem tudnak módosítani a rendszergazdai beállításokon. A rendszergazdai jelszó beállítását a Web Config alkalmazással, a szkennerek kezelőpaneljén, illetve szoftverén (Epson Device Admin, vagy EpsonNet Config) keresztül végezheti el. A szoftver használata esetén tekintse meg az egyes szoftverek dokumentációját.

Kapcsolódó információ

- ➔ „A rendszergazdai jelszó konfigurálása a kezelőpanelről“ 33. oldal
- ➔ „A rendszergazdai jelszó konfigurálása Web Config alkalmazással“ 33. oldal
- ➔ „EpsonNet Config“ 55. oldal
- ➔ „Epson Device Admin“ 55. oldal

A rendszergazdai jelszó konfigurálása a kezelőpanelről

A rendszergazdai jelszó beállítható a lapolvasó kezelőpaneljéről.

1. Koppintson a(z) **Beáll.** elemre a kezdőképernyőn.
2. Koppintson a(z) **Rendszerfelügyelet > Rendszergazdai beáll.** elemre.
Ha az elem nem jelenik meg, pöccintse a képernyőt felfelé a megjelenítéshez.
3. Koppintson a(z) **Rendszergazdai jelszó > Regisztrálás** elemre.
4. Adja meg a jelszót, majd koppintson a(z) **OK** gombra.
5. Adja meg a jelszót újra, majd koppintson a(z) **OK** gombra.
6. Koppintson a(z) **OK** opcióra a megerősítés képernyőn.
Megjelenik a rendszergazda beállítás képernyő.
7. Koppintson a(z) **Beállítás zárolása** elemre, majd a(z) **OK** gombra a megerősítés képernyőn.
A Beállítás zárolása beállítása **Be**, és szükség lesz a rendszergazdai jelszóra, ha a zárolt menüelemet működteti.

Megjegyzés:

- Ha a(z) **Beáll.** > **Általános beállítások > Művelet időtúllépése** beállítását **Be** értékre állítja, akkor a lapolvasó ki fogja jelentkeztetni, ha egy ideig nem használja a kezelőpanelt.
- Ha a **Módosítás** vagy az **Alaphelyzet** opciót választja a **Rendszergazdai jelszó** képernyőn, és megadja a rendszergazdai jelszót, akkor módosíthatja vagy törölheti a rendszergazdai jelszót.

A rendszergazdai jelszó konfigurálása Web Config alkalmazással

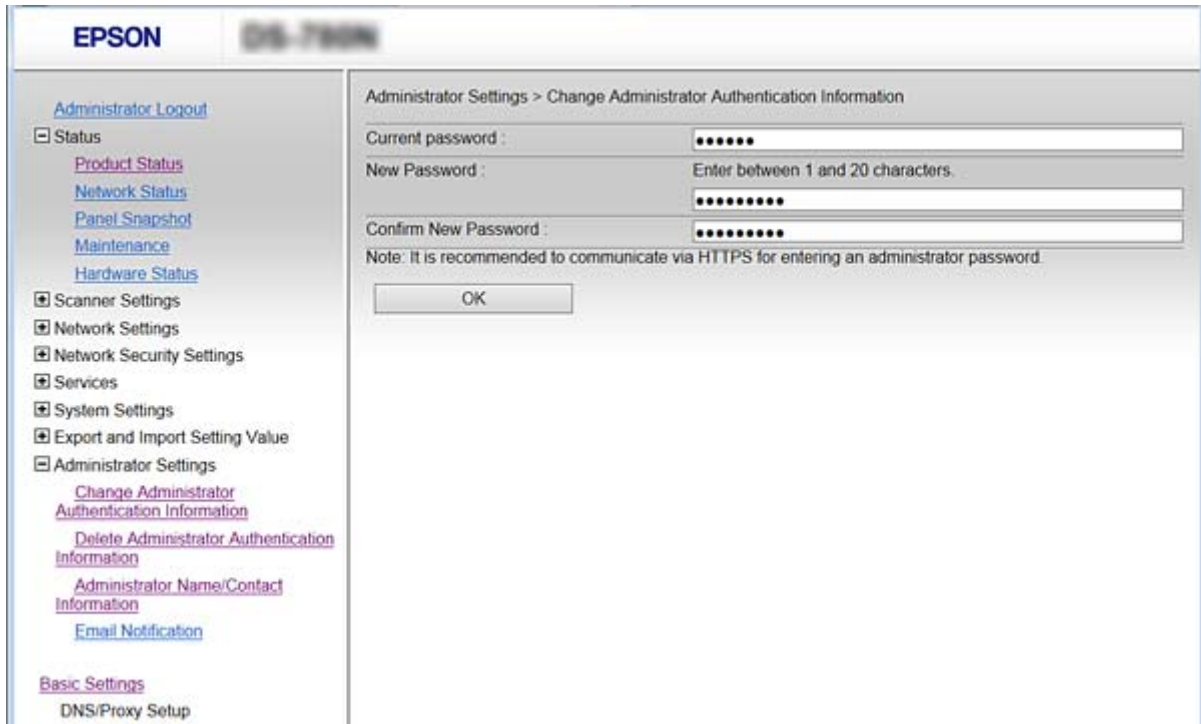
A rendszergazdai jelszó beállítható a(z) Web Config alkalmazással.

1. Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **Administrator Settings > Change Administrator Authentication Information** menüpontot.

Alapvető biztonsági beállítások

2. Írjon be egy új jelszót a **New Password** és a **Confirm New Password** mezőbe. Szükség esetén adja meg a felhasználónevet.

Ha új jelszót szeretne megadni, adja meg először a meglévőt.



3. Válassza a(z) **OK** lehetőséget.

Megjegyzés:

- A zárolt menüelemek beállításához vagy módosításához kattintson a(z) **Administrator Login** elemre, majd írja be a rendszergazdai jelszót.
- A rendszergazdai jelszó törléséhez kattintson a(z) **Administrator Settings > Delete Administrator Authentication Information** lehetőségre, majd adja meg a rendszergazdai jelszót.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

A rendszergazdai jelszóval zárolandó elemek

A rendszergazdák jogosultak minden, az eszközökön megtalálható funkció beállítására és módosítására.

Akkor is, ha Ön állította be az eszközön a rendszergazdai jelszót, zárolhatja az eszközt úgy, hogy az eszköz kezelésével kapcsolatos elemeket ne tudja módosítani.

Az alábbiakban bemutatjuk a rendszergazda által felügyelhető elemeket.

Elem	Leírás
Lapolvasó beállítása	Dupla behúzás észlelésének és Kis sebesség üzemmód beállítása.
Ethernet-kapcsolat beállításai	Az eszköznevek és az IP-cím módosítása, a DNS-kiszolgáló vagy a proxy-kiszolgáló beállítása, valamint a hálózati kapcsolatokra vonatkozó beállítások módosítása.

Alapvető biztonsági beállítások

Elem	Leírás
Felhasználói szolgáltatások beállítása	Kommunikációs protokollok, Hálózati beolvasás és Document Capture Pro szolgáltatások vezérlésének beállítása.
E-mail kiszolgáló beállítása	Olyan e-mail kiszolgáló beállítása, amivel az eszközök közvetlenül kommunikálnak.
Biztonsági beállítás	Hálózati biztonság beállításai, pl.: SSL/TLS-kommunikáció, IPsec-/IP-szűrés és IEEE802.1X funkció.
Gyökértanúsítvány frissítése	A(z) Document Capture Pro Server hitelesítéséhez és a firmware-frissítéshez szükséges gyökértanúsítványok frissítése a(z) Web Config alkalmazásból.
Firmware frissítés	Az eszközök firmware-jének ellenőrzése és frissítése.
Idő-, időzítőbeállítás	Alvó üzemmódba való átváltás időpontja, automatikus kikapcsolás, dátum/idő, az üzemen kívül töltött időt számláló időzítő, és egyéb, időzítőhöz kapcsolódó beállítások.
Alapértelmezett beállítások visszaállítása	A lapolvasó gyári beállításokra való visszaállításának beállítása.
Rendszergazda-beállítás	A rendszergazdai zárolás vagy a rendszergazdai jelszó beállítása.
Tanúsított eszközbeállítás	A hitelesítési eszköz azonosítóbeállítása. Akkor kell beállítani, ha a lapolvasót hitelesítési eszközöket támogató hitelesítési rendszeren használják.

Protokollok vezérlése

Különbféle útvonalak és protokollok segítségével végezhet lapolvasást. Tetszőleges számú hálózati számítógépről végezhet hálózati lapolvasást. Pl.: amikor a lapolvasás kizárólag meghatározott útvonalak és protokollok használatával engedélyezett. A nemkívánatos biztonsági kockázatok csökkentéséhez korlátozhatja a lapolvasást bizonyos útvonalokról, illetve igény szerint vezérelheti a rendelkezésre álló funkciókat.

A protokollbeállítások konfigurálása.

1. Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **Services > Protocol** menüpontot.
2. Konfigurálja az egyes beállításokat.
3. Kattintson a(z) **Next** elemre.
4. Kattintson a(z) **OK** elemre.

A beállítások aktiválódnak a lapolvasón.

Kapcsolódó információ

- ➔ „A Web Config elérése“ 23. oldal
- ➔ „Engedélyezhető és letiltható protokollok“ 36. oldal
- ➔ „Protokollbeállítások“ 37. oldal

Alapvető biztonsági beállítások

Engedélyezhető és letiltható protokollok

Protokoll	Leírás
Bonjour Settings	Megadhatja, hogy szeretné-e használni a Bonjour szolgáltatást. A(z) Bonjour szolgáltatással készülékeket kereshet, lapolvasást végezhet stb.
SLP Settings	Engedélyezheti vagy letilthatja a(z) SLP funkciót. A(z) SLP funkcióval a(z) Epson Scan 2 alkalmazást használhatja, illetve hálózati keresést végezhet a(z) EpsonNet Config. alkalmazásban
WSD Settings	Engedélyezheti vagy letilthatja a WSD funkciót. Ha engedélyezi ezt a funkciót, WSD-készülékeket adhat meg, vagy a WSD-porton keresztül szkennelhet.
LLTD Settings	Engedélyezheti vagy letilthatja a(z) LLTD funkciót. Ha a funkció engedélyezve van, akkor megjelenik a Windows hálózati térképén.
LLMNR Settings	Engedélyezheti vagy letilthatja a(z) LLMNR funkciót. Ha engedélyezi ezt a funkciót, akkor NetBIOS nélkül végezhet névfeloldást, még akkor is, ha a DNS-t nem tudja használni.
SNMPv1/v2c Settings	Megadhatja, hogy engedélyezi-e a(z) SNMPv1/v2c használatát. Ezzel a szolgáltatásokat, nyomon követést stb. állíthatja be.
SNMPv3 Settings	Megadhatja, hogy engedélyezi-e a(z) SNMPv3 használatát. Ezzel beállíthatja a titkosított eszközöket, a nyomon követést stb.

Kapcsolódó információ

- ➔ „Protokollok vezérlése“ 35. oldal
- ➔ „Protokollbeállítások“ 37. oldal

Alapvető biztonsági beállítások

Protokollbeállítások

The screenshot shows the 'Services > Protocol' configuration page in the Epson network utility. The left sidebar contains navigation options like 'Administrator Logout', 'Status', 'Product Status', 'Network Status', 'Panel Snapshot', 'Maintenance', 'Hardware Status', 'Scanner Settings', 'Network Settings', 'Network Security Settings', 'Services', 'System Settings', 'Export and Import Setting Value', 'Administrator Settings', and 'Basic Settings' (including DNS/Proxy Setup, Firmware Update, Root Certificate Update, and Product Status).

The main content area is titled 'Services > Protocol' and includes a note: 'Note: If you need to change the Device Name used on each protocol and the Bonjour Name, change the Device Name in the Network Settings. If you need to change the Location used on each protocol, change it in the Network Settings.'

The settings are organized into several sections:

- Bonjour Settings:**
 - Use Bonjour
 - Bonjour Name: EPSON884045.local
 - Bonjour Service Name: EPSON
 - Location: (empty)
- SLP Settings:**
 - Enable SLP
- WSD Settings:**
 - Enable WSD
 - Scanning Timeout (sec): 300
 - Device Name: EPSON
 - Location: (empty)
- LLTD Settings:**
 - Enable LLTD
 - Device Name: EPSON
- LLMNR Settings:**
 - Enable LLMNR
- SNMPv1/v2c Settings:**
 - Enable SNMPv1/v2c
 - Access Authority: Read/Write
 - Community Name (Read Only): public
 - Community Name (Read/Write): (empty)
- SNMPv3 Settings:**
 - Enable SNMPv3
 - User Name: admin
 - Authentication Settings:**
 - Algorithm: MD5
 - Password: (empty)
 - Confirm Password: (empty)
 - Encryption Settings:**
 - Algorithm: DES
 - Password: (empty)
 - Confirm Password: (empty)
 - Context Name: EPSON

A 'Next' button is located at the bottom of the settings area.

Elemek

Beállítási érték és leírás

Bonjour Settings

Alapvető biztonsági beállítások

Elemek	Beállítási érték és leírás
Use Bonjour	Ezzel a beállítással a(z) Bonjour szolgáltatáson keresztül kereshet vagy használhat készülékeket.
Bonjour Name	Megjeleníti a Bonjour nevét.
Bonjour Service Name	Megjelenítheti vagy beállíthatja a(z) Bonjour szolgáltatás nevét.
Location	Megjeleníti a(z) Bonjour helynevét.
SLP Settings	
Enable SLP	Ezzel a beállítással engedélyezheti az SLP funkciót. Hálózatfelderítésre használják a(z) Epson Scan 2 és EpsonNet Config alkalmazásban.
WSD Settings	
Enable WSD	Ezzel a beállítással engedélyezheti, hogy készülékeket lehessen hozzáadni a WSD segítségével, illetve a(z) WSD-portról lehessen nyomtatni és szkennelni.
Scanning Timeout (sec)	Adja meg a kommunikáció időtűllépésének értékét a WSD-szkenneléshez. 3 és 3600 másodperc közötti értéket adhat meg.
Device Name	Megjeleníti a(z) WSD készüléknevét.
Location	Megjeleníti a(z) WSD helynevét.
LLTD Settings	
Enable LLTD	Ezzel a beállítással engedélyezheti az LLTD használatát. A szkennert megjelenik a Windows hálózati térképen.
Device Name	Megjeleníti a(z) LLTD készüléknevét.
LLMNR Settings	
Enable LLMNR	Ezzel a beállítással engedélyezheti az LLMNR használatát. A NetBIOS nélkül végezhet névfeloldást, még akkor is, ha a DNS-t nem tudja használni.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Ezzel a beállítással engedélyezheti az SNMPv1/v2c használatát. Csak azok a szkennerek jelennek meg, amelyek támogatják a(z) SNMPv3 használatát.
Access Authority	Állítsa be a hozzáférési hatóságot, ha az SNMPv1/v2c engedélyezve van. Válasszon a(z) Read Only és a(z) Read/Write lehetőség közül.
Community Name (Read Only)	Adjon meg 0–32 ASCII (0x20–0x7E) karaktert.
Community Name (Read/Write)	Adjon meg 0–32 ASCII (0x20–0x7E) karaktert.
SNMPv3 Settings	
Enable SNMPv3	A jelölőnégyzet bejelölése esetén a(z) SNMPv3 engedélyezett.

Alapvető biztonsági beállítások

Elemek	Beállítási érték és leírás
User Name	1 bájtos karaktereket használva írjon be 1–32 karaktert.
Authentication Settings	
Algorithm	Válasszon algoritmust a(z) SNMPv3 hitelesítésére.
Password	Adja meg a jelszót a(z) SNMPv3 hitelesítésére. Írjon be 8–32 ASCII-karaktert (0x20–0x7E). Amennyiben nem szeretné megadni ezt az adatot, hagyja üresen a mezőt.
Confirm Password	A megerősítéshez adja meg a beállított jelszót.
Encryption Settings	
Algorithm	Válasszon algoritmust a(z) SNMPv3 titkosítására
Password	Adja meg a jelszót a(z) SNMPv3 titkosítására. Írjon be 8–32 ASCII-karaktert (0x20–0x7E). Amennyiben nem szeretné megadni ezt az adatot, hagyja üresen a mezőt.
Confirm Password	A megerősítéshez adja meg a beállított jelszót.
Context Name	Írjon be 32 vagy kevesebb Unicode-karaktert (UTF-8). Amennyiben nem szeretné megadni ezt az adatot, hagyja üresen a mezőt. A beírható karakterek száma a nyelvtől függően változik.

Kapcsolódó információ

- ➔ [„Protokollok vezérlése“ 35. oldal](#)
- ➔ [„Engedélyezhető és letiltható protokollok“ 36. oldal](#)

Működési és kezelési beállítások

A jelen fejezet az eszköz napi szintű működtetésével és kezelésével kapcsolatos elemeket ismerteti.

Egy eszköz adatainak a megerősítése

Az üzemelő eszköz alábbi adatai ellenőrizhetők a(z) **Status** menüben a(z) Web Config alkalmazással.

- Product Status
Ellenőrizze a nyelvet, az állapotot, a termékszámot, a MAC-címet stb.
- Network Status
Ellenőrizze a hálózati kapcsolatot, az IP-cím, a DNS-kiszolgáló, stb. adatait.
- Panel Snapshot
Jelenítsen meg egy pillanatképet egy, az eszköz kezelőpaneljén látható képernyőképről.
- Maintenance
Ellenőrizze a kezdési dátumot, a lapolvasási adatokat stb.
- Hardware Status
Ellenőrizze a lapolvasó állapotát.

Kapcsolódó információ

➔ [„A Web Config elérése“ 23. oldal](#)

Eszközök kezelése (Epson Device Admin)

Az Epson Device Admin segítségével több eszköz is kezelhető és működtethető. Az Epson Device Admin lehetővé teszi a különböző hálózatokon elhelyezett eszközök kezelését. A főbb kezelési funkciók az alábbiak.

A funkciókkal és a szoftver használatával kapcsolatos további információkhoz lásd az Epson Device Admin dokumentációját, illetve súgóját.

