BIZTONSÁGI ÚTMUTATÓ

imageRUNNER ADVANCE

Canon

BEVEZETÉS

A modern Canon multifunkciós készülékek (Multifunction Devices – MFD-k) nyomtatási, másolási, szkennelési, küldési és faxolási funkciókat biztosítanak. A multifunkciós készülékek számítógépes kiszolgálókként is működnek többféle hálózati szolgáltatást és jelentős merevlemezkapacitást nyújtva.

Amikor egy vállalat bevezeti ezeket a készülékeket az infrastruktúrájában, a hálózati rendszerek megbízhatóságát, integritását és rendelkezésre állását szem előtt tartó átfogó biztonsági stratégia részeként számos területet meg kell vizsgálnia.

Az egyes üzembe helyezések természetesen eltérőek hiszen minden vállalat saját, egyedi biztonsági követelményekkel rendelkezik. Dolgozunk azon, hogy a Canon készülékek szállításkor már megfelelő kezdeti biztonsági beállításokkal rendelkezzenek, egyúttal az eltérő biztonsági követelmények további támogatásához biztosítunk számos konfigurációs beállítást, hogy a készüléket az adott környezet egyedi követelményeit figyelembe véve állíthassa be.

Ezt a dokumentumot úgy terveztük, hogy elegendő információt biztosítson ahhoz, hogy megbeszélhesse a Canon vállalattal vagy a Canon partnereivel a környezete szempontjából legmegfelelőbb beállításokat. A végső konfigurációról hozott döntést követően az alkalmazható a készülékre vagy a teljes flottára. További információért és támogatásért bármikor fordulhat a Canon-hoz vagy a Canon partnereihez.

Kinek ajánljuk ezt a dokumentumot?

Ezt a dokumentumot mindenki figyelmébe ajánljuk, aki multifunkciós irodai készülékek (MFD-k) hálózati környezetbe történő illesztésével, üzemeltetésével és kapcsolódó biztonsági kérdésekkel foglalkozik.

Terjedelem

Az útmutató két tipikus hálózati környezet konfigurációját ismerteti, és ezzel kapcsolatos javaslatokat tartalmaz, hogy a vállalatok biztonságosan, a legjobb gyakorlat alapján valósíthassák meg MFD-k hálózatba integrálását. Ezeket a beállításokat a Canon biztonsági csapata tesztelte és ellenőrizte.

Nem vesszük figyelembe ugyanakkor az egyes iparágak specifikus szabályozási követelményeit, amelyek egyéb biztonsági megfontolásokat igényelhetnek, és amelyek kívül esnek ennek a dokumentumnak a terjedelmén.

Az útmutató elkészítésekor az imageRUNNER ADVANCE platform szokásos funkciókészletét vettük figyelembe, és bár az itt leírt információk az imageRUNNER ADVANCE sorozat összes modelljére és családjára érvényesek, bizonyos funkciók modellenként eltérhetnek.

A megfelelő MFD biztonsági szint kialakítása

Ahhoz, hogy feltárjuk egy multifunkciós készülék adott hálózat részeként való implementálásának hálózatbiztonságra gyakorolt hatásait, két tipikus forgatókönyvet vettünk figyelembe:

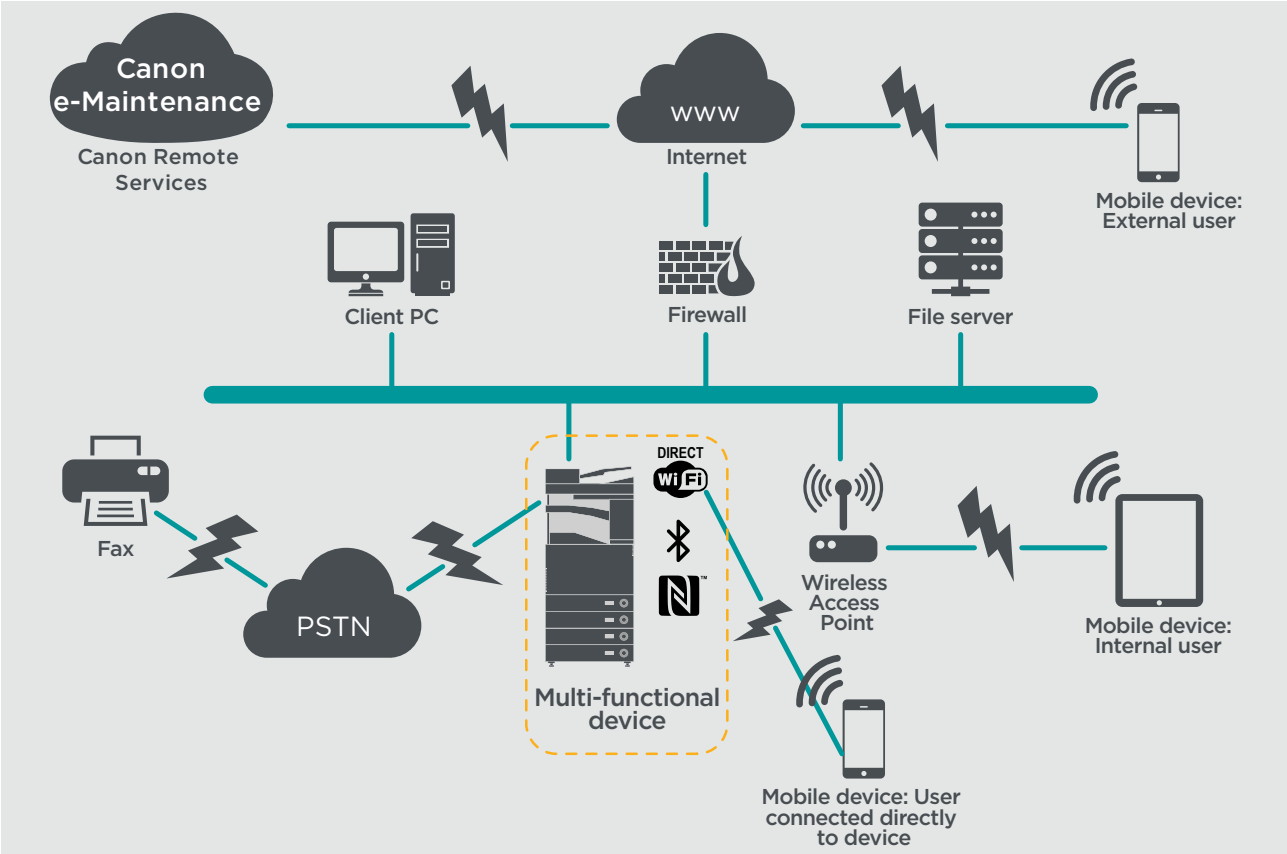
- **Egy tipikus kisirodai környezetet**
- **Egy nagyvállalati irodai környezetet**

KISIRODAI KÖRNYEZET

Általában egy kisvállalati környezetet szegmentálatlan hálózati topológiát jelent, ahol egy vagy két MFD-t üzemeltetnek belső használatra, és ezek a készülékek nem érhetők el az internetről.

A mobilnyomtatás lehetősége rendelkezésre áll, de ahhoz további kiegészítők szükségesek. Azon felhasználók a számára, akik LAN-környezeten kívüli nyomtatási szolgáltatásokat igényelnek biztonságos kapcsolat szükséges, de ezt a témát ez az útmutató nem dolgozza fel. Ettől függetlenül figyelmet kell azonban fordítani a távoli készülék és a nyomtatási infrastruktúra közötti adatátvitel biztonságára.

1. ábra kisirodai hálózat



Az imageRUNNER ADVANCE modellek legújabb generációja vezeték nélküli kapcsolódást kínálnak, melynek segítségével a készülékek Wi-Fi-hálózatra csatlakozhatnak. Végpontok közötti Wi-Fi Direct-kapcsolat is létrehozható a mobilkészülékkel anélkül, hogy hálózati kapcsolatra lenne szükség.

Számos készülékhez Bluetooth és NFC opciók is elérhetők, melyekkel Wi-Fi Direct-kapcsolat létesíthető az iOS-, illetve az Android-készülékekkel.

KONFIGURÁCIÓS LEHETŐSÉGEK

Kérjük vegye figyelembe, hogy amennyiben az alábbiakban nincs megemlítve az imageRUNNER ADVANCE egy funkciója, akkor úgy tekintjük, hogy ehhez a vállalati és hálózati környezethez megfelel az alapértelmezett beállítás.

