

MPC-2610

Biztonsági óvintézkedések

Ez a Súgó útmutató az egység használatával történő fájlvitellel és streameléssel kapcsolatos biztonsági óvintézkedéseket ismerteti.

[Biztonsági óvintézkedések](#)[Az internetes kapcsolatra vonatkozó figyelmeztetések](#)[A hálózati funkcióra vonatkozó figyelmeztetések](#)[Vezeték nélküli hálózattal kapcsolatos figyelmeztetések](#)[Az USB internetmegosztással kapcsolatos figyelmeztetések](#)[Az FTPES \(FTPS\) funkció rövid leírása](#)

Biztonsági óvintézkedések

Ez a témakör az egység hálózati csatlakoztatásával kapcsolatos figyelmeztetéseket ismerteti.

- A jelek környezetében illetéktelenek észrevétlenül lehallgathatják a kommunikáció tartalmát. Vezeték nélküli hálózati kommunikáció használatakor védje megfelelő biztonsági intézkedésekkel a kommunikáció tartalmát.
- Ha a [Security] vezetéknélküli LAN beállítást [None]-ra állítja, és így csatlakozik hozzáférési ponthoz, a kamera és a hozzáférési pont közötti vezetéknélküli kommunikáció nem lesz titkosítva, és a jel hatótávolságán belül lehallgatható. A fokozott biztonság érdekében használja a WPA2 vagy WPA3 biztonsági protokollt.
- A SONY SEMMINEMŰ FELELŐSSÉGET NEM VÁLLAL AZ ÁTVITELI ESZKÖZÖKRE VONATKOZÓ KELLŐ BIZTONSÁGI INTÉZKEDÉSEK ELMULASZTÁSÁBÓL, AZ ÁTVITELI SPECIFIKÁCIÓK MIATT ELKERÜLHETETLEN ADATSZIVÁRGÁSOKBÓL VAGY BÁRMINEMŰ BIZTONSÁGI GONDBÓL FAKADÓ SEMMILYEN KÁRÉRT.
- Az üzemi környezettől függően előfordulhat, hogy illetéktelenek hozzáférnek a készülékhez a hálózaton. A készülék hálózatra kapcsolásakor ellenőrizze, hogy kellően biztonságos-e a hálózat.
- Ha hálózatra kapcsolja ezt a terméket, iktasson közbe védelmi funkciót, például útválasztót vagy tűzfalat. Ilyen védelem nélkül veszélyeztetheti a termék biztonságát.

TP1002221065

Az internetes kapcsolatra vonatkozó figyelmeztetések

Ez a témakör az internetes csatlakoztatással kapcsolatos figyelmeztetéseket ismerteti.

- Az egység nem tud vezeték nélküli LAN hálózaton csatlakozni olyan hozzáférési ponthoz, amely csak WEP vagy WPA biztonsági protokollt használ, mivel ezek sérülékenyek.
- Az egység nem hálózati eszköz (útválasztó, kapcsoló stb.). Nyomatékosan ajánljuk, hogy az egységet olyan hálózathoz csatlakoztassa, ahol a hálózati beállításokat megfelelően konfigurálhatja és kezelheti, hogy megvédje DoS (szolgáltatásmegtagadási) és hasonló támadásoktól.
- Az egységet megfelelően konfigurált és kezelt útválasztó vagy ilyen funkcióval rendelkező LAN-port útján csatlakoztassa hálózatra. Ilyen védelem nélkül (például ingyenes Wi-Fi használatkor) veszélyeztetheti biztonságát. Megfelelő konfigurálás esetén az útválasztók megfelelő védelmet nyújtanak a DoS-támadások vagy a hálózati eszközök működésének kiesése ellen. Ha bármilyen rendellenességet észlel, azonnal válassza le a kamerát a hálózatról.

TP1002221066

A hálózati funkcióra vonatkozó figyelmeztetések

Ez a témakör az egység hálózati funkcióival kapcsolatos figyelmeztetéseket ismerteti.

- Ha jogosulatlan hozzáférést észlel, a kamera elutasíthatja a kommunikáció fogadását. Ilyen esetben ismételje meg a csatlakoztatást.
- Az egységhez való csatlakozáshoz szükséges hitelesítési adatok a [Network] – [Network Setup] – [Show Authentication] használatkor jelennek meg. Vigyázzon, hogy mások ne láthassák a képernyőt és ne másolhassák le a QR-kódot.
- A felhasználónevet és a jelszót a vásárláskor kell beállítani. Felhasználóneve és a jelszava beállításakor ügyeljen arra, hogy mások ne láthassák őket. A felhasználónevet és jelszót a következők szerint állítsa be.

[User Name]	– Állítson be egy 1–16 karakterből álló felhasználónevet. – A gyári alapértelmezett felhasználónév „admin”. – A következő beviteli karakterek tekinthetők érvényesnek. Betűk (nagy- és kisbetűk), számok, szimbólumok (! % + , - . = _)
[Password]	– Állítson be egy 8–16 karakterből álló jelszót, legalább 1 betűvel és 1 számjeggyel. – A következő beviteli karakterek tekinthetők érvényesnek. Betűk (nagy- és kisbetűk), számok, szimbólumok (! % + , - . = _)

TP1002221067

Vezeték nélküli hálózattal kapcsolatos figyelmeztetések

Ez a témakör a vezeték nélküli hálózati csatlakozással kapcsolatos figyelmeztetéseket ismerteti.

