MPC-2610

Precauciones de seguridad

Esta Guía de Ayuda describe las precauciones de seguridad para la transferencia de archivos y la transmisión utilizando la unidad.

MPC-2610
Precauciones de seguridad

Precauciones de seguridad

Este tema describe las precauciones al conectar la unidad a una red.

- Es posible que terceros no autorizados situados cerca de las señales puedan interceptar sin saberlo contenidos de la comunicación. Cuando utilice la comunicación LAN inalámbrica, aplique correctamente las medidas de seguridad para proteger los contenidos de la comunicación.
- Si configura el ajuste [Security] de la LAN inalámbrica en [None] y se conecta a un punto de acceso, la comunicación inalámbrica entre la cámara y el punto de acceso no estará cifrada y podría ser interceptada por un tercero dentro del alcance de la señal. Utilice el protocolo de seguridad WPA2 o WPA3 para una mayor seguridad.
- SONY NO SE HACE RESPONSABLE POR DAÑOS DE NINGÚN TIPO DEBIDOS A LA OMISIÓN DE LAS MEDIDAS DE SEGURIDAD ADECUADAS EN DISPOSITIVOS DE TRANSMISIÓN, FUGAS DE DATOS INEVITABLES DERIVADAS DE LAS ESPECIFICACIONES DE TRANSMISIÓN O PROBLEMAS DE SEGURIDAD DE CUALQUIER TIPO.
- Según el tipo de entorno operativo, es posible que terceras partes no autorizadas puedan acceder a la unidad a través de la red. Cuando conecte la unidad a la red, confirme siempre que la red está correctamente protegida.
- Cuando conecte este producto a una red, conéctelo mediante un sistema con función de protección como, por ejemplo, un router o un firewall. Si se conecta sin dicha protección, pueden producirse problemas de seguridad.

TP1002221017

MPC-2610
Precauciones de seguridad

Precauciones para la conexión a Internet

Este tema describe las precauciones al conectar la unidad a Internet.

- La unidad no puede conectarse mediante LAN inalámbrica a un punto de acceso que utilice únicamente WEP o WPA, ya que son métodos de seguridad con vulnerabilidades.
- La unidad no es un dispositivo de red (por ejemplo, un router o conmutador de red). Se recomienda encarecidamente conectar la unidad a una red en la que pueda configurar y administrar adecuadamente los ajustes para protegerla frente a ataques de red, como ataques de denegación de servicio (DoS).
- Al conectar la unidad a una red, hágalo mediante un router que esté debidamente configurado y administrado, o conéctela a un puerto LAN que tenga la misma funcionalidad. Si se conecta sin dicha protección (por ejemplo, al usar Wi-Fi gratuito), pueden surgir problemas de seguridad. Cuando está correctamente configurado, el router proporciona una protección adecuada frente a ataques DoS o pérdida de funcionalidad de los dispositivos en la red. Si detecta algo inusual, desconecte inmediatamente la cámara de la red.

TP1002221018

MPC-2610
Precauciones de seguridad

Precauciones relacionadas con la función de red

Este tema describe las precauciones sobre la función de red de la unidad.

- Si se detecta un acceso no autorizado, es posible que la cámara deje de aceptar comunicaciones. Si esto ocurre, restablezca la conexión desde el principio.
- La información de autenticación para conectarse a la unidad se visualiza al utilizar [Network] – [Network Setup] – [Show Authentication]. Tenga cuidado de que otras personas no puedan ver la pantalla ni copiar la imagen del código QR.
- En el momento de la compra se deben establecer un nombre de usuario y una contraseña. Al definir el nombre de usuario y la contraseña, asegúrese de que los ajustes no son visibles para el resto. Establezca el nombre de usuario y la contraseña como se especifica a continuación.

[User Name]	– Defina un nombre de usuario que tenga entre 1 y 16 caracteres. – El ajuste predeterminado de fábrica es “admin”. – Los siguientes son caracteres válidos de entrada: Letras alfabéticas (mayúsculas y minúsculas), números, símbolos (! % + , - . = _)
[Password]	– Defina una contraseña que tenga entre 8 y 16 caracteres, que contenga al menos 1 o varios caracteres alfabéticos y 1 o varios caracteres numéricos. – Los siguientes son caracteres válidos de entrada: Letras alfabéticas (mayúsculas y minúsculas), números, símbolos (! % + , - . = _)

TP1002221019

MPC-2610
Precauciones de seguridad

Precauciones relacionadas con la LAN inalámbrica

Este tema describe las precauciones al conectar la unidad mediante LAN inalámbrica.