1. táblázat Konfigurációs lehetőségek kisirodai környezetben

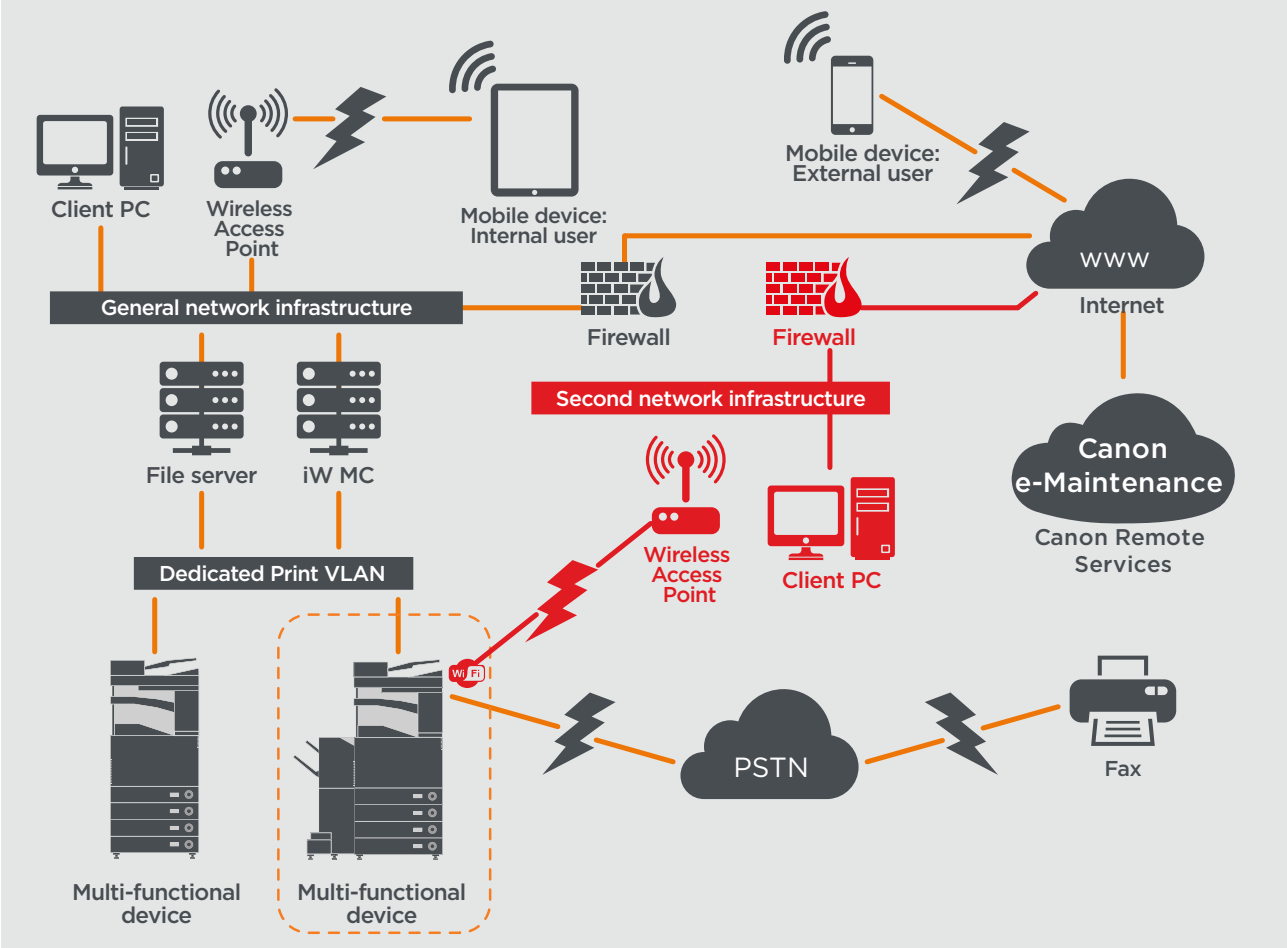
imageRUNNER ADVANCE-funkció	Leírás	Megfontolás tárgya
Szervizmód	Hozzáférést biztosít a szervizmód beállításaihoz.	Jelszavas védelem beállítása egy nem alapértelmezett, nem könnyen kitalálható és maximális hosszúságú jelszóval
Szervizkezelő rendszer	Hozzáférést biztosít számos, nem standard eszközbeállításhoz	Jelszavas védelem beállítása egy nem alapértelmezett, nem könnyen kitalálható és maximális hosszúságú jelszóval
SMB böngészés/küldés	Tárolás Windows/SMB hálózati megosztásokon és lekérés azokról	A rendszergazdáknak javasolt, a házirendbe foglalva, letiltani a felhasználók számára, hogy helyi fiókokat hozzanak létre a számítógépükön a dokumentumoknak az imageRUNNER ADVANCE készülékkel SMB-n keresztül történő megosztáshoz.
Remote UI (Távvezérlési kezelőfelület)	Webalapú konfigurációs eszköz	Az imageRUNNER ADVANCE rendszergazdájának engedélyeznie kell a HTTPS protokollt a távvezérlési kezelőfelülethez, és le kell tiltania a HTTP-hozzáférést. Egyedi PIN-hitelesítés engedélyezése minden egyes eszközhöz
SNMP	Hálózatfigyelés integrációja	Az 1. verzió letiltása és kizárólag a 3. verzió engedélyezése
Küldés e-mailben és/vagy IFAX-on	E-mail küldése a készülékről mellékletekkel	SSL engedélyezése Ne használja a POP3-hitelesítést az SMTP-küldés előtt. SMTP-hitelesítés használata
POP3	Dokumentumok automatikus lekérése és kinyomtatása a postafiókból	SSL engedélyezése Engedélyezze a POP3-hitelesítést.
Címjegyzék/LDAP	Címtárszolgáltatás használata az otthoni telefonszám vagy e-mail-címek megkeresésére a beolvasott dokumentumok küldéséhez.	SSL engedélyezése Ne használjon tartományi hitelesítő adatokat az LDAP-kiszolgálón való hitelesítéshez; használjon az LDAP-ban érvényes hitelesítő adatokat.
FTP-nyomtatás	Dokumentumok feltöltése a beágyazott FTP-kiszolgálóra és letöltése onnan	Kapcsolja be az FTP-hitelesítést. Vegye figyelembe, hogy az FTP-forgalom mindig titkosítatlan szövegként továbbítódik a hálózaton.
WebDAV-küldés	Dokumentumok beolvasása és tárolása távoli helyen	Hitelesítés engedélyezése WebDAV-megosztásokhoz.
Titkosított PDF	Dokumentumok titkosítása	Házirendben szabályozza, hogy a dokumentumok csak a PDF 1.6-os verziójával (AES-128) legyenek titkosíthatók.
Biztonságos nyomtatás	Megtörténik a nyomtatási feladat elküldése az eszköznek, de az zárolva van a nyomtatási sorban a megfelelő PIN-kód megadásáig.	PIN-kóddal védett nyomtatási feladatok engedélyezése
Beágyazott webböngésző (a 3. generáció 2. kiadásához tartozó modellektől áll rendelkezésre)	Hozzáférés böngészővel az internethez	Rendszergazdaként kényszerítse tartalomszűrő webproxy használatát a kártevő vagy vírusos tartalom elérésének megakadályozásához. Kedvencek létrehozásának letiltása
Bluetooth és NFC (a 3. generációs modellektől áll rendelkezésre)	A Wi-Fi Direct-kapcsolat létrehozására használatos.	Wi-Fi Direct-kapcsolat engedélyezése a mobilkészülékekhez való közvetlen kapcsolódáshoz. A Wi-Fi Direct-kapcsolat nem használható, ha Wi-Fi-t használ hálózatra való kapcsolódáshoz.
Vezeték nélküli LAN	Vezeték nélküli hozzáférést biztosít.	Használjon WPA-PSK/WPA2-PSK titkosítást erős jelszóval.
IPP	Kapcsolódás és nyomtatási feladatok küldése IP-n keresztül	Tiltsa le az IPP-t.

NAGYVÁLLALATI IRODAI KÖRNYEZET

Nagyvállalati környezetben általában állandó csapat áll rendelkezésre a hálózati és háttérirodai, valamint az általános számítógép-problémákkal kapcsolatos problémák, kihívások kezelésére, de feltételezzük, hogy nem rendelkeznek külön képzéssel az MFD-k terén.

