

MODE EXPERT & PROTOCOLE ONVIF



www.deltadore.com

Introduction

Le **mode Expert** des **caméras Tycam Guard** et **Tycam Home** s'adresse aux **installateurs** et aux **professionnels avertis** qui souhaitent faire profiter à leurs clients d'une **installation sur-mesure**.

Les caméras dernière génération de la gamme Tycam offrent une interface web qui permet une configuration avancée avec des fonctionnalités non disponibles dans l'application Tydom telles que :

- Configuration de l'accès ONVIF
- Ajustement de la qualité de l'image : luminosité, contraste, saturation, netteté, exposition, balance des blancs, réduction du bruit...
- Ajout d'un masque de confidentialité pour cacher des zones spécifiques du champ de vision de la caméra afin d'éviter qu'elle ne filme des zones publiques, par exemple.

IMPORTANT : l'utilisation du mode Expert nécessite obligatoirement des compétences avancées en matière de réseau et de sécurité dans le but d'assurer la conformité de l'installation et la sécurisation/protection des données personnelles des utilisateurs.

N.B. : aucun support technique Delta Dore n'est assuré dans l'utilisation du mode Expert.

Sommaire

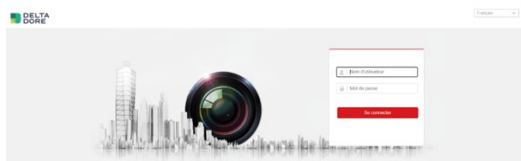
MODE EXPERT

1. Accès à l'interface web..... 2
2. Travailler sur un réseau sécurisé pour protéger les données de vos clients 2
3. Réglages de l'image : les fonctionnalités avancées du mode Expert..... 3

PROTOCOLE ONVIF

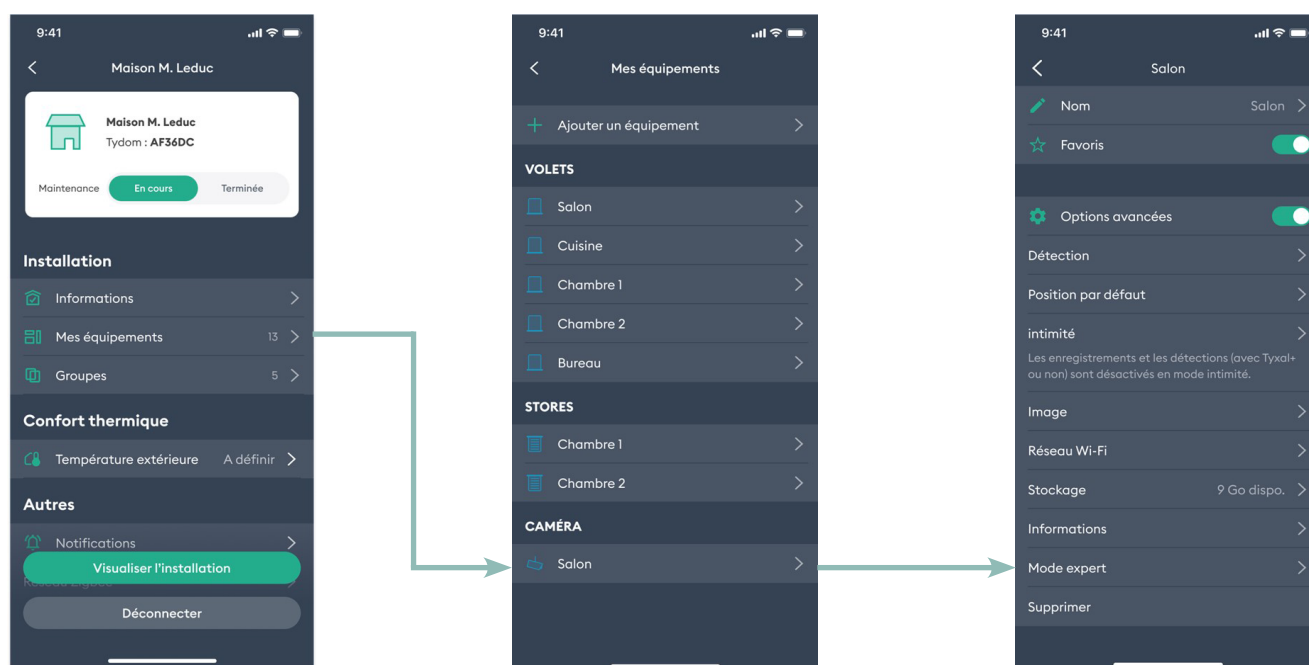
1. Une compatibilité universelle pour une installation pérenne et évolutive 5
2. Configuration en ONVIF des caméras Tycam Home et Guard 5