- Eszközök felismerése
Az eszközök felismerhetők a hálózaton, így listába regisztrálhatja azokat. Ha a rendszergazda számítógépével azonos hálózati szegmenshez Epson eszközöket (pl. nyomtatók és lapolvasók) csatlakoztattak, azokat még akkor is megtalálja, ha nem társítottak hozzájuk IP-címet.
Szintén felismerheti azokat az eszközöket, amelyeket a hálózaton USB-kábellel csatlakoztattak a számítógéphez. Telepítenie kell az Epson Device USB Agent programot a számítógépre.
- Eszközök beállítása
Létrehozhat egy sablont, mely beállításelemeket tartalmaz (pl. hálózati illesztő és papírforrás), és megosztott beállításként alkalmazhatja azokat más eszközökre. Ha csatlakoztatták a hálózathoz, IP-címet társíthat egy olyan eszközhöz, amelyhez még nem társítottak IP-címet.

Működési és kezelési beállítások

Eszközök felügyelete

Rendszeresen lekérheti az eszközök állapotát és részletes információit a hálózaton. Ezen kívül azokat az eszközöket is felügyelheti, amelyeket a hálózaton USB-kábellel csatlakoztattak a számítógépekhez, valamint a más vállalatoktól származó, az eszközlístában szereplő eszközöket is. Az USB-kábellel csatlakoztatott eszközök felügyeletéhez telepítenie kell az Epson Device USB Agent programot.

Riasztások kezelése

Felügyelheti az eszközök és a fogyóeszközök állapotáról szóló riasztásokat. A rendszer a beállított feltételeknek megfelelően automatikusan értesítő e-maileket küld a rendszergazdának.

Jelentések kezelése

Rendszeres jelentéseket hozhat létre, ahogy a rendszer adatokat gyűjt az eszközök felhasználásáról és a fogyóeszközökről. Ezután ezeket a létrehozott jelentéseket elmentheti, és elküldheti e-mailben.

Kapcsolódó információ

➔ [„Epson Device Admin“ 55. oldal](#)

E-mail értesítések fogadása bizonyos események bekövetkeztekor

Az e-mailes értesítésekről

A funkció segítségével e-mailes értesítéseket kaphat olyankor, amikor események történnek. Legfeljebb 5 e-mail-címet regisztrálhat, és kiválaszthatja, hogy melyik eseményekről szeretne értesítéseket fogadni.

A funkció használatához konfigurálni kell a levelezőkiszolgálót.

Kapcsolódó információ

➔ [„Levelezőkiszolgáló beállítása“ 42. oldal](#)

Az e-mailes értesítések konfigurálása

A funkció használatához be kell állítani egy levelezőkiszolgálót.

1. Jelenítse meg a Web Config segédprogramot, és válassza ki a **Administrator Settings > Email Notification** pontot.
2. Adjon meg egy e-mail címet, ahová fogadni szeretné az e-mailes értesítéseket.
3. Válassza ki az e-mailes értesítések nyelvét.

Működési és kezelési beállítások

4. Jelölje be azoknak az értesítéseknek a négyzeteit, amelyeket fogadni szeretne.

Administrator Settings > Email Notification

Set up the Email Server to enable the email notification.

Email Address Settings

Email in selected language will be sent to each address.

1 :	admin@aaa.com	English
2 :	aaa@aaa.com	English
3 :		English
4 :		English
5 :		English

Notification Settings

Email will be sent when product status is as checked.

	1	2	3	4	5
Administrator password changed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Scanner error	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Restore Default Settings

5. Kattintson a(z) OK gombra.

Kapcsolódó információ

- ➔ „A Web Config elérése“ 23. oldal
- ➔ „Levelezőkiszolgáló beállítása“ 42. oldal

Levelezőkiszolgáló beállítása

Konfigurálás előtt ellenőrizze az alábbiakat.

- A lapolvasó csatlakoztatva van egy hálózathoz.
- A számítógép levelezőkiszolgálójának adatai.

1. Jelenítse meg a Web Config segédprogramot, és válassza ki a **Network Settings > Email Server > Basic** pontot.
2. Írjon be egy értéket minden egyes elem számára.
3. Kattintson a **OK** gombra.
Megjelennek a kiválasztott beállítások.

Kapcsolódó információ

- ➔ „A Web Config elérése“ 23. oldal
- ➔ „A levelezőkiszolgáló beállításai“ 43. oldal

A levelezőkiszolgáló beállításai

The screenshot shows the Epson printer's web interface for configuring the Email Server. The left sidebar contains a navigation menu with categories like Status, Contacts, Network Settings, and Services. The main content area is titled 'Network Settings > Email Server > Basic'. It contains a warning about certificates and several input fields for configuring SMTP and POP3 settings. The 'Authentication Method' is set to 'SMTP AUTH'. Other fields include 'Authenticated Account', 'Authenticated Password', 'Sender's Email Address', 'SMTP Server Address', 'SMTP Server Port Number', 'Secure Connection', and 'Certificate Validation' (with 'Enable' selected).

Elemek	Beállítások és magyarázat	
Authentication Method	A levelezőkiszolgáló eléréséhez hitelesítési módot kell megadni a lapolvasó számára.	
	Off	A hitelesztés le van tiltva a levelezőkiszolgálóval való kommunikáció közben.
	SMTP AUTH	Szükséges, hogy a levelezőkiszolgáló támogassa az SMTP-hitelesítést.
	POP before SMTP	E módszer kiválasztásakor állítsa be a POP3 kiszolgálót.
Authenticated Account	Ha az SMTP AUTH vagy a POP before SMTP lehetőséget választja ki a Authentication Method beállításnál, adja meg a hitelesített fióknevet 0 és 255 közötti ASCII (0x20–0x7E) karakterrel.	
Authenticated Password	Ha az SMTP AUTH vagy a POP before SMTP lehetőséget választja ki a Authentication Method beállításnál, adja meg a hitelesített jelszót 0 és 20 közötti karakterrel A–Z, a–z, 0–9! # \$ % & ' * + - . / = ? ^ _ { } ~ @.	
Sender's Email Address	Írja be a feladó e-mail címét. Írjon be legfeljebb 255 ASCII-karaktert (0x20–0x7E), amelyek nem tartalmazhatják ezeket: () < > [] ; ¥. A pont (.) nem lehet kezdő karakter.	
SMTP Server Address	0 és 255 közötti számú karaktert írjon be, amely az A–Z, a–z, 0–9 karaktereket tartalmazhatja. - . Az IPv4 és az FQDN formátumot használhatja.	
SMTP Server Port Number	Írjon be egy 1 és 65535 közötti számot.	

Működési és kezelési beállítások

Elemek	Beállítások és magyarázat	
Secure Connection	Adja meg a biztonsági csatlakozási módszert a levelezőkiszolgáló számára.	
	None	Ha a POP before SMTP lehetőséget választja ki a Authentication Method beállításnál, akkor csatlakozási módként a None lesz beállítva.
	SSL/TLS	Ez a beállítás akkor használható, ha a Authentication Method Off vagy SMTP AUTH értékre van állítva.
	STARTTLS	Ez a beállítás akkor használható, ha a Authentication Method Off vagy SMTP AUTH értékre van állítva.
Certificate Validation	Ha engedélyezve van ez a beállítás, akkor a rendszer ellenőrzi a tanúsítványt. Azt javasoljuk, hogy ezt a beállítást állítsa Enable értékre.	
POP3 Server Address	Ha a POP before SMTP lehetőséget választja ki a Authentication Method beállításnál, adja meg a POP3 kiszolgálócímet 0 és 255 közötti karakterrel A–Z, a–z, 0–9 . - . Az IPv4 és az FQDN formátumot használhatja.	
POP3 Server Port Number	Ha a POP before SMTP lehetőséget választja ki a Authentication Method beállításnál, írjon be egy számot 1 és 65535 között.	

Kapcsolódó információ

➔ „Levelezőkiszolgáló beállítása“ 42. oldal

A levelezőkiszolgáló kapcsolódásának ellenőrzése

- Jelenítse meg a Web Config segédprogramot, és válassza ki a **Network Settings > Email Server > Connection Test** pontot.
- Kattintson a **Start** gombra.
Megkezdődik a levelezőkiszolgáló csatlakozási tesztje. A teszt végeztével egy ellenőrzési jelentés jelenik meg.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

➔ „Levelezőkiszolgáló-kapcsolódási teszt — referenciák“ 44. oldal

Levelezőkiszolgáló-kapcsolódási teszt — referenciák

Üzenetek	Magyarázat
Connection test was successful.	Ez az üzenet akkor jelenik meg, ha sikeresen létrejött a kapcsolat a kiszolgálóval.
SMTP server communication error. Check the following. - Network Settings	Ez az üzenet akkor jelenik meg, ha <ul style="list-style-type: none"> <input type="checkbox"/> A lapolvasó nincs csatlakoztatva hálózathoz <input type="checkbox"/> Az SMTP-kiszolgáló nem érhető el <input type="checkbox"/> Kommunikáció közben megszakadt a hálózati kapcsolat <input type="checkbox"/> Hiányos adatok érkeztek

Működési és kezelési beállítások

Üzenetek	Magyarázat
POP3 server communication error. Check the following. - Network Settings	Ez az üzenet akkor jelenik meg, ha <ul style="list-style-type: none"> <input type="checkbox"/> A lapolvasó nincs csatlakoztatva hálózathoz <input type="checkbox"/> Az POP3-kiszolgáló nem érhető el <input type="checkbox"/> Kommunikáció közben megszakadt a hálózati kapcsolat <input type="checkbox"/> Hiányos adatok érkeztek
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Ez az üzenet akkor jelenik meg, ha <ul style="list-style-type: none"> <input type="checkbox"/> A DNS-kiszolgálóhoz nem lehetett csatlakozni <input type="checkbox"/> Az SMTP-kiszolgáló nevének feloldása sikertelen
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Ez az üzenet akkor jelenik meg, ha <ul style="list-style-type: none"> <input type="checkbox"/> A DNS-kiszolgálóhoz nem lehetett csatlakozni <input type="checkbox"/> Az POP3-kiszolgáló nevének feloldása sikertelen
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Ez az üzenet akkor jelenik meg, ha az SMTP-kiszolgáló hitelesítése sikertelen.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Ez az üzenet akkor jelenik meg, ha az POP3-kiszolgáló hitelesítése sikertelen.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Ez az üzenet akkor jelenik meg, ha nem támogatott protokollokkal próbál kommunikálni.
Connection to SMTP server failed. Change Secure Connection to None.	Ez az üzenet akkor jelenik meg, ha SMTP-eltérés tapasztalható egy kiszolgáló és egy ügyfélgép között, vagy ha a kiszolgáló nem támogatja a biztonságos SMTP-kapcsolatot (SSL-kapcsolatot).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Ez az üzenet akkor jelenik meg, ha SMTP-eltérés tapasztalható egy kiszolgáló és egy ügyfélgép között, vagy ha a kiszolgáló SSL/TLS-kapcsolat használatát kéri egy biztonságos SMTP-kapcsolathoz.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Ez az üzenet akkor jelenik meg, ha SMTP-eltérés tapasztalható egy kiszolgáló és egy ügyfélgép között, vagy ha a kiszolgáló STARTTLS-kapcsolat használatát kéri egy biztonságos SMTP-kapcsolathoz.
The connection is untrusted. Check the following. - Date and Time	Ez az üzenet akkor jelenik meg, ha a lapolvasó dátum- és időbeállítása hibás, vagy a tanúsítvány lejárt.
The connection is untrusted. Check the following. - CA Certificate	Ez az üzenet akkor jelenik meg, ha a lapolvasó nem rendelkezik olyan gyökértanúsítvánnyal, amely megfelel a kiszolgálónak, vagy ha egy CA Certificate nem lett importálva.
The connection is not secured.	Ez az üzenet akkor jelenik meg, ha a beszerzett tanúsítvány sérült.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Ez az üzenet akkor jelenik meg, ha hitelesítési módszerrel kapcsolatos eltérés tapasztalható egy kiszolgáló és egy ügyfélgép között. A kiszolgáló támogatja az SMTP AUTH hitelesítést.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Ez az üzenet akkor jelenik meg, ha hitelesítési módszerrel kapcsolatos eltérés tapasztalható egy kiszolgáló és egy ügyfélgép között. A kiszolgáló nem támogatja az SMTP AUTH használatát.

Működési és kezelési beállítások

Üzenetek	Magyarázat
Sender's Email Address is incorrect. Change to the email address for your email service.	Ez az üzenet akkor jelenik meg, ha a megadott feladó e-mail címe hibás.
Cannot access the product until processing is complete.	Ez az üzenet akkor jelenik meg, ha a lapolvasó foglalt.

Kapcsolódó információ

➔ „A levelezőkiszolgáló kapcsolódásának ellenőrzése“ 44. oldal

Firmware frissítése

Firmware frissítése Web Config használatával

Frissíti a firmware-t Web Config használatával. Az eszköznek csatlakoznia kell az internethez.

- Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **Basic Settings > Firmware Update** menüpontot.
- Kattintson a(z) **Start** elemre.
A firmware megerősítése elindul, és amennyiben létezik frissített firmware, megjelennek a firmware információi.
- Kattintson a(z) **Start** menüre, és kövesse a képernyőn megjelenő utasításokat.

Megjegyzés:

A firmware az Epson Device Admin funkcióval is frissíthető. A firmware információkat az eszközlistában szemrevételezéssel megerősítheti. Ez akkor hasznos, ha több eszköz firmware programját szeretné frissíteni. További részletekért lásd az Epson Device Admin útmutatóját, illetve súgóját.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

➔ „Epson Device Admin“ 55. oldal

Firmware frissítése az Epson Firmware Updater használatával

Töltse le a számítógépre az eszközhöz tartozó firmware-t az Epson weboldaláról, majd a firmware frissítéséhez csatlakoztassa össze az eszközt és a számítógépet egy USB-kábel segítségével. Amennyiben a hálózaton keresztül nem lehet frissíteni, próbálja ki ezt a módszert.

- Lépjen fel az Epson weboldalára, és töltse le a firmware-t.
- Egy USB-kábel segítségével csatlakoztassa a letöltött firmware-t tároló számítógépet az eszközhöz.
- Kattintson kétszer a letöltött .exe fájlra.
Az Epson Firmware Updater elindul.

4. Kövesse a képernyőn megjelenő utasításokat.

Biztonsági mentés készítése a beállításokról

A beállítási elemek Web Config alkalmazásban való exportálásával átmásolhatóak az elemek más lapolvasókra.

A beállítások exportálása

Exportálja a lapolvasó egyes beállításait.

1. A Web Config menüben válassza ki a **Export and Import Setting Value > Export** pontot.

2. Válassza ki az exportálni kívánt beállításokat.

Válassza ki azokat a beállításokat, amelyeket exportálni szeretne. Ha kiválasztja a szülőkategóriát, az alkategóriákat is kiválaszthatja. Olyan alkategóriákat azonban nem lehet kiválasztani, amelyek ugyanazon a hálózaton megkettőzik az adatokat (pl. az IP-címet stb.), és emiatt hibát okoznak.

3. Írjon be egy jelszót az exportált fájl titkosításához.

A fájl importálásához szüksége lesz a jelszóra. Ha nem szeretné titkosítani a fájlt, akkor hagyja üresen ezt a beállítást.

4. Kattintson a(z) **Export** gombra.



Fontos:

*Ha a lapolvasó hálózati beállításait, például a lapolvasó nevét és IP-címét exportálni szeretné, jelölje be a **Enable to select the individual settings of device** lehetőséget, és válasszon ki további elemeket. A cserelapolvasóhoz kizárólag a kijelölt értékeket használja.*

Kapcsolódó információ

➔ [„A Web Config elérése“ 23. oldal](#)

A beállítások importálása

Az exportált Web Config-fájlt igény szerint importálhatja a lapolvasóba.



Fontos:

Ha olyan értékeket importál, amelyek különálló adatokat, például lapolvasónevet vagy IP-címet tartalmaznak, győződjön meg arról, hogy ugyanaz az IP-cím nem szerepel az adott hálózaton. Ha az IP-cím átfedésben van egy másik címmel, a lapolvasó nem tükrözi az értéket.

1. A Web Config menüben válassza ki a **Export and Import Setting Value > Import** pontot.

2. Jelölje ki az exportált fájlt, majd adja meg a titkosított jelszót.

3. Kattintson a(z) **Next** gombra.

Működési és kezelési beállítások

4. Jelölje ki az importálni kívánt beállításokat, majd kattintson a **Next** lehetőségre.
5. Kattintson a(z) **OK** gombra.

A beállítások aktiválódnak a lapolvasón.

Kapcsolódó információ

➔ [„A Web Config elérése“ 23. oldal](#)

Problémák megoldása

Problémamegoldási tippek

Bővebb tájékoztatás az alábbi kézikönyvben található.

Használati útmutató

Utasításokat tartalmaz a lapolvasó használatával, a karbantartással és a problémák megoldásával kapcsolatban.

A Kiszolgálónapló és a Hálózati eszköz naplójának ellenőrzése

Amennyiben probléma merült fel a hálózati kapcsolattal, akkor meghatározhatja annak okát, ha a hálózati eszköz rendszernaplóinak és vezérlőinek (pl.: útválasztók) segítségével ellenőrzi a levelezőkiszolgáló, az LDAP-kiszolgáló, stb. naplóját vagy az állapotot.

Hálózati beállítások inicializálása

Hálózati beállítások visszaállítása a nyomtatót kezelőpaneljén

Az összes hálózati beállítás visszaállítható az alapértelmezett értékre.

1. Koppintson a(z) **Beáll.** elemre a kezdőképernyőn.
2. Koppintson a(z) **Rendszerfelügyelet > Alapértékek visszaállítása > Hálózati beállítások** elemre.
3. Olvassa el az üzenetet, majd koppintson a(z) **Igen** elemre.
4. Miután megjelenik a befejezést jelző üzenet, koppintson a(z) **Bezár** gombra.

A képernyő automatikusan bezáródik meghatározott idő elteltével, ha nem koppint a(z) **Bezár** gombra.

