

EXPERTENMODUS UND ONVIF-PROTOKOLL

www.deltadore.com

Einleitung

Der **Expertenmodus** der **Kameras Tycam Guard** und **Tycam Home** ist für **Installateure** und **versierte Profis** bestimmt, die ihren Kunden eine **Installation nach Maß bieten** möchten.

Die Kameras der neuesten Generation der Tycam-Reihe bieten eine Web-Schnittstelle, die eine erweiterte Konfiguration mit Funktionsmerkmalen ermöglicht, die in der Tydom-App nicht verfügbar sind, wie z.B.:

- Konfiguration des ONVIF-Zugangs.
- Einstellung der Bildqualität: Helligkeit, Kontrast, Sättigung, Schärfe, Belichtung, Weißabgleich, Rauschunterdrückung etc.
- Es wurde eine Datenschutzmaske hinzugefügt, um bestimmte Bereiche des Sichtfelds der Kamera auszublenden, damit sie z. B. keine öffentlichen Bereiche filmt.

WICHTIG: Die Verwendung des Expertenmodus erfordert zwingend Fachkenntnisse in Netzwerk- und Sicherheitsfragen, um die Vorschriftsmäßigkeit der Installation und den Schutz der personenbezogenen Daten der Nutzer zu gewährleisten.

Hinweis: Bei Anwendung des Expertenmodus leistet Delta Dore keinen technischen Support.

Inhaltsverzeichnis

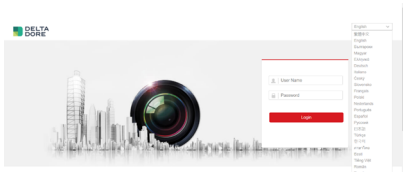
EXPERTENMODUS

1. Zugang zur Web-Schnittstelle 2
2. Arbeiten Sie in einem sicheren Netzwerk, um die Daten Ihrer Kunden zu schützen..... 2
3. Bildeinstellungen: erweiterte Funktionsmerkmale des Expertenmodus 3

ONVIF-PROTOKOLL

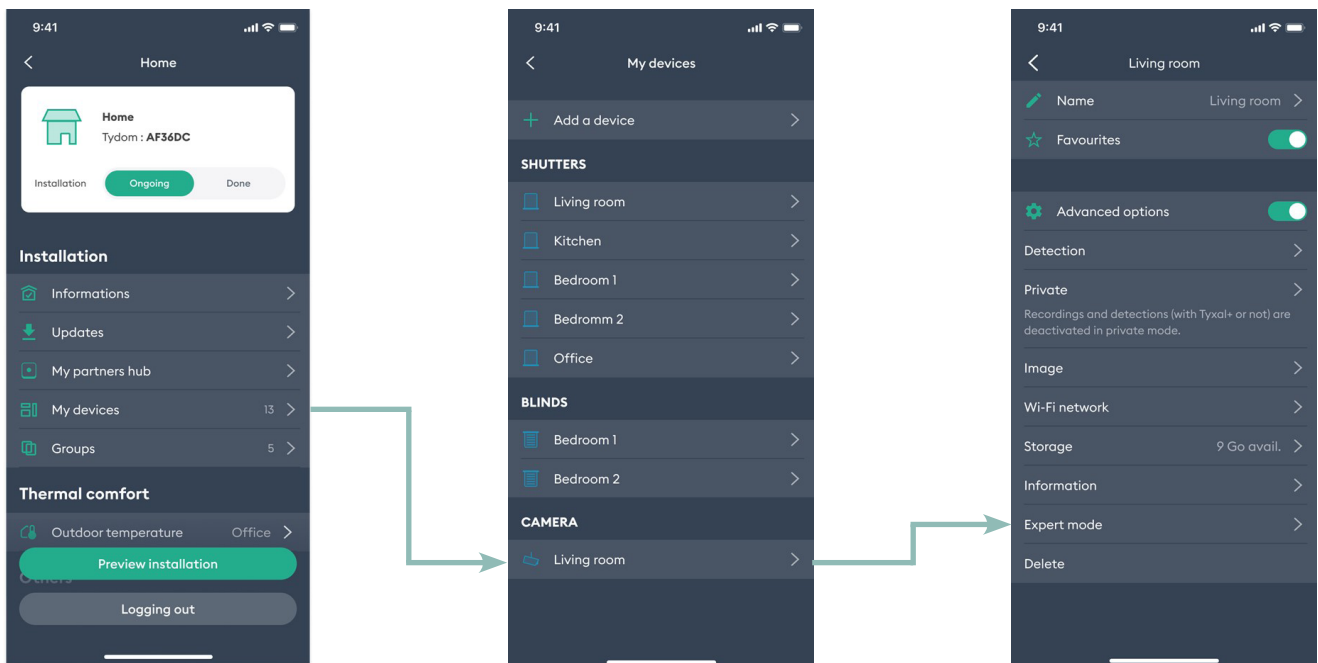
1. Universelle Kompatibilität für eine dauerhafte und skalierbare Installation .. 5
2. ONVIF-Konfiguration der Kameras Tycam Home und Guard 5

