SONY

Οδηγός βοήθειας

MPC-2610

Προφυλάξεις ασφάλειας

Ο παρών Οδηγός βοήθειας περιγράφει τις προφυλάξεις ασφάλειας για τη μεταφορά αρχείων και τη δυνατότητα streaming κατά τη χρήση της μονάδας.

5-073-645-21(1) Copyright 2025 Sony Corporation

MPC-2610
Προφυλάξεις ασφάλειας

Προφυλάξεις ασφάλειας

Στην τρέχουσα ενότητα περιγράφονται οι προφυλάξεις που πρέπει να παίρνετε κατά τη σύνδεση της μονάδας σε δίκτυο.

- Το περιεχόμενο της επικοινωνίας ενδέχεται να υποκλαπεί εν αγνοία σας από μη εξουσιοδοτημένα τρίτα πρόσωπα πλησίον των σημάτων. Κατά τη χρήση ασύρματης επικοινωνίας LAN, εφαρμόζετε καταλλήλως μέτρα ασφαλείας για λόγους προστασίας του περιεχομένου της επικοινωνίας.
- Αν καθορίσετε στη ρύθμιση [Security] για το ασύρματο LAN την επιλογή [None] και συνδεθείτε σε κάποιο σημείο πρόσβασης, η ασύρματη επικοινωνία μεταξύ της κάμερας και του σημείου πρόσβασης δεν θα είναι κρυπτογραφημένη και υπάρχει κίνδυνος να υποκλαπεί από τρίτους που βρίσκονται στην εμβέλεια του σήματος. Χρησιμοποιήστε το πρωτόκολλο ασφάλειας WPA2 ή WPA3 για επαυξημένη ασφάλεια.
- Η SONY ΔΕΝ ΦΕΡΕΙ ΕΥΘΥΝΗ ΓΙΑ ΟΠΟΙΑΔΗΠΟΤΕ ΖΗΜΙΑ ΠΡΟΚΛΗΘΕΙ ΑΠΟ ΤΗΝ ΑΔΥΝΑΜΙΑ ΕΦΑΡΜΟΓΗΣ ΤΩΝ ΚΑΤΑΛΛΗΛΩΝ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ ΣΕ ΣΥΣΚΕΥΕΣ ΜΕΤΑΔΟΣΗΣ, ΑΝΑΠΟΦΕΥΚΤΕΣ ΔΙΑΡΡΟΕΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΚΛΗΘΟΥΝ ΑΠΟ ΤΙΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΜΕΤΑΔΟΣΗΣ Ή ΟΠΟΙΟΔΗΠΟΤΕ ΠΡΟΒΛΗΜΑ ΠΟΥ ΑΦΟΡΑ ΣΤΗΝ ΑΣΦΑΛΕΙΑ.
- Ανάλογα με το περιβάλλον λειτουργίας, τυχόν μη εξουσιοδοτημένα τρίτα πρόσωπα στο δίκτυο ενδέχεται να είναι σε θέση να αποκτήσουν πρόσβαση στη μονάδα. Κατά τη σύνδεση της μονάδας στο δίκτυο, βεβαιωθείτε ότι το δίκτυο προστατεύεται με ασφαλή τρόπο.
- Κατά τη σύνδεση του προϊόντος αυτού σε ένα δίκτυο, χρησιμοποιήστε ένα σύστημα που παρέχει μια λειτουργία προστασίας, όπως router ή firewall. Αν συνδεθεί χωρίς τέτοιου είδους προστασίας, μπορεί να ανακύψουν προβλήματα ασφάλειας.

TP1002221033

5-073-645-21(1) Copyright 2025 Sony Corporation

MPC-2610
Προφυλάξεις ασφάλειας

Προφυλάξεις κατά τη σύνδεση στο Internet

Στην τρέχουσα ενότητα περιγράφονται οι προφυλάξεις που πρέπει να παίρνετε κατά τη σύνδεση της μονάδας στο Internet.