1. Accès à l'interface web



Page d'authentification de l'interface web

Le mode Expert est **accessible uniquement depuis un compte PRO dans l'application Tydom**, et activable dans les réglages de la caméra, une fois cette dernière installée et connectée au cloud. En effet, afin de rendre la caméra compatible avec certains systèmes tiers, l'utilisation du ONVIF et des fonctions exploitables par ce mode nécessite que le réseau local sur lequel la caméra communique soit sécurisé tout au long de l'utilisation du produit.



2. Travailler sur un réseau sécurisé pour protéger les données de vos clients

Un réseau sécurisé dans une résidence privée est un ensemble de dispositifs et de configurations conçus pour protéger les données, les appareils et la vie privée des résidents contre les menaces en ligne et les accès non autorisés. En voici quelques éléments clés :

- **Chiffrement du réseau Wi-Fi** : le réseau Wi-Fi de la maison doit être protégé par un chiffrement fort, tel que WPA2 au minimum, avec un mot de passe complexe (entre 13 et 16 caractères/quatre types de caractères dans le mot de passe : majuscules, minuscules, chiffres, caractères spéciaux). Cela empêche les personnes non autorisées d'accéder au réseau sans fil.
- **Mots de passe forts** : tous les appareils connectés au réseau, y compris le routeur, les ordinateurs, les smartphones, les caméras de sécurité, etc., devraient utiliser des mots de passe forts et uniques pour empêcher l'accès non autorisé (entre 13 et 16 caractères/cinq types de caractères dans le mot de passe : majuscules, minuscules, lettres, chiffres, caractères spéciaux).

- **Mises à jour régulières** : les routeurs, le logiciel embarqué « firmware » des appareils et les logiciels devraient être régulièrement mis à jour pour remédier aux vulnérabilités connues.
- **Pare-feu** : un pare-feu doit être configuré pour surveiller le trafic entrant et sortant et bloquer les activités suspectes.
- **Réseaux invités** : il peut être bénéfique de créer un réseau Wi-Fi séparé pour les invités avec un accès limité aux ressources du réseau principal de la maison.
- **Antivirus et anti-malware** : tous les appareils connectés au réseau devraient disposer d'un logiciel antivirus et anti-malware à jour pour détecter et supprimer les menaces potentielles.
- **Sécurité pour les caméras et les appareils IoT** : les caméras de sécurité et les appareils IoT doivent être configurés avec des mots de passe forts et régulièrement mis à jour. Les mises à jour du firmware doivent également être réalisées. Pour la caméra Delta Dore, les conditions d'identification pour accéder à l'interface web sont conformes à la politique de mots de passe forts.
- **Segmentation du réseau** : il est très fortement recommandé de séparer les dispositifs sensibles, tels que les caméras de sécurité, les NVR, des appareils personnels tels que les ordinateurs et les smartphones en utilisant des sous-réseaux virtuels ou des VLAN.
- **Utilisation de connexions chiffrées (HTTPS) lorsque cela est possible** : TLS 1.3 ou au moins TLS 1.2. TLS 1.1 ou SSL sont interdits.
- **Surveillance du trafic** : un système de surveillance du trafic réseau peut aider à détecter les activités suspectes et à protéger contre les intrusions.
- **Sauvegardes régulières** : les données importantes devraient être régulièrement sauvegardées pour éviter toute perte en cas de cyberattaque ou de défaillance matérielle.

