

MPC-3628/MPC-3626

Veiligheidsmaatregelen

Deze Help-gids beschrijft de veiligheidsmaatregelen voor bestandsoverdracht en streaming met behulp van het apparaat.

[Veiligheidsmaatregelen](#)[Voorzorgsmaatregelen voor internetverbinding](#)[Voorzorgsmaatregelen met betrekking tot de netwerkfunctie](#)[Voorzorgsmaatregelen met betrekking tot draadloos LAN](#)

Veiligheidsmaatregelen

Dit onderwerp beschrijft de veiligheidsmaatregelen bij het verbinden van het apparaat met een netwerk.

- De inhoud van communicatie kan zonder dat u dat weet worden onderschept door onbevoegden in de buurt van het signaal. Wanneer u draadloze LAN-communicatie gebruikt, pas dan correcte beveiligingsmaatregelen toe om de inhoud van uw communicatie te beschermen.
- **SONY IS NIET AANSPRAKELIJK VOOR WELKE SCHADE DAN OOK DIE VOORTKOMT UIT HET NIET NEMEN VAN VOLDOENDE BEVEILIGINGSMAATREGELEN OP TRANSMISSIEAPPARATEN, ONVERMIJDBARE GEGEVENSLEKKEN DOOR TRANSMISSIESPECIFICATIES OF BEVEILIGINGSPROBLEMEN VAN WELKE AARD DAN OOK.**
- Afhankelijk van de gebruiksomgeving kunnen onbevoegden via het netwerk toegang krijgen tot het apparaat. Wanneer u het apparaat verbinding laat maken met het netwerk, zorg er dan voor dat het netwerk goed is beveiligd.
- Wanneer u dit product aansluit op een netwerk, maak dan verbinding via een systeem dat beveiliging biedt, zoals een router of firewall. Als u verbinding maakt zonder dergelijke bescherming kunnen beveiligingsproblemen ontstaan.

TP1002273746

Voorzorgsmaatregelen voor internetverbinding

Dit onderwerp beschrijft de voorzorgsmaatregelen bij het verbinden van het apparaat met het internet.

- Het apparaat kan niet via een draadloos LAN met een toegangspunt verbinden dat alleen WEP of WPA gebruikt. Dat zijn beveiligingsmethodes die kwetsbaarheden vertonen.
- Het apparaat is geen netwerkkapparaat (bijvoorbeeld een router of switchhub). Het wordt ten eerste aangeraden om het apparaat met een netwerk te verbinden, waar u de netwerkinstellingen op de juiste manier kunt configureren en beheren om u tegen netwerkaanvallen, zoals DoS-aanvallen (Denial-of-Service-aanvallen), te beschermen.
- Verbind het apparaat bij het verbinden met een netwerk via een router die op de juiste manier is geconfigureerd en wordt beheerd of verbind het met een LAN-poort met dezelfde functionaliteit. Als er verbinding wordt gemaakt zonder een dergelijke bescherming (bijvoorbeeld bij gebruik van gratis wifi), kunnen er beveiligingsproblemen optreden. Indien goed geconfigureerd, bieden routers voldoende bescherming tegen DoS-aanvallen of verlies van functionaliteit bij apparaten in het netwerk. Als u iets ongewoon opmerkt, koppel de camera dan onmiddellijk los van het netwerk.

TP1002273747

Voorzorgsmaatregelen met betrekking tot de netwerkfunctie

Dit onderwerp beschrijft de voorzorgsmaatregelen met betrekking tot de netwerkfunctie van het apparaat.

- Als er onbevoegde toegang wordt gedetecteerd, kan de camera mogelijk geen communicatie meer aanvaarden. Als dit gebeurt, maak dan opnieuw verbinding vanaf het begin.
- De authenticatie-informatie voor verbinding met dit apparaat wordt weergegeven wanneer u [Technical] – [Network] – [Wireless] – [SSID] en [Password] gebruikt in het hoofdmenu. Zorg dat het scherm niet bekeken kan worden door anderen.
- Wanneer netwerkfuncties voor het eerst worden gebruikt, is de instelling [Technical] – [Authentication] – [Password] leeg in het hoofdmenu. Als er geen wachtwoord is geconfigureerd, zijn [Network]-menu-items in het installatiemenu uitgeschakeld (grijs weergegeven) en kunnen netwerkinstellingen niet worden geconfigureerd.
- Gebruik Basisauthenticatie voor toegangsauthenticatie tot het apparaat. Er bestaat een risico dat communicatie wordt onderschept, tenzij u rechtstreeks toegang heeft tot het apparaat (geen verbinding maakt via een toegangspunt of netwerkhub) of u de netwerkklientmodus gebruikt. Sony is niet aansprakelijk voor schade als gevolg van het niet nemen van beveiligingsmaatregelen of als er een beveiligingsprobleem optreedt als gevolg van onvermijdelijke omstandigheden met betrekking tot de verbinding.
- Zorg er bij het instellen van uw gebruikersnaam en wachtwoord voor dat anderen de instellingen niet kunnen zien. Stel de gebruikersnaam en het wachtwoord als volgt in.

[User Name]	– Stel een gebruikersnaam in van 1 tot 16 tekens. – Dit is standaard ingesteld op "admin". – De volgende tekens zijn geldige invoertekens. Alfabetische tekens (hoofdletters en kleine letters), numerieke tekens, symbolen (! % + , - . = _)
[Password]	– Stel een wachtwoord in van 8 tot 16 tekens met ten minste 1 of meer alfabetische tekens en 1 of meer numerieke tekens. – De volgende tekens zijn geldige invoertekens. Alfabetische tekens (hoofdletters en kleine letters), numerieke tekens, symbolen (! % + , - . = _)

TP1002273748

Voorzorgsmaatregelen met betrekking tot draadloos LAN

Dit onderwerp beschrijft de voorzorgsmaatregelen bij het verbinden van het apparaat met draadloos LAN.

- In de Help-gids voor dit apparaat worden draadloze LAN-toegangspunten en draadloze LAN-routers die LAN-verbindingen doorsturen "toegangspunten" genoemd.
- Alleen de beveiligingsmethode WPA2 (AES) wordt ondersteund.
- Als u met een toegangspunt verbinding maakt zonder enige beveiligingsinstelling, kunt u worden blootgesteld aan hacken, toegang door kwaadwillende derden of aanvallen op kwetsbaarheden. Tenzij het onvermijdelijk is, wordt een verbinding zonder beveiligingsinstellingen niet aanbevolen.
- Het instellen van beveiliging op een draadloos LAN is heel belangrijk. Sony is niet aansprakelijk voor schade als gevolg van het niet nemen van beveiligingsmaatregelen of als er een beveiligingsprobleem optreedt als gevolg van onvermijdelijke omstandigheden bij het gebruik van draadloos LAN.

TP1002273749