- Η μονάδα δεν μπορεί να συνδεθεί μέσω ασύρματου LAN σε κάποιο σημείο πρόσβασης που χρησιμοποιεί μόνο πρωτόκολλο WEP ή WPA, τα οποία είναι μέθοδοι ασφάλειας που έχουν τρωτά σημεία.
- Η μονάδα δεν είναι συσκευή δικτύου (π.χ. δρομολογητής ή κόμβος μεταγωγής). Συνιστάται ανεπιφύλακτα να συνδέετε τη μονάδα σε δίκτυο όπου μπορείτε να διαμορφώσετε και να διαχειριστείτε τις ρυθμίσεις δικτύου με τον ενδεδειγμένο τρόπο για προστασία από επιθέσεις βάσει του δικτύου, όπως επιθέσεις DoS (δηλαδή επιθέσεις που εκδηλώνονται ως άρνηση παροχής υπηρεσίας).
- Όποτε συνδέετε τη μονάδα σε κάποιο δίκτυο, πρέπει να κάνετε τη σύνδεσή της μέσω ενός δρομολογητή του οποίου τις ρυθμίσεις μπορείτε να διαμορφώσετε και να διαχειριστείτε με τον ενδεδειγμένο τρόπο ή σε μια θύρα LAN που έχει την ίδια λειτουργικότητα. Αν συνδεθεί χωρίς την εν λόγω προστασία (π.χ. κατά τη χρήση δωρεάν Wi-Fi), υπάρχει κίνδυνος να παρουσιαστούν ζητήματα ασφάλειας. Με την ενδεδειγμένη διαμόρφωση ρυθμίσεων, οι δρομολογητές παρέχουν επαρκή προστασία από επιθέσεις DoS ή απώλεια λειτουργικότητας συσκευών στο δίκτυο. Αν παρατηρήσετε οτιδήποτε ασυνήθιστο, αποσυνδέστε αμέσως την κάμερα από το δίκτυο.

TP1002221034

5-073-645-21(1) Copyright 2025 Sony Corporation

MPC-2610
Προφυλάξεις ασφάλειας

Προφυλάξεις όσον αφορά τη λειτουργία δικτύου

Στην τρέχουσα ενότητα περιγράφονται οι προφυλάξεις που πρέπει να παίρνετε για τη λειτουργία δικτύου της μονάδας.

- Αν ανιχνευτεί μη εξουσιοδοτημένη πρόσβαση, η κάμερα ενδέχεται να πάψει να έχει τη δυνατότητα αποδοχής επικοινωνιών. Στην περίπτωση αυτή, επαναλάβετε τη διαδικασία σύνδεσης από την αρχή.
- Οι πληροφορίες επαλήθευσης ταυτότητας για τη σύνδεση με τη μονάδα εμφανίζονται εφόσον χρησιμοποιήσετε τις επιλογές [Network] – [Network Setup] – [Show Authentication]. Θα πρέπει να προσέξετε να μη δουν άλλα άτομα την οθόνη και να μην μπορέσουν να αντιγράψουν την εικόνα του κωδικού QR.
- Πρέπει να καθορίσετε όνομα χρήστη και κωδικό πρόσβασης κατά την αγορά του προϊόντος. Κατά τον καθορισμό του ατομικού σας ονόματος χρήστη και του κωδικού πρόσβασής σας, πρέπει να βεβαιωθείτε ότι κανείς άλλος δεν μπορεί να δει τις ρυθμίσεις σας. Καθορίστε το όνομα χρήστη και τον κωδικό πρόσβασης όπως υποδεικνύεται παρακάτω.

[User Name]	– Καθορίστε ένα όνομα χρήστη που να αποτελείται από 1 έως 16 χαρακτήρες. – Με βάση τις εργοστασιακές προεπιλεγμένες ρυθμίσεις, είναι επιλεγμένο το όνομα "admin". – Έγκυροι για την καταχώρησή σας είναι οι χαρακτήρες που παρατίθενται παρακάτω. Αλφαβητικοί χαρακτήρες (πεζά και κεφαλαία γράμματα), αριθμικοί χαρακτήρες, σύμβολα (! % + , - . = _)
[Password]	– Καθορίστε έναν κωδικό πρόσβασης που να αποτελείται από 8 έως 16 στους οποίους πρέπει να περιλαμβάνονται τουλάχιστον 1 ή περισσότεροι αλφαβητικοί χαρακτήρες και 1 ή περισσότεροι αριθμικοί χαρακτήρες. – Έγκυροι για την καταχώρησή σας είναι οι χαρακτήρες που παρατίθενται παρακάτω. Αλφαβητικοί χαρακτήρες (πεζά και κεφαλαία γράμματα), αριθμικοί χαρακτήρες, σύμβολα (! % + , - . = _)

TP1002221035

5-073-645-21(1) Copyright 2025 Sony Corporation

MPC-2610
Προφυλάξεις ασφάλειας

Προφυλάξεις όσον αφορά το ασύρματο LAN

Στην τρέχουσα ενότητα περιγράφονται οι προφυλάξεις που πρέπει να παίρνετε κατά τη σύνδεση της μονάδας μέσω ασύρματου LAN.