A nagyvállalati környezet általában egy több telephellyel és irodával rendelkező környezet szegmentált hálózati architektúrával. Több, belső használatra nyomtatókiszolgálókon keresztül elérhető MFD is van telepítve különálló VLAN hálózatokon. Ezek az MFD-k az internetről nem érhetők el.

2. ábra Nagyvállalati irodai munkakörnyezet



A pirossal kiemelt kapcsolatok a 3. generáció 2. kiadásához tartozó modellektől lesznek elérhetők.

KONFIGURÁCIÓS LEHETŐSÉGEK

Kérjük vegye figyelembe, hogy amennyiben az alábbiakban nincs megemlítve az imageRUNNER ADVANCE egy funkciója, akkor úgy tekintjük, hogy ehhez a vállalati és hálózati környezethez megfelel az alapértelmezett beállítás.

2. táblázat Konfigurációs lehetőségek nagyvállalati irodai környezetben

imageRUNNER ADVANCE-funkció	Leírás	Megfontolás tárgya
Szervizmód	Hozzáférést biztosít a szervizmód beállításaihoz.	Jelszavas védelem beállítása egy nem alapértelmezett, nem könnyen kitalálható és maximális hosszúságú jelszóval
Szervizkezelő rendszer	Hozzáférést biztosít számos, nem standard eszközbeállításhoz	Jelszavas védelem beállítása egy nem alapértelmezett, nem könnyen kitalálható és maximális hosszúságú jelszóval
SMB böngészés/küldés	Tárolás Windows/SMB hálózati megosztásokon és lekérés azokról	A rendszergazdáknak javasolt, a házirendbe foglalva, letiltani a felhasználók számára, hogy helyi fiókokat hozzanak létre a számítógépükön a dokumentumoknak az imageRUNNER ADVANCE készülékkel SMB-n keresztül történő megosztáshoz.
Remote UI (Távvezérlési kezelőfelület)	Webalapú konfigurációs eszköz	A készülék kezdeti konfigurációját követően tiltsa le teljesen a távvezérlési kezelőfelületet a HTTP és a HTTPS letiltásával.
SNMP	Hálózatfigyelés integrációja	Az 1. verzió letiltása és kizárólag a 3. verzió engedélyezése
Küldés e-mailben és/vagy IFAX-on	E-mail küldése a készülékről mellékletekkel	SSL engedélyezése Engedélyezze a következőket: – Tanúsítvány ellenőrzése az SMTP-kiszolgálón Vagy, ha ez nem kivitelezhető: – Csak olyan környezetben használja ezt a funkciót, ahol a hálózati behatolóészlelő rendszer gyűjtője jelen van. Ne használja a POP3-hitelesítést az SMTP-küldés előtt. Használjon SMTP-hitelesítést.
POP3	Dokumentumok automatikus lekérése és kinyomtatása a postafiókból	SSL engedélyezése Engedélyezze a következőket: – Tanúsítvány ellenőrzése a POP3-kiszolgálón Vagy, ha ez nem kivitelezhető: – Csak olyan környezetben használja ezt a funkciót, ahol a hálózati behatolóészlelő rendszer gyűjtője jelen van. Engedélyezze a POP3-hitelesítést.
Címjegyzék/LDAP	Használjon címtárszolgáltatást a telefonszám vagy e-mail-címek megkeresésére a beolvasott dokumentumok küldéséhez.	SSL engedélyezése Engedélyezze a következőket: – Tanúsítvány ellenőrzése az LDAP-kiszolgálón Vagy, ha ez nem kivitelezhető: – Csak olyan környezetben használja ezt a funkciót, ahol a hálózati behatolóészlelő rendszer gyűjtője jelen van. Ne használja a tartományi hitelesítő adatokat az LDAP-kiszolgálón való hitelesítéshez; használjon az LDAP-ban érvényes hitelesítő adatokat.
IPP	Kapcsolódás és nyomtatási feladatok küldése IP-n keresztül	Tiltsa le az IPP-t.
WebDAV-küldés	Dokumentumok beolvasása és tárolása távoli helyen	Hitelesítés engedélyezése a WebDAV-megosztásokhoz. SSL engedélyezése Konfigurálja úgy a nyomtatót, hogy csak a „fájlnyomtatási kiterjesztés” végződéssel rendelkező fájlok feltöltését engedélyezze.
IEEE802.1X	Hálózati hozzáférési hitelesítési mechanizmus	Az EAPOL V1 támogatott.
Titkosított PDF	Dokumentumok titkosítása	Házirendben szabályozza, hogy a dokumentumok csak a PDF 1.6-os verziójával (AES-128) legyenek titkosíthatók.
Titkosított biztonságos nyomtatás	Növelje a biztonságos nyomtatás védelmét a fájl és a jelszó átvitel közbeni titkosításával.	A nyomtató konfigurációs kliensében a Nyomtató fülön más felhasználónevet állítson be, mint a felhasználó LDAP/tartomány helyen érvényes hitelesítő adatai. Gondoskodjon róla, hogy a „Nyomtatási feladatok korlátozása” be legyen kapcsolva.
Vezeték nélküli LAN	Vezeték nélküli hozzáférést biztosít.	Használjon WPA-PSK/WPA2-PSK titkosítást erős jelszóval.
Wi-Fi Direct	A Wi-Fi Direct-kapcsolat létrehozására használatos.	Wi-Fi Direct letiltása
Beágyazott webböngésző (a 3. generáció 2. kiadásához tartozó modellektől áll rendelkezésre)	Hozzáférés böngészővel az internethez	Alkalmazzon megfelelő korlátozásokat, vagy tiltsa le a böngészővel való fájlletöltést.

Az imageRUNNER ADVANCE modellek legújabb generációja vezeték nélküli kapcsolódási lehetőséget kínálnak, melynek segítségével a készülékek Wi-Fi-hálózatra csatlakozhatnak, miközben vezetékes hálózatra is csatlakoznak. Ez a forgatókönyv hasznos lehet, ha az ügyfél két hálózaton is szeretné megosztani a készüléket. Az iskolai környezet tipikus példája annak, amikor a személyzet és a diákok számára különálló hálózat áll rendelkezésre.

KÉSZÜLÉKTÁMOGATÁS TÁVOLRÓL

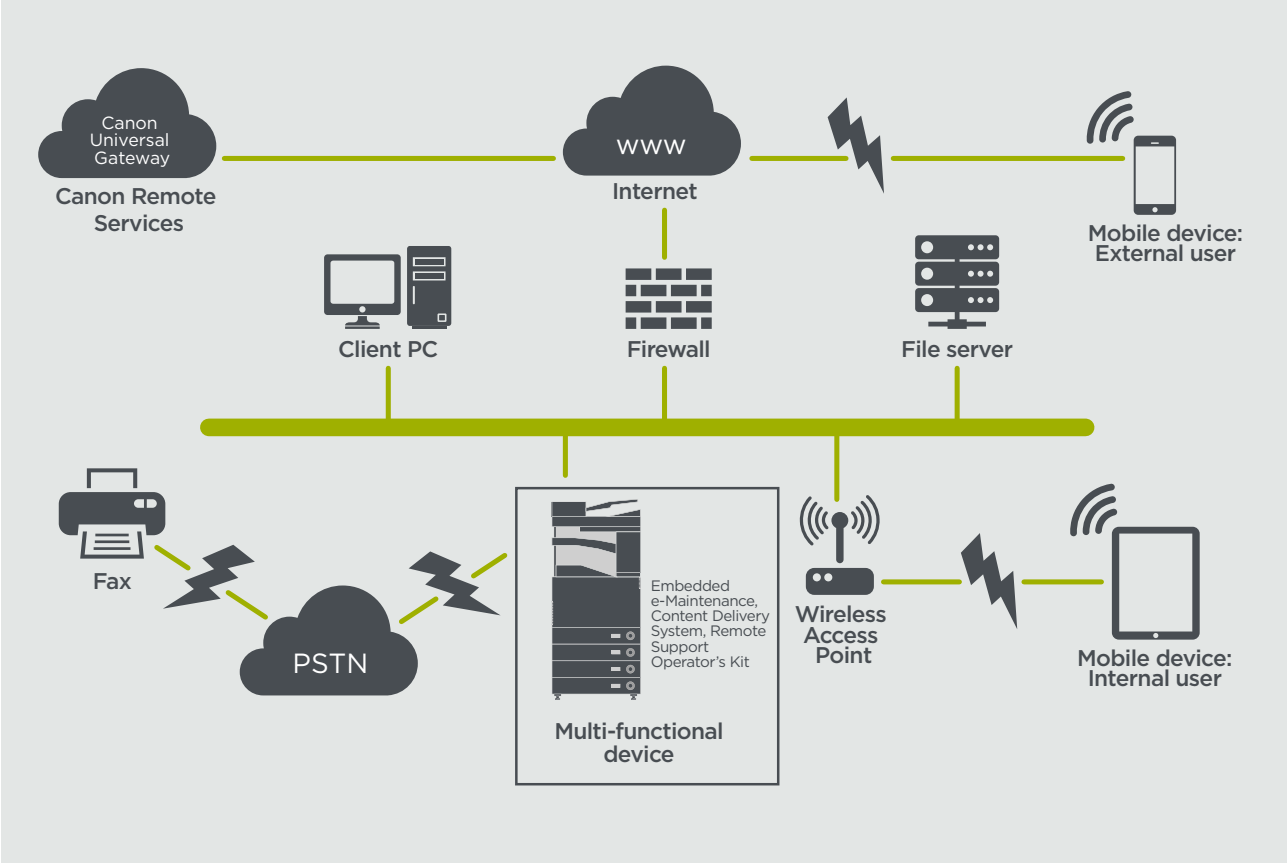
Ahhoz, hogy a Canon vagy a Canon egyik partnere hatékony szolgáltatást nyújthasson, az imageRUNNER ADVANCE képes elküldeni a szervizzel kapcsolatos adatokat, valamint firmware-frissítéseket vagy szoftvereket fogadni. Fontos megjegyezni, hogy a készülék sem a képeket, sem azok metaadatait nem küldi el.