1. Zugang zur Web-Schnittstelle



Authentifizierungsseite der Web-Schnittstelle

Der Expertenmodus ist **nur über ein PRO-Konto in der Tydom-App zugänglich** und kann in den Kameraeinstellungen aktiviert werden, sobald die Kamera installiert und mit der Cloud verbunden ist. Um die Kamera mit bestimmten Drittanbietersystemen kompatibel zu machen, muss das lokale Netzwerk, über das die Kamera kommuniziert, während der gesamten Nutzung des Produkts gesichert sein, damit ONVIF und die Funktionen, die über diesen Modus zur Verfügung stehen, genutzt werden können.



2. Arbeiten Sie in einem sicheren Netzwerk, um die Daten Ihrer Kunden zu schützen.

Ein sicheres Netzwerk in einem Privathaus besteht aus einer Reihe von Geräten und Konfigurationen, die dazu dienen, die Daten, Geräte und die Privatsphäre der Bewohner vor Online-Gefahren und unberechtigt Zugriff zu schützen. Hier einige Kernelemente:

- **Verschlüsselung des WLAN-Netzwerks:** Das WLAN-Netzwerk im Haus sollte durch eine starke Verschlüsselung wie mindestens WPA2, mit einem komplexen Passwort (zwischen 13 und 16 Zeichen/vier Arten von Zeichen im Passwort: Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen) geschützt werden. Dies verhindert, dass unbefugte Personen auf das Drahtlosnetzwerk zugreifen können.

- **Starke Passwörter:** Alle mit dem Netzwerk verbundenen Geräte, zum Beispiel Router, Computer, Smartphones, Überwachungskameras usw., sollten durch starke und eindeutige Passwörter gesichert sein, um unbefugten Zugriff zu verhindern (zwischen 13 und 16 Zeichen/fünf Zeichenarten im Passwort: Großbuchstaben, Kleinbuchstaben, andere Buchstaben, Zahlen, Sonderzeichen).

● **Regelmäßige Updates:** Router, die eingebaute „ Firmware “ der Geräte und die Software sollten regelmäßig aktualisiert werden, um bekannte Schwachstellen zu beheben.

● **Firewall:** Eine Firewall muss so konfiguriert sein, dass sie den ein- und ausgehenden Datenverkehr überwacht und verdächtige Aktivitäten blockiert.

● **Netzwerke für Gäste:** Es kann hilfreich sein, ein separates WLAN-Netzwerk für Gäste mit eingeschränktem Zugriff auf die Ressourcen des Hauptnetzwerks im Haus einzurichten.

● **Antiviren- und Anti-Malware-Software:** Auf allen mit dem Netzwerk verbundenen Geräten sollte eine aktuelle Antivirus- und Anti-Malware-Software installiert sein, um potenzielle Bedrohungen zu erkennen und zu unterbinden.

● **Sicherheit für Kameras und IoT-Geräte:** Sicherheitskameras und IoT-Geräte sollten mit starken Passwörtern konfiguriert und regelmäßig aktualisiert werden. Auch Firmware-Updates müssen durchgeführt werden. Bei der Delta Dore-Kamera entsprechen die Anmeldebedingungen für den Zugriff auf die Web-Schnittstelle den Richtlinien für starke Passwörter.

