

Tento sprievodca s nápo vedou opisuje bezpečnostné opatrenia pre prenos súborov a streamovanie pomocou jednotky.

[Bezpečnostné opatrenia](#)

[Bezpečnostné opatrenia týkajúce sa internetového pripojenia](#)

[Bezpečnostné opatrenia súvisiace so sieťovou funkciou](#)

[Bezpečnostné opatrenia týkajúce sa bezdrôtovej siete LAN](#)

[Bezpečnostné opatrenia týkajúce sa USB tetheringu](#)

[Informácie o funkcii FTPES \(FTPS\)](#)

Bezpečnostné opatrenia

Táto téma opisuje opatrenia, ktoré je potrebné dodržiavať pri pripájaní jednotky do siete.

- Komunikačný obsah môžu nevedomky zachytiť neoprávnené tretie strany v blízkosti signálov. Ak používate komunikáciu prostredníctvom bezdrôtovej siete LAN, správne implementujte bezpečnostné opatrenia na ochranu komunikačného obsahu.
- Ak nastavíte bezdrôtovú sieť LAN [Security] na hodnotu [None] a pripojíte sa k prístupovému bodu, bezdrôtová komunikácia medzi kamerou a prístupovým bodom nebude šifrovaná a môže ju zachytiť tretia strana v dosahu signálu. Na zvýšenie bezpečnosti použite bezpečnostný protokol WPA2 alebo WPA3.
- **SONY NEPREBERÁ ZODPOVEDNOSŤ ZA ŠKODY AKÉHOKOL'VEK DRUHU VYPLÝVAJÚCE Z NEVYKONANIA RIADNYCH BEZPEČNOSTNÝCH OPATRENÍ NA PRENOSOVÝCH ZARIADENIACH, ZA NEODVRÁTITEĽNÉ ÚNIKY ÚDAJOV, KTORÉ VYPLÝVAJÚ ZO ŠPECIFIKÁCIE PRENOSU, ALEBO ZA BEZPEČNOSTNÉ PROBLÉMY VŠETKÉHO DRUHU.**
- V závislosti na operačnom prostredí môžu neoprávnené tretie osoby v sieti získať prístup k zariadeniu. Pri pripojení zariadenia do siete sa uistite, že sieť je bezpečne chránená.
- Ak pripájate tento výrobok na sieť, pripájajte sa prostredníctvom systému, ktorý poskytuje funkciu ochrany, napríklad smerovač alebo firewall. Ak sa pripojíte bez takejto ochrany, môžu nastať problémy so zabezpečením.

TP1002221121

Bezpečnostné opatrenia týkajúce sa internetového pripojenia

Táto téma opisuje bezpečnostné opatrenia pri pripájaní jednotky do internetu.

- Jednotka sa nemôže pripojiť prostredníctvom bezdrôtovej siete LAN k prístupovému bodu, ktorý používa iba protokol WEP alebo WPA, čo sú metódy zabezpečenia, ktoré majú zraniteľnosti.
- Jednotka nie je sieťové zariadenie (napríklad smerovač alebo prepínací rozbočovač). Dôrazne sa odporúčame, aby ste jednotku pripojili k sieti, v ktorej môžete vhodne konfigurovať a spravovať sieťové nastavenia na ochranu pred sieťovými útokmi, ako sú útoky DoS (Denial of Service).
- Pri pripájaní jednotky k sieti ju pripojte cez smerovač, ktorý je vhodne nakonfigurovaný a spravovaný, alebo ju pripojte k portu LAN, ktorý má rovnakú funkciu. Ak sa pripojíte bez takejto ochrany (napríklad pri používaní bezplatného pripojenia Wi-Fi), môže dôjsť k bezpečnostným problémom. Pri správnej konfigurácii poskytujú smerovače dostatočnú ochranu proti útokom DoS alebo strate funkčnosti zariadení v sieti. Ak spozorujete niečo nezvyčajné, okamžite odpojte kameru od siete.

