

MPC-2610

Tindakan Keamanan

Panduan Bantuan ini menjelaskan tindakan keamanan untuk transfer file dan streaming menggunakan unit.

[Tindakan Keamanan](#)[Tindakan Pencegahan Koneksi Internet](#)[Tindakan Pencegahan Terkait Fungsi Jaringan](#)[Tindakan Pencegahan Terkait LAN Nirkabel](#)[Tindakan Pencegahan Terkait Penambatan USB](#)[Tentang Fungsi FTPES \(FTPS\)](#)

Tindakan Keamanan

Topik ini menjelaskan tindakan pencegahan saat menghubungkan unit ke jaringan.

- Konten komunikasi mungkin dicegat secara sembunyi-sembunyi oleh pihak ketiga yang tidak sah di sekitar lokasi sinyal. Saat menggunakan komunikasi LAN nirkabel, terapkan langkah pengamanan yang tepat untuk melindungi konten komunikasi.
- Jika Anda menyetel pengaturan LAN nirkabel [Security] ke [None] dan terhubung ke titik akses, komunikasi nirkabel antara kamera dan titik akses tidak akan dienkripsi dan dapat disadap oleh pihak ketiga dalam jangkauan sinyal. Gunakan protokol keamanan WPA2 atau WPA3 untuk keamanan yang lebih baik.
- SONY TIDAK AKAN BERTANGGUNG JAWAB ATAS GANTI RUGI APA PUN AKIBAT KELALAIAN DALAM MENERAPKAN UPAYA KEAMANAN YANG BAIK PADA PERANGKAT TRANSMISI, KEBOCORAN DATA YANG TIDAK DAPAT DIHINDARI AKIBAT SPESIFIKASI TRANSMISI, ATAU MASALAH KEAMANAN APA PUN.
- Tergantung pada lingkungan pengoperasian, pihak ketiga tidak sah di jaringan mungkin dapat mengakses unit. Saat menyambungkan unit ke jaringan, pastikan bahwa jaringan terlindung dengan aman.
- Saat menyambungkan produk ini ke jaringan, sambungkan melalui sistem yang memberikan fungsi perlindungan, seperti router atau firewall. Jika tersambung tanpa perlindungan tersebut, masalah keamanan dapat terjadi.

TP1002221097

Tindakan Pencegahan Koneksi Internet

Topik ini menjelaskan tindakan pencegahan saat menghubungkan unit ke Internet.

- Unit tidak dapat terhubung melalui LAN nirkabel ke titik akses yang hanya menggunakan WEP atau WPA, yang merupakan metode keamanan yang memiliki kerentanan.
- Unit tersebut bukan perangkat jaringan (misalnya, router atau switching hub). Sangat disarankan agar Anda menghubungkan unit ke jaringan tempat Anda dapat mengonfigurasi dan mengelola pengaturan jaringan dengan tepat untuk melindungi dari serangan berbasis jaringan, seperti serangan DoS (serangan Denial of Service).
- Saat menghubungkan unit ke jaringan, hubungkan melalui router yang dikonfigurasi dan dikelola dengan tepat, atau hubungkan ke port LAN yang memiliki fungsi yang sama. Jika terhubung tanpa perlindungan tersebut (misalnya saat menggunakan Wi-Fi gratis), masalah keamanan dapat terjadi. Bila dikonfigurasi dengan benar, router memberikan perlindungan yang memadai terhadap serangan DoS atau hilangnya fungsionalitas perangkat dalam jaringan. Jika Anda melihat sesuatu yang tidak biasa, segera putuskan sambungan kamera dari jaringan.

TP1002221098

Tindakan Pencegahan Terkait Fungsi Jaringan

Topik ini menjelaskan tindakan pencegahan terkait fungsi jaringan unit.

- Jika akses tidak sah terdeteksi, kamera mungkin tidak dapat menerima komunikasi. Jika ini terjadi, sambungkan kembali dari awal.
- Informasi autentikasi untuk menghubungkan ke unit ditampilkan saat Anda menggunakan [Network] – [Network Setup] – [Show Authentication]. Berhati-hatilah agar layar tidak dapat dilihat dan gambar kode QR tidak dapat disalin oleh orang lain.
- Nama pengguna dan kata sandi harus ditetapkan pada saat pembelian. Saat mengatur nama pengguna dan kata sandi Anda, pastikan pengaturan tersebut tidak terlihat oleh orang lain. Tetapkan nama pengguna dan kata sandi sebagai berikut.

[User Name]	– Tetapkan nama pengguna yang terdiri dari 1 hingga 16 karakter. – Ini akan ditetapkan sebagai "admin" sesuai default pabrik. – Berikut ini adalah karakter masukan yang valid. Karakter alfabet (huruf besar dan kecil), karakter numerik, simbol (! % + , - . = _)
[Password]	– Tetapkan kata sandi yang terdiri dari 8 hingga 16 karakter, yang setidaknya memiliki 1 atau lebih karakter alfabet dan 1 atau lebih karakter numerik. – Berikut ini adalah karakter masukan yang valid. Karakter alfabet (huruf besar dan kecil), karakter numerik, simbol (! % + , - . = _)

TP1002221099

Tindakan Pencegahan Terkait LAN Nirkabel

Topik ini menjelaskan tindakan pencegahan saat menghubungkan unit menggunakan LAN nirkabel.