- En la Guía de Ayuda de esta unidad, los puntos de acceso de LAN inalámbricos y los enrutadores de LAN inalámbricos que retransmiten conexiones LAN se denominan “puntos de acceso”.
- [Security] (método de cifrado) puede configurarse en [None], [WPA2] o [WPA3]. Desde el punto de vista de la seguridad, se recomienda el uso de [WPA2] o [WPA3]. Cuando se selecciona [None], se muestra un mensaje antes de establecer la conexión. Para una conexión LAN inalámbrica segura, se recomienda encarecidamente la conexión a puntos de acceso con configuración de seguridad WPA2 o WPA3.
- De forma predeterminada, el método de seguridad WPA2 se selecciona al registrar un punto de acceso LAN inalámbrico mediante [Manual Register].
- Si se conecta a un punto de acceso sin ninguna configuración de seguridad, podría ser víctima de hackeo, acceso por parte de terceros malintencionados o ataques a vulnerabilidades. Salvo que sea estrictamente necesario, no se recomienda la conexión sin configuración de seguridad.
- Configurar la seguridad en una LAN inalámbrica es muy importante. Sony no se hace responsable de ningún daño derivado de no tomar medidas de seguridad o de los problemas de seguridad que pueden generarse como consecuencia de circunstancias inevitables en el uso de la LAN inalámbrica.

TP1002221020

MPC-2610
Precauciones de seguridad

Precauciones relacionadas con la conexión USB compartida

Este tema describe las precauciones al conectar la unidad mediante conexión USB compartida.

- Utilice únicamente teléfonos inteligentes de confianza para el anclaje. No se recomienda conectar dispositivos de origen desconocido debido a preocupaciones de seguridad.

TP1002221021

Acerca de la función FTPES (FTPS)

La función FTPS admite varios algoritmos de encriptación para garantizar una transferencia segura de archivos. Se admiten múltiples algoritmos de encriptación, algunos de los cuales podrían no cumplir con las prácticas recomendadas de seguridad actuales, para garantizar la compatibilidad con una amplia gama de servidores.

Algoritmos de cifrado compatibles con la función de FTPS

Los siguientes algoritmos de cifrado son compatibles.

- 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

Algoritmos de cifrado recomendados

Los siguientes algoritmos de cifrado se recomiendan según las recomendaciones de NIST (NIST SP 800-57 parte 1, revisión 5) y los estándares de seguridad relacionados.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Acerca de los algoritmos obsoletos

La función FTPS también es compatible con los siguientes algoritmos, pero están obsoletos según las recomendaciones de NIST (NIST SP 800-57 parte 1, revisión 5) y los estándares de seguridad relativos, por lo que podrían quitarse en una versión futura.

- 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

Acerca de la compatibilidad de conexión

La función FTPS está diseñada con un equilibrio entre seguridad y compatibilidad. Actualmente, se admiten algoritmos obsoletos por las siguientes razones, aunque podrían eliminarse en una versión futura para mejorar la seguridad:

- Los fotógrafos y videógrafos autónomos necesitan conectarse a servidores que funcionan con diversos clientes.
- Es necesario mantener la compatibilidad con sistemas antiguos y servidores heredados.
- No todos los usuarios están preparados para cambiar a una configuración más segura, ya que modificar los ajustes del algoritmo de cifrado en el servidor es complicado.
- La configuración de FTPS suele compartirse con otros servicios seguros. Cualquier cambio debe considerarse cuidadosamente, ya que podría afectar a otros servicios en el servidor.
- Debe admitirse una amplia gama de algoritmos de cifrado para garantizar la interoperabilidad en distintos entornos.

El algoritmo de cifrado utilizado durante una conexión FTPS se determina mediante negociación automática con el servidor de destino y, por lo tanto, depende de la configuración del servidor. A pesar de estar al tanto de los riesgos de seguridad, actualmente se prioriza la compatibilidad para satisfacer las diversas necesidades de los usuarios.

Riesgos de seguridad

El uso de algoritmos obsoletos, incluidos CBC/DHE/RSA/SHA-1, incrementa el riesgo de que los datos cifrados sean descifrados o manipulados por un atacante, exponiendo los datos durante su transferencia.

Recomendación para una conexión segura

Antes de utilizar la función FTPS, compruebe que el servidor de destino de la conexión admita el algoritmo de cifrado recomendado. Habilite únicamente los algoritmos recomendados en el servidor y desactive los algoritmos obsoletos.

Carga a través de FTP segura

Puede cargar archivos cifrados a través de FTPS en el modo Explicit (FTPES) para conectarse con el servidor de archivos de destino.
Para una transferencia de FTP segura, ajuste [Using Secure Protocol] en [On] en el servidor de destino de transferencia de archivos e importe un certificado.

Referencias

- 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 (incluye las actualizaciones del 10/06/2016).

Certificado

Escriba el certificado utilizado por la función FTPES (FTPS) en el directorio raíz de una tarjeta de memoria. Defina el nombre del archivo como se especifica a continuación.
certification.pem (formato PEM)
En los certificados, el tamaño máximo que puede cargarse es de 1 MB por cada uno.

TP1002221022