● **Netzwerksegmentierung:** Es wird dringend empfohlen, sensible Geräte wie Sicherheitskameras, NVRs und persönliche Geräte wie Computer und Smartphones mithilfe von virtuellen Subnetzen oder VLANs voneinander zu trennen.

● **Nutzung verschlüsselter Verbindungen (HTTPS), sofern dies möglich ist:** TLS 1.3 oder mindestens TLS 1.2. TLS 1.1 oder SSL sind nicht zulässig.

● **Überwachung des Datenverkehrs:** Ein System zur Überwachung des Netzwerktraffics kann dabei helfen, verdächtige Aktivitäten zu erkennen und das System vor Eindringlingen zu schützen.

● **Regelmäßige Backups:** Wichtige Daten sollten regelmäßig gesichert werden, um einen Verlust durch Cyberangriffe oder Hardwareausfälle zu vermeiden..

3. Bildeinstellungen: erweiterte Funktionsmerkmale des Expertenmodus

Nachdem der Installateur sich vergewissert hat, dass er in einem sicheren Netzwerk arbeitet, kann er ein Passwort festlegen und ein Konto für den Zugriff auf die Web-Schnittstelle der Kamera erstellen.

Anschließend greift er auf die Web-Schnittstelle zu, indem er Folgendes angibt:

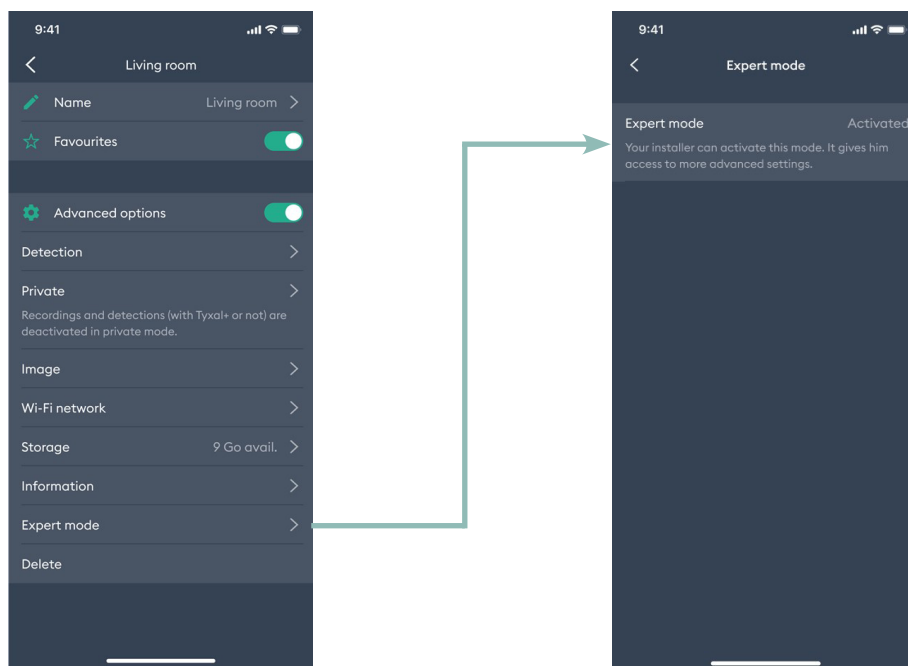
https://[Lokale IP-Adresse der Kamera]

Die Angabe erfolgt in einem Internetbrowser, wobei er sich mit demselben Netzwerk wie die Kamera verbindet. Diese Adresse kann durch Scannen des lokalen Netzwerks abgerufen werden (z. B.: Verwendung eines kostenlosen Tools wie SADP).

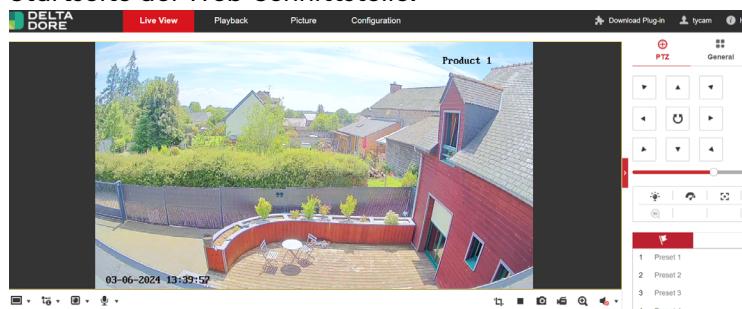
The image shows two screenshots of a mobile application interface for 'Expert mode'. The left screenshot displays the 'Expert mode' screen with a warning about security risks and a 'Continue' button. The right screenshot displays the 'Web ID' screen where a password is created and confirmed, with a 'Save' button and instructions on how to connect to the camera's web interface.