- Az egység Súgó útmutatójában a vezeték nélküli LAN-hozzáférési pontokat és a LAN-kapcsolatot használó vezeték nélküli LAN-útválasztók mint „hozzáférési pontok” szerepelnek.
- A [Security] (titkosítási módszer) beállítása [None], [WPA2] vagy [WPA3] lehet. Biztonsági szempontból a [WPA2] vagy [WPA3] beállítás használatát ajánljuk. A [None] lehetőség választásakor a csatlakozás előtt üzenet jelenik meg. A vezeték nélküli LAN-kapcsolat biztonsága érdekében nyomatékosan ajánljuk WPA2 vagy WPA3 biztonsági beállítású hozzáférési pontok használatát.
- Vezeték nélküli hálózati hozzáférési pont [Manual Register] útján történő választásakor az alapértelmezett biztonsági módszer WPA2 lesz.
- Ha biztonsági beállítások nélkül csatlakozik egy hozzáférési ponthoz, akkor hackereknek, rosszindulatú betolakodóknak vagy támadásoknak lehet kitéve. Biztonsági beállítás nélküli csatlakozást csak akkor használjon, ha már nincs más lehetőség.
- Nagyon fontos a biztonság beállítása egy vezeték nélküli LAN hálózaton. A Sony nem vállal felelősséget az elmulasztott biztonsági intézkedésekből eredő károkért, vagy vezeték nélküli LAN használata során elkerülhetetlen körülmények miatt fellépő biztonsági problémákért.

TP1002221068

Az USB internetmegosztással kapcsolatos figyelmeztetések

Ez a témakör az USB internetmegosztással történő csatlakozással kapcsolatos figyelmeztetéseket ismerteti.

- Az internetmegosztáshoz csak megbízható okostelefont használjon. Ismeretlen eredetű eszközökhöz való kapcsolódás biztonsági okokból nem ajánlott.

TP1002221069

Az FTPES (FTPS) funkció rövid leírása

Az FTPS funkció különféle titkosító algoritmusokat támogat a biztonságos fájlátvitelhez. A szerverek széles skálájával való kompatibilitás érdekében többféle titkosító algoritmust támogat, amelyek közül néhány nem feltétlenül felel meg a jelenlegi legjobb biztonsági megoldásoknak.

A FTPS funkció által támogatott titkosító algoritmusok

A következő titkosító algoritmusokat támogatja.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Ajánlott titkosító algoritmusok

A NIST ajánlások (NIST SP 800-57 Part 1 Revision 5) és kapcsolódó biztonsági szabványok alapján a következő titkosító algoritmusok használatát ajánljuk.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Elavult titkosító algoritmusok

Az FTPS funkció a kompatibilitás érdekében a következő algoritmusokat is támogatja, de ezek a NIST ajánlásai (NIST SP 800-57 Part 1 Revision 5) és a kapcsolódó biztonsági szabványok szerint elavultak, és egy későbbi verzióban eltávolításra kerülhetnek.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

A kapcsolat kompatibilitása

Az FTPS funkció a biztonság és a kompatibilitás között egyensúlyoz. Pillanatnyilag a következő okokból támogat elavult algoritmusokat, de előfordulhat, hogy ezek el lesznek távolítva egy későbbi verzióból a biztonság javítása végett.

- Szabadúszó fotósoknak és videósoknak különböző klienseken futó szerverekhez kell csatlakozniuk.
- Emiatt fenn kell tartani a kompatibilitást a régebbi rendszerekkel és a hagyományos szerverekkel.
- Nem minden felhasználó hajlandó biztonságosabb beállításra váltani, mivel bonyolult a titkosító algoritmus beállításainak megváltoztatása a szerveroldalon.
- Az FTPS-beállítások gyakran kerülnek megosztásra más biztonságos szolgáltatásokkal. Minden változtatást figyelembe kell venni, mert hatással lehetnek a szerver más szolgáltatásaira.
- Az interoperabilitás különböző környezetekben való biztosításához titkosító algoritmusok széles körét kell támogatni.

Az FTPS-kapcsolat során használt titkosító algoritmust a célszerverrel végzett automatikus egyeztetés határozza meg, ezért ez a szerver beállításaitól függ. A biztonsági kockázatok tudatában jelenleg a kompatibilitás élvez elsőbbséget, hogy a felhasználók sokféle igényét kielégítsük.

Biztonsági kockázatok

A CBC/DHE/RSA/SHA-1 és más elavult algoritmusok használata növeli annak kockázatát, hogy a titkosított adatokat illetéktelenek visszafejtek vagy meghamisítják, és az adatok átvitel közben hozzáférhetővé válnak.

Ajánlás a kapcsolat biztonságossá tételére

Az FTPS funkció használata előtt ellenőrizze, hogy a kapcsolat célszervere támogatja-e az ajánlott titkosító algoritmust. Csak az ajánlott algoritmusokat engedélyezze a szerveroldalon, és tiltsa le az elavult algoritmusokat.

Feltöltés biztonságos FTP protokollal

A fájlokat titkosítva, FTPS-sel, Explicit módban (FTPES) töltheti fel a célfájlszerverre.

Biztonságos FTP átvitelhez a fájltviteli célszerver beállítás [Using Secure Protocol] pontját állítsa [On] értékre és importáljon tanúsítványt.

Hivatkozott szakirodalom

- Recommendation for Key Management, Special Publication 800-57 Part 1 Revision 5, NIST, 2020.
- Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication 800-131A Revision 2, NIST, 2019.
- Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, NIST, 2005 (tartalmazza a 2016.10.06-i frissítéseket).

Tanúsítvány

Az FTPES (FTPS) funkció által használt tanúsítványt írja be a memóriakártya gyökérkönyvtárába. A fájl nevét a következőképpen állítsa be.

certification.pem (PEM formátum)

A betölthető tanúsítványok maximális mérete tanúsítványonként 1 MB.

TP1002221070