Az alábbiakban bemutatjuk a Canon távszolgáltatásainak a vállalati hálózaton történő két lehetséges megvalósítását.

1. megvalósítási forgatókönyv: Elosztott kapcsolat

Ebben a forgatókönyvben minden egyes MFD közvetlen kapcsolatot engedélyez a távoli szolgáltatáshoz az interneten keresztül.

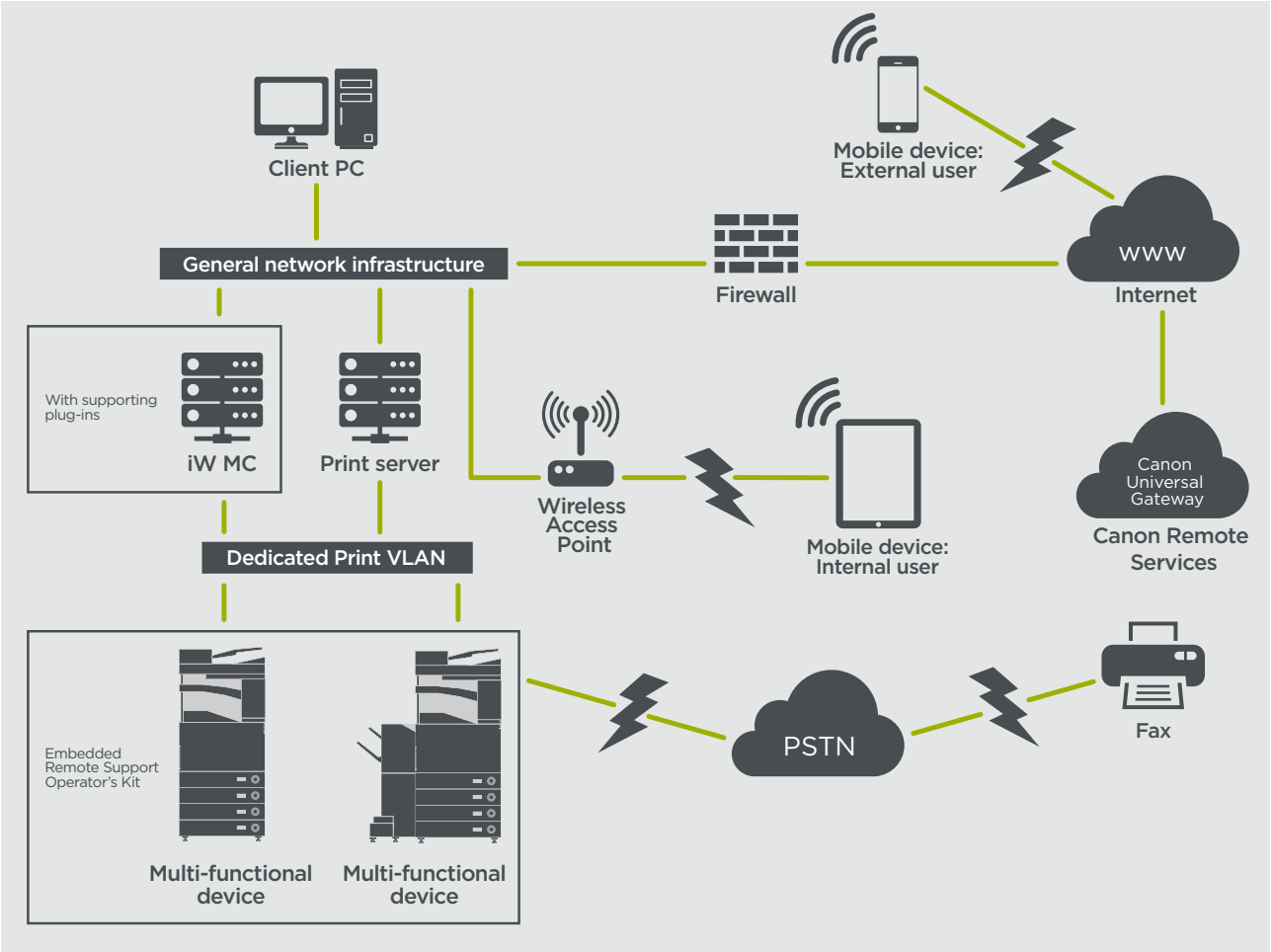
3. ábra Elosztott kapcsolat



2. megvalósítási forgatókönyv: Központosított, felügyelt kapcsolat

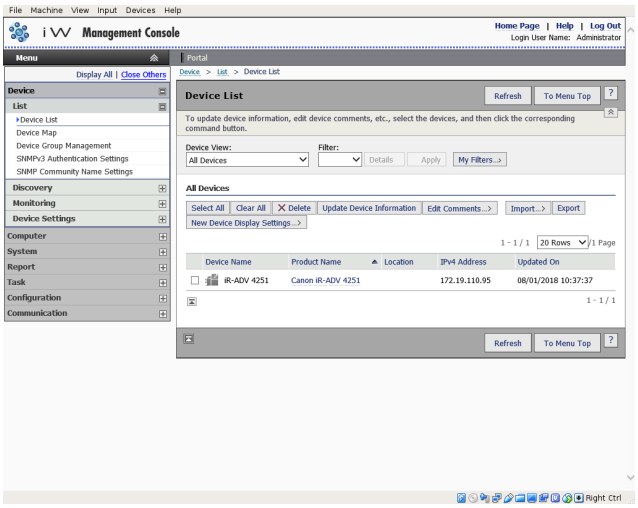
A nagyvállalati környezetekben, ahol több MFD is telepítve van, igény jelentkezik ezeknek a készülékeknek egyetlen, központi helyről történő hatékony kezelésére, és ez a Canon távoli szolgáltatásaihoz való kapcsolódást is magában foglalja. A holisztikus felügyeleti megközelítés megvalósításához az egyes készülékek egyetlen iW Management Console (iWMC – iW felügyeleti konzol) csatlakozási pontján keresztül hoznak létre felügyeleti kapcsolatokat. A Device Firmware Upgrade (DFU) beépülő modul és a többfunkciós készülékek közötti kommunikációra a 47545-ös UDP-port használatos.

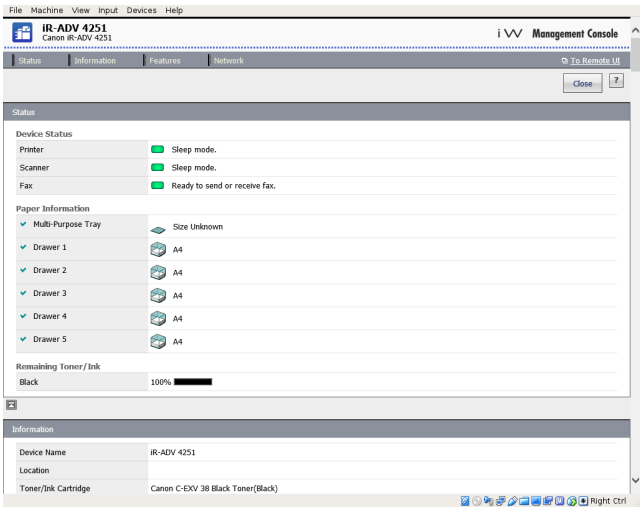
4. ábra Központosított, felügyelt kapcsolat



5a. ábra Készüléklista (ebben az esetben egyetlen készülék), amint az az imageWARE felügyeleti konzolján látható és

5b. ábra Készülék részletes adatai és beállításai





e-Maintenance

Az e-Maintenance rendszer képes automatikus úton begyűjteni a készülékek számlálóállását számlázási célból, valamint támogatni a fogyóeszközök kezelését és állapot-, hiba jelentések segítségével a távoli eszköz felügyeletet.