- Στον Οδηγό βοήθειας για τη συγκεκριμένη μονάδα, τα σημεία πρόσβασης σε ασύρματο LAN και οι δρομολογητές ασύρματου LAN που αναμεταδίδουν συνδέσεις LAN αναφέρονται ως "σημεία πρόσβασης".
- Στην επιλογή [Security] (μέθοδο κρυπτογράφησης) μπορείτε να καθορίσετε τη ρύθμιση [None], τη ρύθμιση [WPA2] ή τη ρύθμιση [WPA3]. Από άποψη ασφάλειας συνιστάται η χρήση της ρύθμισης [WPA2] ή της ρύθμισης [WPA3]. Εφόσον είναι επιλεγμένη η ρύθμιση [None], εμφανίζεται ένα μήνυμα προτού πραγματοποιηθεί η σύνδεση. Για ασφαλή σύνδεση σε ασύρματο LAN, συνιστάται ανεπιφύλακτα η σύνδεση σε σημεία πρόσβασης με χρήση της ρύθμισης ασφάλειας WPA2 ή WPA3.
- Από προεπιλογή, είναι καθορισμένη η μέθοδος ασφάλειας WPA2 κατά την καταχώρηση ενός σημείου πρόσβασης ασύρματου LAN με χρήση της ρύθμισης [Manual Register].
- Αν συνδεθείτε σε κάποιο σημείο πρόσβασης χωρίς καμία ρύθμιση ασφάλειας, διατρέχετε τον κίνδυνο πειρατείας, πρόσβασης από κακόβουλους τρίτους ή επιθέσεων στα τρωτά σημεία. Αν δεν είναι αναπόφευκτο για οποιονδήποτε άλλο λόγο, δεν συνιστάται η σύνδεση χωρίς ρύθμιση ασφάλειας.
- Η διαμόρφωση των ρυθμίσεων για την ασφάλεια σε ένα ασύρματο LAN είναι πολύ σημαντική. Η Sony δεν θα φέρει ευθύνη για ζημιές που ενδέχεται να προκληθούν αν δεν ληφθούν μέτρα ασφάλειας ή αν παρουσιαστεί κάποιο πρόβλημα λόγω αναπόφευκτων περιστάσεων κατά τη χρήση ασύρματου LAN.

TP1002221036

5-073-645-21(1) Copyright 2025 Sony Corporation

MPC-2610
Προφυλάξεις ασφάλειας

Προφυλάξεις όσον αφορά την πρόσδεση μέσω USB

Στην τρέχουσα ενότητα περιγράφονται οι προφυλάξεις που πρέπει να παίρνετε κατά τη σύνδεση της μονάδας με πρόσδεση μέσω USB.

- Πρέπει να χρησιμοποιείτε μόνο αξιόπιστες συσκευές smartphone για την πρόσδεση. Λόγω ζητημάτων ασφάλειας, δεν συνιστάται η σύνδεση με συσκευές άγνωστης προέλευσης.

TP1002221037

5-073-645-21(1) Copyright 2025 Sony Corporation

Πληροφορίες για τη λειτουργία FTPES (FTPS)

Η λειτουργία FTPS υποστηρίζει διάφορους αλγορίθμους κρυπτογράφησης για προστασία της ασφαλούς μεταφοράς αρχείων. Για λόγους συμβατότητας με ένα ευρύ φάσμα διακομιστών, υποστηρίζονται πολλαπλοί αλγόριθμοι κρυπτογράφησης, εκ των οποίων ορισμένοι ενδέχεται να μη συμμορφώνονται με τις τρέχουσες βέλτιστες πρακτικές ασφάλειας.

Αλγόριθμοι κρυπτογράφησης που υποστηρίζονται από τη λειτουργία FTPS

Υποστηρίζονται οι παρακάτω αλγόριθμοι κρυπτογράφησης.

- 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

Συνιστώμενοι αλγόριθμοι κρυπτογράφησης

Συνιστώνται οι παρακάτω αλγόριθμοι κρυπτογράφησης με βάση τις συστάσεις του οργανισμού NIST (NIST SP 800-57, Τμήμα 1, Αναθεώρηση 5) και σχετικών προτύπων ασφάλειας.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Πληροφορίες για παρωχημένους αλγορίθμους

Η λειτουργία FTPS υποστηρίζει επίσης τους παρακάτω αλγορίθμους για λόγους συμβατότητας, αλλά είναι παρωχημένοι με βάση τις συστάσεις του οργανισμού NIST (NIST SP 800-57, Τμήμα 1, Αναθεώρηση 5) και σχετικών προτύπων ασφάλειας και ενδέχεται να καταργηθούν σε κάποια μελλοντική έκδοση.

