MPC-2610

Security Precautions

This Help Guide describes the security precautions for file transfer and streaming using the unit.

Security Precautions

This topic describes precautions when connecting the unit to a network.

- Communication content may be unknowingly intercepted by unauthorized third parties in the vicinity of the signals. When using wireless LAN communication, implement security measures properly to protect the communication content.
- If you set the [Security] wireless LAN setting to [None] and connect to an access point, wireless communication between the camera and the access point will not be encrypted and may be intercepted by a third party within the range of the signal. Use the WPA2 or WPA3 security protocol for enhanced security.
- SONY WILL NOT BE LIABLE FOR DAMAGES OF ANY KIND RESULTING FROM A FAILURE TO IMPLEMENT PROPER SECURITY MEASURES ON TRANSMISSION DEVICES, UNAVOIDABLE DATA LEAKS RESULTING FROM TRANSMISSION SPECIFICATIONS, OR SECURITY PROBLEMS OF ANY KIND.
- Depending on the operating environment, unauthorized third parties on the network may be able to access the unit. When connecting the unit to the network, be sure to confirm that the network is protected securely.
- When connecting this product to a network, connect via a system that provides a protection function, such as a router or firewall. If connected without such protection, security issues may occur.

TP1002107990

Internet Connection Precautions

This topic describes precautions when connecting the unit to the Internet.

- The unit cannot connect via wireless LAN to an access point that uses only WEP or WPA, which are security methods that have vulnerabilities.
- The unit is not a network device (for example, a router or switching hub). It is strongly recommended that you connect the unit to a network where you can configure and manage the network settings appropriately to protect against network-based attacks, such as DoS attacks (Denial of Service attacks).
- When connecting the unit to a network, connect it via a router that is configured and managed appropriately, or connect it to a LAN port that has the same functionality. If connected without such protection (for example when using free Wi-Fi), security issues may occur. When properly configured, routers provide sufficient protection against DoS attacks or loss of functionality of devices in the network. If you notice anything unusual, immediately disconnect the camera from the network.

TP1002107991

Precautions Related to the Network Function

This topic describes precautions about the network function of the unit.

- If unauthorized access is detected, the camera may become unable to accept communications. If this occurs, reconnect from the beginning.
- The authentication information for connecting to the unit is displayed when you use [Network] – [Network Setup] – [Show Authentication]. Take care that the screen cannot be viewed and the QR code image cannot be copied by others.
- A user name and password must be set at the time of purchase. When setting your user name and password, make sure that the settings are not visible to others. Set the user name and password as follows.

[User Name]	Set a user name comprising 1 to 16 characters. This is set to “admin” by factory default. The following are valid input characters. Alphabetic characters (uppercase and lowercase), numeric characters, symbols (! % + , - . = _)
[Password]	Set a password comprising 8 to 16 characters containing at least 1 or more alphabetic characters and 1 or more numeric characters. The following are valid input characters. Alphabetic characters (uppercase and lowercase), numeric characters, symbols (! % + , - . = _)

Precautions Related to Wireless LAN

This topic describes precautions when connecting the unit via wireless LAN.

- In the Help Guide for this unit, wireless LAN access points and wireless LAN routers that relay LAN connections are referred to as “access points.”
- [Security] (encryption method) can be set to [None], [WPA2], or [WPA3]. The use of [WPA2] or [WPA3] is recommended from a security standpoint. When [None] is selected, a message is displayed before connecting. For secure wireless LAN connection, connection to access points with WPA2 or WPA3 security setting is strongly recommended.
- By default, the WPA2 security method is selected when registering a wireless LAN access point using [Manual Register].
- If you connect to an access point without any security setting, you may be subject to hacking, access by malicious third parties, or attacks upon vulnerabilities. Unless it is otherwise unavoidable, connection without any security setting is not recommended.
- Configuring security on a wireless LAN is very important. Sony will not be liable for any damages resulting from security measures not being taken, or if a security problem occurs due to unavoidable circumstances in the use of wireless LAN.

TP1002107993

MPC-2610
Security Precautions

Precautions Related to USB Tethering

This topic describes precautions when connecting the unit via USB tethering.

- Only use trusted smartphone devices for tethering. Connecting to devices of unknown origin is not recommended due to security concerns.

TP1002107994

MPC-2610
Security Precautions

About the FTPES (FTPS) Function

The FTPS function supports various encryption algorithms to ensure secure file transfer. Multiple encryption algorithms, some of which may not comply with current security best practices, are supported for compatibility with a wide range of servers.

Encryption algorithms supported by the FTPS function

The following encryption algorithms are supported.

- 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

Recommended encryption algorithms

The following encryption algorithms are recommended based on the NIST recommendations (NIST SP 800-57 Part 1 Revision 5) and related security standards.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

About deprecated algorithms

The FTPS function also supports the following algorithms for compatibility, but they are deprecated based on the NIST recommendations (NIST SP 800-57 Part 1 Revision 5) and related security standards, and may be removed in a future version.

- 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

About connection compatibility

The FTPS function is designed with a balance between security and compatibility. Currently, deprecated algorithms are supported for the following reasons, but they may be removed in a future version to improve security.

- Freelance photographers and videographers need to connect to servers running on various clients.
- Compatibility with older systems and legacy servers needs to be maintained.
- Not all users are prepared to change to a more secure setting because changing the encryption algorithm settings on the server side is complicated.
- The FTPS settings are often shared with other secure services. Any changes must be considered carefully as they may have an impact on other services on the server.
- A wide range of encryption algorithms must be supported to ensure interoperability in different environments.

The encryption algorithm used during an FTPS connection is determined by automatic negotiation with the destination server, and therefore depends on the server settings. While aware of the security risks, compatibility is currently prioritized to satisfy the diverse needs of users.

Security risks

Using deprecated algorithms, including CBC/DHE/RSA/SHA-1, increases the risk that encrypted data may be decrypted or tampered with by an attacker, exposing data during transfer.

Recommendation for secure connection

Before using the FTPS function, check that the connection destination server supports the recommended encryption algorithm. Enable only the recommended algorithms on the server side and disable the deprecated algorithms.

Uploading using secure FTP

You can upload files with encryption using FTPS in Explicit mode (FTPES) for the connection with the destination file server.
For secure FTP transfer, set [Using Secure Protocol] to [On] in the file transfer destination server settings and import a certificate.

References

- 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 (includes updates as of 10/06/2016).

Certificate

Write the certificate used by the FTPES (FTPS) function to the root directory of a memory card. Set the file name as follows.
certification.pem (PEM format)
The maximum certificate size that can be loaded is 1 MB per certificate.

TP1002107995