ILME-FX6

Precauções de segurança

Este Guia de ajuda descreve as precauções de segurança para transferência de ficheiros e transmissão utilizando a unidade.

5-075-080-81(1) Copyright 2026 Sony Corporation

ILME-FX6
Precauções de segurança

Precauções de segurança

Este tópico descreve precauções ao ligar a unidade a uma rede.

- O conteúdo das comunicações pode ser intercetado inadvertidamente por terceiros não autorizados na proximidade dos sinais. Ao utilizar a comunicação LAN sem fios, implemente medidas de segurança adequadas para proteger o conteúdo das comunicações.
- Se definir a definição da LAN sem fios [Security] para [None] e ligar a um ponto de acesso, a comunicação sem fios entre a câmara e o ponto de acesso não será encriptada e poderá ser intercetada por terceiros dentro do alcance do sinal. Utilize o protocolo de segurança WPA2 ou WPA3 para segurança melhorada.
- A SONY NÃO É RESPONSÁVEL POR QUALQUER TIPO DE DANOS RESULTANTES DA NÃO IMPLEMENTAÇÃO DE MEDIDAS DE PROTEÇÃO ADEQUADAS EM DISPOSITIVOS DE TRANSMISSÃO, FUGAS DE DADOS INEVITÁVEIS RESULTANTES DAS ESPECIFICAÇÕES DA TRANSMISSÃO OU QUALQUER TIPO DE PROBLEMA DE SEGURANÇA.
- Dependendo do ambiente de funcionamento, terceiros não autorizados na rede podem ter acesso à unidade. Ao ligar a unidade à rede, certifique-se de que a rede está bem protegida.
- Ao ligar este produto a uma rede, ligue através de um sistema com uma função de proteção, tal como um router ou firewall. Se ligado sem tal proteção, poderão ocorrer problemas de segurança.

TP1002274470

5-075-080-81(1) Copyright 2026 Sony Corporation

ILME-FX6
Precauções de segurança

Precauções de ligação à internet

Este tópico descreve precauções ao ligar a unidade à internet.

- A unidade não pode ser ligada por LAN sem fios a um ponto de acesso que apenas utiliza WEP ou WPA, que são métodos de segurança com vulnerabilidades.
- A unidade não é um dispositivo de rede (por exemplo, um router ou switch de rede). É altamente recomendado ligar a unidade a uma rede na qual pode configurar e gerir adequadamente as definições de rede para proteção contra ataques baseados na rede, tais como ataques DoS (ataques de negação de serviço).
- Ao ligar a unidade a uma rede, ligue-a através de um router configurado e gerido adequadamente ou ligue-a a uma porta LAN com a mesma funcionalidade. Se ligada sem tal proteção (por exemplo, ao utilizar Wi-Fi gratuito), podem ocorrer problemas de segurança. Quando devidamente configurados, os routers fornecem proteção suficiente contra ataques DoS ou perda de funcionalidade dos dispositivos na rede. Se reparar em algo invulgar, desligue imediatamente a câmara da rede.

TP1002274471

5-075-080-81(1) Copyright 2026 Sony Corporation

ILME-FX6
Precauções de segurança

Precauções relacionadas com a função de rede

Este tópico descreve precauções sobre a função de rede da unidade.

- Se for detetado um acesso não autorizado, a câmara pode não conseguir aceitar comunicações. Se isto acontecer, volte a ligar a partir do início.
- Prima o botão [Show Authentication] no ecrã de estado [Network] para visualizar as informações de autenticação para ligar à unidade. Tome cuidado para que o ecrã não seja visto por outras pessoas e para que o código QR não seja copiado.
- O nome de utilizador e a palavra-passe são automaticamente gerados e definidos na câmara aquando da compra. Ao definir o nome de utilizador e a palavra-passe, certifique-se de que as definições não são visíveis para terceiros. Defina o nome de utilizador e a palavra-passe da seguinte forma.

[User Name]	– Defina um nome de utilizador composto por 1 a 16 caracteres. – Por predefinição, isto está definido para “admin”. – Os seguintes são caracteres de entrada válidos. Caracteres alfabéticos (maiúsculas e minúsculas), caracteres numéricos, símbolos (! % + , - . = _)
[Password]	– Defina uma palavra-passe composta por 8 a 16 caracteres com, no mínimo, 1 ou mais caracteres alfabéticos e 1 ou mais caracteres numéricos. – Os seguintes são caracteres de entrada válidos. Caracteres alfabéticos (maiúsculas e minúsculas), caracteres numéricos, símbolos (! % + , - . = _)

TP1002274472

5-075-080-81(1) Copyright 2026 Sony Corporation

ILME-FX6
Precauções de segurança

Precauções relacionadas com a LAN sem fios

Este tópico descreve precauções ao ligar a unidade através de LAN sem fios.

