ILME-FX6

Säkerhetsåtgärder

I den här hjälpguiden beskrivs säkerhetsåtgärder när enheten används för filöverföring och strömning.

ILME-FX6
Säkerhetsåtgärder

Säkerhetsåtgärder

I det här avsnittet beskrivs försiktighetsåtgärder när enheten ansluts till ett nätverk.

- Kommunikationsinnehåll kan utan att man vet det avläsas av obehöriga tredje parter i närheten av signalerna. När du använder trådlös LAN-kommunikation ska du vidta säkerhetsåtgärder för att skydda kommunikationsinnehållet.
- Om du ställer in inställningen för [Security] trådlös LAN till [None] och ansluter till en åtkomstpunkt, kommer den trådlösa kommunikationen mellan kameran och åtkomstpunkten inte att krypteras och kan komma att avlyssnas av tredje part inom signalens räckvidd. Använd säkerhetsprotokollet WPA2 eller WPA3 för förbättrad säkerhet.
- SONY KOMMER INTE ATT ANSVARA FÖR SKADOR AV NÅGOT SLAG TILL FÖLJD AV UNDERLÅTENHET ATT UPPRÄTTA LÄMPLIGA SÄKERHETSÅTGÄRDER PÅ ÖVERFÖRINGSENHETER, OUNDVIKLIGA DATALÄCKAGE PÅ GRUND AV ÖVERFÖRINGSSPECIFIKATIONER, ELLER SÄKERHETSPROBLEM AV NÅGOT SLAG.
- Beroende på användningsförhållandena kan obehöriga tredje parter på nätverket eventuellt få tillgång till apparaten. När apparaten ansluts till nätverket ska det bekräftas att nätverket är skyddat på rätt sätt.
- När du ansluter den här produkten till ett nätverk, anslut den via ett system som ger en skyddsfunktion, som en router eller brandvägg. Om den ansluts utan sådant skydd kan säkerhetsproblem uppstå.

TP1002274478

ILME-FX6
Säkerhetsåtgärder

Försiktighetsåtgärder vid internetanslutning

I det här avsnittet beskrivs försiktighetsåtgärder när enheten ansluts till internet.

- Enheten kan inte ansluta via trådlöst LAN till en åtkomstpunkt som endast använder WEP eller WPA, som är säkerhetsmetoder med sårbarheter.
- Enheten är inte en nätverksenhet (till exempel en router eller en switch). Vi rekommenderar starkt att du ansluter enheten till ett nätverk där du kan konfigurera och hantera nätverksinställningarna på lämpligt sätt för att skydda mot nätverksbaserade attacker, såsom DoS-attacker (Denial of Service-attacker).
- När du ansluter enheten till ett nätverk ska du ansluta den via en router som är korrekt konfigurerad och hanterad, eller ansluta den till en LAN-port som har samma funktion. Om du ansluter utan sådant skydd (till exempel när du använder gratis Wi-Fi) kan säkerhetsproblem uppstå. När routrar är korrekt konfigurerade ger de tillräckligt skydd mot DoS-attacker eller funktionsförlust hos enheter i nätverket. Om du märker något ovanligt ska du omedelbart koppla bort kameran från nätverket.

TP1002274479

ILME-FX6
Säkerhetsåtgärder

Försiktighetsåtgärder som rör nätverksfunktionen

I det här avsnittet beskrivs försiktighetsåtgärder som rör enhetens nätverksfunktion.

- Om obehörig åtkomst upptäcks kan kameran sluta ta emot kommunikation. Om detta inträffar, börja om anslutningen.
- Tryck på knappen [Show Authentication] på statusskärmen [Network] för att visa autentiseringsinformationen för anslutning till enheten. Se till att skärmen inte kan ses och QR-kodbilden inte kan kopieras av andra.
- Användarnamnet och lösenordet genereras automatiskt och ställs in i kameran vid köpet. När du anger ditt användarnamn och lösenord ska du se till att inställningarna inte är synliga för andra. Ställ in användarnamn och lösenord enligt följande.

[User Name]	– Ange ett användarnamn som består av 1 till 16 tecken. – Fabriksinställningen är ”admin”. – Följande är giltiga inmatningstecken. Bokstäver (versaler och gemener), siffror, symboler (! % + , - . = _)
[Password]	– Ställ in ett lösenord som består av 8 till 16 tecken och innehåller minst 1 eller flera bokstäver och 1 eller flera siffror. – Följande är giltiga inmatningstecken. Bokstäver (versaler och gemener), siffror, symboler (! % + , - . = _)

TP1002274480

ILME-FX6
Säkerhetsåtgärder

Försiktighetsåtgärder som rör trådlöst LAN

I det här avsnittet beskrivs försiktighetsåtgärder när enheten ansluts via trådlöst LAN.

