ILME-FX6

Previdnostni ukrepi

V tem Vodniku za pomoč so opisani previdnostni ukrepi za prenos datotek in pretakanje z enoto.

5-075-082-31(1) Copyright 2026 Sony Corporation

ILME-FX6
Previdnostni ukrepi

Previdnostni ukrepi

Ta tema opisuje previdnostne ukrepe pri povezovanju enote z omrežjem.

- Vsebino komunikacije lahko nevede prestrežejo nepooblaščene tretje osebe v bližini signalov. Ko uporabljate brezžično komunikacijo LAN, izvedite ustrezne varnostne ukrepe za zaščito vsebine komunikacije.
- Če nastavitev brezžičnega LAN [Security] nastavite na [None] in se povežete z dostopno točko, brezžična komunikacija med fotoaparatom in dostopno točko ne bo šifrirana in jo lahko prestreže tretja oseba v dosegu signala. Za večjo varnost uporabite varnostni protokol WPA2 ali WPA3.
- NOBENO ŠKODO, KI JE POSLEDICA NEIZVEDENIH USTREZNIH VARNOSTNIH UKREPOV GLEDE NAPRAV ZA PRENOS PODATKOV, IZGUBO PODATKOV, DO KATERE JE NEIZOGIBNO PRIŠLO ZARADI SPECIFIKACIJ PRENOSA PODATKOV, OZIROMA ZA KAKRŠNE KOLI TEŽAVE, POVEZANE Z VARNOSTJO.
- Do enote lahko morda dostop pridobijo tudi nepooblaščene tretje osebe, kar je odvisno od delovnega okolja. Ko enoto priključujete v omrežje, ne pozabite preveriti, ali je omrežje varno zaščiteno.
- Ta izdelek povežite v omrežje prek sistema, ki zagotavlja zaščitno funkcijo, kot je usmerjevalnik ali požarni zid. Če ga povežete brez omenjene zaščite, se lahko pojavijo težave z varnostjo.

TP1002274598

5-075-082-31(1) Copyright 2026 Sony Corporation

ILME-FX6
Previdnostni ukrepi

Previdnostni ukrepi za internetno povezavo

Ta tema opisuje previdnostne ukrepe pri povezovanju enote z internetom.

- Enota ne more vzpostaviti povezave prek brezžičnega omrežja LAN z dostopno točko, ki uporablja samo WEP ali WPA, ki sta varnostni metodi, ki imata ranljivosti.
- Enota ni omrežna naprava (na primer usmerjevalnik ali preklopno vozlišče). Priporočamo, da enoto povežete v omrežje, kjer lahko ustrezno konfigurirate in upravljate omrežne nastavitve, da se zaščitite pred napadi na omrežju, kot so napadi DoS (napadi zavrnitve storitve).
- Ko enoto povezujete v omrežje, jo povežite z usmerjevalnikom, ki je konfiguriran in ustrezno upravljan, ali pa jo povežite z vrati LAN, ki imajo enako funkcionalnost. Če je povezava vzpostavljena brez takšne zaščite (na primer pri uporabi brezplačnega omrežja Wi-Fi), lahko pride do varnostnih težav. Ko so usmerjevalniki pravilno konfigurirani, zagotavljajo zadostno zaščito pred napadi DoS ali izgubo funkcionalnosti naprav v omrežju. Če opazite karkoli nenavadnega, takoj odklopite kamero iz omrežja.

TP1002274599

5-075-082-31(1) Copyright 2026 Sony Corporation

ILME-FX6
Previdnostni ukrepi

Previdnostni ukrepi v zvezi s funkcijo omrežja

Ta tema opisuje previdnostne ukrepe glede funkcije omrežja enote.

- Če je zaznan nepooblaščen dostop, kamera morda ne bo mogla sprejeti komunikacije. Če se to zgodi, znova vzpostavite povezavo od začetka.
- Pritisnite gumb [Show Authentication] na zaslonu stanja [Network] da prikažete informacije za preverjanje pristnosti za povezavo z enoto. Pazite, da zaslona ni mogoče videti in da slike kode QR ne morejo kopirati drugi.
- Uporabniško ime in geslo se samodejno ustvarita in nastavita v kameri ob nakupu. Pri nastavljanju uporabniškega imena in gesla se prepričajte, da nastavitve niso vidne drugim. Ime uporabnika in geslo nastavite na naslednji način.

[User Name]	– Nastavite uporabniško ime z 1 do 16 znaki. – Privzeto je nastavljeno na »admin«. – Spodaj so prikazani veljavni vnosni znaki. Abecedni znaki (velike in male črke), številke, simboli (! % + , - . = _)
[Password]	– Nastavite geslo z 8 do 16 znaki, ki vključujejo vsaj 1 črko in vsaj 1 številko. – Spodaj so prikazani veljavni vnosni znaki. Abecedni znaki (velike in male črke), številke, simboli (! % + , - . = _)

TP1002274600

5-075-082-31(1) Copyright 2026 Sony Corporation

ILME-FX6
Previdnostni ukrepi

Previdnostni ukrepi v zvezi z brezžičnim omrežjem LAN

Ta tema opisuje previdnostne ukrepe pri povezovanju enote z brezžičnim LAN omrežjem.