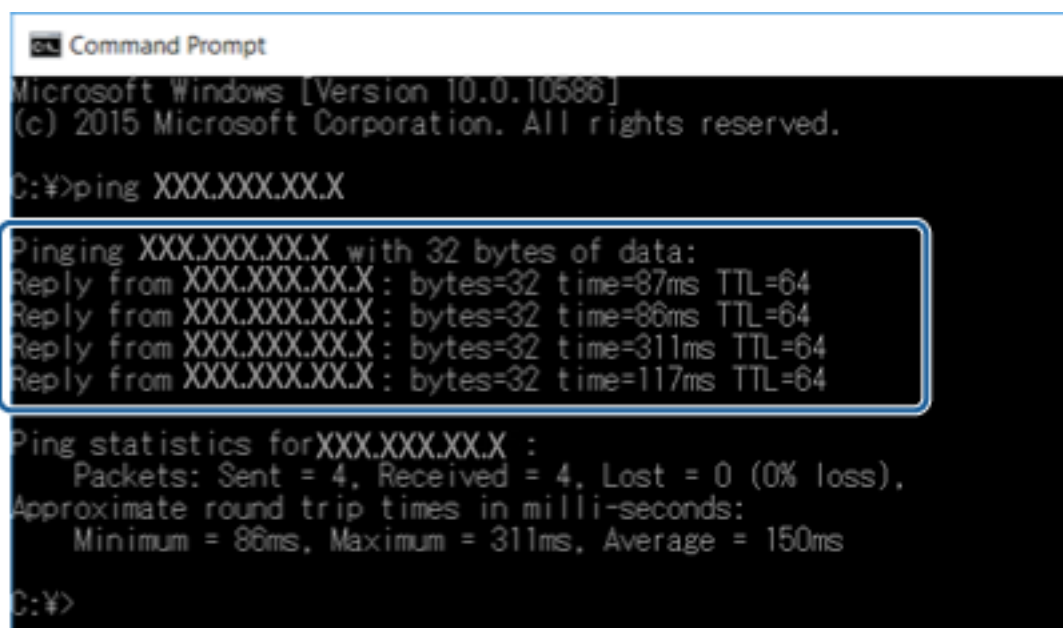
Az eszközök és a számítógépek közötti kommunikáció ellenőrzése

Csatlakozás ellenőrzése Ping paranccsal — Windows

A számítógép és a lapolvasó közötti kapcsolat ellenőrzéséhez a ping parancsot is használhatja. A kapcsolat ping paranccsal történő ellenőrzéséhez kövesse az alábbi lépéseket.

Problémák megoldása

1. Ellenőrizze a lapolvasó ellenőrizendő kapcsolatra vonatkozó IP-címét.
Ezt az Epson Scan 2 alkalmazás segítségével teheti meg.
2. Jelenítse meg a számítógép parancssori képernyőjét.
 - ❑ Windows 10
Jobb egérgombbal kattintson a Start gombra, vagy érintse meg és tartsa lenyomva a Start gombot, majd válassza a **Parancssor** lehetőséget.
 - ❑ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
Jelenítse meg az alkalmazások képernyőjét, majd válassza a **Parancssor** lehetőséget.
 - ❑ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 vagy régebbi
Kattintson a Start gombra, majd válassza a **Minden program** vagy **Programok > Kellékek > Parancssor** lehetőséget.
3. Írja be a „ping xxx.xxx.xxx.xxx” kifejezést, majd nyomja meg az Enter billentyűt.
Az xxx.xxx.xxx.xxx helyére a lapolvasó IP-címét írja be.
4. Ellenőrizze a kommunikáció állapotát.
Ha a lapolvasó és a számítógép kommunikál egymással, akkor a következő üzenet jelenik meg.



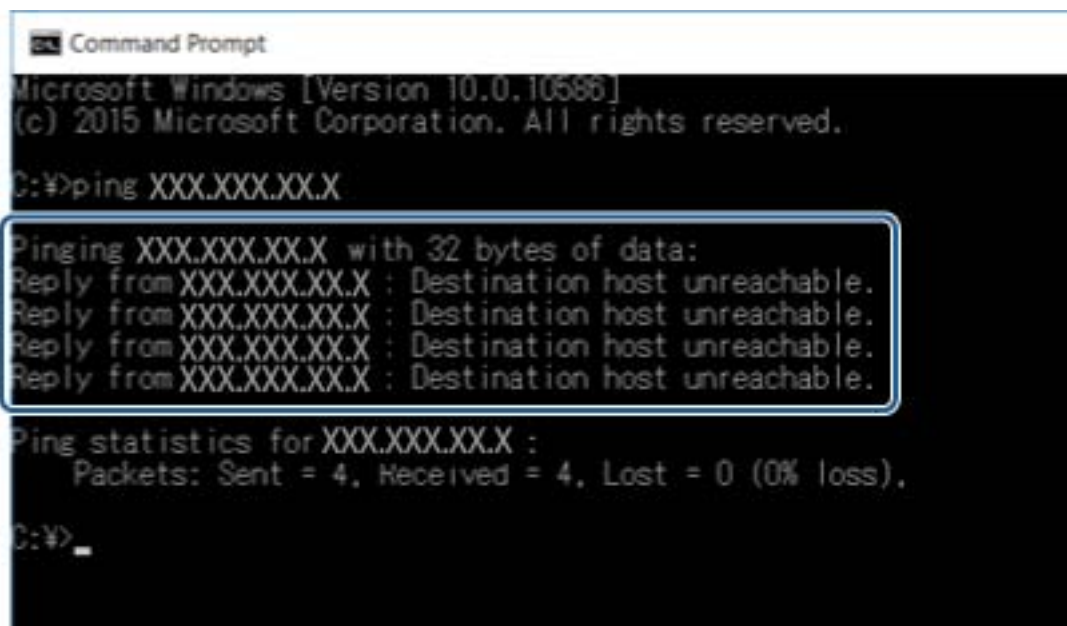
```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\>ping XXX.XXX.XX.X

Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X : bytes=32 time=87ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=86ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=311ms TTL=64
Reply from XXX.XXX.XX.X : bytes=32 time=117ms TTL=64

Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 86ms, Maximum = 311ms, Average = 150ms
C:\>
```

Problémák megoldása

Ha a lapolvasó és a számítógép nem kommunikál egymással, akkor a következő üzenet jelenik meg.



```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\>ping XXX.XXX.XX.X

Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.
Reply from XXX.XXX.XX.X : Destination host unreachable.

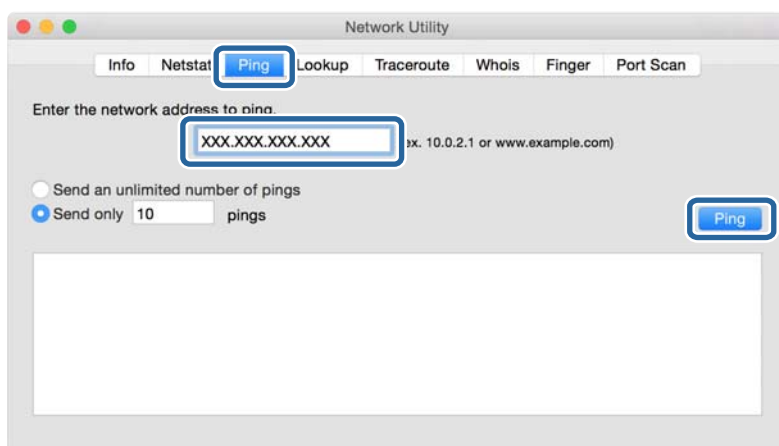
Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\>
```

Csatlakozás ellenőrzése Ping paranccsal — Mac OS

A számítógép és a lapolvasó közötti kapcsolat ellenőrzéséhez a ping parancsot is használhatja. A kapcsolat ping paranccsal történő ellenőrzéséhez kövesse az alábbi lépéseket.

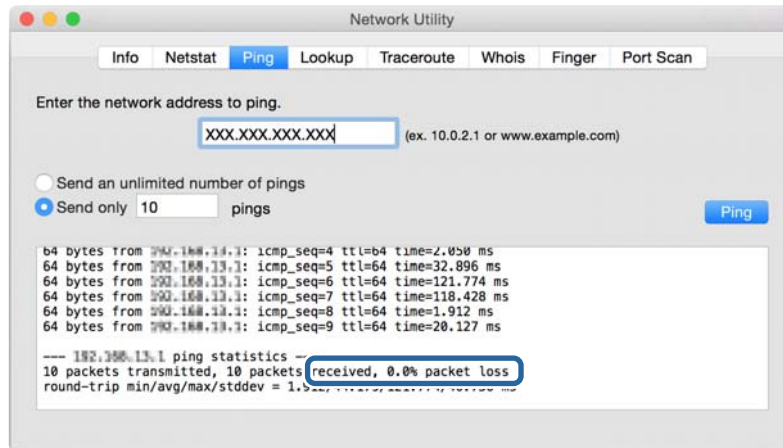
1. Ellenőrizze a lapolvasó ellenőrizendő kapcsolatra vonatkozó IP-címét.
Ezt az Epson Scan 2 alkalmazás segítségével teheti meg.
2. Futtassa a Hálózati segédprogramot.
Írja be a „Hálózati segédprogram” kifejezést a **Spotlight** felületen.
3. Kattintson a **Ping** lapra, írja be az 1. lépésben ellenőrzött IP-címet, majd kattintson a **Ping** elemre.



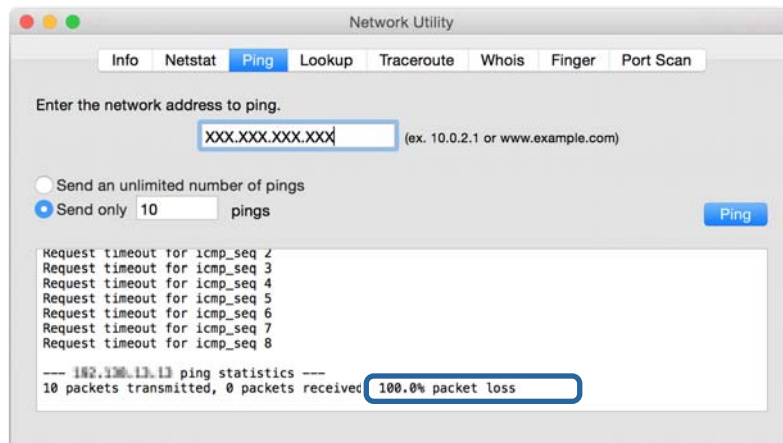
Problémák megoldása

4. A kommunikációs állapot ellenőrzése.

Ha a lapolvasó és a számítógép kommunikál egymással, akkor a következő üzenet jelenik meg.



Ha a lapolvasó és a számítógép nem kommunikál egymással, akkor a következő üzenet jelenik meg.



Problémák a hálózati szoftver használatával

Nem sikerül elérni a Web Config alkalmazást

Megfelelően van beállítva a lapolvasó IP-címe?

Konfigurálja az IP-címet az Epson Device Admin vagy az EpsonNet Config segítségével.

Támogatja a böngészője az Encryption Strength tömeges titkosításokat SSL/TLS-nél?

Az Encryption Strength tömeges titkosítások SSL/TLS a következők. A Web Config csak olyan böngészőből érhető el, amelyik támogatja a következő tömeges titkosításokat. Ellenőrizze, hogy a böngészője milyen titkosítást támogat.

- 80 bit: AES256/AES128/3DES
- 112 bit: AES256/AES128/3DES
- 128 bit: AES256/AES128

Problémák megoldása

- 192 bit: AES256
- 256 bit: AES256

Az „Elavult” üzenet jelenik meg, ha a Web Config elérése SSL (https) kommunikációval történik.

Ha a tanúsítvány lejárt, szerezze be újból a tanúsítványt. Ha az üzenet a lejáratási időpontja előtt jelenik meg, ellenőrizze, hogy a lapolvasó dátuma megfelelően van-e beállítva.

„A biztonsági tanúsítvány neve nem egyezik...” üzenet jelenik meg, ha a Web Config elérése SSL (https) kommunikáció segítségével történik.

A lapolvasó **Common Name** alatt saját aláírású tanúsítvány vagy CSR létrehozása érdekében beírt IP-címe nem felel meg a böngészőbe beírt címnek. Szerezzen be és importáljon újból egy tanúsítványt, vagy módosítsa a lapolvasó nevét.

A lapolvasó elérése proxykiszolgálón keresztül történik.

Ha proxykiszolgálót használ a lapolvasóhoz, meg kell adnia a böngésző proxybeállításait.

- Windows:

Kattintson a **Vezérlőpult > Hálózat és Internet > Internetbeállítások > Kapcsolatok > LAN-beállítások > Proxykiszolgáló** elemre, majd állítsa be, hogy a helyi címek elérése ne proxykiszolgálón keresztül történjen.

- Mac OS:

Kattintson a **Rendszerbeállítások > Hálózat > Speciális > Proxyk** elemre, majd regisztrálja a helyi címet a **A proxybeállítások figyelmen kívül hagyása ezeknek a hosztoknak és doméneknek az esetén** esetében.

Példa:

192.168.1.*: Helyi cím: 192.168.1.XXX, alhálózati maszk: 255.255.255.0

192.168.*.*: Helyi cím: 192.168.XXX.XXX, alhálózati maszk: 255.255.0.0

Kapcsolódó információ

- ➔ [„A Web Config elérése” 23. oldal](#)
- ➔ [„Az IP-cím hozzárendelése” 15. oldal](#)
- ➔ [„IP-cím hozzárendelése EpsonNet Config alkalmazással” 56. oldal](#)

A modell neve és/vagy IP-címe nem jelenik meg az EpsonNet Config alkalmazásban.

Kijelölte a Tiltás, Visszavonás, vagy Leállítás lehetőséget, amikor megjelent egy Windows biztonsági figyelmeztetés vagy a tűzfal képernyője?

A **Tiltás, Visszavonás** vagy **Leállítás** kijelölése esetén az IP-cím és a modell neve nem jelenik meg az EpsonNet Config vagy az EpsonNet Setup alkalmazásban.

Ennek kijavításához regisztrálja kivételként az EpsonNet Config alkalmazást a Windows tűzfal és kereskedelmi biztonsági szoftver segítségével. Ha vírusirtó vagy biztonsági programot használ, zárja be az EpsonNet Config használatakor.

Problémák megoldása

Túl rövid a kommunikációs hiba időtúllépési beállítása?

Indítsa el az EpsonNet Config alkalmazást, válassza a **Tools > Options > Timeout** parancsot, majd növelje az időtartamot a **Communication Error** beállítás esetében. Ha ezt teszi, előfordulhat, hogy az EpsonNet Config lassabban fog futni.

Kapcsolódó információ

- ➔ [„A\(z\) EpsonNet Config futtatása Windows alatt“ 56. oldal](#)
- ➔ [„A\(z\) EpsonNet Config futtatása Mac OS alatt“ 56. oldal](#)

Melléklet

A hálózati szoftver bemutatása

Az alábbiakban az eszközöket konfiguráló és kezelő szoftvert mutatjuk be.

Epson Device Admin

Az Epson Device Admin alkalmazással lehetősége van eszközöket telepíteni a hálózatra, majd konfigurálhatja és kezelheti ezeket az eszközöket. Részletes információkat szerezhet be eszközökről, pl.: állapot és fogyóeszközök, riasztási értesítések kiküldése és eszközhasználati jelentések készítése. Létrehozhat egy sablont is, mely beállításelemeket tartalmaz, és, megosztott beállításként alkalmazhatja azokat más eszközökre. Az Epson Device Admin alkalmazást az Epson támogatási weboldaláról töltheti le. Bővebb tájékoztatásért lásd az Epson Device Admin dokumentációját vagy súgóját.

Az Epson Device Admin futtatása (csak Windows)

Válassza ki a **Minden program > EPSON > Epson Device Admin > Epson Device Admin** lehetőséget.

Megjegyzés:

Ha tűzfalra figyelmeztető üzenet jelenik meg, engedjen hozzáférést az Epson Device Admin számára.

EpsonNet Config

Az EpsonNet Config segítségével a rendszergazda meg tudja adni a lapolvasó hálózati beállításait, például IP-címet tud hozzárendelni és módosítani tudja a kapcsolódási módot. A Windows támogatja a csoportos beállítás funkciót. Bővebb tájékoztatásért lásd az EpsonNet Config dokumentációját vagy súgóját.



A(z) EpsonNet Config futtatása Windows alatt

Válassza ki az **Minden program > EpsonNet > EpsonNet Config SE > EpsonNet Config** lehetőséget.

Megjegyzés:

Ha tűzfalra figyelmeztető üzenet jelenik meg, engedjen hozzáférést az EpsonNet Config számára.

A(z) EpsonNet Config futtatása Mac OS alatt

Válassza ki az **Ugrás > Alkalmazások > Epson Software > EpsonNet > EpsonNet Config SE > EpsonNet Config** elemet.

EpsonNet SetupManager

Az EpsonNet SetupManager egy olyan szoftver, amellyel csomag hozható létre a lapolvasó egyszerű telepítéséhez, így például a lapolvasó illesztőprogramjának telepítéséhez és konfigurálásához, illetve a Document Capture Pro telepítéséhez. A szoftver segítségével a rendszergazda egyedi szoftvercsomagokat hozhat létre és megoszthatja azokat csoportok között.

Ha további információt szeretne, látogasson el az Epson regionális webhelyére.

IP-cím hozzárendelése EpsonNet Config alkalmazással

Az EpsonNet Config alkalmazás segítségével IP-címet rendelhet hozzá a lapolvasóhoz. Az EpsonNet Config lehetővé teszi, hogy IP-címet rendeljen hozzá egy olyan lapolvasóhoz, amely esetében ez nem történt meg az Ethernet-kábellel való csatlakoztatást követően.

IP-cím hozzárendelése csoportos beállítások alkalmazásával

Fájl létrehozása csoportos beállításokhoz

A MAC-cím és a modellnév kulcsként való használatával létrehozhat egy új SYLK-fájlt az IP-cím beállításához.

1. Nyisson meg egy táblázatkezelő vagy egy szövegszerkesztő alkalmazást (pl.: Microsoft Excel).
2. Adja meg az alábbiakat az első sorban a beállítási elemek megnevezéseiként: „Info_MACAddress”, „Info_ModelName”, és „TCPIP_IPAddress”.