Az e-Maintenance rendszer egy internetoldali kiszolgálót (UGW), egy beágyazott multifunkciós eszköz szoftvert (eRDS) és/vagy további kiszolgálóalapú szoftvert (RDS beépülő modul) tartalmaz a készülék szervizeléssel kapcsolatos adatainak gyűjtéséhez. Az eRDS egy olyan figyelőprogram, amely az imageRUNNER ADVANCE készüléken fut. Ha a figyelés engedélyezve van a készülék beállításaiban, az eRDS beszerzi a az adott készülék adatait, és elküldi az UGW-nek. Az RDS egy általános számítógépre telepített figyelőprogram, amely 1 és 3000 közötti készülék figyelésére képes. Lekéri az adatokat minden egyes készülékről a hálózaton keresztül, és elküldi az UGW-nek.

A következő táblázat áttekinti az átvitt adatokat, a használt protokollokat (a tervezési és megvalósítási fázisban kiválasztott opcióktól függően) és portokat. Soha nem küld semmilyen másolási, nyomtatási, beolvasási vagy faxolási képadatot.

3. táblázat E-Maintenance adatok áttekintése

Leírás	Kezelt adatok	Protokoll/port	Port
Az eMaintenance (eRDS vagy RDS beépülő modul) és az UGW közötti kommunikáció	UGW webszolgáltatási címe Proxykiszolgáló címe/portszáma, Proxyfiók/jelszó UGW levelezési küldési címe SMTP-kiszolgáló címe POP-kiszolgáló címe Készülékállapot, számláló- és modelladatok Gyári szám Fennmaradó toner/tinta adatai, Firmware-adatok Javítási kérelem adatai Naplózási adatok Szerviz hívása Szervizriasztás Elakadás Környezet Állapot napló	HTTP/HTTPS/SMTP/POP3	TCP/80 TCP/443 TCP/25 TCP/110
Az eMaintenance és a készülék közötti kommunikáció (csak az RDS beépülő modul, mivel az eRDS beágyazott szoftver)		SNMP A Canon tulajdona SLP/SLP/HTTPS	UDP/161 TCP/47546, UDP/47545, TCP9007 UDP/427 UDP/11427 TCP/443

Tartalombiztosítási rendszer

A Content Delivery System (tartalombiztosítási rendszer) kapcsolatot hoz létre az MFD és a Canon Universal Gateway (UGW – univerzális átjáró) között. Firmware- és alkalmazásfrissítéseket biztosít a készülékhez.

4. táblázat A tartalombiztosítási rendszer adatainak áttekintése

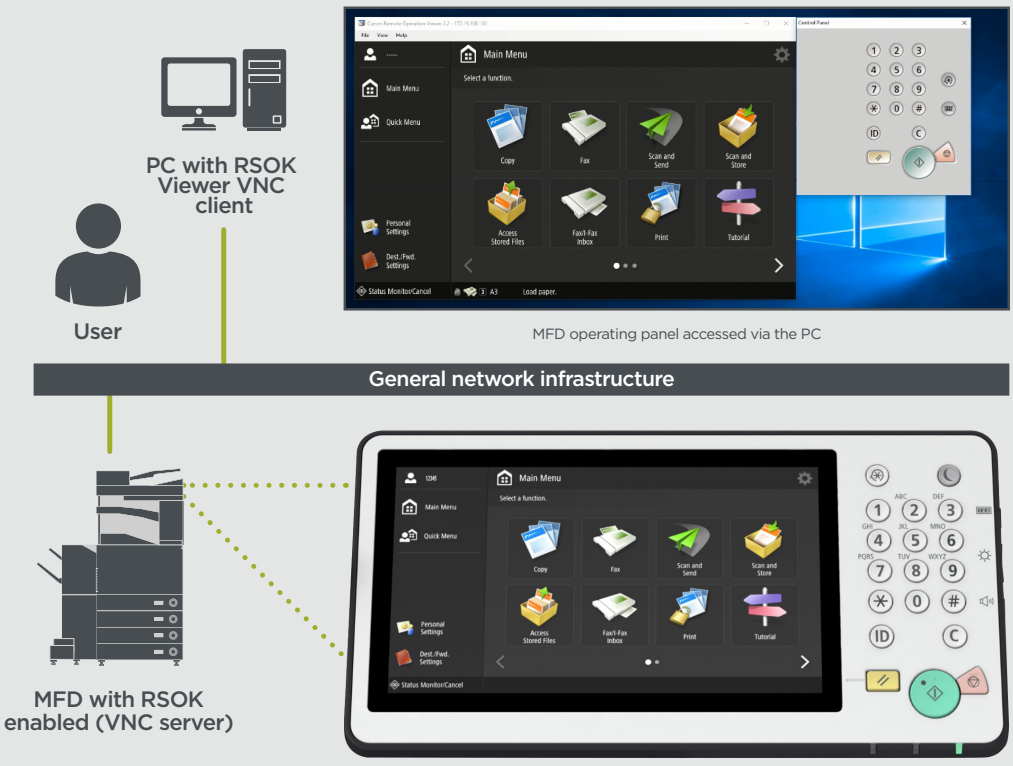
Leírás	Elküldött adatok	Protokoll/port	Port
Az MFD és az UGW közötti kommunikáció	Készülék sorozatszáma Firmware verzió Nyelv Ország A készülék végfelhasználói licencszerződésére vonatkozó információ	HTTP/HTTPS	TCP/80 TCP/443
Az UGW és az MFD közötti kommunikáció	Tesztfájl (bináris véletlenszerű adatok) a kommunikáció teszteléséhez A firmware vagy a MEAP alkalmazás bináris adatai	HTTP/HTTPS	TCP/80 TCP/443

A készülék konfigurációjában előre be van állítva egy meghatározott CDS-hozzáférési URL-cím. Ha követelmény az infrastruktúrán belül a központosított firmware és alkalmazásfelügyelet a készülékhez, akkor szükség lesz az iWMC és a Device Firmware Upgrade (DFU), valamint a Device Application Management beépülő modul helyi telepítésére.

Távoli támogatáskezelői készlet

A Távoli támogatáskezelői készlet (Remote Support Operators's Kit – RSOK) távoli hozzáférést biztosít a készülék kezelőpaneléhez. Ez a kiszolgáló-kliens típusú rendszer egy, MFP-n futó VNC-kiszolgálóból és a Remote Operation Viewer (Távoli műveletmegtekintő) VNC Microsoft Windows kliens alkalmazásból áll.

6. ábra A Távoli támogatáskezelői készlet (RSOK) telepítése



5. táblázat A Távoli támogatáskezelői készlet adatainak áttekintése

Leírás	Elküldött adatok	Protokoll	Port
VNC-jelszóhitelesítés	Felhasználói jelszó	DES titkosítás	5900
Műveletmegtekintő	Készülék irányítópultja – képernyőadatok – hardvereskulcs-művelet	Verzió 3.3 RFB protokoll	5900

FÜGGELÉK

A Canon imageRUNNER ADVANCE biztonsággal kapcsolatos funkciói

Az imageRUNNER ADVANCE platform távoli konfigurációt tesz lehetővé a Remote User Interface (távvezérlési kezelőfelület, RUI) néven ismert webes szolgáltatási felületen keresztül. Ez a felület hozzáférést biztosít a készülék konfigurációs beállításainak nagy részéhez, és le lehet tiltani, ha a használata nem engedélyezett, vagy le lehet védeni jelszóval a jogosulatlan hozzáférés megakadályozásához.

