

MPC-3628/MPC-3626
Sicherheitsmaßnahmen

In dieser Hilfe werden die Sicherheitsmaßnahmen für die Dateiübertragung und das Streaming mit dem Gerät beschrieben.

[Sicherheitsmaßnahmen](#)

[Vorsichtsmaßnahmen für die Internet-Verbindung](#)

[Vorsichtsmaßnahmen bezüglich der Netzwerkfunktion](#)

[Vorsichtsmaßnahmen bezüglich WLAN](#)

Sicherheitsmaßnahmen

Unter diesem Thema werden Vorsichtsmaßnahmen für die Verbindung des Geräts mit einem Netzwerk beschrieben.

- Der Kommunikationsinhalt kann von unautorisierten Dritten in der Nähe des Signals abgefangen werden, ohne dass Sie es merken. Wenn Sie die WLAN-Kommunikation nutzen, implementieren Sie geeignete Sicherheitsmaßnahmen, um den Kommunikationsinhalt zu schützen.
- SONY KANN KEINE HAFTUNG FÜR SCHÄDEN JEDER ART DURCH UNTERLASSENE GEEIGNETE SICHERHEITSMASSENNAHMEN AN ÜBERTRAGUNGSGERÄTEN, DURCH UNVERMEIDBARE DATENPREISGABE AUFGRUND DER ÜBERTRAGUNGSSPEZIFIKATIONEN ODER DURCH SICHERHEITSPROBLEME JEGLICHER ART ÜBERNEHMEN.
- Je nach Betriebsumgebung können unbefugte Dritte im Netzwerk unter Umständen auf dieses Gerät zugreifen. Achten Sie beim Verbinden des Geräts mit dem Netzwerk darauf, dass das Netzwerk gut abgesichert ist.
- Schließen Sie dieses Produkt beim Verbinden mit einem Netzwerk über ein System an, das eine Schutzfunktion bietet, wie etwa ein Router oder eine Firewall. Andernfalls können Sicherheitsprobleme auftreten.

TP1002273770

Vorsichtsmaßnahmen für die Internet-Verbindung

Unter diesem Thema werden Vorsichtsmaßnahmen für die Verbindung des Geräts mit dem Internet beschrieben.

- Das Gerät kann sich nicht per WLAN mit Zugangspunkten verbinden, die lediglich die mit Schwachstellen behafteten Verschlüsselungsmethoden WEP oder WPA verwenden.
- Das Gerät ist kein Netzwerkgerät (z. B. Router oder Switch/Hub). Es wird dringend empfohlen, dass Sie das Gerät mit einem Netzwerk verbinden, bei dem Sie die Netzwerkeinstellungen geeignet konfigurieren und verwalten können, um sich vor netzwerkbasierten Angriffen wie DoS-Angriffen (Denial of Service) zu schützen.
- Verbinden Sie das Gerät mit dem Netzwerk über einen Router, der geeignet konfiguriert ist und verwaltet wird, oder verbinden Sie das Gerät mit einem LAN-Anschluss, der über die gleichen Eigenschaften verfügt. Wenn Verbindungen ohne derartigen Schutz hergestellt werden (z. B. bei der Verwendung von kostenfreiem WLAN), können Sicherheitsprobleme auftreten. Bei ordnungsgemäßer Konfiguration bieten Router ausreichenden Schutz vor DoS-Angriffen oder Funktionsverlust bei Geräten im Netzwerk. Falls Sie ungewöhnliche Aktivitäten bemerken, trennen Sie die Kamera umgehend vom Netzwerk.

TP1002273771

Vorsichtsmaßnahmen bezüglich der Netzwerkfunktion

Unter diesem Thema werden Vorsichtsmaßnahmen bezüglich der Netzwerkfunktion des Geräts beschrieben.

- Falls unbefugter Zugriff erkannt wird, ist die Kamera ggf. nicht mehr zu Kommunikation in der Lage. Stellen Sie in diesem Fall die Verbindung von Anfang an wieder her.
- Die Authentifizierungsdaten zum Verbinden mit dem Gerät werden angezeigt, wenn Sie [Technical] – [Network] – [Wireless] – [SSID] und [Password] im vollständigen Menü verwenden. Achten Sie darauf, dass der Bildschirm von niemandem betrachtet werden kann.
- Wenn die Netzwerkfunktion erstmals verwendet wird, ist die Einstellung [Technical] – [Authentication] – [Password] im vollständigen Menü leer. Wenn kein Kennwort konfiguriert ist, sind die Punkte des Menüs [Network] im Konfigurationsmenü nicht verfügbar (grau unterlegt) und die Netzwerkeinstellungen können nicht konfiguriert werden.
- Verwenden Sie beim Zugriff auf das Gerät grundlegende Authentifizierung. Es besteht die Gefahr, dass die Kommunikation von Dritten abgefangen wird, außer wenn Sie direkt (d. h. nicht über einen Zugangspunkt oder einen Netzwerkhub) auf das Gerät zugreifen oder den Netzwerkclientmodus verwenden. Sony übernimmt keine Haftung für Schäden, die aus Unterlassung von Sicherheitsmaßnahmen resultieren oder falls ein Sicherheitsproblem durch unvermeidliche Umstände in Bezug auf die Verbindung auftritt.
- Achten Sie beim Festlegen Ihres Benutzernamens und des Passworts darauf, dass die Einstellungen nicht für andere Personen sichtbar sind. Legen Sie den Benutzernamen und das Kennwort wie folgt fest.

[User Name]	– Legen Sie einen Benutzernamen fest, der aus 1 bis 16 Zeichen besteht. – Werkseitig ist hierfür „admin“ eingestellt. – Die folgenden Zeichen sind gültig. Buchstaben (groß und klein), Ziffern, Sonderzeichen (! % + , - . = _)
[Password]	– Legen Sie ein Kennwort fest, das aus 8 bis 16 Zeichen besteht, darunter mindestens einen Buchstaben und mindestens eine Ziffer. – Die folgenden Zeichen sind gültig. Buchstaben (groß und klein), Ziffern, Sonderzeichen (! % + , - . = _)

TP1002273772

Vorsichtsmaßnahmen bezüglich WLAN

Unter diesem Thema werden Vorsichtsmaßnahmen für die Verbindung des Geräts per WLAN beschrieben.

- In der Hilfe zu diesem Gerät werden WLAN-Zugangspunkte und WLAN-Router, die LAN-Verbindungen weiterleiten, als „Zugangspunkte“ bezeichnet.
- Nur die Sicherheitsmethode WPA2 (AES) wird unterstützt.
- Wenn Sie eine Verbindung zu einem Zugangspunkt ohne jegliche Sicherheitseinstellungen herstellen, können Sie Hackerangriffen, böswilligen Zugriffen Dritter oder Angriffen aufgrund von Schwachstellen ausgesetzt sein. Sofern nicht unvermeidlich, wird eine Verbindung ohne jegliche Sicherheitseinstellung nicht empfohlen.
- Es ist sehr wichtig, die Sicherheit eines WLAN zu konfigurieren. Sony übernimmt keine Haftung für Schäden, die aus Unterlassung von Sicherheitsmaßnahmen resultieren oder falls ein Sicherheitsproblem durch unvermeidliche Umstände bei der Verwendung eines WLAN auftritt.

TP1002273773