Adja meg a beállítási elemeket a következő szöveges karakterláncokhoz. A kis- és nagybetűk, valamint a két- és egybájtos karakter megkülönböztetése érdekében a rendszer nem ismeri fel az elemet, ha annak egyetlen karaktere is eltérő.

Az alább leírtak szerint adja meg a beállítási elem nevét; amennyiben nem így tesz, az EpsonNet Config nem lesz képes felismerni a beállítási elemeket.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

Melléklet

3. Adja meg a MAC-címet, a modellnevet és az IP-címet az egyes hálózati illesztőkhöz.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress
0000XXXX0001	ALC-XXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. Írjon be egy nevet és mentse el SYLK-fájlként (*.slk).

Csoportos beállítások végrehajtása konfigurációs fájl segítségével

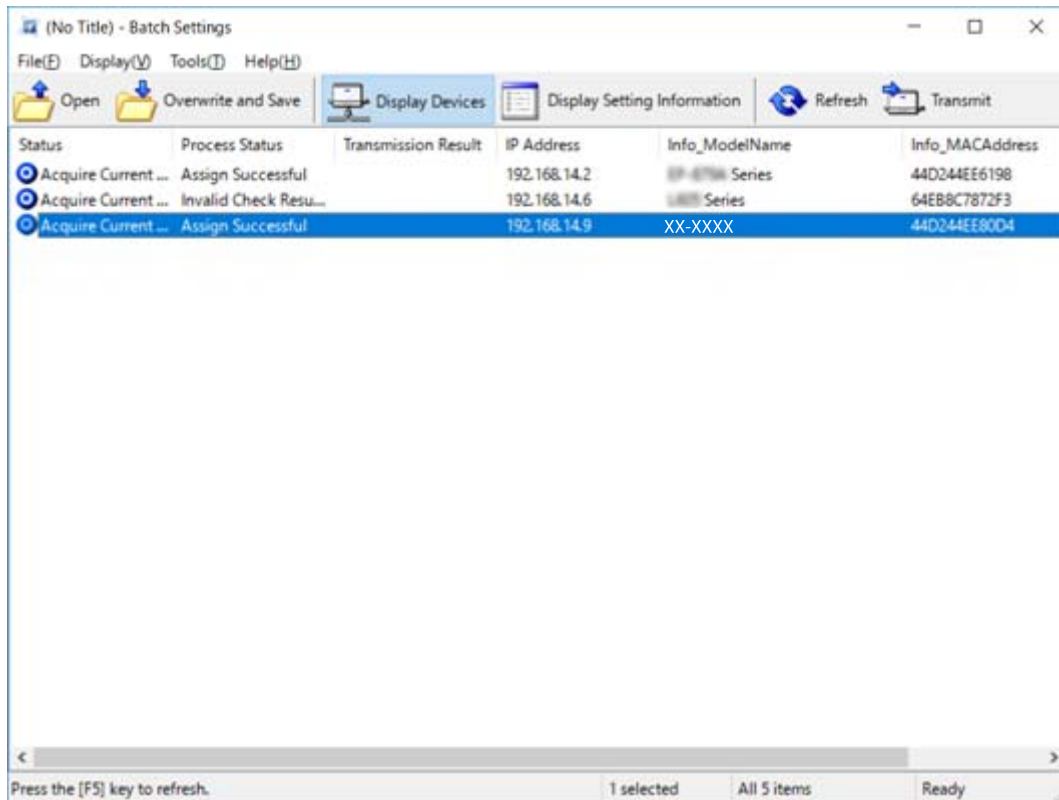
Társítson egyszerre IP-címeket a konfigurációs fájlban (SYLK-fájl). A társítás előtt létre kell hoznia a konfigurációs fájlt.

1. Csatlakoztasson minden eszközt a hálózathoz egy Ethernet-kábellel.
2. Kapcsolja be a lapolvasót.
3. Indítsa le a(z) EpsonNet Config alkalmazást.
Megjelenik a hálózaton lévő lapolvasók listája. A megjelenítés eltarthat egy ideig.
4. Kattintson a(z) **Tools > Batch Settings** elemre.
5. Kattintson a(z) **Open** elemre.
6. A fájlkiválasztási képernyőn válassza ki a beállításokat tartalmazó SYLK-fájlt (*.slk), majd kattintson a(z) **Open** elemre.

Melléklet

7. Az **Status** oszlop **Unassigned** lehetőségével, majd a **Process Status** menüpont **Assign Successful** elemre állításával válassza ki azokat az eszközöket, amelyekre szeretné érvényesíteni a csoportos beállításokat.

Több elem kiválasztásához nyomja meg a Ctrl vagy Shift billentyűt, és kattintson az elemekre, vagy húzza el az egeret.



8. Kattintson a(z) **Transmit** elemre.
9. Amikor megjelenik a jelszóbeírási képernyő, adja meg a jelszót, majd kattintson a(z) **OK** gombra. Továbbítsa a beállításokat.

Megjegyzés:



A rendszer az információkat mindaddig továbbítja a hálózati illesztőre, amíg a folyamatsáv be nem fejezi a folyamatot. Ne kapcsolja ki az eszközt vagy a vezeték nélküli adaptert, és ne küldjön adatokat az eszközre.






10. A **Transmitting Settings** képernyőn kattintson a(z) **OK** elemre.



Melléklet

11. Ellenőrizze a beállított eszköz állapotát.

A  vagy  ikont megjelenítő eszközök esetén ellenőrizze a beállításokat tartalmazó fájl tartalmát, illetve hogy az eszközt megfelelően újraindították-e.

Ikonn	Status	Process Status	Magyarázat
	Setup Complete	Setup Successful	A beállítás megfelelően végbement.
	Setup Complete	Rebooting	Ha a rendszer továbbította az információkat, a beállítások engedélyezéséhez az egyes eszközöket újra kell indítani. Az újraindítás után a rendszer ellenőrzi, hogy az eszközhöz végezhető-e csatlakoztatás.
	Setup Complete	Reboot Failed	A beállítások továbbítása után az eszköz nem igazolható. Ellenőrizze, hogy az eszköz be van-e kapcsolva, illetve hogy megfelelően újraindult-e.
	Setup Complete	Searching	A beállításokat tartalmazó fájlban jelölt eszköz keresése.*
	Setup Complete	Search Failed	A már beállított eszközök nem ellenőrizhetők. Ellenőrizze, hogy az eszköz be van-e kapcsolva, illetve hogy megfelelően újraindult-e.*

* Csak a beállítási információk kijelzésekor.

Kapcsolódó információ

- ➔ [„A\(z\) EpsonNet Config futtatása Windows alatt“ 56. oldal](#)
- ➔ [„A\(z\) EpsonNet Config futtatása Mac OS alatt“ 56. oldal](#)

IP-cím hozzárendelése az egyes eszközökhöz

IP-cím hozzárendelése a lapolvasóhoz a(z) EpsonNet Config alkalmazással.

1. Kapcsolja be a lapolvasót.
2. Csatlakoztassa a lapolvasót a hálózathoz egy Ethernet kábellel.
3. Indítsa le a(z) EpsonNet Config alkalmazást.
Megjelenik a hálózaton lévő lapolvasók listája. A megjelenítés eltarthat egy ideig.
4. Kattintson kétszer a hozzárendelni kívánt lapolvasóra.

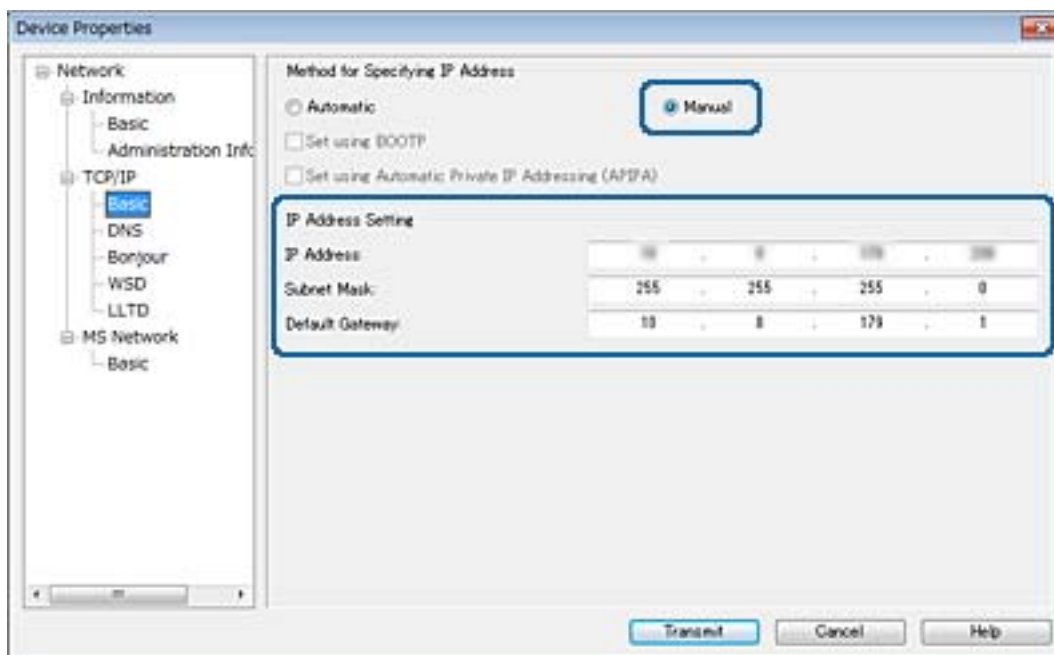
Megjegyzés:

Ha több, ugyanolyan típusú lapolvasót csatlakoztatott, akkor a MAC-cím segítségével azonosíthatja a lapolvasót.

5. Válassza a következőt: **Network > TCP/IP > Basic.**

Melléklet

6. Adja meg a címeket a következőkhöz: **IP Address**, **Subnet Mask** és **Default Gateway**.

**Megjegyzés:**

Ha a lapolvasót biztonságos hálózathoz csatlakoztatja, statikus címet adjon meg.

7. Kattintson a(z) **Transmit** elemre.

Megjelenik az információ továbbítására vonatkozó megerősítő képernyő.

8. Kattintson a(z) **OK** elemre.

Megjelenik a továbbítás befejezését jelző képernyő.

Megjegyzés:

A rendszer az információkat az eszközre továbbítja, majd a „A konfigurálás sikeresen befejeződött.” üzenet jelenik meg. Ne kapcsolja ki az eszközt, és ne küldjön adatokat a szolgáltatónak.

9. Kattintson a(z) **OK** elemre.

Kapcsolódó információ

- ➔ „A(z) EpsonNet Config futtatása Windows alatt“ 56. oldal
- ➔ „A(z) EpsonNet Config futtatása Mac OS alatt“ 56. oldal

Port használata a lapolvasóhoz

A lapolvasó az alábbi portot használja. Ezeket a portokat szükség szerint a hálózati rendszergazdának kell elérhetővé tennie.

Melléklet

Küldő (Ügyfél)	Alkalmazás	Cél (Kiszolgáló)	Protokoll	Portszám
Lapolvasó	E-mail küldés (értesítő e-mail)	SMTP-kiszolgáló	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP az SMTP-kapcsolat előtt (értesítő e-mail)	POP-kiszolgáló	POP3 (TCP)	110
	WSD vezérlése	Ügyfélszámítógép	WSD (TCP)	5357
	Számítógép keresése, amikor push beolvasást végeznek a Document Capture Pro programból	Ügyfélszámítógép	Hálózati push beolvasás felismerése	2968
Nyomatási adatok összegyűjtése, amikor push beolvasást végeznek a Document Capture Pro programból	Ügyfélszámítógép	Hálózati push beolvasás	2968	
Ügyfélszámítógép	A szkennert felismerése olyan alkalmazásokból, mint a(z) EpsonNet Config és a lapolvasó-illesztőprogram.	Lapolvasó	ENPC (UDP)	3289
	MIB-információk összegyűjtése és beállítása olyan alkalmazásokból, mint a(z) EpsonNet Config és a lapolvasó-illesztőprogram.	Lapolvasó	SNMP (UDP)	161
	WSD-szkennert keresése	Lapolvasó	WS-Discovery (UDP)	3702
	Beolvasási adatok továbbítása a Document Capture Pro programból	Lapolvasó	Hálózati beolvasás (TCP)	1865

Speciális biztonsági beállítások vállalatok számára

Ebben a fejezetben a speciális biztonsági funkciókat ismertetjük.

Biztonsági beállítások, és a veszélyek megelőzése

Ha egy eszköz egy hálózathoz csatlakozik, egy távoli helyről elérhető. Továbbá több személy megoszthatja az eszközt, ami hasznos lehet az üzemi hatékonyság és a kényelem növelése terén. Azonban ezzel együtt az olyan kockázatok, mint pl. az illegális hozzáférés, illegális felhasználás és az adatokkal való visszaélés nőnek. Ha olyan környezetben használja az eszközt, ahol internethozzáférés is elérhető, a kockázatok még ennél is nagyobbak.

E kockázat elkerülése érdekében az Epson eszközök számos biztonsági technológiával vannak felszerelve.

Állítsa be az eszközt a környezeti feltételeknek megfelelő szükséges módon, amelyet az ügyfél környezeti információit figyelembe véve építettek ki.

Név	A funkció típusa	Beállítandó	Megelőzendő
SSL/TLS kommunikáció	Egy számítógép és egy eszköz kommunikációs útvonala SSL/TLS kommunikáció segítségével titkosított. A kommunikáció tartalma egy böngészőn keresztül védett.	Állítson be CA hitelesítést a kiszolgálóhoz. A hitelesítést a CA (Hitelesítésszolgáltató) írta alá az eszközhöz.	Akadályozza meg, hogy a beállítási információk és a továbbított adatok tartalma a számítógépről a szkennelhez kerüljön. Az eszközről az Epson kiszolgálóra történő internetes fellépés szintén védhető firmware-frissítéssel stb.
IPsec/IP-szűrés	Beállítható, hogy a rendszer kiszűrje és kiválassza az egy bizonyos ügyféltől érkező vagy egy bizonyos típusú adatokat. Mivel az IPsec az adatokat IP-csomagokba csomagolja, védi (titkosítás és hitelesítés), biztonságosan kommunikálhat nem biztonságos beolvasási protokollal.	Hozzon létre alapvető házirendet és egyéni házirendet, hogy ezáltal beállítsa azt az ügyfelet vagy adattípust, amely hozzáférhet az eszközhöz.	Nyújtson védelmet a jogosulatlan hozzáférés, valamint az eszköz kommunikációs adataival való visszaélés, illetve azok illetéktelen megszerzése ellen.
SNMPv3	Kiegészítés további funkciókkal, például a hálózatban található, csatlakoztatott eszközök figyelése, az SNMP-protokoll felé vezérlés céljából továbbított adatok integritásának biztosítása, titkosítás, felhasználóhitelesítés stb.	Engedélyezze az SNMPv3 protokollt, majd állítsa be a hitelesítési és titkosítási módot.	Gondoskodjon a beállítások módosításáról a hálózaton keresztül, valamint az állapotfigyelés bizalmas jellegéről.

Speciális biztonsági beállítások vállalatok számára

Név	A funkció típusa	Beállítandó	Megelőzendő
IEEE802.1X	A funkció révén kizárólag Ethernet szolgáltatásra jogosult felhasználó csatlakozhat. A funkció révén az eszközt csakis engedéllyel rendelkező felhasználó használhatja.	Hitelesítési beállítás a RADIUS kiszolgálón (hitelesítési kiszolgáló).	Nyújtson védelmet a jogosulatlan hozzáférés és az eszköz illetéktelen használata ellen.
Igazolványkártya beolvasása	Az eszköz úgy is használható, ha a hozzá csatlakoztatott hitelesítési eszköz fölé odatart egy igazolványkártyát. Korlátozhatja az egyes felhasználók részére a naplók lekérdezését, az eszközök használatát, valamint az egyes felhasználók és csoportok számára elérhető funkciókat.	Csatlakoztasson egy hitelesítési eszközt az eszközhöz, majd állítsa be a hitelesítési rendszerben a felhasználók adatait.	Előzze meg az eszköz illetéktelen használatát és imitációját.

Kapcsolódó információ

- ➔ „SSL/TLS kommunikáció a lapolvasóval“ 63. oldal
- ➔ „Titkosított kommunikáció IPsec-/IP-szűrés funkcióval“ 71. oldal
- ➔ „Az SNMPv3 protokoll használata“ 83. oldal
- ➔ „A lapolvasó csatlakoztatása IEEE802.1X hálózathoz“ 85. oldal

A biztonsági funkciók beállításai

Az IPsec/IP szűrés, illetve az IEEE802.1X beállítások adatainak kommunikálása céljából ajánlott az SSL/TLS segítségével fellépni a Web Config rendszerre, hogy csökkentse az olyan biztonsági kockázatokat, mint a visszaélés, illetve az illetéktelen hozzáférés.

SSL/TLS kommunikáció a lapolvasóval

Amennyiben a lapolvasóhoz a kiszolgálói tanúsítványt SSL/TLS (Secure Sockets Layer/Transport Layer Security) kommunikációval állították be, a számítógépek közötti kommunikációs útvonal titkosítható. Ez a funkció akkor hasznos, ha szeretné megakadályozni a távoli és illetéktelen hozzáférést.

Tudnivalók a digitális tanúsítványról

- Hitelesítésszolgáltató által aláírt tanúsítvány

A hitelesítésszolgáltató által aláírt tanúsítványt közvetlenül a hitelesítésszolgáltatótól kell beszerezni. A hitelesítésszolgáltató által aláírt tanúsítvány használatával biztosítani lehet a biztonságos kommunikációt. A hitelesítésszolgáltató által aláírt tanúsítvány valamennyi biztonsági funkcióhoz használható.

Speciális biztonsági beállítások vállalatok számára

Hitelesítésszolgáltató tanúsítványa

A hitelesítésszolgáltató tanúsítványa azt jelzi, hogy egy harmadik fél igazolta a kiszolgáló azonosítóját. Ez a WOT biztonsági típus kulcsfontosságú eleme. A kiszolgáló hitelesítésére szolgáló hitelesítésszolgáltatói tanúsítványt az azt kibocsátó hitelesítésszolgáltatótól kell beszerezni.