Jóllehet a készülék beállításainak többsége elérhető a távvezérlési kezelőfelületen, szükség van a készülék vezérlőpanelére is azoknak az elemeknek a beállításához, amelyek ezen a felületen keresztül nem konfigurálhatók. Javasoljuk, hogy tiltson le minden nem használt szolgáltatást. A rugalmasság és támogatás biztosításához a Távoli támogatáskezelői készlet (Remote Support Operators's Kit – RSOK) távoli hozzáférést biztosít a készülék kezelőpaneléhez. Ez VNC technológián alapul, amely egy kiszolgálóból (a készülék) és egy kliensből (a hálózati számítógép) áll. Rendelkezésre áll egy erre a célra alkalmas, ügyfélszámítógépre telepíthető megtekintőprogram a Canontól, amely szimulált hozzáférést biztosít a vezérlőpult billentyűihez.

Ez a szakasz áttekintést biztosít az imageRUNNER ADVANCE legfontosabb biztonsággal kapcsolatos funkcióiról és azok konfigurációjáról.

A készülék kezelése

A személyes adatok kiszivárgásának és a jogosulatlan használatnak a megakadályozásához állandó és hatékony biztonsági intézkedések szükségesek. Rendszergazda kijelölésével a készülék beállításainak, a felhasználóknak és a biztonsági beállításoknak a kezelése azokra a személyekre korlátozható, akik erre jogosultak.

Az alábbi hivatkozások a következőket részletezik:

- A készülék alapvető kezelése
- A hanyagságból, felhasználó hibájából és visszaélésből eredő kockázatok csökkentése
- Készülékkezelés
- A rendszerkonfiguráció és a beállítások kezelése

http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0001.html
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0037.html

IEEE P2600 szabvány

Számos imageRUNNER ADVANCE készülék megfelel az IEEE P2600 szabványnak, amely egy globális biztonsági szabvány multifunkciós perifériás eszközökhöz és nyomtatókhoz.

Az alábbi hivatkozáson elérhető weboldal ismerteti az IEEE 2600 szabványban meghatározott biztonsági követelményeket, és hogy a készülék funkciói hogyan teljesítik ezeket.
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0095.html#345_h1_01

IEEE 802.1X hitelesítés

Ha követelmény a 802.1X hálózathoz való csatlakozás, akkor a készüléknek hitelesítést kell végeznie, hogy igazolja a csatlakozásra való jogosultságát.

Az alábbi hivatkozásra kattintva megismerheti a rendelkezésre álló hitelesítési módszereket és konfigurációkat.
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0036.html#296_h1_01

Biztonsági házirend alkalmazása a készülékre

A legújabb imageRUNNER ADVANCE modellek lehetővé teszik a biztonsági beállítások és a biztonsági házirend batch formájában történő megadását a távvezérlési felületen keresztül. Különálló jelszóval biztosítható, hogy csak a biztonsági rendszergazda módosíthassa a beállításokat.

Az alábbi hivatkozáson elérhető weboldal a következőket részletezi:

- Jelszó használata a biztonsági házirend beállításainak védelmére
- A biztonsági házirend beállításainak konfigurálása
- A biztonsági házirend beállításainak elemei

http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0002.html

Felhasználók kezelése

A magasabb szintű biztonságot és hatékonyságot igénylő ügyfelek kihasználhatják a beépített funkcionalitás előnyeit, vagy alkalmazhatnak olyan nyomtatókezelési megoldást, mint a uniFLOW.

A nyomtatókezelési megoldások részleteinek megismerése érdekében forduljon a helyi képviselőinkhez vagy tekintse át a uniFLOW termékbrossúráját.

A hálózati biztonsági beállítások konfigurálása

A felhasználók nem várt adatvesztést tapasztalhatnak az adatok hálózaton át történő továbbításakor rosszindulatú harmadik felek támadásai, például hálózatlehallgatás, adathalászat és adatmanipulálás következtében. Ahhoz, hogy fontos és értékes adatait megvédje ezektől a támadásoktól a készülék a biztonság és a titokvédelem növelése érdekében a következő funkciókat támogatja.

http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0028.html

Merevlemez adatainak kezelése

A készülék merevlemezén tárolódik a készülék operációs rendszere, konfigurációi és feladatai. A legtöbb készülékmodell teljes merevlemez titkosítást biztosít (FIPS 140-2 kompatibilis), amellyel a merevlemezt az adott készülékkel párosítja, és megakadályozza, hogy azt jogosulatlan személyek leolvashassák. A Canon MFP biztonság chip kriptográfiai modulként tanúsítvánnyal rendelkezik, teljesítve az USA és Kanada által létrehozott Cryptographic Module Validation Program (Kriptográfiai Modulellenőrzési Program, CMVP), valamint a Japan Cryptographic Module Validation Program (Japán Kriptográfiai Modulellenőrzési Program, JCMVP) előírásait.

http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0092.html

A BIZTONSÁGI HÁZIREND BEÁLLÍTÁSAINAK ÁTTEKINTÉSE

Az imageRUNNER ADVANCE harmadik generációjához tartozó modellek bevezetik a biztonsági házirend beállításait és a biztonsági rendszergazda alkalmazásának lehetőségét. Ez megköveteli, hogy a rendszergazda sikeresen bejelentkezzen, és ha konfigurálva van, akkor biztonsági rendszergazdaként további bejelentkezésre van szükség jelszó megadásával.

Az alábbi táblázat részletezi a rendelkezésre álló beállításokat.

