SONY

Ohjekirja

ILME-FX6

Turvallisuusvaroitukset

Tässä ohjekirjassa kuvataan tiedoston siirtoa ja suoratoistoa koskevia turvallisuusvaroituksia laitteen käytön aikana.

Turvallisuusvaroitukset

Tässä kohdassa kuvataan muistettavia asioita, jotka koskevat laitteen liittämistä verkkoon.

- Viestinnän sisältö saattaa käyttäjän tietämättä joutua signaalien läheisyydessä olevien valtuuttamattomien ulkopuolisten haltuun. Kun käytät langatonta yhteyttä, suojaa viestinnän sisältö asianmukaisilla turvatoimenpiteillä.
- Jos asetat [Security] langaton lähiverkko -asetukseksi [None] ja muodostat yhteyden tukiasemaan, kameran ja tukiaseman välinen langaton yhteys ei ole salattu, ja kolmas osapuoli voi tunkeutua sinne signaalialueen sisällä. Käytä WPA2- tai WPA3-turvallisuusprotokollaa, jotka takaavat paremman turvallisuuden.
- SONY EI VASTAA MINKÄÄNLAISISTA VAHINGOISTA, JOTKA AIHEUTUVAT LÄHETYSLAITTEIDEN ASIANMUKAISTEN TURVATOIMENPITEIDEN LAIMINLYÖNNISTÄ, LÄHETYSMÄÄRITYSTEN AIHUETTAMISTA VÄISTÄMÄTTÖMISTÄ TIETOVUODOISTA TAI MINKÄÄNLAISISTA TURVALLISUUSONGELMISTA.
- Käyttöympäristöstä riippuen verkon valtuuttamattomat kolmannet osapuolet saattavat pystyä käyttämään laitetta. Kun liität laitteen verkkoon, muista varmistaa, että verkon tietoturva on suojattu.
- Yhdistä tuote verkkoon suojaustoiminnolla varustetun järjestelmän, esimerkiksi reitittimen tai palomuurin, kautta. Yhdistäminen ilman tällaista suojausta voi johtaa tietoturvaongelmiin.

TP1002274454

Muistettavaa Internetyhteydestä

Tässä kohdassa kuvataan muistettavia asioita, jotka koskevat laitteen yhdistämistä Internetiin.

- Laite ei voi muodostaa yhteyttä langaton lähiverkon kautta tukiasemaan, joka käyttää vain WEP:iä tai WPA:ta, jotka ovat haavoittuvaisia suojausmenetelmiä.
- Laite ei ole verkkolaite (esimerkiksi reititin tai kytkentäkeskus). On erittäin suositeltavaa, että yhdistät laitteen verkkoon, jossa voit konfiguroida ja hallita verkkoasetuksia asianmukaisesti suojataksesi sen verkkoa koskevilta hyökkäyksiltä, kuten DoS-hyökkäyksiltä (Denial of Service -hyökkäykset).
- Kun yhdistät laitteen verkkoon, tee se sellaisen reitittimen kautta, joka on asianmukaisesti konfiguroitu ja hallittu, tai yhdistä se LAN-porttiin, jolla on sama toiminnallisuus. Jos laite yhdistetään ilman tällaista suojausta (esimerkiksi käyttämällä ilmaista Wi-Fi-yhteyttä), turvallisuusongelmia saattaa ilmetä. Asianmukaisesti konfiguroidut reitittimet tarjoavat riittävän suojauksen DoS-hyökkäyksiä tai laitteiden toiminnallisuuden menetyksiä vastaan verkossa. Jos huomaat jotakin epätavallista, kytke kamera heti irti verkosta.

TP1002274455

Muistettavaa verkkotoiminnosta

Tässä kohdassa kuvataan muistettavia asioita laitteen verkkotoiminnosta.