Saját aláírású tanúsítvány

A saját aláírású tanúsítvány egy olyan tanúsítvány, amelyet a lapolvasó ad ki és ír alá. Ez a tanúsítvány nem megbízható és nem tudja megakadályozni az imitációt. Ha ezt a tanúsítványt használja SSL/TLS tanúsítvány esetében, előfordulhat, hogy a böngésző biztonsági figyelmeztetést jelenít meg. Ezt a tanúsítványt kizárólag SSL/TLS kommunikáció esetében használhatja.

Kapcsolódó információ

- ➔ „CA által aláírt tanúsítvány beszerzése és importálása“ 64. oldal
- ➔ „Hitelesítésszolgáltató által aláírt tanúsítvány törlése“ 68. oldal
- ➔ „Saját aláírású tanúsítvány frissítése“ 68. oldal

CA által aláírt tanúsítvány beszerzése és importálása

Hitelesítésszolgáltató által aláírt tanúsítvány beszerzése

A hitelesítésszolgáltató által aláírt tanúsítvány beszerzéséhez hozzon létre egy CSR-t (tanúsítvány-aláírási kérelmet), és alkalmazza azt a hitelesítésszolgáltatóra. A CSR-t a lapolvasó Web Config alkalmazása és egy számítógép segítségével hozhatja létre.

Kövesse a CSR létrehozásának és a hitelesítésszolgáltató által aláírt tanúsítvány megszerzésének lépéseit a Web Config segítségével. Ha a CSR létrehozása a Web Config segítségével történik, a tanúsítvány PEM/DER formátumú lesz.

1. A Web Config menüben válassza ki a **Network Security Settings** pontot. Ezután válassza ki az **SSL/TLS > Certificate** vagy **IPsec/IP Filtering > Client Certificate** vagy **IEEE802.1X > Client Certificate** lehetőséget.
2. Kattintson a **Generate CSR** elemére.
Megnyílik egy CSR-létrehozási oldal.

3. Írjon be egy értéket minden egyes elem számára.

Megjegyzés:

A rendelkezésre álló kulcshosszúságok és rövidítések hitelesítésszolgáltatónként változnak. Hozzon létre egy kérelmet az egyes hitelesítésszolgáltatók szabályai szerint.

4. Kattintson a(z) **OK** gombra.
Megjelenik egy befejezést jelző üzenet.
5. Kattintson a **Network Security Settings** gombra. Ezután válassza ki az **SSL/TLS > Certificate** vagy **IPsec/IP Filtering > Client Certificate** vagy az **IEEE802.1X > Client Certificate** lehetőséget.

Speciális biztonsági beállítások vállalatok számára

6. A CSR számítógépre való letöltéséhez kattintson a **CSR** egyik letöltési gombjára az adott hitelesítésszolgáltató által meghatározott formátum szerint.



Fontos:

Ne hozzon létre ismét CSR-t. Ellenkező esetben előfordulhat, hogy a kiadott CA-signed Certificate nem importálható.

7. Küldje el a CSR-t egy hitelesítésszolgáltatónak, és szerezzen be egy CA-signed Certificatet.
A küldési mód és forma tekintetében az adott hitelesítésszolgáltató szabályai szerint járjon el.
8. Mentse el a kiadott CA-signed Certificatet a lapolvasóhoz csatlakoztatott számítógépre.
A CA-signed Certificate beszerzése akkor fejeződik be, miután elmentette a tanúsítványt a célállomásra.

Kapcsolódó információ

- ➔ „A Web Config elérése“ 23. oldal
- ➔ „CSR-elemek beállítása“ 65. oldal
- ➔ „Hitelesítésszolgáltató által aláírt tanúsítvány importálása“ 66. oldal

CSR-elemek beállítása

Elemek	Beállítások és magyarázat
Key Length	Válassza ki a CSR-kulcs hosszúságát.

Speciális biztonsági beállítások vállalatok számára

Elemek	Beállítások és magyarázat
Common Name	1 és 128 közötti számú karaktert adhat meg. Ha ez egy IP-cím, akkor annak statikus IP-címnek kell lennie. Példa: A(z) Web Config elérési URL-címe: https://10.152.12.225 Általános név: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	0–64 ASCII-karaktert (0x20–0x7E) írhat be. A megkülönböztető neveket vesszőkkel választhatja el.
Country	Írja be az ISO-3166 által meghatározott kétszámjegyű országkódot.

Kapcsolódó információ

➔ „Hitelesítésszolgáltató által aláírt tanúsítvány beszerzése“ 64. oldal

Hitelesítésszolgáltató által aláírt tanúsítvány importálása

**Fontos:**

- Ellenőrizze hogy a lapolvasó dátuma és ideje megfelelően van-e beállítva.
- Ha a tanúsítványt a Web Config alkalmazásban létrehozott CSR segítségével szerzi be, egyszerre csak egy tanúsítványt importálhat.

1. Érje el a Web Config menüt, majd válassza ki a **Network Security Settings** pontot. Ezután válassza ki az **SSL/TLS > Certificate** vagy **IPsec/IP Filtering > Client Certificate** vagy az **IEEE802.1X > Client Certificate** lehetőséget.

2. Kattintson a(z) **Import** gombra.

Megnyílik egy tanúsítvány-importálási oldal.

3. Írjon be egy értéket minden egyes elem számára.

A CSR létrehozási helyétől és a tanúsítvány fájlformátumától függően a kötelező beállítások változhatnak. Írja be a kötelezően kitöltendő mezők értékeit az alábbiak szerint.

- A Web Config alkalmazástól beszerzett PEM/DER formátumú tanúsítvány
 - Private Key:** Ne állítsa be, mert a lapolvasó tartalmaz egy privát kulcsot.
 - Password:** Ne állítsa be.
 - CA Certificate 1/CA Certificate 2:** Választható
- A számítógéptől beszerzett PEM/DER formátumú tanúsítvány
 - Private Key:** Be kell állítani.
 - Password:** Ne állítsa be.
 - CA Certificate 1/CA Certificate 2:** Választható

Speciális biztonsági beállítások vállalatok számára

- A számítógéptől beszerzett PKCS#12 formátumú tanúsítvány
 - Private Key:** Ne állítsa be.
 - Password:** Választható
 - CA Certificate 1/CA Certificate 2:** Ne állítsa be.

4. Kattintson a(z) **OK** gombra.

Megjelenik egy befejezést jelző üzenet.

Megjegyzés:

A tanúsítvány adatainak ellenőrzéséhez kattintson a **Confirm** gombra.

Kapcsolódó információ

- ➔ „A Web Config elérése“ 23. oldal
- ➔ „CA által aláírt tanúsítvány: beállítások importálása“ 67. oldal

CA által aláírt tanúsítvány: beállítások importálása

Elemek	Beállítások és magyarázat
Server Certificate vagy Client Certificate	Válassza ki a tanúsítvány formátumát.
Private Key	Ha PEM/DER formátumú tanúsítványt szerez be egy számítógéppel létrehozott CSR segítségével, adja meg azt a privát kulcsot, amely megfelel a tanúsítványnak.
Password	Írjon be egy jelszót a privát kulcs titkosításához.

Speciális biztonsági beállítások vállalatok számára

Elemek	Beállítások és magyarázat
CA Certificate 1	Ha a tanúsítvány formátuma Certificate (PEM/DER) , importálja egy olyan tanúsító hatóság tanúsítványát, amely szervertanúsítványt ad ki. Szükség esetén adjon meg egy fájlt.
CA Certificate 2	Ha a tanúsítvány formátuma Certificate (PEM/DER) , importálja egy olyan tanúsító hatóság tanúsítványát, amely CA Certificate 1 tanúsítványt ad ki. Szükség esetén adjon meg egy fájlt.

Kapcsolódó információ

➔ „Hitelesítésszolgáltató által aláírt tanúsítvány importálása“ 66. oldal

Hitelesítésszolgáltató által aláírt tanúsítvány törlése

Lehetőség van egy importált tanúsítvány törlésére, ha a tanúsítvány lejárt, vagy ha már nincs szükség a titkosított kapcsolatra.

**Fontos:**

Ha a tanúsítványt a Web Config alkalmazásban létrehozott CSR segítségével szerzi be, nem importálhat egy már törölt tanúsítványt. Ebben az esetben hozzon létre egy CSR-t és szerezzen be újból egy tanúsítványt.

1. Lépjen be a Web Config segédprogramba, és válassza ki a(z) **Network Security Settings** menüpontot. Ezután válassza ki az **SSL/TLS > Certificate** vagy **IPsec/IP Filtering > Client Certificate** vagy **IEEE802.1X > Client Certificate** lehetőséget.
2. Kattintson a(z) **Delete** elemre.
3. A megjelenő üzenetben hagyja jóvá a tanúsítvány törlését.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

Saját aláírású tanúsítvány frissítése

Ha a lapolvasó támogatja a HTTPS-kiszolgáló funkciót, lehetőség van a saját aláírású tanúsítványok frissítésére. Ha a Web Config elérése saját aláírású tanúsítvánnyal történik, figyelmeztető üzenet jelenik meg.

A saját aláírású tanúsítványt ideiglenesen használja, amíg be nem szerez egy hitelesítésszolgáltató által aláírt tanúsítványt.

1. Jelenítse meg a Web Config segédprogramot, és válassza ki a **Network Security Settings > SSL/TLS > Certificate** pontot.
2. Kattintson a(z) **Update** elemre.
3. Töltse ki a **Common Name** mezőt.

Írjon be egy IP-címet vagy egy azonosítót — például FQDN-nevet — a lapolvasó számára. 1 és 128 közötti számú karaktert adhat meg.

Speciális biztonsági beállítások vállalatok számára

Megjegyzés:

A megkülönböztető neveket (CN) vesszőkkel választhatja el.

- Adja meg a tanúsítvány érvényességi időtartamát.

- Kattintson a(z) **Next** elemre.

Megjelenik egy megerősítő képernyő.

- Kattintson a(z) **OK** elemre.

A lapolvasó frissítése megtörténik.

Megjegyzés:

A tanúsítvány adatainak ellenőrzéséhez kattintson a(z) **Confirm** gombra.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

A CA Certificate konfigurálása

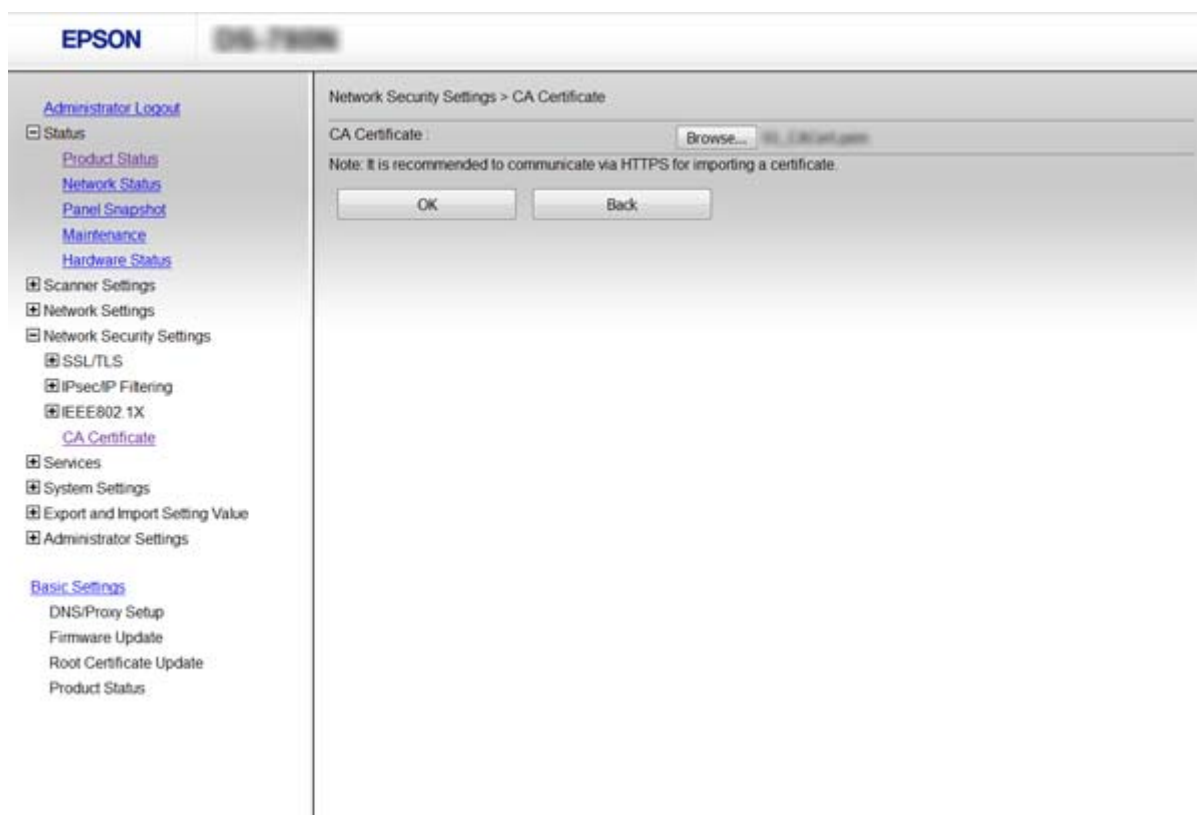
A CA Certificate igény szerint importálható, megjeleníthető és törölhető.

CA Certificate importálása

- Jelenítse meg a Web Config segédprogramot, és válassza ki a **Network Security Settings > CA Certificate** pontot.

Speciális biztonsági beállítások vállalatok számára

2. Kattintson a(z) **Import** gombra.
3. Adja meg, hogy melyik CA Certificate legyen importálva.



4. Kattintson a(z) **OK** gombra.

Miután az importálás befejeződött, ismét a **CA Certificate** képernyő jelenik meg, és az importált CA Certificate látható.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

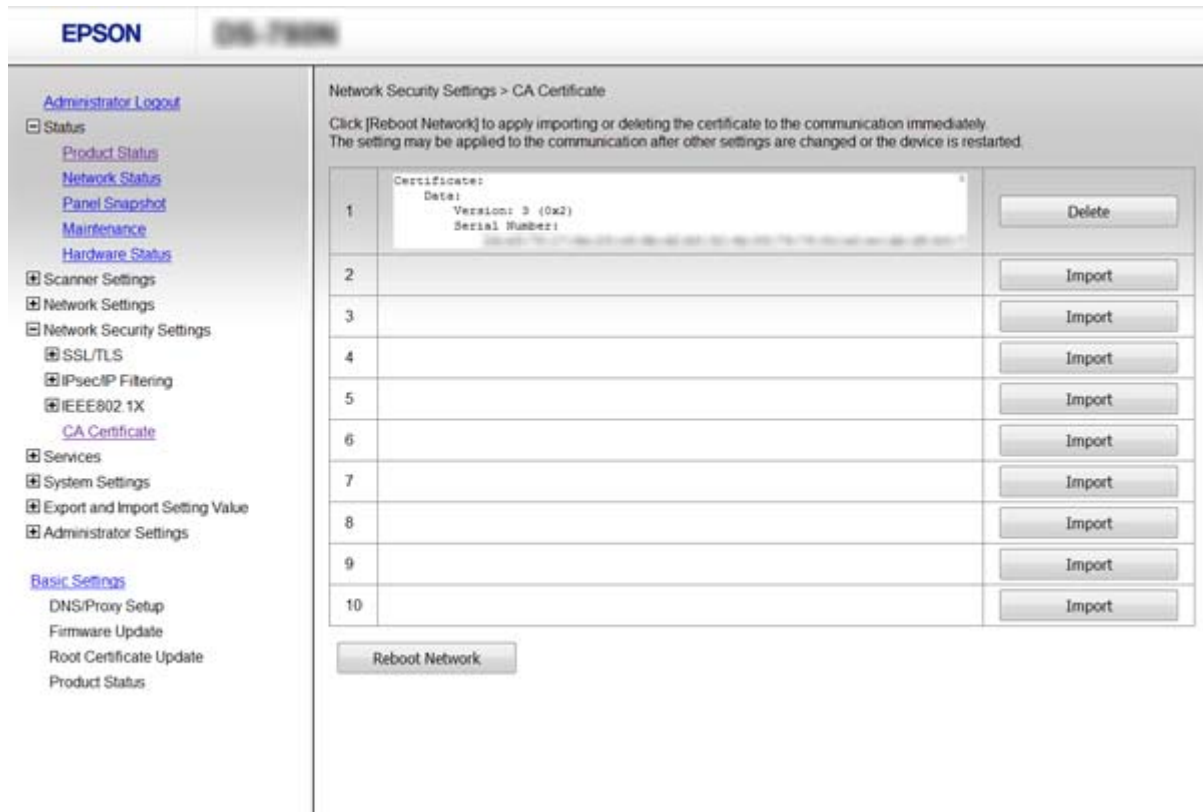
CA Certificate törlése

Az importált CA Certificate igény szerint törölhető.

1. Jelenítse meg a Web Config segédprogramot, és válassza ki a **Network Security Settings > CA Certificate** pontot.

Speciális biztonsági beállítások vállalatok számára

- Kattintson a **Delete** gombra a törölni kívánt CA Certificate mellett.



- A megjelenő üzenetben hagyja jóvá a tanúsítvány törlését.

Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

Titkosított kommunikáció IPsec-/IP-szűrés funkcióval

Tudnivalók az IPsec/IP Filtering alkalmazásról

Ha a lapolvasó támogatja az IPsec/IP-szűrést, beállíthatja a forgalom IP-cím, szolgáltatások és port alapján történő szűrését. A szűrés kombinálásával beállíthatja, hogy a lapolvasó elfogadjon vagy blokkoljon-e meghatározott ügyfeleket és adatokat. Emellett az IPsec alkalmazásával a biztonsági szintet is javíthatja.

A forgalom szűréséhez állítsa be az alapértelmezett házirendet. Az alapértelmezett házirend a lapolvasóhoz kapcsolódó valamennyi felhasználóra vagy csoportra vonatkozik. Ha részletesebb kontrollt szeretne a felhasználók és a felhasználói csoportok fölött, állítson be csoportos házirendeket. A csoportos házirend egy adott felhasználóra vagy felhasználói csoportra érvényes egy vagy több szabály. A lapolvasó vezérli azokat az IP-csomagokat, amelyek megfelelnek a beállított házirendeknek. Az IP-csomagok hitelesítési sorrendje: 1–10. csoportos házirend és végül alapértelmezett házirend.