1. Illesztőfelület	Megjegyzések
Vezeték nélküli kapcsolat házirendje	
Letiltja a közvetlen csatlakozás használatát	A <Wi-Fi Direct használata (Use Wi-Fi Direct)> beállítása <Ki (Off)> állapotba. Mobilkészülékekről nem lehet a nyomtatót elérni.
Vezeték nélküli LAN használatának letiltása	A <Vezetékes/vezeték nélküli LAN kiválasztása (Select Wired/Wireless LAN)> beállítása <Vezetékes LAN (Wired LAN)> állapotba. Nem lehet vezeték nélküli kapcsolatot létrehozni a készülékkel vezeték nélküli LAN routeren vagy hozzáférési ponton keresztül.
USB-házirend	
USB-eszköz használatának letiltása	A <Használat USB-eszközként (Use as USB Device)> beállítása <Ki (Off)> állapotba. Ha az USB-eszközként való használat le van tiltva, akkor nem lehet USB-n keresztül csatlakoztatott számítógépekről használni a nyomtatási vagy beolvasási funkciót.
USB-tárolóeszközként való használat letiltása	Az <USB-tárolóeszköz használata (Use USB Storage Device)> beállítása <Ki (Off)> állapotba. Nem lehet USB-tárolóeszközöket használni. Az alábbi szervizfunkciók azonban akkor is működnek, ha az „USB-tárolóeszközként való használat letiltása” beállítá BE (ON) állapotban van. • Firmware-frissítés USB-adathordozóról (a letöltési üzemmódból) • Részleges naplóadatok másolása a készülékről USB-eszközre. (LOG2USB) • Jelentés másolása a készülékről USB-eszközre (RPT2USB)
Hálózati kommunikációs működési házirend Megjegyzés: Ezek a beállítások IEEE 802.1X hálózatokkal való kommunikációra nem vonatkoznak, még akkor sem ha a [TLS használatakor mindig ellenőrizze a kiszolgálói tanúsítványt (Always Verify Server Certificate When Using TLS)] jelölőnégyzete be van jelölve.	
Mindig ellenőrizze az SMS/WebDAV kiszolgálói funkciók aláírásait	Az <SMB-kiszolgálói beállítások (SMB Server Settings)> -ban az <SMB-aláírás megkövetelése csatlakozáshoz (Require SMB Signature for Connection)> és az <SMB-hitelesítés használata (Use SMB Authentication)> lehetőségeknél a <Be (On)> beállítás van megadva, a <TLS használata (Use TLS)> a <WebDAV-kiszolgálói beállítások (WebDAV Server Settings)> -ban szintén <Be (On)> állapotra van beállítva. Ha a készüléket SMB-kiszolgálóként vagy WebDAV-kiszolgálóként használják, akkor a készülék ellenőrzi a digitális tanúsítvány aláírásait a kommunikáció során.
TLS használatakor mindig ellenőrizze a kiszolgálói tanúsítványt	A <TLS-tanúsítvány megerősítése WebDAV TX-hez (Confirm TLS Certificate for WebDAV TX)>, <TLS-tanúsítvány megerősítése SMTP TX-hez (Confirm TLS Certificate for SMTP TX)>, <TLS-tanúsítvány megerősítése POP RX-hez (Confirm TLS Certificate for POP RX)>, <TLS-tanúsítvány megerősítése hálózati hozzáféréshez (Confirm TLS Certificate for Network Access)> és a <TLS-tanúsítvány megerősítése MEAP alkalmazással (Confirm TLS Certificate Using MEAP Application)> is mind a <Be (On)> értékre van beállítva, és ki van pipálva a <CN>. Ezenkívül a <Kiszolgálói tanúsítvány ellenőrzése (Verify Server Certificate)> és a <CN ellenőrzése (Verify CN)> beállítások a <SIP-beállítások (SIP Settings)> > <TLS-beállítások (TLS Settings)> -ban a <Be (On)> beállítás van megadva. A TLS-kommunikáció során a készülék ellenőrzi a digitális tanúsítványokat és azok neveit.
Tiltsa le az egyszerű szöveges hitelesítést a kiszolgálói funkcióknál.	• Az <FTP-nyomtatás használata (Use FTP Printing)> az <FTP-nyomtatási beállítások (FTP Print Settings)> -ban a <Ki (Off)> állapotra van beállítva. • A <TLS engedélyezése (SMTP RX) (Allow TLS (SMTP RX))> az < E-Mail/I-Fax Beállítások (E-Mail/I-Fax Settings)> <Kommunikációs Beállítások (Communication Settings)>-ban a <Mindig TLS (Always TLS)> állapotra van állítva, míg a <Dedikált Porthitelesítés (Dedicated Port Authentication Method)> a <Hálózat (Network)> beállításokban a <2. mód (Mode 2)>-ra van beállítva. • a <TLS használata (Use TLS)> a <WebDAV-kiszolgálói beállítások (WebDAV Server Settings)> -ban a <Be (On)> állapotra van beállítva. Ha a készüléket kiszolgálóként használja, az egyszerű szöveges hitelesítést használó funkciók nem állnak rendelkezésre. Ha az egyszerű szöveges hitelesítés le van tiltva, a készülék TLS-t használ. Ezen túlmenően nem fog tudni olyan alkalmazásokat vagy kiszolgálói funkciókat, például FTP-t használni, amelyek csak az egyszerű szöveges hitelesítést támogatják. Előfordulhat, hogy nem lehet elérni a készüléket eszközkezelő szoftverrel vagy illesztőprogrammal
SNMPv1 használatának letiltása	Az <SNMP-beállítások (SNMP Settings)> -ban az <SNMPv1 használata (Use SNMPv1)> <Ki (Off)> állapotra van beállítva. Ha le van tiltva az SNMPv1 használata, akkor előfordulhat, hogy nem lehet lekérni a készülékadatokat a nyomtatóillesztő-programból vagy a felügyeleti szoftverből, vagy nem lehet beállítani azokat.
Porthasználati házirend	
LPD-port korlátozása	Portszám: 515 Az <LPD-nyomtatási beállítások (LPD Print Settings)> a <Ki (Off)> értékre van beállítva. Nem lehet LPD-nyomtatást végezni.
RAW-port korlátozása	9100-as portszám A <RAW-nyomtatási beállítások (RAW Print Settings)> a <Ki (Off)> állapotra van beállítva. Nem lehet RAW-nyomtatást végezni.
FTP-port korlátozása	21-es portszám Az <FTP-nyomtatási beállítások (FTP Print Settings)> -ban az <FTP-nyomtatás használata (Use FTP Printing)> a <Ki (Off)> állapotra van beállítva. Nem lehet FTP-nyomtatást végezni.
WSD-port korlátozása	3702-es, 60000-es portszám A <WSD-beállítások (WSD Settings)> -ban a <WSD használata (Use WSD)>, <WSD-böngészés használata (Use WSD Browsing)> és a <WSD-beolvasás használata (Use WSD Scan)> beállításoknál mindnél a <Ki (Off)> érték van megadva. Nem lehet WSD-funkciókat használni.

BMLinkS-port korlátozása	1900-as portszám Az európai régióban nem használatos.
IPP-port korlátozása	631-es portszám Ha az IPP-port korlátozva van, nem fogja tudni használni a Mopria, az AirPrint és az IPP funkciót.
SMB-port korlátozása	Portszám: 137, 138, 139, 445 Az <SMB-kiszolgálói beállítások (SMB Server Settings)> -ban az <SMB-kiszolgáló használata (Use SMB Server)> megadott értéke a <Ki (Off)>. A készüléket nem lehet SMB-kiszolgálóként használni.
SMTP-port korlátozása	25-ös portszám Az <E-mail/I-Fax beállításai (E-Mail/I-Fax Settings)> > <Kommunikációs beállítások (Communication Settings)> -ban az <SMTP RX> funkció <Ki (Off)> állapotra van beállítva. Az SMTP-fogadás nem lehetséges.
Dedikált port korlátozása	Portszám: 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545–47547 Ha a dedikált port korlátozva van, nem fogja tudni használni a távoli másolás, távoli faxolás, távoli beolvasás és távoli nyomtatás funkciókat vagy alkalmazásokat stb.
A távoli operátori szoftver portjának korlátozása	5900-as portszám A <Távoli művelet beállításai (Remote Operation Settings)> megadott értéke a <Ki (Off)>. Nem lehet a távoli műveleti funkciókat használni.
SIP (IP-fax) portjának korlátozása	Portszám: 5004, 5005, 5060, 5061, 49152 Az <Intranet használata (Use Intranet)> az <Intranetes beállítások (Intranet Settings)>, az <NGN használata (Use NGN)> az <NGN-beállítások (NGN Settings)> és a <VoIP-átjáró használata (Use VoIP Gateway)> a <VoIP-átjáróbeállítások (VoIP Gateway Settings)> -ban mind <Ki (Off)> értékre van beállítva. Nem lehet IP-faxot használni.
mDNS-port korlátozása	5353-as portszám Az <mDNS-beállítások (mDNS Settings)> -ban az <IPv4 mDNS használata (Use IPv4 mDNS)> és az <IPv6 mDNS használata (Use IPv6 mDNS)> beállítások mindegyikénél a <Ki (Off)> érték van megadva. A <Mopria használata (Use Mopria)> beállítása <Ki (Off)> állapotba. Nem lehetséges keresni a hálózaton vagy automatikus beállításokat megadni az mDNS használatával. Nyomtatni sem lehet a Mopria™ vagy az AirPrint használatával.
SLP-port korlátozása	427-es portszám A <Multicast felderítési beállítások (Multicast Discovery Settings)> beállításnál a <Válasz (Response)> értéke <Ki (Off)> állapotra van beállítva. Nem lehetséges keresni a hálózaton vagy automatikus beállításokat megadni az SLP használatával.
SNMP-port korlátozása	161-es portszám Ha le van tiltva az SNMP-port, akkor előfordulhat, hogy nem lehet lekérni a készülékadatokat a nyomtatóillesztő-programból vagy a felügyeleti szoftverből, vagy nem lehet beállítani azokat. Az <SNMP-beállítások (SNMP Settings)> megadásakor az <SNMPv1 használata (Use SNMPv1)> és az <SNMPv3 használata (Use SNMPv3)> beállítások értéke <Ki (Off)> állapotra van beállítva.