- No Guia de ajuda para esta unidade, os pontos de acesso da LAN sem fios e os routers da LAN sem fios que transmitem as ligações da LAN são referidos como “pontos de acesso”.
- [Security] (método de encriptação) pode ser definido para [None], [WPA2] ou [WPA3]. De um ponto de vista da segurança, é recomendada a utilização de [WPA2] ou [WPA3]. Quando [None] está selecionado, é apresentada uma mensagem antes de ligar. Para uma ligação LAN sem fios segura, é altamente recomendada a ligação a pontos de acesso com definição de segurança WPA2 ou WPA3.
- Por predefinição, o método de segurança WPA2 está selecionado ao registar um ponto de acesso da LAN sem fios através de [Manual Register].
- Se ligar a um ponto de acesso sem qualquer definição de segurança, pode sujeitar-se a pirataria, acesso por terceiros de má-fé ou ataques às vulnerabilidades. A menos que seja inevitável, não é recomendada a ligação sem qualquer definição de segurança.
- É muito importante configurar a segurança numa LAN sem fios. A Sony não será responsável por danos resultantes da inexistência de medidas de segurança ou se ocorrer um problema de segurança devido a circunstâncias inevitáveis na utilização da LAN sem fios.

TP1002274473

5-075-080-81(1) Copyright 2026 Sony Corporation

Precauções relacionadas com a partilha de ligação USB

Este tópico descreve precauções ao ligar a unidade através de partilha de ligação USB.

- Apenas utilize smartphones fidedignos para a partilha de ligação. Por motivos de segurança, não é recomendada a ligação a dispositivos de origem desconhecida.

TP1002274474

5-075-080-81(1) Copyright 2026 Sony Corporation

Sobre a função FTPES (FTPS)

A função FTPS suporta vários algoritmos de encriptação para garantir uma transferência segura de ficheiros. São suportados vários algoritmos de encriptação, alguns dos quais podem não estar em conformidade com as atuais melhores práticas de segurança, para compatibilidade com uma vasta gama de servidores.

Algoritmos de encriptação suportados pela função FTPS

São suportados os seguintes algoritmos de encriptação.

- 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

Algoritmos de encriptação recomendados

Os seguintes algoritmos de encriptação são recomendados com base nas recomendações NIST (NIST SP 800-57 Parte 1 Revisão 5) e normas de segurança relacionadas.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Sobre os algoritmos descontinuados

A função FTPS também suporta os seguintes algoritmos para compatibilidade, mas são descontinuados com base nas recomendações NIST (NIST SP 800-57 Parte 1 Revisão 5) e normas de segurança relacionadas e pode ser removida numa versão futura.

- 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

Sobre a compatibilidade da ligação

A função FTPS foi criada com um equilíbrio entre a segurança e a compatibilidade. De momento, os algoritmos descontinuados são suportados pelos seguintes motivos, mas podem ser removidos numa versão futura para melhorar a segurança.

- Os fotógrafos e videógrafos independentes necessitam de ligar a servidores em execução em vários clientes.
- A compatibilidade com sistemas e servidores mais antigos necessita de ser mantida.
- Nem todos os utilizadores estão preparados para mudar para uma definição mais segura porque é complicado alterar as definições do algoritmo de encriptação no lado do servidor.
- As definições de FTPS são frequentemente partilhadas com outros serviços seguros. Quaisquer alterações têm de ser consideradas com cuidado uma vez que podem ter impacto noutros serviços no servidor.
- Tem de ser suportada uma vasta gama de algoritmos de encriptação para garantir interoperabilidade em diferentes ambientes.

O algoritmo de encriptação utilizado durante uma ligação FTPS é determinado pela negociação automática com o servidor de destino e, por isso, depende das definições do servidor. Embora ciente dos riscos de segurança, é dada prioridade à compatibilidade para corresponder às diversas necessidades dos utilizadores.

Riscos de segurança

Utilizar algoritmos descontinuados, incluindo CBC/DHE/RSA/SHA-1, aumenta o risco de os dados encriptados poderem ser desencriptados ou modificados por um pirata informático, expondo os dados durante a transferência.

Recomendação para ligação segura

Antes de utilizar a função FTPS, certifique-se de que o servidor de destino da ligação suporta o algoritmo de encriptação recomendado. Ative apenas os algoritmos recomendados no lado do servidor e desative os algoritmos descontinuados.

Carregar através de FTP seguro

Pode carregar ficheiros com encriptação através de FTPS no modo Explícito (FTPES) para a ligação ao servidor de ficheiros de destino.
Para uma transferência FTP seguro, defina [Using Secure Protocol] para [On] nas definições do servidor de destino da transferência de ficheiros e importe um certificado.

Referências

- 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 (inclui atualizações a partir de 10/06/2016).

Certificado

Guarde o certificado utilizado pela função FTPES (FTPS) no diretório raiz de um cartão de memória. Defina o nome do ficheiro da seguinte forma.
certification.pem (formato PEM)
O tamanho máximo do certificado que pode ser carregado é 1 MB por certificado.

TP1002274475

5-075-080-81(1) Copyright 2026 Sony Corporation