Megjegyzés:

A Windows Vista vagy későbbi, illetve a Windows Server 2008 vagy későbbi verziót futtató számítógépek támogatják az IPsec funkciót.

A(z) Default Policy beállítása

1. Jelenítse meg a Web Config segédprogramot, és válassza ki a **Network Security Settings > IPsec/IP Filtering > Basic** pontot.
2. Írjon be egy értéket minden egyes elem számára.
3. Kattintson a(z) **Next** gombra.
Megjelenik egy megerősítő képernyő.
4. Kattintson a(z) **OK** gombra.
A lapolvasó frissítése megtörténik.

Kapcsolódó információ

- ➔ „A Web Config elérése“ 23. oldal
- ➔ „Default Policy beállítások“ 72. oldal

Default Policy beállítások

EPSON

Administrator Logout

- Status
 - Product Status
 - Network Status
 - Panel Snapshot
 - Maintenance
 - Hardware Status
- Scanner Settings
- Network Settings
- Network Security Settings
 - SSL/TLS
 - IPsec/IP Filtering
 - Basic
 - Client Certificate
 - IEEE802.1X
 - CA Certificate
- Services
- System Settings
- Export and Import Setting Value
- Administrator Settings
- Basic Settings
 - DNS/Proxy Setup
 - Firmware Update
 - Root Certificate Update
 - Product Status

Network Security Settings > IPsec/IP Filtering > Basic

Each policy is applied with following priorities:
Group Policy 1 > Group Policy 2 > ... > Group Policy 10 > Default Policy

Default Policy 1 2 3 4 5 6 7 8 9 10

IPsec/IP Filtering: Enable Disable

Default Policy

Access Control: IPsec

IKE Version: IKEv1 IKEv2

Authentication Method: Pre-Shared Key

Pre-Shared Key: _____

Confirm Pre-Shared Key: _____

Encapsulation: Transport Mode

Remote Gateway(Tunnel Mode): _____

Security Protocol: ESP

Algorithm Settings

IKE

Encryption: Any

Authentication: Any

Key Exchange: Any

ESP

Encryption: Any

Authentication: Any

Elemek	Beállítások és magyarázat
IPsec/IP Filtering	Engedélyezheti vagy kikapcsolhatja az IPsec-/IP-szűrés funkciót.

Speciális biztonsági beállítások vállalatok számára

Elemek	Beállítások és magyarázat	
Access Control	Állítson be egy vezérlési módszert az IP-csomagok forgalma számára.	
	Permit Access	Akkor jelölje ki, ha engedélyezni szeretné a beállított IP-csomagok áthaladását.
	Refuse Access	Akkor jelölje ki, ha el szeretné utasítani a beállított IP-csomagok áthaladását.
	IPsec	Akkor jelölje ki, ha engedélyezni szeretné a beállított IPsec-csomagok áthaladását.
IKE Version	Az internetes kulcscsere verziójánál válassza az IKEv1 vagy az IKEv2 protokollt. Ahhoz az eszközhöz megfelelőt válassza, amihez a lapolvasó kapcsolódik.	
IKEv1	Az alábbi elemek jelennek meg, ha a(z) IKEv1 protokollt választja a(z) IKE Version menüben.	
	Authentication Method	A(z) Certificate kijelöléséhez előre be kell szereznie és importálnia kell egy hitelesítésszolgáltató által aláírt tanúsítványt.
	Pre-Shared Key	Ha a(z) Pre-Shared Key lehetőséget választja ki a(z) Authentication Method beállításnál, írjon be egy legalább 1, legfeljebb 127 karakterből álló előre megosztott kulcsot.
	Confirm Pre-Shared Key	A megerősítéshez adja meg a beállított kulcsot.
IKEv2	Az alábbi elemek jelennek meg, ha a(z) IKEv2 protokollt választja a(z) IKE Version menüben.	
Local	Authentication Method	A(z) Certificate kijelöléséhez előre be kell szereznie és importálnia kell egy hitelesítésszolgáltató által aláírt tanúsítványt.
	ID Type	Válassza ki a lapolvasóhoz tartozó azonosító típusát.
	ID	Írja be a lapolvasó típusának megfelelő nyomtatóazonosítót. Az első karakter nem lehet „@”, „#” vagy „=”. Distinguished Name: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert. A névnek tartalmaznia kell az „=” karaktert. IP Address: IPv4 vagy IPv6 formátumban írja be. FQDN: 1 és 255 közötti számú karaktert írjon be, ami az A–Z, a–z, 0–9, „-” karaktereket, illetve az időszakot (.) tartalmazhatja. Email Address: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert. A névnek tartalmaznia kell a „@” karaktert. Key ID: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert.
	Pre-Shared Key	Ha a(z) Pre-Shared Key lehetőséget választja ki a(z) Authentication Method beállításnál, írjon be egy legalább 1, legfeljebb 127 karakterből álló előre megosztott kulcsot.
	Confirm Pre-Shared Key	A megerősítéshez adja meg a beállított kulcsot.

Speciális biztonsági beállítások vállalatok számára

Elemek	Beállítások és magyarázat	
Remote	Authentication Method	A(z) Certificate kijelöléséhez előre be kell szereznie és importálnia kell egy hitelesítésszolgáltató által aláírt tanúsítványt.
	ID Type	Válassza ki a hitelesíteni kívánt eszköz azonosítójának a típusát.
	ID	Írja be a lapolvasó típusának megfelelő nyomtatóazonosítót. Az első karakter nem lehet „@”, „#” vagy „=”. Distinguished Name: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert. A névnek tartalmaznia kell az „=” karaktert. IP Address: IPv4 vagy IPv6 formátumban írja be. FQDN: 1 és 255 közötti számú karaktert írjon be, ami az A–Z, a–z, 0–9, „-” karaktereket, illetve az időszakot (.) tartalmazhatja. Email Address: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert. A névnek tartalmaznia kell a „@” karaktert. Key ID: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert.
	Pre-Shared Key	Ha a(z) Pre-Shared Key lehetőséget választja ki a(z) Authentication Method beállításnál, írjon be egy legalább 1, legfeljebb 127 karakterből álló előre megosztott kulcsot.
	Confirm Pre-Shared Key	A megerősítéshez adja meg a beállított kulcsot.
Encapsulation	Ha a(z) IPsec lehetőséget választja ki a(z) Access Control beállításnál, be kell állítania egy beágyazási módot.	
	Transport Mode	Válassza ezt, ha csak ugyanazon a LAN-on használja a lapolvasót. A 4. rétegű vagy újabb IP-csomagok titkosítva vannak.
	Tunnel Mode	Ha internetképes hálózaton, például IPsec-VPN-en használja a lapolvasót, válassza ki ezt a lehetőséget. Az IP-csomagok fejléce és adatai titkosítódnak.
Remote Gateway(Tunnel Mode)	Ha a Tunnel Mode lehetőséget választja ki a Encapsulation beállításnál, írjon be egy legalább 1, legfeljebb 39 karakterből álló átjárócímet.	
Security Protocol	IPsec a(z) Access Control funkcióhoz, válasszon egy beállítást.	
	ESP	Válassza ezt, ha biztosítani szeretné a hitelesítés és az adatok sértetlenségét, és titkosítani szeretné az adatokat.
	AH	Válassza ezt, ha biztosítani szeretné a hitelesítés és az adatok sértetlenségét. Az IPsec még akkor is használható, ha az adatok titkosítása tilos.
Algorithm Settings		

Speciális biztonsági beállítások vállalatok számára

Elemek	Beállítások és magyarázat	
IKE	Encryption	Válassza ki az internetes kulcscsere titkosítási algoritmusát. Az elemek az internetes kulcscsere verziójától függően változnak.
	Authentication	Válassza ki az internetes kulcscsere hitelesítési algoritmusát.
	Key Exchange	Válassza ki az internetes kulcscsere kulcscsere-algoritmusát. Az elemek az internetes kulcscsere verziójától függően változnak.
ESP	Encryption	Válassza ki az ESP titkosítási algoritmusát. Ez akkor használható, ha a(z) ESP van kiválasztva a(z) Security Protocol beállításnál.
	Authentication	Válassza ki az ESP hitelesítési algoritmusát. Ez akkor használható, ha a(z) ESP van kiválasztva a(z) Security Protocol beállításnál.
AH	Authentication	Válassza ki az AH titkosítási algoritmusát. Ez akkor használható, ha a(z) AH van kiválasztva a(z) Security Protocol beállításnál.

Kapcsolódó információ

➔ „A(z) Default Policy beállítása“ 72. oldal

A(z) Group Policy beállítása

1. Jelenítse meg a Web Config segédprogramot, és válassza ki a **Network Security Settings > IPsec/IP Filtering > Basic** pontot.
2. Kattintson a konfigurálni kívánt számozott lapok valamelyikére.
3. Írjon be egy értéket minden egyes elem számára.
4. Kattintson a(z) **Next** gombra.
Megjelenik egy megerősítő képernyő.
5. Kattintson a(z) **OK** gombra.
A lapolvasó frissítése megtörténik.

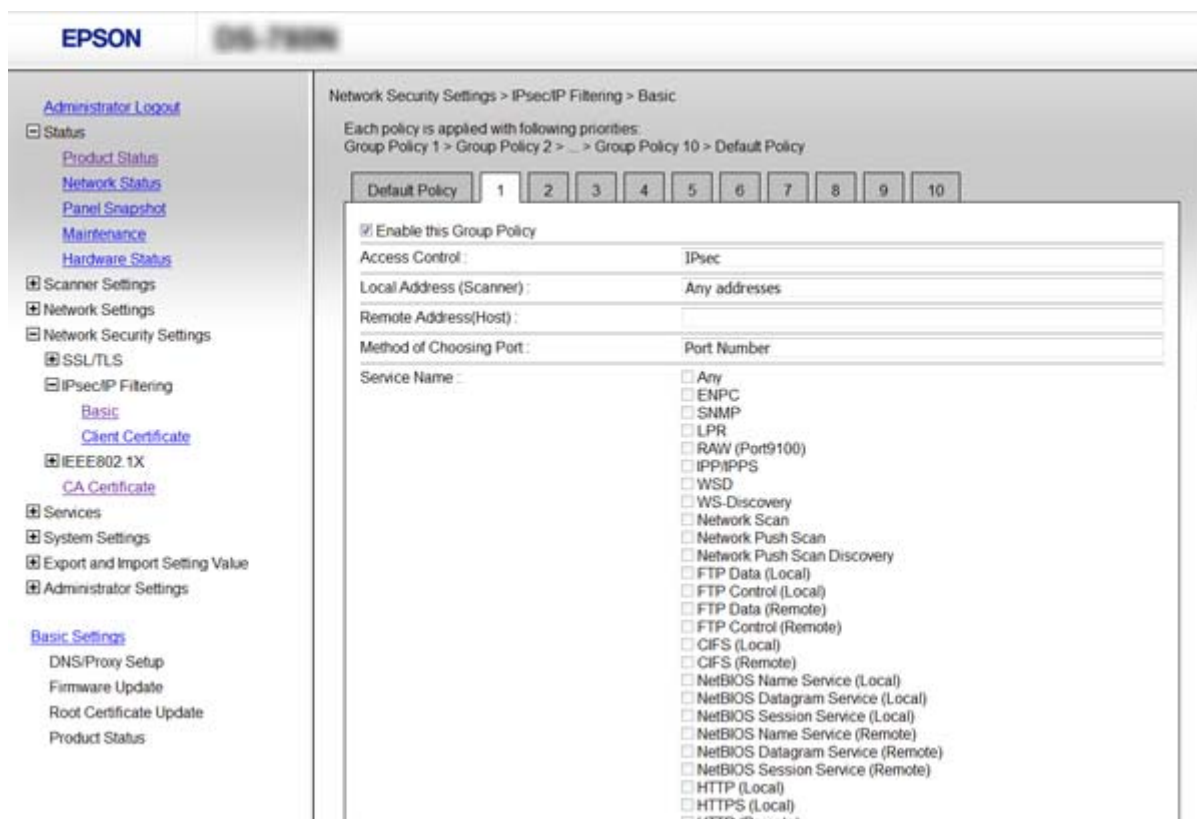
Kapcsolódó információ

➔ „A Web Config elérése“ 23. oldal

➔ „Group Policy beállítások“ 76. oldal

Speciális biztonsági beállítások vállalatok számára

Group Policy beállítások



Elemek	Beállítások és magyarázat	
Enable this Group Policy	Lehetőség van a csoportos házirendek engedélyezésére és letiltására.	
Access Control	Állítson be egy vezérlési módszert az IP-csomagok forgalma számára.	
	Permit Access	Akkor jelölje ki, ha engedélyezni szeretné a beállított IP-csomagok áthaladását.
	Refuse Access	Akkor jelölje ki, ha el szeretné utasítani a beállított IP-csomagok áthaladását.
IPsec	Akkor jelölje ki, ha engedélyezni szeretné a beállított IPsec-csomagok áthaladását.	
Local Address (Scanner)	Válassza ki a hálózati környezetének megfelelő IPv4- vagy IPv6-címet. Ha automatikusan megtörténik az IP-cím hozzárendelése, kiválaszthatja a(z) Use auto-obtained IPv4 address lehetőséget.	
Remote Address(Host)	Írja be a készülék IP-címét a hozzáférés vezérlése érdekében. Az IP-cím maximum 43 karakterből állhat. Ha nem ír be IP-címet, az összes cím vezérelve lesz. Megjegyzés: <i>Ha az IP-cím hozzárendelése automatikusan történik (pl. a DHCP által), előfordulhat, hogy a kapcsolat nem lesz elérhető. Állítson be egy statikus IP-címet.</i>	
Method of Choosing Port	Válasszon ki egy módszert a portok megadására.	
Service Name	Ha a(z) Service Name lehetőséget választja a(z) Method of Choosing Port beállításnál, akkor válasszon egy lehetőséget.	

Speciális biztonsági beállítások vállalatok számára

Elemek	Beállítások és magyarázat	
Transport Protocol	Ha a(z) Port Number lehetőséget választja ki a(z) Method of Choosing Port beállításnál, be kell állítania egy beágyazási módot.	
	Any Protocol	Válassza ezt az összes protokolltípus vezérléséhez.
	TCP	Válassza ezt az adatok vezérléséhez unicast esetében.
	UDP	Válassza ezt az adatok vezérléséhez broadcast és multicast esetében.
	ICMPv4	Válassza ezt a ping parancs vezérléséhez.
Local Port	Ha a(z) Port Number lehetőséget választja ki a(z) Method of Choosing Port beállításnál, és kiválasztja a(z) TCP vagy UDP elemet a(z) Transport Protocol beállításnál, adja meg a portszámokat vesszővel elválasztva a beérkező csomagok vezérléséhez. Legfeljebb 10 portszámot írhat be. Példa: 20,80,119,5220 Ha nem ír be portszámot, az összes port vezérelve lesz.	
Remote Port	Ha a(z) Port Number lehetőséget választja ki a(z) Method of Choosing Port beállításnál, és kiválasztja a(z) TCP vagy UDP elemet a(z) Transport Protocol beállításnál, adja meg a portszámokat vesszővel elválasztva az elküldött csomagok vezérléséhez. Legfeljebb 10 portszámot írhat be. Példa: 25,80,143,5220 Ha nem ír be portszámot, az összes port vezérelve lesz.	
IKE Version	Az internetes kulcscsere verziójánál válassza az IKEv1 vagy az IKEv2 protokollt. Ahhoz az eszközhöz megfelelőt válassza, amihez a lapolvasó kapcsolódik.	
IKEv1	Az alábbi elemek jelennek meg, ha a(z) IKEv1 protokollt választja a(z) IKE Version menüben.	
	Authentication Method	Ha a(z) IPsec lehetőséget választja a(z) Access Control beállításnál, akkor válasszon egy lehetőséget. Az alkalmazott tanúsítvány azonos az alapértelmezett házirendével.
	Pre-Shared Key	Ha a(z) Pre-Shared Key lehetőséget választja ki a(z) Authentication Method beállításnál, írjon be egy legalább 1, legfeljebb 127 karakterből álló előre megosztott kulcsot.
	Confirm Pre-Shared Key	A megerősítéshez adja meg a beállított kulcsot.
IKEv2	Az alábbi elemek jelennek meg, ha a(z) IKEv2 protokollt választja a(z) IKE Version menüben.	

Speciális biztonsági beállítások vállalatok számára

Elemek	Beállítások és magyarázat	
Local	Authentication Method	Ha a(z) IPsec lehetőséget választja a(z) Access Control beállításnál, akkor válasszon egy lehetőséget. Az alkalmazott tanúsítvány azonos az alapértelmezett házirendével.
	ID Type	Válassza ki a lapolvasóhoz tartozó azonosító típusát.
	ID	Írja be a lapolvasó típusának megfelelő nyomtatóazonosítót. Az első karakter nem lehet „@”, „#” vagy „=”. Distinguished Name: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert. A névnek tartalmaznia kell az „=” karaktert. IP Address: IPv4 vagy IPv6 formátumban írja be. FQDN: 1 és 255 közötti számú karaktert írjon be, ami az A–Z, a–z, 0–9, „-” karaktereket, illetve az időszakot (.) tartalmazhatja. Email Address: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert. A névnek tartalmaznia kell a „@” karaktert. Key ID: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert.
	Pre-Shared Key	Ha a(z) Pre-Shared Key lehetőséget választja ki a(z) Authentication Method beállításnál, írjon be egy legalább 1, legfeljebb 127 karakterből álló előre megosztott kulcsot.
	Confirm Pre-Shared Key	A megerősítéshez adja meg a beállított kulcsot.
Remote	Authentication Method	Ha a(z) IPsec lehetőséget választja a(z) Access Control beállításnál, akkor válasszon egy lehetőséget. Az alkalmazott tanúsítvány azonos az alapértelmezett házirendével.
	ID Type	Válassza ki a hitelesíteni kívánt eszköz azonosítójának a típusát.
	ID	Írja be a lapolvasó típusának megfelelő nyomtatóazonosítót. Az első karakter nem lehet „@”, „#” vagy „=”. Distinguished Name: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert. A névnek tartalmaznia kell az „=” karaktert. IP Address: IPv4 vagy IPv6 formátumban írja be. FQDN: 1 és 255 közötti számú karaktert írjon be, ami az A–Z, a–z, 0–9, „-” karaktereket, illetve az időszakot (.) tartalmazhatja. Email Address: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert. A névnek tartalmaznia kell a „@” karaktert. Key ID: Adjon meg legalább 1, de legfeljebb 128 darab egybájtos ASCII (0x20–0x7E) karaktert.
	Pre-Shared Key	Ha a(z) Pre-Shared Key lehetőséget választja ki a(z) Authentication Method beállításnál, írjon be egy legalább 1, legfeljebb 127 karakterből álló előre megosztott kulcsot.
	Confirm Pre-Shared Key	A megerősítéshez adja meg a beállított kulcsot.