2. Hitelesítés	Megjegyzések
Hitelesítési működési házirend	
Vendégfelhasználók letiltása	• A <Speciális helybeállítások (Advanced Space Settings)> <Hitelesítéskezelés (Authentication Management)> beállítása <Be (On)> állapotra van beállítva • A <Bejelentkezési képernyő megjelenítési beállításai (Login Screen Display Settings)> a <Megjelenítés a készülék működésnek megkezdésekor (Display When Device Operation Starts)> állapotra van beállítva • A <Felhasználói hitelesítés nélküli távoli eszközről érkező feladat korlátozása (Restrict Job from Remote Device without User Auth.)> beállítása <Be (On)> állapotra A nem regisztrált felhasználók nem tudnak bejelentkezni a készülékre. A számítógépről küldött nyomtatási feladatok szintén törlődnek.
Automatikus kijelentkezés beállításának kényszerítése	Ez a beállítás a kezelőpanelről való kijelentkezést szolgálja. Ez más kijelentkezési módszerekre nem vonatkozik (a beállítható értéktartomány 10 mp–9 perc). Az <Automatikus visszaállítás időzítése (Auto Reset Time)> engedélyezett. Ha a megadott ideig nem végeznek műveletet, a készülék a felhasználót automatikusan kijelentkezteti. A távvezérlési kezelőfelület beállítási képernyőjén válassza ki az [Időzítőegység általi kijelentkeztetés (Time Until Logout)] beállítást.
Jelszómegadási működési házirend	
Tiltsa le a jelszó külső kiszolgálókhoz történő tárolását	Ez a beállítás nem vonatkozik a felhasználó által kifejezetten mentett jelszavakra, például a címjegyzékek jelszavaira stb. A <Hitelesítési jelszó gyorsítótárazásának letiltása (Prohibit Caching of Authentication Password)> beállítása <Be (On)> állapotra. A felhasználóknak mindig jelszót kell megadniuk külső kiszolgálók elérésekor.
Figyelmeztetés megjelenítése, amikor az alapértelmezett jelszó használatban van	A <Figyelmeztetés megjelenítése, amikor az alapértelmezett jelszó használatban van (Display Warning When Default Password Is in Use)> beállítása <Be (On)> állapotra. Figyelmeztető üzenet jelenik meg, amikor a készülék gyári alapértelmezett jelszavát használják.
Alapértelmezett jelszó használatának letiltása távoli hozzáféréskor	Az <Alapértelmezett jelszó használatának engedélyezése távoli hozzáféréskor (Allow Use of Default Password for Remote Access)> beállítása <Ki (Off)> állapotra. Nem lehet a gyári alapértelmezett jelszót használni, amikor a készüléket egy számítógépről éri el
Jelszóbeállítási házirend (a házirend nem vonatkozik a részleg azonosítóinak kezelésére vagy a PIN-kódra)	
Jelszavankénti minimális karakterszám megadása	A karakterek minimális számát 1 és 32 közötti értékre lehet beállítani.
Jelszó érvényességi időszakának beállítása	Az érvényességi időszakot 1 és 180 nap közötti értékre lehet beállítani.
3 egymást követő azonos karakter használatának letiltása	
Legalább 1 nagybetűs karakter használatának kényszerítése	
Legalább 1 kisbetűs karakter használatának kényszerítése	
Legalább 1 szám használatának kényszerítése	
Legalább 1 szimbólum használatának kényszerítése	
Kizárási házirend	
Kizárás engedélyezése	Nem vonatkozik a részlegazonosítóra/postafiók PIN-kódjára vagy a biztonságos nyomtatás hitelesítésére stb. Kizárási küszöbérték: 1 és 10 alkalom közötti lehet Kizárási időszak: 1 és 60 perc közötti lehet

3. Kulcs/tanúsítvány	Megjegyzések
Gyenge titkosítás használatának letiltása	Az IPSec, TLS, Kerberos, S/MIME, SNMPv3 és a vezeték nélküli LAN beállításaira vonatkozik. Nem fog tudni a csak gyenge titkosítást támogató készülékekkel kommunikálni.
Gyenge titkosítással rendelkező kulcs/tanúsítvány használatának letiltása	Az IPSec, TLS és S/MIME beállításokra vonatkozik. Ha gyenge titkosítással rendelkező kulcsot/tanúsítványt használ a TLS-hez, az le fog cserélődni az előre telepített kulcsra/tanúsítványra. Ha a TLS-en kívül más funkciókhoz használ gyenge titkosítással rendelkező kulcsot/tanúsítványt, nem fog tudni kommunikálni.
Platformmegbízhatóság modul (TPM) használata a jelszó és kulcs tárolására	Csak a telepített TPM-mel rendelkező készülékekhez áll rendelkezésre. Ha a TPM engedélyezve van, mindig készítsen biztonsági másolatot a TPM-kulcsokról. Részleteket a felhasználói útmutatóban talál. Fontos a TPM-beállítások engedélyezésekor: • Változtassa meg a „rendszergazdai" jelszó alapértelmezett értékét, hogy a rendszergazdán kívül más külső személy ne tudjon biztonsági másolatot készíteni a TPM-kulcsról. Ha egy külső fél megszerzi a TPM biztonsági másolat kulcsát, akkor nem fogja tudni visszaállítani a TPM-kulcsot. • A fokozott biztonság miatt a TPM-kulcsról csak egyszer lehet biztonsági másolatot készíteni. Ha engedélyezve vannak a TPM-beállítások, készítsen biztonsági másolatot a TPM-kulcsról egy USB-memóriaeszközre, és tárolja azt biztonságos helyen az elvesztésének vagy ellopásának megakadályozása érdekében. • A TPM által nyújtott biztonsági funkciók nem garantálják az adatok vagy a hardver teljeskörű védelmét.

4. Napló	Megjegyzések
Auditálási napló rögzítésének kényszerítése	• A <Műveleti napló mentése (Save Operation Log)> beállítása <Be (On)> állapotra • A <Feladatnapló megjelenítése (Display Job Log)> beállítása <Be (On)> állapotra • A <Feladatnapló lekérése a felügyeleti szoftverrel (Retrieve Job Log with Management Software)> beállítás a <Feladatnapló megjelenítése (Display Job Log)> menüpontban az <Engedélyezés (Allow)> állapotra van beállítva • Az <Auditálási napló mentése (Save Audit Log)> beállítása <Be (On)> állapotra • A <Hálózati hitelesítési napló lekérése (Retrieve Network Authentication Log)> beállítása <Be (On)> állapotra Ha ez a beállítás engedélyezve van, a készülék mindig rögzíti az auditálási naplókat.
SNTP-beállítások kényszerítése	SNTP-kiszolgáló címének megadása Az <SNTP-beállítások (SNTP Settings)> -ban az <SNTP használata (Use SNTP)> beállítása <Be (On)> állapotba. A pontos idő SNTP-n keresztüli szinkronizálása szükséges. Adjon meg egy értéket a [Kiszolgálónév (Server Name)] számára távvezérlési kezelőfelület beállítási képernyőjén.

5. Munka	Megjegyzések
Nyomtatási házirend	
Fogadott feladatok azonnali nyomtatásának megakadályozása	A fogadott feladatok a fax/I-Fax memóriájában lesznek tárolva, ha a fogadott feladatok azonnali nyomtatása le van tiltva. • A <Továbbítási hibákkal rendelkező fájlok kezelése (Handle Files with Forwarding Errors)> beállítása <Ki (Off)> állapotra • A <Faxmemóriazár használata (Use Fax Memory Lock)> beállítása <Be (On)> állapotra • Az <I-Fax-memóriazár használata (Use I-Fax Memory Lock)> beállítása <Be (On)> állapotra • A <Memóriazárolás befejezési ideje (Memory Lock End Time)> beállítása <Ki (Off)> állapotra • A <Nyomat megjelenítése a nyomtatóillesztőből való tároláskor (Display Print When Storing from Printer Driver)> a <Bizalmas beérkező faxok beállítása/regisztrálása (Set/Register Confidential Fax Inboxes)> -ban a <Ki (Off)> állapotra van beállítva • A <Beállítások minden postafiókhoz (Settings for All Mail Boxes)> <Nyomtatás a nyomtatóillesztő-programból való tároláskor (Print When Storing from Printer Driver)> beállítása <Ki (Off)> állapotra • A <Postaláda biztonsági beállításai (Box Security Settings)> menüben a <Nyomat megjelenítése a nyomtatóillesztőből való tároláskor (Display Print When Storing from Printer Driver)> beállítása <Ki (Off)> állapotra • Az <Ismeretlen felhasználótól érkező feladat letiltása (Prohibit Job from Unknown User)> beállítása <Be (On)> állapotra és a <Kényszerített tartás (Forced Hold)> beállítása <Be (On)> állapotra. A nyomtatás még akkor sem indul el azonnal, ha elvégzik a nyomtatási műveleteket.
Küldési/fogadási házirend	
Csak a regisztrált címekre történő küldés engedélyezése	Az <Új címzett korlátozása (Limit New Destination)> beállításban a <Fax>, <E-Mail>, <I-Fax> és <Fájl (File)> beállítások megadott értéke a <Be (On)> állapotra. Csak azokra a címekre lehetséges a küldés, amelyek regisztrálva vannak a címjegyzékben.
Faxszám megerősítésének kényszerítése	A felhasználóknak fax küldésekor kötelező megerősítés céljából újra megadniuk a faxszámot.
Automatikus továbbítás letiltása	A <Továbbítási beállítások használata (Use Forwarding Settings)> beállítása <Ki (Off)> állapotra. Nem lehet a faxokat automatikusan továbbítani.

6. Tárolás	Megjegyzések
Adatok teljes törlésének kényszerítése	A <Merevlemez adatainak teljes törlése (Hard Disk Data Complete Deletion)> beállítása <Be (On)> állapotra

Canon Inc.
canon.com

Canon Europe
canon-europe.com

Canon Hungária Kft.
1031 Budapest,
Graphisoft Park 1. (Záhony utca 7.)
Telefon: (+361) 2375904
Fax: (+361) 2375901
canon.hu

Hungarian edition