- Dalam Panduan Bantuan untuk unit ini, titik akses LAN nirkabel dan router LAN nirkabel yang meneruskan koneksi LAN disebut sebagai "titik akses".
- [Security] (metode enkripsi) dapat diatur ke [None], [WPA2], atau [WPA3]. Dari sudut pandang keamanan, penggunaan [WPA2] atau [WPA3] direkomendasikan. Saat [None] dipilih, pesan ditampilkan sebelum menghubungkan. Untuk koneksi LAN nirkabel yang aman, koneksi ke titik akses dengan pengaturan keamanan WPA2 atau WPA3 sangat disarankan.
- Secara default, metode keamanan WPA2 dipilih saat mendaftarkan titik akses LAN nirkabel menggunakan [Manual Register].
- Jika Anda terhubung ke titik akses tanpa pengaturan keamanan apa pun, Anda dapat menjadi sasaran peretasan, akses oleh pihak ketiga yang jahat, atau serangan terhadap kerentanan. Kecuali jika tidak dapat dihindari, koneksi tanpa pengaturan keamanan apa pun tidak disarankan.
- Sangat penting untuk mengonfigurasi keamanan pada LAN nirkabel. Sony tidak bertanggung jawab atas segala kerusakan yang terjadi akibat tidak dilakukannya tindakan pengamanan, atau jika terjadi masalah keamanan akibat keadaan yang tidak dapat dihindari dalam penggunaan LAN nirkabel.

TP1002221100

Tindakan Pencegahan Terkait Penambatan USB

Topik ini menjelaskan tindakan pencegahan saat menghubungkan unit menggunakan penambatan USB.

- Hanya gunakan perangkat smartphone yang tepercaya untuk penambatan. Menghubungkan ke perangkat yang tidak diketahui asalnya tidak disarankan karena masalah keamanan.

TP1002221101

Tentang Fungsi FTPES (FTPS)

Fungsi FTPS mendukung berbagai algoritma enkripsi untuk memastikan transfer file aman. Beberapa algoritma enkripsi, yang beberapa di antaranya mungkin tidak mematuhi praktik terbaik keamanan saat ini, didukung untuk kompatibilitas dengan berbagai server.

Algoritma enkripsi yang didukung oleh fungsi FTPS

Algoritma enkripsi berikut didukung.

- 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

Algoritma enkripsi yang direkomendasikan

Algoritma enkripsi berikut direkomendasikan berdasarkan rekomendasi NIST (NIST SP 800-57 Bagian 1 Revisi 5) dan standar keamanan terkait.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Tentang algoritma yang sudah tidak digunakan lagi

Fungsi FTPS juga mendukung algoritme berikut untuk kompatibilitas, namun algoritma tersebut tidak lagi digunakan berdasarkan rekomendasi NIST (NIST SP 800-57 Bagian 1 Revisi 5) dan standar keamanan terkait, dan mungkin dihapus di versi mendatang.

- 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

Tentang kompatibilitas koneksi

Fungsi FTPS dirancang dengan keseimbangan antara keamanan dan kompatibilitas. Saat ini, algoritma yang sudah tidak digunakan lagi didukung karena alasan berikut, tetapi algoritma tersebut mungkin dihapus di versi mendatang untuk meningkatkan keamanan.

- Fotografer dan videografer lepas perlu terhubung ke server yang berjalan pada berbagai klien.
- Kompatibilitas dengan sistem lama dan server lama perlu dipertahankan.
- Tidak semua pengguna siap untuk mengubah ke pengaturan yang lebih aman karena mengubah pengaturan algoritma enkripsi di sisi server itu rumit.
- Pengaturan FTPS sering kali dibagikan dengan layanan aman lainnya. Perubahan apa pun harus dipertimbangkan dengan baik karena dapat berdampak terhadap layanan lain pada server.
- Berbagai macam algoritma enkripsi harus didukung untuk memastikan interoperabilitas di berbagai lingkungan.

Algoritma enkripsi yang digunakan selama koneksi FTPS ditentukan oleh negosiasi otomatis dengan server tujuan, dan oleh karena itu bergantung pada pengaturan server. Meskipun menyadari risiko keamanan, kompatibilitas saat ini diutamakan untuk memenuhi beragam kebutuhan pengguna.

Risiko keamanan

Menggunakan algoritma yang sudah tidak digunakan lagi, termasuk CBC/DHE/RSA/SHA-1, meningkatkan risiko bahwa data terenkripsi dapat didekripsi atau dirusak oleh penyerang, sehingga mengekspos data selama transfer.

Rekomendasi untuk koneksi aman

Sebelum menggunakan fungsi FTPS, periksa apakah server tujuan koneksi mendukung algoritma enkripsi yang direkomendasikan. Aktifkan hanya algoritma yang direkomendasikan di sisi server dan nonaktifkan algoritma yang tidak digunakan lagi.

Mengunggah menggunakan FTP aman

Anda dapat mengunggah file dengan enkripsi menggunakan FTPS dalam mode Eksplisit (FTPES) untuk koneksi dengan server file tujuan.

Untuk transfer FTP aman, atur [Using Secure Protocol] ke [On] pada pengaturan server tujuan transfer file dan impor sertifikat.

Referensi

- 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 (termasuk pembaruan per 10/06/2016).

Sertifikat

Tulis sertifikat yang digunakan oleh fungsi FTPES (FTPS) ke direktori root kartu memori. Tetapkan nama file sebagai berikut.

sertifikasi.pem (format PEM)

Ukuran sertifikat maksimum yang dapat dimuat adalah 1 MB per sertifikat.

TP1002221102