Speciális biztonsági beállítások vállalatok számára

Elemek	Beállítások és magyarázat	
Encapsulation	Ha a(z) IPsec lehetőséget választja ki a(z) Access Control beállításnál, be kell állítania egy beágyazási módot.	
	Transport Mode	Válassza ezt, ha csak ugyanazon a LAN-on használja a lapolvasót. A 4. rétegű vagy újabb IP-csomagok titkosítva vannak.
	Tunnel Mode	Ha internetképes hálózaton, például IPsec-VPN-en használja a lapolvasót, válassza ki ezt a lehetőséget. Az IP-csomagok fejléce és adatai titkosítódnak.
Remote Gateway(Tunnel Mode)	Ha a Tunnel Mode lehetőséget választja ki a Encapsulation beállításnál, írjon be egy legalább 1, legfeljebb 39 karakterből álló átjárócímet.	
Security Protocol	Ha a(z) IPsec lehetőséget választja a(z) Access Control beállításnál, akkor válasszon egy lehetőséget.	
	ESP	Válassza ezt, ha biztosítani szeretné a hitelesítés és az adatok sértetlenségét, és titkosítani szeretné az adatokat.
	AH	Válassza ezt, ha biztosítani szeretné a hitelesítés és az adatok sértetlenségét. Az IPsec még akkor is használható, ha az adatok titkosítása tilos.
Algorithm Settings		
IKE	Encryption	Válassza ki az internetes kulcscsere titkosítási algoritmusát. Az elemek az internetes kulcscsere verziójától függően változnak.
	Authentication	Válassza ki az internetes kulcscsere hitelesítési algoritmusát.
	Key Exchange	Válassza ki az internetes kulcscsere kulcscsere-algoritmusát. Az elemek az internetes kulcscsere verziójától függően változnak.
ESP	Encryption	Válassza ki az ESP titkosítási algoritmusát. Ez akkor használható, ha a(z) ESP van kiválasztva a(z) Security Protocol beállításnál.
	Authentication	Válassza ki az ESP hitelesítési algoritmusát. Ez akkor használható, ha a(z) ESP van kiválasztva a(z) Security Protocol beállításnál.
AH	Authentication	Válassza ki az AH hitelesítési algoritmusát. Ez akkor használható, ha a(z) AH van kiválasztva a(z) Security Protocol beállításnál.

Kapcsolódó információ

- ➔ „A(z) Group Policy beállítása“ 75. oldal
- ➔ „A Local Address (Scanner) és a Remote Address(Host) kombinációja a Group Policy beállításnál“ 80. oldal
- ➔ „Szolgáltatásnevek referenciái a csoportházirendben“ 80. oldal

Speciális biztonsági beállítások vállalatok számára

A Local Address (Scanner) és a Remote Address(Host) kombinációja a Group Policy beállításnál

		A Local Address (Scanner) beállítása		
		IPv4	IPv6* ²	Any addresses* ³
A Remote Address(Host) beállítása	IPv4* ¹	✓	–	✓
	IPv6* ¹ , * ²	–	✓	✓
	Üres	✓	✓	✓

*1 Ha az **IPsec** érték van kiválasztva az **Access Control** beállításnál, akkor nem adhatja meg az előtag hosszát.

*2 Ha az **IPsec** érték van kiválasztva az **Access Control** beállításnál, kiválaszthat egy link-local címet (fe80::), de a csoportos házirend le lesz tiltva.

*3 Kivéve az IPv6 link-local címeinél.

Szolgáltatásnevek referenciái a csoportházirendben

Megjegyzés:

Az el nem érhető szolgáltatások megjelennek, de nem választhatók ki.

Szolgáltatás neve	Protokolltípus	Helyi portszám	Távoli portszám	Vezérelt funkciók
Any	–	–	–	Minden szolgáltatás
ENPC	UDP	3289	Bármely port	Lapolvasó keresése olyan alkalmazásokból, mint az EpsonNet Config vagy a szkennel illesztőprogram
SNMP	UDP	161	Bármely port	MIB lekérése vagy konfigurálása olyan alkalmazásokból, mint a EpsonNet Config és az Epson lapolvasó- illesztőprogram
WSD	TCP	Bármely port	5357	WSD vezérlése
WS-Discovery	UDP	3702	Bármely port	Lapolvasó keresése WSD-ből
Network Scan	TCP	1865	Bármely port	Lapolvasási adatok továbbítása a(z) Document Capture Pro alkalmazásból
Network Push Scan Discovery	UDP	2968	Bármely port	Számítógép keresése a lapolvasóról.
Network Push Scan	TCP	Bármely port	2968	Push szkennelés munkainformációinak lekérése a(z) Document Capture Pro vagy a(z) Document Capture alkalmazásból
HTTP (Local)	TCP	80	Bármely port	HTTP(S)-kiszolgáló (a(z) Web Config és a WSD adatainak a továbbítása)
HTTPS (Local)	TCP	443	Bármely port	

Speciális biztonsági beállítások vállalatok számára

Szolgáltatás neve	Protokolltípus	Helyi portszám	Távoli portszám	Vezérelt funkciók
HTTP (Remote)	TCP	Bármely port	80	HTTP(S)-ügyfél (kommunikáció a firmware-frissítés és a gyökértanúsítvány-frissítés között)
HTTPS (Remote)	TCP	Bármely port	443	

IPsec/IP Filtering konfigurációs példák

Csak IPsec-csomagok fogadása

Ez a példa csak az alapértelmezett házirend beállítását mutatja be.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: IPsec
- Authentication Method: Pre-Shared Key
- Pre-Shared Key: Legfeljebb 127 karaktert írhat be.

Group Policy:

Ne állítsa be.

Lapolvasás elfogadása a(z) Epson Scan 2 és a lapolvasó beállításainak segítségével

Ez a példa lehetővé teszi a lapolvasási adatok és lapolvasó-konfiguráció kommunikációit a meghatározott szolgáltatásoktól.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: Refuse Access

Group Policy:

- Enable this Group Policy: Jelölje be a négyzetet.
- Access Control: Permit Access
- Remote Address(Host): Egy ügyfél IP-címe
- Method of Choosing Port: Service Name
- Service Name: Jelölje be az ENPC, SNMP, Network Scan, HTTP (Local) és HTTPS (Local) négyzetet.

Hozzáférés fogadása csak egy adott IP-címről

Ebben a példában egy adott IP-cím férhet csak hozzá a lapolvasóhoz.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: Refuse Access

Group Policy:

- Enable this Group Policy: Jelölje be a négyzetet.
- Access Control: Permit Access

Speciális biztonsági beállítások vállalatok számára

❑ **Remote Address(Host)**: Egy rendszergazdai ügyfél IP-címe

Megjegyzés:

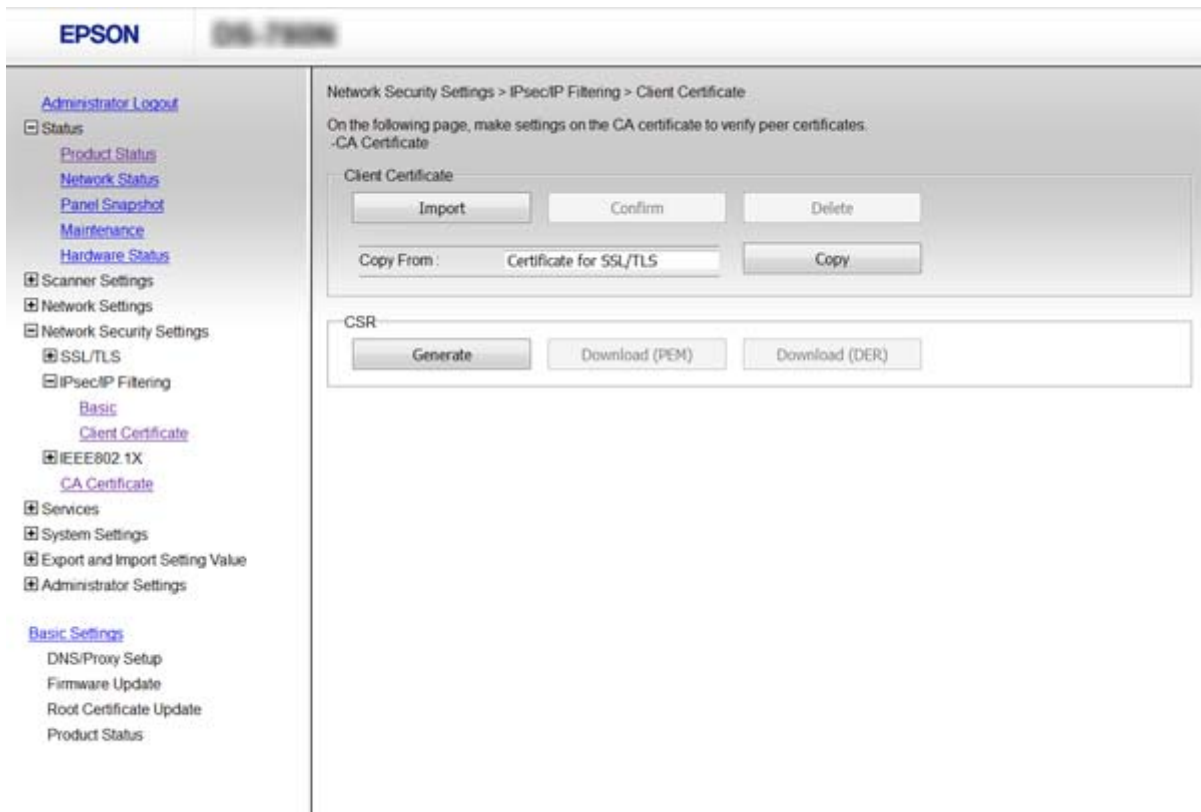
A házi rend konfigurációjától függetlenül az ügyfél hozzá tud férni a lapolvasóhoz és be tudja állítani azt.

Tanúsítvány beállítása az IPsec/IP Filtering hálózathoz

Konfigurálja az IPsec/IP-szűrés ügyféltanúsítványát. Ha a hitelesítésszolgáltatót konfigurálni szeretné, navigáljon a **CA Certificate** beállításhoz.

1. Jelenítse meg a Web Config segédprogramot, és válassza ki a **Network Security Settings > IPsec/IP Filtering > Client Certificate** pontot.
2. Importálja a tanúsítványt a **Client Certificate** beállításnál.

Ha korábban már importált olyan tanúsítványt, amelyet egy hitelesítésszolgáltató tett közzé IEEE802.1X vagy SSL/TLS hálózaton, akkor igény szerint átmásolhatja a tanúsítványt, és az IPsec/IP-szűréshez használhatja. A másoláshoz jelölje ki a tanúsítványt a **Copy From** részben, majd kattintson a **Copy** gombra.



Kapcsolódó információ

- ➔ „A Web Config elérése“ 23. oldal
- ➔ „CA által aláírt tanúsítvány beszerzése és importálása“ 64. oldal

Az SNMPv3 protokoll használata

Tudnivalók az SNMPv3 protokollról

Az SNMP egy, a hálózathoz csatlakoztatott eszközökről történő adatgyűjtés érdekében felügyeletet és vezérlést végző protokoll. Az SNMPv3 a továbbfejlesztett, kezelésbiztonsági funkciót ellátó verzió.

Az SNMPv3 használatakor az SNMP-kommunikáció (csomag) állapotfigyelése és beállításainak módosítása hitelesíthető és titkosítható annak érdekében, hogy az SNMP-kommunikáció (csomag) védve legyen az olyan hálózati kockázatokkal szemben, mint például a lehallgatás, a megszemélyesítés és az illetéktelen módosítás.

Az SNMPv3 konfigurálása

Ha a lapolvasó támogatja az SNMPv3 protokollt, figyelheti és szabályozhatja a lapolvasóhoz való hozzáféréseket.

1. Jelenítse meg a Web Config segédprogramot, és válassza ki a **Services > Protocol** pontot.
2. Írjon be egy értéket az **SNMPv3 Settings** minden egyes eleme számára.
3. Kattintson a(z) **Next** gombra.
Megjelenik egy megerősítő képernyő.
4. Kattintson a(z) **OK** gombra.
A lapolvasó frissítése megtörténik.

Kapcsolódó információ

- ➔ „A Web Config elérése“ 23. oldal
- ➔ „SNMPv3 elemek beállítása“ 84. oldal

SNMPv3 elemek beállítása

Elemek	Beállítások és magyarázat
Enable SNMPv3	Az SNMPv3 engedélyezett, ha a jelölőnégyzet be van jelölve.
User Name	1 és 32 közötti számú, 1 bájtos karaktert írjon be.
Authentication Settings	
Algorithm	Adja meg a hitelesítési algoritmust.
Password	8 és 32 közötti számú ASCII-karaktert (0x20–0x7E) karaktert írjon be.
Confirm Password	A megerősítéshez adja meg a beállított jelszót.
Encryption Settings	
Algorithm	Adja meg a titkosítási algoritmust.
Password	8 és 32 közötti számú ASCII-karaktert (0x20–0x7E) karaktert írjon be.
Confirm Password	A megerősítéshez adja meg a beállított jelszót.
Context Name	1 és 32 közötti számú, 1 bájtos karaktert írjon be.

Kapcsolódó információ

➔ „Az SNMPv3 konfigurálása“ 83. oldal

A lapolvasó csatlakoztatása IEEE802.1X hálózathoz

IEEE802.1X hálózat beállítása

Ha a lapolvasó támogatja az IEEE802.1X hálózatot, akkor a lapolvasó használható olyan hitelesítést igénylő hálózaton, amely egy RADIUS-kiszolgálóhoz és egy hitelesítő hubhoz kapcsolódik.

1. Jelenítse meg a Web Config segédprogramot, és válassza ki a **Network Security Settings > IEEE802.1X > Basic** pontot.
2. Írjon be egy értéket minden egyes elem számára.
3. Kattintson a(z) **Next** elemre.
Megjelenik egy megerősítő képernyő.
4. Kattintson a(z) **OK** elemre.
A lapolvasó frissítése megtörténik.

Kapcsolódó információ

- ➔ [„A Web Config elérése“ 23. oldal](#)
- ➔ [„IEEE802.1X hálózati beállítások“ 86. oldal](#)
- ➔ [„Nem sikerül elérni a nyomtatót vagy a szkennert az IEEE802.1X konfigurálása után“ 91. oldal](#)

Speciális biztonsági beállítások vállalatok számára

IEEE802.1X hálózati beállítások

Elemek	Beállítások és magyarázat	
IEEE802.1X (Wired LAN)	Igény szerint engedélyezheti vagy letilthatja az oldal beállításait (IEEE802.1X > Basic) az IEEE802.1X (vezeték LAN) hálózathoz.	
EAP Type	Válasszon ki egy beállítást a lapolvasó és a RADIUS-kiszolgáló közötti hitelesítés módszereként.	
	EAP-TLS	Be kell szereznie és importálnia kell a hitelesítésszolgáltató által aláírt tanúsítványt.
	PEAP-TLS	Be kell állítania egy jelszót.
PEAP/MSCHAPv2	Be kell állítania egy jelszót.	
User ID	Állítson be egy azonosítót a RADIUS-kiszolgáló hitelesítéséhez. Adjon meg legalább 1, de legfeljebb 128 egybájtos ASCII (0x20–0x7E) karaktert.	
Password	Hozzon létre egy azonosítót a lapolvasó hitelesítéséhez. Adjon meg legalább 1, de legfeljebb 128 egybájtos ASCII (0x20–0x7E) karaktert. Ha Windows-kiszolgálót használ RADIUS-kiszolgálóként, legfeljebb 127 karaktert adhat meg.	
Confirm Password	A megerősítéshez adja meg a beállított jelszót.	
Server ID	Létrehozhat egy kiszolgálóazonosítót egy adott RADIUS-kiszolgálóval történő hitelesítéshez. A hitelesítő ellenőrzi, hogy a RADIUS-kiszolgálótól kapott kiszolgálótanúsítvány subject/subjectAltName mezője tartalmazza-e a kiszolgáló azonosítóját. Adjon meg legalább 0, de legfeljebb 128 egybájtos ASCII (0x20–0x7E) karaktert.	