- I enhetens hjälpguide kallas trådlösa LAN-åtkomstpunkter och trådlösa LAN-routrar som vidarebefordrar LAN-anslutningar för ”åtkomstpunkter”.
- [Security] (krypteringsmetod) kan ställas in till [None], [WPA2], eller [WPA3]. Användningen av [WPA2] eller [WPA3] rekommenderas av säkerhetsskäl. När [None] är vald visas ett meddelande före anslutning. För en säker trådlös LAN-anslutning rekommenderas starkt anslutning till åtkomstpunkter med säkerhetsinställningen WPA2 eller WPA3.
- Som standard är säkerhetsmetoden WPA2 vald när du registrerar en trådlös LAN-åtkomstpunkt med [Manual Register].
- Om du ansluter till en åtkomstpunkt utan säkerhetsinställningar kan du utsättas för hackning, åtkomst av illvilliga tredje parter eller attacker mot sårbarheter. Om det inte är absolut nödvändigt rekommenderas ingen anslutning utan säkerhetsinställningar.
- Det är mycket viktigt att konfigurera säkerheten med ett trådlöst LAN. Sony ansvarar inte för skador som uppstår till följd av att säkerhetsåtgärder inte vidtagits eller om ett säkerhetsproblem uppstår på grund av oundvikliga omständigheter vid användning av trådlöst LAN.

TP1002274481

ILME-FX6
Säkerhetsåtgärder

Försiktighetsåtgärder som rör USB-tjudring

I det här avsnittet beskrivs försiktighetsåtgärder när enheten ansluts via USB-tjudring.

- Använd endast betrodda smartphones för tjudring. Det rekommenderas inte att enheter av okänt ursprung ansluts, av säkerhetsskäl.

TP1002274482

Om FTPES (FTPS)-funktionen

FTPS-funktionen stöder olika krypteringsalgoritmer för att säkerställa säker filöverföring. Flera krypteringsalgoritmer, varav vissa kanske inte uppfyller gällande säkerhetsstandarder, stöds på grund av kompatibilitet med ett stort antal servrar.

Krypteringsalgoritmer som stöds av FTPS-funktionen

Följande krypteringsalgoritmer stöds.

- 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

Rekommenderade krypteringsalgoritmer

Följande krypteringsalgoritmer rekommenderas baserat på NIST:s rekommendationer (NIST SP 800-57 del 1 revision 5) och relaterade säkerhetsstandarder.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Om föråldrade algoritmer

FTPS-funktionen stöder även följande algoritmer för kompatibilitet, men de är föråldrade enligt NIST-rekommendationerna (NIST SP 800-57 Del 1 Revidering 5) och relaterade säkerhetsstandarder och kan komma att tas bort i en framtida version.

- 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

Om anslutningskompatibilitet

FTPS-funktionen är utformad med en balans mellan säkerhet och kompatibilitet. För närvarande stöds föråldrade algoritmer av följande skäl, men de kan komma att tas bort i en framtida version för att förbättra säkerheten.

- Frilansfotografer och filmare behöver ansluta till servrar som körs på olika klienter.
- Kompatibilitet med äldre system och äldre servrar måste upprätthållas.
- Alla användare är inte beredda att byta till en säkrare inställning eftersom det är komplicerat att ändra inställningarna för krypteringsalgoritmen på serversidan.
- FTPS-inställningarna delas ofta av flera säkra tjänster. Eventuella ändringar ska övervägas noga eftersom de kan påverka andra tjänster på servern.
- Ett brett spektrum av krypteringsalgoritmer måste stödjas för att säkerställa interoperabilitet i olika miljöer.

Krypteringsalgoritmen som används under en FTPS-anslutning bestäms genom automatisk förhandling med destinationsservern och beror därför på serverinställningarna. Vi är medvetna om säkerhetsriskerna, men kompatibilitet prioriteras för närvarande för att tillgodose användarnas olika behov.

Säkerhetsrisker

Användning av föråldrade algoritmer, inklusive CBC/DHE/RSA/SHA-1, ökar risken för att krypterade data kan dekrypteras eller manipuleras av en angripare, vilket exponerar data under överföringen.

Rekommendation för säker anslutning

Innan du använder FTPS-funktionen ska du kontrollera att servern som anslutningen ska gå till stöder den rekommenderade krypteringsalgoritmen. Aktivera endast de rekommenderade algoritmerna på serversidan och inaktivera de föråldrade algoritmerna.

Ladda upp med säker FTP

Du kan ladda upp filer med kryptering med FTPS i explicit läge (FTPES) för anslutningen till destinationsfilservern.
För säker FTP-överföring, ställ [Using Secure Protocol] till [On] i inställningarna i filöverföringens destinationsserver och importera ett certifikat.

Referenser

- 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 (inkluderar uppdateringar från och med 10/06/2016).

Certifikat

Skriv certifikatet som används av FTPES (FTPS)-funktionen till rotkatalogen på ett minneskort. Ange filnamnet på följande sätt.
certification.pem (PEM-format)
Den maximala certifikatstorleken som kan laddas är 1 MB per certifikat.

TP1002274483