Zustimmungserklärung zum Expertenmodus

Parallel dazu wird der Nutzer darüber informiert, dass der Expertenmodus in den Einstellungen seiner Kamera aktiviert wurde:

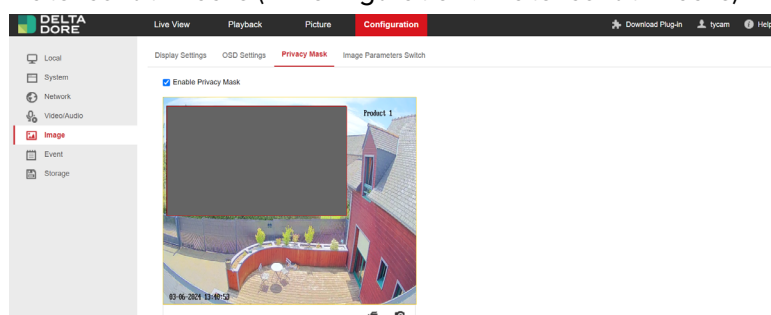


Startseite der Web-Schnittstelle:

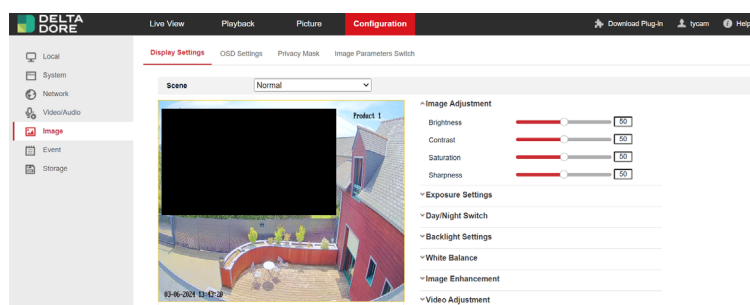


Hinweis: Damit das Livebild angezeigt wird, ist es in manchen Fällen notwendig, oben rechts auf dem Bildschirm „Add-on herunterladen“ anzuklicken.

Datenschutzmaske (in Konfiguration > Datenschutzmaske):



Bildeinstellungen konfigurieren: Helligkeit, Kontrast, Sättigung, Schärfe, Belichtungszeit, Gegenlicht-/Helligkeitskompensation, Entnebelung, Rauschunterdrückung, Weißabgleich etc. (in Konfiguration > Einstellungen anzeigen):



1. Universelle Kompatibilität für eine dauerhafte und skalierbare Installation

ONVIF (Open Network Video Interface Forum) ist ein internationaler Standard, der die Interoperabilität von Überwachungs- und Sicherheitsgeräten gewährleistet.

ONVIF bietet ein **gemeinsames Kommunikationsprotokoll** und eine **Reihe von Standards**, die es Produkten verschiedener Marken ermöglichen, innerhalb einer Netzwerkumgebung (z. B. zentral in einem NVR) nahtlos zusammenzuarbeiten. Es ermöglicht somit den Aufbau von flexiblen und skalierbaren Überwachungs-/Sicherheitssystemen.

Darüber hinaus ermöglicht der ONVIF-Standard den Zugang zu verschiedenen Funktionsmerkmalen wie Videostreaming, PTZ-Steuerung (Pan-Tilt-Zoom), Geräteerkennung, Ereignismanagement und vieles mehr.

Einige Beispiele für die Verwendung der ONVIF-Kompatibilität:

- Zur Kombination verschiedener Kameramarken und -modelle in einem einzigen Sicherheitssystem.
- Für fortgeschrittenere Anwendungsmöglichkeiten, wie etwa das Abrufen von Kamera-Streams auf Videotelefonen.
- Um bei Bedarf einen NVR mit Tycam-Kameras hinzuzufügen, um eine höhere Speicherkapazität zu nutzen.