- 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

Πληροφορίες για τη συμβατότητα σύνδεσης

Η λειτουργία FTPS είναι σχεδιασμένη με μια ισορροπία μεταξύ ασφάλειας και συμβατότητας. Προς το παρόν, οι παρωχημένοι αλγόριθμοι υποστηρίζονται για τους λόγους που παρατίθενται παρακάτω, αλλά ενδέχεται να καταργηθούν σε κάποια μελλοντική έκδοση για βελτίωση της ασφάλειας.

- Οι ανεξάρτητοι φωτογράφοι και βιντεολήπτες χρειάζεται να συνδέονται σε διακομιστές που χρησιμοποιούν ποικίλα προγράμματα-πελάτες.
- Χρειάζεται να διατηρηθεί η συμβατότητα με παλαιότερα συστήματα και προϋπάρχοντες διακομιστές.
- Δεν είναι όλοι οι χρήστες προετοιμασμένοι να περάσουν σε μια ασφαλέστερη ρύθμιση, επειδή η αλλαγή των ρυθμίσεων για τους αλγορίθμους κρυπτογράφησης στα συστήματα των διακομιστών είναι μια πολύπλοκη διαδικασία.
- Οι ρυθμίσεις FTPS συχνά χρησιμοποιούνται από κοινού με άλλες ασφαλείς υπηρεσίες. Κάθε αλλαγή πρέπει να εξετάζεται προσεκτικά, επειδή ενδέχεται να έχει αντίκτυπο σε άλλες υπηρεσίες στον διακομιστή.
- Πρέπει να υποστηρίζεται ένα ευρύ φάσμα αλγορίθμων κρυπτογράφησης για να διασφαλίζεται η διαλειτουργικότητα σε διαφορετικά περιβάλλοντα.

Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται κατά τη διάρκεια μιας σύνδεσης FTPS καθορίζεται κατόπιν αυτόματης διαπραγμάτευσης με τον διακομιστή προορισμού, πράγμα που σημαίνει ότι εξαρτάται από τις ρυθμίσεις του διακομιστή. Παρόλο που έχουμε επίγνωση των κινδύνων για την ασφάλεια, προς το παρόν δίνουμε προτεραιότητα στη συμβατότητα για να μπορούμε να ικανοποιήσουμε τις ποικίλες ανάγκες των χρηστών.

Κίνδυνοι για την ασφάλεια

Αν χρησιμοποιήσετε παρωχημένους αλγορίθμους, στους οποίους περιλαμβάνονται οι CBC/DHE/RSA/SHA-1, αυξάνεται ο κίνδυνος αποκρυπτογράφησης ή παραποίησης των κρυπτογραφημένων δεδομένων από κάποιον δράστη επίθεσης, με συνέπεια την έκθεση των δεδομένων κατά τη μεταφορά τους.

Συστάσεις για ασφαλή σύνδεση

Προτού χρησιμοποιήσετε τη λειτουργία FTPS, ελέγξτε αν ο διακομιστής προορισμού της σύνδεσης υποστηρίζει τον συνιστώμενο αλγόριθμο κρυπτογράφησης. Ενεργοποιήστε μόνο τους συνιστώμενους αλγορίθμους στο σύστημα του διακομιστή και απενεργοποιήστε τους παρωχημένους.

Μεταφόρτωση με χρήση ασφαλούς πρωτοκόλλου FTP

Μπορείτε να μεταφορτώσετε αρχεία με κρυπτογράφηση χρησιμοποιώντας το πρωτόκολλο FTPS σε λειτουργία ρητής (Explicit) εντολής (FTPES) για τη σύνδεση με τον διακομιστή προορισμού των αρχείων.
Για μεταφορά με χρήση ασφαλούς πρωτοκόλλου FTP, στην επιλογή [Using Secure Protocol] καθορίστε τη ρύθμιση [On] στις ρυθμίσεις για τον διακομιστή προορισμού της μεταφοράς αρχείων και προχωρήστε στην εισαγωγή ενός πιστοποιητικού.

Πηγές αναφοράς

- 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 (περιλαμβάνονται επικαιροποιήσεις από 10/06/2016).

Πιστοποιητικό

Πραγματοποιήστε εγγραφή του πιστοποιητικού που χρησιμοποιείται από τη λειτουργία FTPES (FTPS) στον ριζικό κατάλογο μιας κάρτας μνήμης. Καθορίστε το όνομα του αρχείου όπως υποδεικνύεται παρακάτω.
certification.pem (μορφότυπο PEM)
Το μέγιστο μέγεθος αρχείου που μπορεί να φορτωθεί είναι 1 MB ανά πιστοποιητικό.

TP1002221038

5-073-645-21(1) Copyright 2025 Sony Corporation