- Jos havaitset luvattoman pääsyn, kamera ei välttämättä voi enää hyväksyä kommunikaatioita. Jos näin tapahtuu, muodosta yhteys alusta alkaen.
- Paina [Network]-tilanäytön [Show Authentication] -painiketta, niin näet laitteen yhdistämiseen tarvittavat todennustiedot. Varmista, etteivät muut ihmiset näe näyttöä eivätkä voi kopioida QR-koodin kuvaa.
- Käyttäjänimi ja salasana luodaan automaattisesti ja määritetään kameralle ostohetkellä. Kun määrität käyttäjänimesi ja salasanasi, varmista etteivät muut näe asetuksiasi. Määritä käyttäjänimi ja salasana seuraavalla tavalla.

[User Name]	– Määritä käyttäjänimi, jossa on 1–16 merkkiä. – Se on oletusarvoisesti ”admin”. – Seuraavat ovat kelvollisia syöttömerkkejä. Aakkoset (pienet ja isot kirjaimet), numerot, symbolit (! % + , - . = _)
[Password]	– Määritä 8–16 merkkiä pitkä salasana, jossa on vähintään 1 kirjain ja vähintään 1 numero. – Seuraavat ovat kelvollisia syöttömerkkejä. Aakkoset (pienet ja isot kirjaimet), numerot, symbolit (! % + , - . = _)

TP1002274456

Muistettavaa langattomasta lähiverkosta

Tässä kohdassa kuvataan muistettavia asioita, jotka koskevat laitteen yhdistämistä langattoman lähiverkon kautta.

- Tämän laitteen ohjekirjassa LAN-liittimet yhdistäviä langattomia LAN-tukiasemia ja langattomia LAN-reitittimiä kutsutaan ”tukiasemiksi”.
- [Security] (salaustapa) voidaan asettaa arvoon [None], [WPA2], tai [WPA3]. Asetuksen [WPA2] tai [WPA3] käyttö on suositeltavaa turvallisuuden näkökulmasta. Kun [None] on valittuna, näkyviin tulee viesti ennen yhteyden muodostamista. Langattoman lähiverkkoyhteyden suojaamiseksi suositellaan yhteyttä tukiasemiin WPA2- tai WPA3-turvallisuusasetuksilla.
- WPA2-suojaustapa valitaan oletusarvoisesti, kun langattoman lähiverkon tukiasema rekisteröidään toiminnolla [Manual Register].
- Jos muodostat yhteyden tukiasemaan ilman turvallisuusasetuksia, saatat joutua hakkeroinnin, pahanilkisten kolmansien osapuolten tunkeutumisen tai haavoittuvuuksia hyväksikäyttävien hyökkäysten kohteeksi. Yhteyttä ilman turvallisuusasetuksia ei suositella, paitsi jos sitä mahdollisuutta ei voida välttää muulla tavoin.
- Langattoman lähiverkon turvallisuuden konfiguroiminen on erittäin tärkeää. Sony ei ole vastuussa vahingoista, jotka aiheutuvat turvallisuustoimenpiteiden tekemättä jättämisestä, tai jos turvallisuusongelma aiheutuu langattoman lähiverkon käytön väistämättömien olosuhteiden tuloksena.

TP1002274457

Muistettavaa USB-yhteydenjaosta

Tässä kohdassa kuvataan muistettavia asioita, jotka koskevat laitteen yhdistämistä USB-yhteydenjaon kautta.

- Käytä yhteydenjakoon vain luotettavia älypuhelinlaitteita. Laitteiden yhdistäminen alkuperältään tuntemattomiin kohteisiin ei ole suositeltavaa turvallisuussyistä.

TP1002274458

Tietoja FTPES (FTPS) -toiminnosta

FTPS-toiminto tukee useita salausalgoritmeja, jotka varmistavat turvallisen tiedoston siirron. Monet palvelintyypit ovat yhteensopivia ja tukevat useita salausalgoritmeja, joista osa ei välttämättä ole yhteensopivia tämänhetkisten parhaiden turvallisuuskäytäntöjen kanssa.