TP1002221122

Bezpečnostné opatrenia súvisiace so sieťovou funkciou

Táto téma opisuje bezpečnostné opatrenia týkajúce sa sieťových funkcií jednotky.

- Ak sa zistí neoprávnený prístup, kamera nemusí byť schopná prijímať komunikáciu. Ak k tomu dôjde, pripojte sa znova od začiatku.
- Informácie o overení pre pripojenie k jednotke sa zobrazia, keď použijete [Network] – [Network Setup] – [Show Authentication]. Dbajte na to, aby sa obrazovka nedala prezerať a aby obrázok QR kódu nemohli skopírovať iné osoby.
- Pri nákupe je potrebné nastaviť používateľské meno a heslo. Pri nastavovaní používateľského mena a hesla sa uistite, že tieto nastavenia nie sú viditeľné pre ostatných. Používateľské meno a heslo nastavte nasledujúcim spôsobom.

[User Name]	– Nastavte meno používateľa pozostávajúce z 1 až 16 znakov. – V predvolenom nastavení z výroby je hodnota nastavená na „admin“. – Platné sú tieto vstupné znaky. Abecedné znaky (veľké a malé písmená), číselné znaky, symboly (! % + , - . = _)
[Password]	– Nastavte heslo pozostávajúce z 8 až 16 znakov, ktoré obsahuje aspoň 1 alebo viac abecedných znakov a 1 alebo viac číselných znakov. – Platné sú tieto vstupné znaky. Abecedné znaky (veľké a malé písmená), číselné znaky, symboly (! % + , - . = _)

TP1002221123

Bezpečnostné opatrenia týkajúce sa bezdrôtovej siete LAN

Táto téma opisuje bezpečnostné opatrenia pri pripájaní jednotky prostredníctvom bezdrôtovej siete LAN.

- V sprievodcovi s nápo vedou pre túto jednotku sa bezdrôtová sieť LAN, prístupové body a bezdrôtové smerovače LAN, ktoré prenášajú pripojenia LAN, označujú ako „prístupové body“.
- [Security] (spôsob šifrovania) môžete nastaviť na [None], [WPA2] alebo [WPA3]. Z hľadiska bezpečnosti sa odporúča používať [WPA2] alebo [WPA3]. Pred pripojením sa zobrazí správa, ak je zvolená možnosť [None]. Pre bezpečné pripojenie k bezdrôtovej sieti LAN sa dôrazne odporúča pripojenie k prístupovým bodom s nastavením zabezpečenia WPA2 alebo WPA3.
- Pri registrácii bezdrôtového prístupového bodu LAN pomocou [Manual Register] je predvolene vybraná metóda zabezpečenia WPA2.
- Ak sa pripojíte k prístupovému bodu bez akéhokoľvek nastavenia zabezpečenia, môžete byť vystavení hackerskému útoku, prístupu zlomyseľných tretích strán alebo útokom na zraniteľné miesta. Ak to nie je nevyhnutné, pripojenie bez akéhokoľvek nastavenia zabezpečenia sa neodporúča.
- Konfigurácia zabezpečenia bezdrôtovej siete LAN je veľmi dôležitá. Spoločnosť Sony nenesie zodpovednosť za žiadne škody vyplývajúce z neprijatých bezpečnostných opatrení alebo ak sa vyskytne bezpečnostný problém v dôsledku nevyhnutných okolností pri používaní bezdrôtovej siete LAN.

TP1002221124

Bezpečnostné opatrenia týkajúce sa USB tetheringu

Táto téma opisuje opatrenia, ktoré je potrebné dodržiavať pri pripájaní jednotky prostredníctvom USB tetheringu.

- Na tethering používajte len dôveryhodné zariadenia smartfónu. Pripojenie k zariadeniam neznámeho pôvodu sa neodporúča z bezpečnostných dôvodov.