ONVIF-Empfehlungen zu bewährten Cybersicherheitspraktiken bei IP-basierten physischen Sicherheitsprodukten sind unter folgender Internetadresse abrufbar:

<https://www.onvif.org/profiles/whitepapers/onvif-recommendations-for-cybersecurity-best-practices-for-ip-based-physical-security-products/>

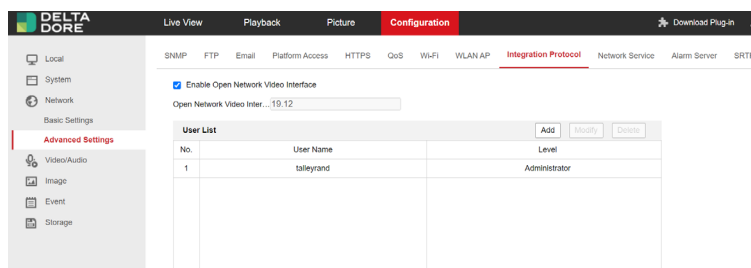
2. ONVIF-Konfiguration der Kameras Tycam Home und Guard

Hinweis: Die ONVIF-Konfiguration der Kameras Tycam Home und Tycam Guard erfordert die Installation einer Delta Dore Smart-Home-Box (Tydom 1.0, Tydom Home/Pro/Tywell, Tydom 2.0).

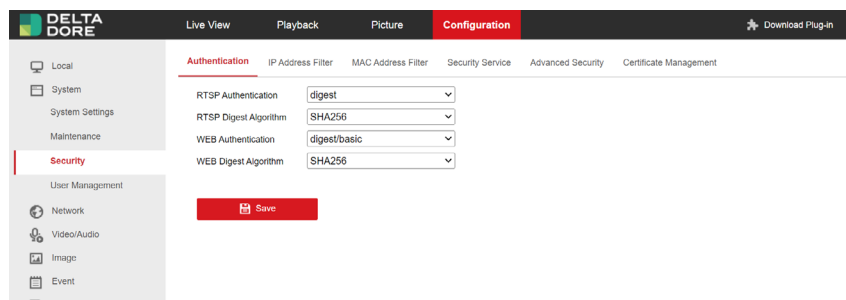
Um auf die ONVIF-Konfiguration der Kamera zuzugreifen (standardmäßig inaktiv), müssen Sie in der Tydom-App den Expertenmodus aktivieren und dann auf die Web-Schnittstelle gehen.

ONVIF ist konfigurierbar unter: Netzwerk > Erweitert > Integrationsprotokoll.

Über diese Seite können Sie ONVIF aktivieren und ONVIF-Benutzer erstellen, die mit dem zentralen Überwachungssystem verbunden werden sollen.



Möglicherweise ist eine Konfiguration der lokalen Authentifizierungseinstellungen erforderlich, damit sie mit Ihrer zentralen Aufzeichnungslösung kompatibel sind (System > Sicherheit > Authentifizierung).



The screenshot shows the Delta Dore configuration web interface. The top navigation bar includes 'Live View', 'Playback', 'Picture', and 'Configuration' (which is highlighted). A 'Download Plug-in' button is on the right. The left sidebar contains a tree view with categories: Local, System, System Settings, Maintenance, Security (highlighted), User Management, Network, Video/Audio, Image, Event, and Storage. The main content area is titled 'Authentication' and includes sub-tabs: 'Authentication' (active), 'IP Address Filter', 'MAC Address Filter', 'Security Service', 'Advanced Security', and 'Certificate Management'. Under the 'Authentication' tab, there are four settings: 'RTSP Authentication' set to 'digest', 'RTSP Digest Algorithm' set to 'SHA256', 'WEB Authentication' set to 'digest/basic', and 'WEB Digest Algorithm' set to 'SHA256'. A red 'Save' button is located at the bottom of the settings.

Setting	Value
RTSP Authentication	digest
RTSP Digest Algorithm	SHA256
WEB Authentication	digest/basic
WEB Digest Algorithm	SHA256

Die ONVIF-URL lautet wie folgt : **https://[IP-Adresse der Kamera]/onvif/device_service**