Speciális biztonsági beállítások vállalatok számára

Elemek	Beállítások és magyarázat	
Certificate Validation	A hitelesítési módszertől függetlenül tanúsítvány-ellenőrzést állíthat be. Importálja a tanúsítványt a CA Certificate beállításnál.	
Anonymous Name	Ha a PEAP-TLS vagy a PEAP/MSCHAPv2 lehetőséget választja az Authentication Method esetében, a felhasználói név helyett anonim nevet is megadhat a PEAP-hitelesítés 1. fázisában. Adjon meg legalább 0, de legfeljebb 128 egybájtos ASCII (0x20–0x7E) karaktert.	
Encryption Strength	Az alábbiak egyikét választhatja ki.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Kapcsolódó információ

➔ „IEEE802.1X hálózat beállítása“ 85. oldal

Tanúsítvány beállítása az IEEE802.1X hálózathoz

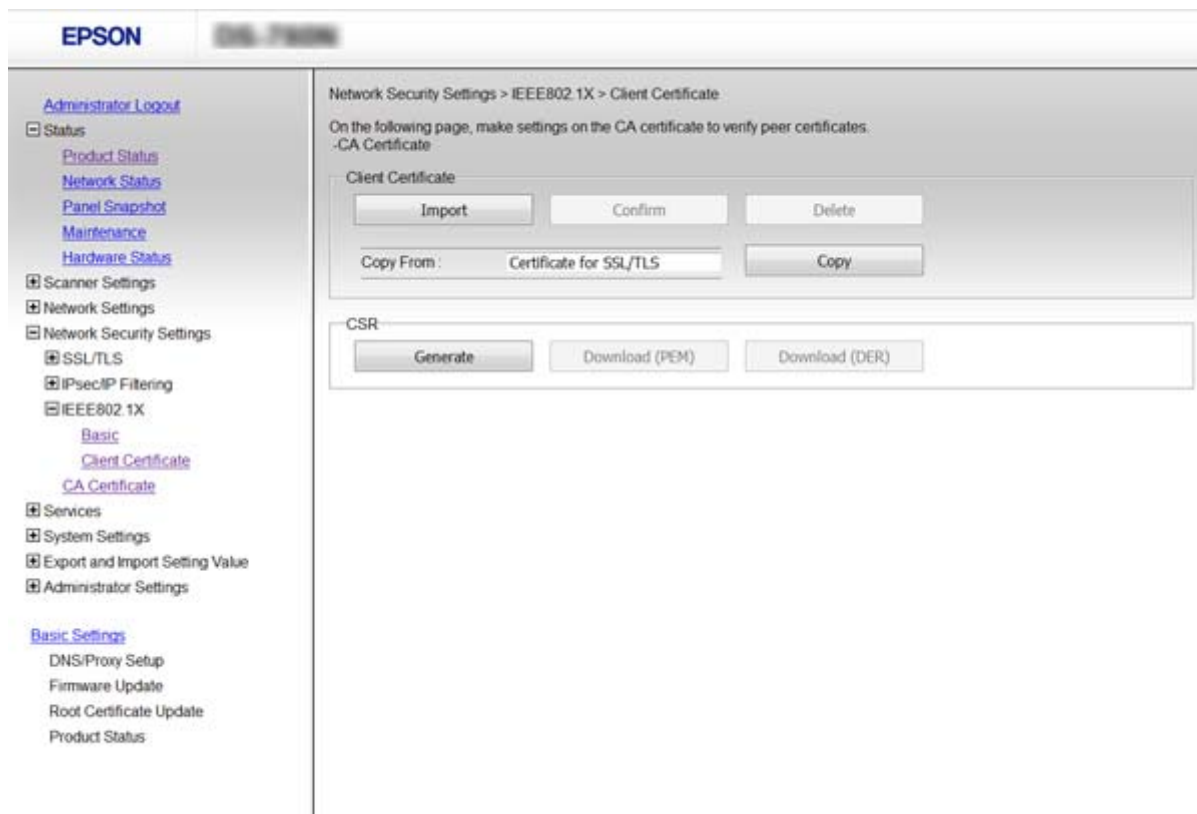
Konfigurálja az ügyféltanúsítványt az IEEE802.1X hálózathoz. Ha a hitelesítésszolgáltató által kiadott tanúsítványt konfigurálni szeretné, navigáljon a **CA Certificate** beállításához.

1. Jelenítse meg a Web Config segédprogramot, és válassza ki a **Network Security Settings > IEEE802.1X > Client Certificate** pontot.

Speciális biztonsági beállítások vállalatok számára

2. Adjon meg egy tanúsítványt a **Client Certificate** részben.

Ha a tanúsítványt egy hitelesítésszolgáltató tette közzé, akkor igény szerint másolhatja a tanúsítványt. A másoláshoz jelölje ki a tanúsítványt a **Copy From** részben, majd kattintson a **Copy** gombra.



Kapcsolódó információ

- ➔ „A Web Config elérése“ 23. oldal
- ➔ „CA által aláírt tanúsítvány beszerzése és importálása“ 64. oldal

Problémák megoldása a fokozott biztonság érdekében

A biztonsági beállítások visszaállítása

Ha olyan nagymértékben biztonságos környezetet épít ki, mint az IPsec/IP szűrés vagy az IEEE802.1X, elképzelhető, hogy az eszköz vagy a kiszolgáló helytelen beállításai vagy hibája miatt nem tud kommunikálni az eszközökkel. Ebben az esetben állítsa vissza a biztonsági beállításokat, és végezze el újra az eszköz beállításait, vagy tegye lehetővé az ideiglenes használatot.

A biztonsági funkció kikapcsolása a Kezelőpanelen keresztül

Az IPsec/IP Filtering vagy az IEEE802.1X letiltható a lapolvasó kezelőpaneljének segítségével.

Speciális biztonsági beállítások vállalatok számára

1. Koppintson a(z) **Beáll.** > **Hálózati beállítások** elemre.
2. Koppintson a(z) **Beállítások módosítása** elemre.
3. Az alábbiak közül koppintson a letiltani kívánt elemekre.
 - IPsec/IP-szűrés**
 - IEEE802.1X**
4. Miután megjelenik a befejezést jelző üzenet, koppintson a(z) **Tov.** gombra.

A biztonsági funkció visszaállítása Web Config segítségével

IEEE802.1X esetén a rendszer lehet, hogy nem tudja felismerni az eszközöket a hálózaton. Ebben az esetben a lapolvasón található kezelőpanellel tiltsa le a funkciót.

IPsec/IP szűrés esetén ha a számítógépről el tudja érni az eszközt, a funkció letiltható.

IPsec/IP-szűrés letiltása Web Config alkalmazással

1. Lépjen be a(z) Web Config segédprogramba, és válassza ki a(z) **Network Security Settings** > **IPsec/IP Filtering** > **Basic** menüpontot.
2. Válassza ki a(z) **Disable** lehetőséget a(z) **IPsec/IP Filtering** paraméterhez a(z) **Default Policy** menüben.
3. Kattintson a(z) **Next**, elemre, majd minden csoportos házirendnél törölje a(z) **Enable this Group Policy** beállítást.
4. Kattintson a(z) **OK** elemre.

Kapcsolódó információ

➔ [„A Web Config elérése“ 23. oldal](#)

A hálózati biztonsági funkciókkal kapcsolatos problémák

Elfelejtett előre megosztott kulcs

Állítsa be újból a kulcsot a Web Config segítségével.

A kulcs módosításához nyissa meg a Web Config menüt, és válassza ki a **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** vagy **Group Policy** lehetőséget.

Ha módosítja az előzetesen megosztott kulcsot, akkor a konfigurálását a számítógépekhez végezze.

Kapcsolódó információ

➔ [„A Web Config elérése“ 23. oldal](#)

Nem lehet kommunikálni IPsec kommunikációval

Lehet, hogy nem támogatott algoritmust használ a számítógép beállításai esetében?

A lapolvasó az alábbi algoritmusokat támogatja.

Biztonsági módok	Algoritmusok
Internetes kulcscsere titkosítási algoritmus	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
Internetes kulcscsere hitelesítési algoritmus	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Internetes kulcscsere kulcscsere-algoritmus	DH-csoport 1, DH-csoport 2, DH-csoport 5, DH-csoport 14, DH-csoport 15, DH-csoport 16, DH-csoport 17, DH-csoport 18, DH-csoport 19, DH-csoport 20, DH-csoport 21, DH-csoport 22, DH-csoport 23, DH-csoport 24, DH-csoport 25, DH-csoport 26, DH-csoport 27*, DH-csoport 28*, DH-csoport 29*, DH-csoport 30*
ESP titkosítási algoritmus	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP hitelesítési algoritmus	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH hitelesítési algoritmus	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* csak IKEv2 protokoll esetében érhető el

Kapcsolódó információ

➔ [„Titkosított kommunikáció IPsec-/IP-szűrés funkcióval“ 71. oldal](#)

Hirtelen nem lehet kommunikálni

Érvénytelen vagy megváltozott a lapolvasó IP-címe?

Tiltsa le az IPsec funkciót a lapolvasó kezelőpaneljén keresztül.

Ha a DHCP lejárt, a készülék újraindult vagy az IPv6 cím lejárt/nem került megszerzésre, akkor lehetséges, hogy a lapolvasó Web Config alkalmazásában regisztrált IP-cím (**Network Security Settings > IPsec/IP Filtering > Basic > Group Policy > Local Address (Scanner)**) nem található.

Használjon statikus IP-címet.

Érvénytelen vagy megváltozott a számítógép IP-címe?

Tiltsa le az IPsec funkciót a lapolvasó kezelőpaneljén keresztül.

Ha a DHCP lejárt, a készülék újraindult vagy az IPv6 cím lejárt/nem került megszerzésre, akkor lehetséges, hogy a lapolvasó Web Config alkalmazásában regisztrált IP-cím (**Network Security Settings > IPsec/IP Filtering > Basic > Group Policy > Remote Address(Host)**) nem található.

Használjon statikus IP-címet.

Kapcsolódó információ

➔ [„A Web Config elérése“ 23. oldal](#)

Speciális biztonsági beállítások vállalatok számára

➔ „Titkosított kommunikáció IPsec-/IP-szűrés funkcióval“ 71. oldal

Az IPsec/IP-szűrés konfigurálása után nem lehet csatlakozni

Elképzelhető, hogy hibás érték lett beállítva.

Tiltsa le az IPsec/IP Filtering funkciót a lapolvasó kezelőpaneljén keresztül. Csatlakoztassa a lapolvasót és a számítógépet, és adja meg ismét az IPsec/IP Filtering beállításait.

Kapcsolódó információ

➔ „Titkosított kommunikáció IPsec-/IP-szűrés funkcióval“ 71. oldal

Nem sikerül elérni a nyomtatót vagy a szkennert az IEEE802.1X konfigurálása után

Lehet, hogy helytelenek a beállítások.

Tiltsa le az IEEE802.1X funkciót a lapolvasó kezelőpanelén keresztül. Csatlakoztassa a lapolvasót és a számítógépet, majd végezze el újra az IEEE802.1X konfigurálását.

Kapcsolódó információ

➔ „IEEE802.1X hálózat beállítása“ 85. oldal

A digitális tanúsítvány használatával kapcsolatos problémák

Nem lehet hitelesítésszolgáltató által aláírt tanúsítványt importálni

Megfelel egymásnak a hitelesítésszolgáltató által aláírt tanúsítvány és a CSR-ben található információ?

Ha a hitelesítésszolgáltató által aláírt tanúsítvány és a CSR nem ugyanazokat az információkat tartalmazza, a CSR-t nem lehet importálni. Ellenőrizze a következőket:

- Olyan eszközre próbálja meg importálni a tanúsítványt, amely nem ugyanazokkal az információkkal rendelkezik?
Ellenőrizze a CSR adatait, majd importálja a tanúsítványt egy olyan eszközre, amely azonos adatokkal rendelkezik.
- Felülírta a lapolvasóban mentett CSR-t, miután elküldte azt a hitelesítésszolgáltatónak?
Szerezze meg újból a hitelesítésszolgáltató által aláírt tanúsítványt a CSR-rel.

A hitelesítésszolgáltató által aláírt tanúsítvány mérete nagyobb, mint 5 kB?

Nem importálhatók a hitelesítésszolgáltató által aláírt olyan tanúsítványok, amelyek mérete nagyobb, mint 5 kB.

Helyes a tanúsítvány importálására használt jelszó?

Ha elfelejtette a jelszót, nem tudja importálni a tanúsítványt.

Speciális biztonsági beállítások vállalatok számára

Kapcsolódó információ

➔ „Hitelesítésszolgáltató által aláírt tanúsítvány importálása“ 66. oldal

Nem lehet frissíteni saját aláírású tanúsítványt

Be van írva a Common Name?

Be kell írni a Common Name adatot.

A Common Name nem támogatott karaktereket tartalmaz? Például a japán nyelv nincs támogatva.

1 és 128 közötti számú ASCII (0x20-0x7E) karaktert írjon be IPv4, IPv6, hostnév vagy FQDN-formátumban.

A Common Name vesszőt vagy szóközt tartalmaz?

Vessző beírása esetén azon a ponton elválasztódik a Common Name. Ha csak szóköz van beírva egy vessző előtt vagy után, hiba történik.

Kapcsolódó információ

➔ „Saját aláírású tanúsítvány frissítése“ 68. oldal

Nem lehet CSR-t létrehozni

Be van írva a Common Name?

Be kell írni a Common Name adatot.

A Common Name, Organization, Organizational Unit, Locality, State/Province nem támogatott karaktereket tartalmaz? Például a japán nyelv nincs támogatva.

ASCII (0x20-0x7E) karaktert írjon be IPv4, IPv6, hostnév vagy FQDN-formátumban.

A Common Name vesszőt vagy szóközt tartalmaz?

Vessző beírása esetén azon a ponton elválasztódik a Common Name. Ha csak szóköz van beírva egy vessző előtt vagy után, hiba történik.

Kapcsolódó információ

➔ „Hitelesítésszolgáltató által aláírt tanúsítvány beszerzése“ 64. oldal

Digitális tanúsítvánnyal kapcsolatos figyelmeztetés jelenik meg

Üzenetek	Ok/Teendő
Enter a Server Certificate.	<p>Ok: Nem választott ki fájlt importálásra.</p> <p>Teendő: Válasszon ki egy fájlt és kattintson az Import gombra.</p>

Speciális biztonsági beállítások vállalatok számára

Üzenetek	Ok/Teendő
CA Certificate 1 is not entered.	<p>Ok:</p> <p>Az 1. hitelesítésszolgáltatói tanúsítvány nincs beírva, és csak a 2. hitelesítésszolgáltatói tanúsítvány van beírva.</p> <p>Teendő:</p> <p>Először importálja az 1. hitelesítésszolgáltatói tanúsítványt.</p>
Invalid value below.	<p>Ok:</p> <p>A fájl elérési útja és/vagy jelszava nem támogatott karaktereket tartalmaz.</p> <p>Teendő:</p> <p>Ügyeljen rá, hogy a megfelelő karakterek legyenek beírva.</p>
Invalid date and time.	<p>Ok:</p> <p>A lapolvasó dátuma és ideje nincs beállítva.</p> <p>Teendő:</p> <p>Állítsa be a dátumot és az időt a Web Config vagy az EpsonNet Config segítségével.</p>
Invalid password.	<p>Ok:</p> <p>A hitelesítésszolgáltatói tanúsítvány számára beállított és a beírt jelszó nem egyezik.</p> <p>Teendő:</p> <p>Írja be a helyes jelszót.</p>
Invalid file.	<p>Ok:</p> <p>Nem X509 formátumban importálja a tanúsítványt.</p> <p>Teendő:</p> <p>Ügyeljen rá, hogy egy megbízható hitelesítésszolgáltató által küldött megfelelő tanúsítványt használjon.</p>
	<p>Ok:</p> <p>Az importált fájl túl nagyméretű. A fájl maximális mérete 5 kB.</p> <p>Teendő:</p> <p>Ha a helyes fájlt választja ki, előfordulhat, hogy a tanúsítvány sérült vagy hamisított.</p>
	<p>Ok:</p> <p>A tanúsítvány által tartalmazott lánc érvénytelen.</p> <p>Teendő:</p> <p>A hitelesítésszolgáltató weboldalán bővebb tájékoztatás található a tanúsítványokkal kapcsolatban.</p>
Cannot use the Server Certificates that include more than three CA certificates.	<p>Ok:</p> <p>A PKCS#12 formátumú tanúsítványfájl több mint 3 hitelesítésszolgáltatói tanúsítványt tartalmaz.</p> <p>Teendő:</p> <p>Az egyes tanúsítványok importálásakor konvertálja át azokat PKCS#12 formátumból PEM formátumba, vagy olyan PKCS#12 formátumú tanúsítványfájlt importáljon, amely legfeljebb 2 hitelesítésszolgáltatói tanúsítványt tartalmaz.</p>

Speciális biztonsági beállítások vállalatok számára

Üzenetek	Ok/Teendő
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	<p>Ok: A tanúsítvány lejárt.</p> <p>Teendő:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ha a tanúsítvány lejárt, szerezzen be és importáljon egy új tanúsítványt. <input type="checkbox"/> Ha a tanúsítvány nem járt le, ellenőrizze, hogy a lapolvasó dátuma és ideje megfelelően van-e beállítva.
Private key is required.	<p>Ok: Nincs párosítva privát kulcs a tanúsítvánnyal.</p> <p>Teendő:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Ha a tanúsítvány PEM/DER formátumban van, és egy CSR alapján lett beszerezve egy számítógép segítségével, adja meg a privát kulcs fájlt. <input type="checkbox"/> Ha a tanúsítvány PKCS#12 formátumban van, és egy CSR alapján lett beszerezve egy számítógép segítségével, hozzon létre egy privát kulcsot tartalmazó fájlt.
	<p>Ok: Újból importált egy CSR alapján beszerezett PEM/DER tanúsítványt a Web Config segítségével.</p> <p>Teendő: Ha a tanúsítvány PEM/DER formátumban van, és egy CSR-től lett beszerezve a Web Config segítségével, csak egyszer tudja importálni.</p>
Setup failed.	<p>Ok: Nem lehet befejezni a beállítást, mert a lapolvasó és a számítógép közötti kommunikáció sikertelen, vagy a fájlt nem lehet olvasni valamilyen hiba miatt.</p> <p>Teendő: Az adott fájl és a kommunikáció ellenőrzése után importálja újból a fájlt.</p>

Kapcsolódó információ

➔ [„Tudnivalók a digitális tanúsítványról“ 63. oldal](#)

Tévedésből töröltött egy CA által aláírt tanúsítvány**Létezik biztonsági másolat a tanúsítványról?**

Ha megvan a biztonsági másolat, importálja újból a tanúsítványt.

Ha a tanúsítványt a Web Config alkalmazásban létrehozott CSR segítségével szerzi be, nem importálhat egy már törölt tanúsítványt. Hozzon létre egy CSR-t és szerezzen be új tanúsítványt.

Kapcsolódó információ

➔ [„Hitelesítésszolgáltató által aláírt tanúsítvány törlése“ 68. oldal](#)

➔ [„Hitelesítésszolgáltató által aláírt tanúsítvány importálása“ 66. oldal](#)