TP1002221125

Informácie o funkcii FTPES (FTPS)

Funkcia FTPS podporuje rôzne šifrovacie algoritmy na zabezpečenie bezpečného prenosu súborov. Na zabezpečenie kompatibility so širokou škálou serverov je podporovaných viacero šifrovacích algoritmov, z ktorých niektoré nemusia byť v súlade so súčasnými osvedčenými bezpečnostnými postupmi.

Šifrovacie algoritmy podporované funkciou FTPS

Podporované sú nasledujúce šifrovacie algoritmy.

- 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

Odporúčané šifrovacie algoritmy

Na základe odporúčaní NIST (NIST SP 800-57 časť 1 revízia 5) a súvisiacich bezpečnostných noriem sa odporúčajú nasledujúce šifrovacie algoritmy.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

O zastaraných algoritmo ch

Funkcia FTPS podporuje z dôvodu kompatibility aj nasledujúce algoritmy, ktoré sú však na základe odporúčaní NIST (NIST SP 800-57 časť 1 revízia 5) a súvisiacich bezpečnostných štandardov zastarané a v budúcej verzii môžu byť odstránené.

- 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

O kompatibilitě pripojenia

Funkcia FTPS je navrhnutá s ohľadom na rovnováhu medzi bezpečnosťou a kompatibilitou. V súčasnosti sú zastarané algoritmy podporované z nasledujúcich dôvodov, ale v budúcej verzii môžu byť odstránené s cieľom zlepšiť bezpečnosť.

- Fotografovia a kameramani na voľnej nohe sa musia pripájať k serverom, ktoré bežia na rôznych klientoch.
- Je potrebné zachovať kompatibilitu so staršími systémami a staršími servermi.
- Nie všetci používatelia sú pripravení prejsť na bezpečnejšie nastavenie, pretože zmena nastavení šifrovacieho algoritmu na strane servera je komplikovaná.
- Nastavenia FTPS sa často zdieľajú s inými zabezpečenými službami. Akékoľvek zmeny je potrebné starostlivo zvážiť, pretože môžu mať vplyv na ostatné služby na serveri.
- Na zabezpečenie interoperability v rôznych prostrediach je potrebné podporovať širokú škálu šifrovacích algoritmov.

Šifrovací algoritmus používaný počas pripojenia FTPS sa určuje automatickým vyjednávaním s cieľovým serverom, a preto závisí od nastavení servera. Hoci si uvedomujeme bezpečnostné riziká, v súčasnosti sa uprednostňuje kompatibilita, aby sa uspokojili rôzne potreby používateľov.

Bezpečnostné riziká

Používanie zastaraných algoritmov vrátane CBC/DHE/RSA/SHA-1 zvyšuje riziko, že zašifrované údaje môže útočník dešifrovať alebo s nimi manipulovať, čím sa údaje počas prenosu odhalia.

Odkazy

Pred použitím funkcie FTPS skontrolujte, či cieľový server pripojenia podporuje odporúčaný šifrovací algoritmus. Na strane servera povoľte iba odporúčané algoritmy a zakážte zastarané algoritmy.

Nahrávanie pomocou zabezpečeného FTP

Súbory môžete odosielať so šifrovaním pomocou protokolu FTPS v explicitnom režime (FTPES) pre spojenie s cieľovým súborovým serverom.

Pre zabezpečený prenos FTP nastavte [Using Secure Protocol] na [On] v nastaveniach cieľového servera prenosu súborov a importujte certifikát.

Odkazy

- 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 (obsahuje aktualizácie k 10. 6. 2016).

Certifikát

Zapíšte certifikát používaný funkciou FTPES (FTPS) do koreňového adresára pamätevej karty. Názov súboru nastavte takto.

certification.pem (formát PEM)

Maximálna veľkosť certifikátu, ktorú možno načítať, je 1 MB na certifikát.

TP1002221126