FTPS-toiminnon tukemat salausalgoritmit

Seuraavia salausalgoritmeja tuetaan.

- 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

Suositeltavat salausalgoritmit

Seuraavia salausalgoritmeja suositellaan NIST-suositusten (NIST SP 800-57 Part 1 Revision 5) ja niihin liittyvien turvallisuusstandardien perusteella.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Tietoja vanhentuneista algoritmeista

FTPS-toiminto tukee myös seuraavia algoritmeja, mutta ne ovat vanhentuneita NIST-suositusten (NIST SP 800-57 Part 1 Revision 5) ja niihin liittyvien turvallisuusstandardien perusteella. Ne voidaan poistaa tulevista versioista.

- 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

Tietoja yhteyden yhteensopivuudesta

FTPS-toiminto on suunniteltu tarjoamaan tasapainoa turvallisuuden ja yhteensopivuuden välillä. Tällä hetkellä vanhentuneita algoritmeja tuetaan seuraavista syistä, mutta ne voidaan poistaa tulevista versioista turvallisuuden

parantamiseksi.

- Freelance-valokuvaajien ja -videokuvaajien on kyettävä muodostamaan yhteys eri asiakkaiden palvelimiin.
- Yhteensopivuus vanhempien järjestelmien ja perinteisten palvelimien kanssa on säilytettävä.
- Kaikki käyttäjät eivät ole valmiita vaihtamaan turvallisempaan kokoonpanoon, sillä palvelimen salausalgoritmiasetusten muuttaminen on monimutkaista.
- FTPS-asetukset jaetaan usein muiden turvallisuuspalveluiden kanssa. Kaikkia muutoksia on harkittava huolellisesti, sillä ne voivat vaikuttaa palvelimen muihin palveluihin.
- Salausalgoritmien laaja tuki on tarpeen, jotta voidaan varmistaa eri ympäristöjen välinen käyttö.

FTPS-yhteyden aikana käytetty algoritmi määräytyy kohdepalvelimen kanssa käydyn automaattisen neuvottelun tuloksena, ja siksi se riippuu palvelinasetuksista. Vaikka käyttäjät ovat tietoisia turvallisuusriskeistä, yhteensopivuus on yleensä etusijalla käyttäjien erilaisten tarpeiden tyydyttämiseksi.

Turvallisuusriskit

Vanhentuneiden algoritmien, kuten CBC/DHE/RSA/SHA-1, käyttö lisää salattujen tietojen salauksen purkautumis- tai peukalointiriskiä, mikä altistaa tiedot hyökkäyksille siirron aikana.

Suositukset turvalliselle yhteydelle

Ennen kuin käytät FTPS-toimintoa, tarkista että yhteyden kohdepalvelin tukee suositeltavaa salausalgoritmia. Salli vain suositeltujen algoritmien käyttö palvelinpuolella ja poista vanhentuneet algoritmit käytöstä.

Lataaminen palvelimelle käyttämällä suojattua FTP:tä

Voit lähettää tiedostoja salatusti FTPS-yhteydellä käyttämällä FTPS-yhteyttä kohdetiedostopalvelimeen Explicit-tilassa (FTPES).
Jos haluat käyttää suodattua FTP-siirtoa, määritä kohdan [Using Secure Protocol] asetukseksi [On] tiedostonsiirron kohdepalvelimen asetuksissa ja tuo varmenne.

Lähteet

- 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 (sisältää 10/06/2016 tehdyt päivitykset).

Varmenne

Kirjoita FTPES (FTPS) -toiminnon käyttämä varmenne muistikortin juurihakemistoon. Määritä tiedoston nimi seuraavalla tavalla.
certification.pem (PEM-muoto)
Ladattavan varmenteen maksimikoko on 1 Mt per varmenne.

TP1002274459