- V Vodniku za pomoč za to enoto so dostopne točke brezžičnega LAN in usmerjevalniki brezžičnega LAN, ki posredujejo povezave LAN, poimenovani »dostopne točke«.
- [Security] (način šifriranja) lahko nastavite na [None], [WPA2] ali [WPA3]. Uporaba [WPA2] ali [WPA3] je priporočljiva z varnostnega vidika. Ko je izbrana [None], se pred vzpostavitvijo povezave prikaže sporočilo. Za varno brezžično povezavo LAN priporočamo povezavo z dostopnimi točkami z varnostno nastavitvijo WPA2 ali WPA3.
- Privzeto je izbrana varnostna metoda WPA2 pri registraciji dostopne točke brezžičnega LAN z uporabo [Manual Register].
- Če se povežete z dostopno točko brez varnostnih nastavitev, ste lahko žrtev vdora, dostopa zlonamernih tretjih oseb ali napadov na ranljivosti. Razen če se temu ni mogoče izogniti, povezava brez varnostnih nastavitev ni priporočljiva.
- Konfiguriranje varnosti v brezžičnem omrežju LAN je zelo pomembno. Družba Sony ne odgovarja za morebitno škodo, ki bi nastala zaradi neupoštevanja varnostnih ukrepov ali če bi prišlo do varnostne težave zaradi neizogibnih okoliščin pri uporabi brezžičnega omrežja LAN.

TP1002274601

5-075-082-31(1) Copyright 2026 Sony Corporation

Previdnostni ukrepi v zvezi z USB-povezavo

Ta tema opisuje previdnostne ukrepe pri povezovanju enote prek USB.

- Uporabljajte samo zaupanja vredne pametne naprave za deljenje povezave. Povezava z napravami neznanega izvora ni priporočljiva zaradi varnostnih pomislekov.

TP1002274602

5-075-082-31(1) Copyright 2026 Sony Corporation

Funkcija FTPES (FTPS)

Funkcija FTPS podpira različne algoritme šifriranja, ki zagotavljajo varen prenos datotek. Več algoritmov šifriranja, od katerih nekateri morda niso v skladu s trenutnimi najboljšimi varnostnimi praksami, je podprtih za združljivost s širokim naborom strežnikov.

Algoritmi šifriranja, ki jih podpira funkcija FTPS

Podprti so naslednji algoritmi šifriranja.

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- 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

Priporočeni algoritmi šifriranja

Naslednji algoritmi šifriranja so priporočeni na podlagi priporočil NIST (NIST SP 800-57 1. del, revizija 5) in sorodnih varnostnih standardov.

- 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 zastarelih algoritmih

Funkcija FTPS podpira tudi naslednje algoritme za združljivost, vendar so ti na podlagi priporočil NIST (NIST SP 800-57 1. del, revizija 5) in sorodnih varnostnih standardov opuščeni in bodo morda v prihodnji različici odstranjeni.

- 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 združljivosti povezave

Funkcija FTPS je zasnovana z ravnovesjem med varnostjo in združljivostjo. Trenutno so zastareli algoritmi podprti iz naslednjih razlogov, vendar bodo morda v prihodnji različici odstranjeni zaradi izboljšanja varnosti.

- Samostojni fotografi in snemalci se morajo povezati s strežniki, ki delujejo na različnih odjemalcih.
- Ohraniti je treba združljivost s starejšimi sistemi in starejšimi strežniki.
- Vsi uporabniki niso pripravljeni preiti na varnejšo nastavitev, ker je spreminjanje nastavitev algoritma šifriranja na strani strežnika zapleteno.
- Nastavitve FTPS se pogosto delijo z drugimi varnimi storitvami. Vse spremembe je treba skrbno pretehtati, saj lahko vplivajo na druge storitve na strežniku.
- Za zagotovitev interoperabilnosti v različnih okoljih je treba podpirati širok spekter algoritmov šifriranja.

Algoritem šifriranja, ki se uporablja med povezavo FTPS, se določi s samodejnim pogajanjem s ciljnim strežnikom in je zato odvisen od nastavitev strežnika. Čeprav se zavedamo varnostnih tveganj, je združljivost trenutno prednostna naloga, da zadovolji različne potrebe uporabnikov.

Varnostna tveganja

Uporaba zastarelih algoritmov, vključno s CBC/DHE/RSA/SHA-1, povečuje tveganje, da napadalec dešifrira ali spremeni šifrirane podatke, s čimer jih razkrije med prenosom.

Priporočila za varno povezavo

Pred uporabo funkcije FTPS preverite, ali ciljni strežnik povezave podpira priporočeni šifrirni algoritem. Na strani strežnika omogočite samo priporočene algoritme in onemogočite zastarele algoritme.

Nalaganje z uporabo varnega FTP

Šifrirane datoteke lahko naložite prek protokola FTPS v eksplicitnem načinu (FTPES) za povezavo s ciljnim datotečnim strežnikom.
Za varen prenos prek FTP nastavite [Using Secure Protocol] na [On] v nastavitvah ciljnega strežnika za prenos datotek in uvozite certifikat.

Reference

- 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 (vključuje posodobitve od 10/06/2016).

Potrdilo

Zapišite potrdilo, ki ga uporablja funkcija FTPES (FTPS), v korenski imenik pomnilniške kartice. Ime datoteke nastavite na naslednji način.
certification.pem (oblika zapisa PEM)
Največja velikost potrdila, ki jo je mogoče naložiti, je 1 MB na potrdilo.

TP1002274603

5-075-082-31(1) Copyright 2026 Sony Corporation