3. Réglages de l'image : les fonctionnalités avancées du mode Expert

Après s'être assuré de travailler sur un réseau sécurisé, l'installateur peut définir un mot de passe et créer un compte d'accès à l'interface web de la caméra.

Il accède ensuite à l'interface web en renseignant :

https://[adresse ip locale de la caméra]

dans un navigateur internet, en se connectant sur le même réseau que la caméra. Cette adresse peut être récupérée en scannant le réseau local (ex : usage d'un outil gratuit comme SADP).

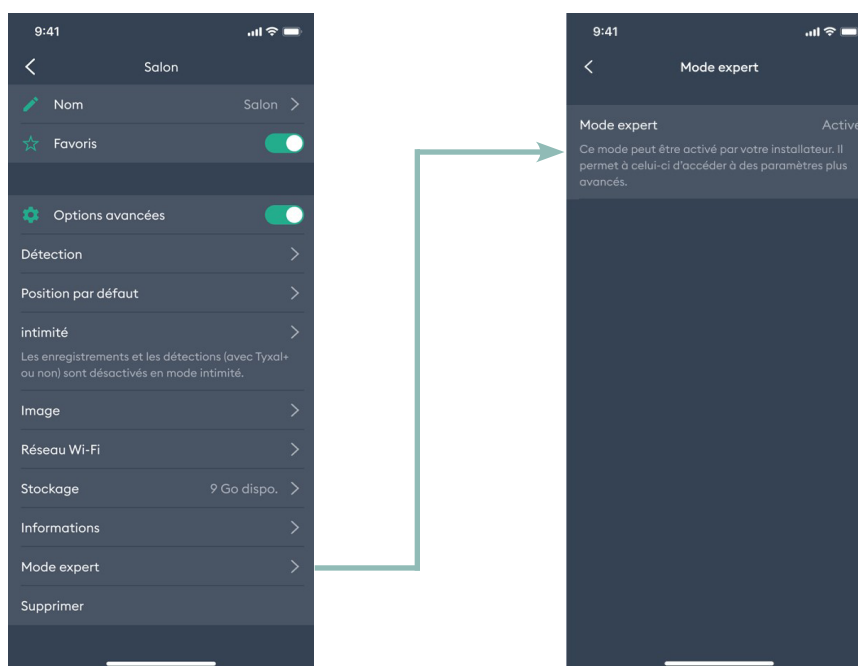
The image shows two screenshots of a mobile application interface for configuring a camera in 'Mode expert'.

Left Screenshot: The screen is titled 'Mode expert' with a subtitle 'Pour les utilisateurs avertis'. It contains a paragraph explaining that for full integration with third-party systems, advanced network and security features must be used, and that this mode is for experienced users. Below this, it states that to access the web interface locally, the user must enter the ID and password provided. An 'Attention' note mentions that using this mode requires a secure network. At the bottom, there is a green 'Continuer' button.

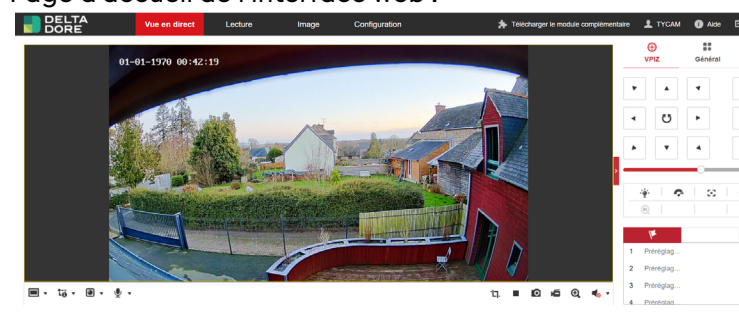
Right Screenshot: The screen is titled 'Identifiant Web'. It prompts the user to create a password for the web interface. There is a text field for 'Identifiant' (username) with 'tycam' entered. Below it is a 'Mot de passe' (password) field with a toggle for visibility. The password requirements are listed: at least 1 uppercase letter, at least 1 lowercase letter, at least 1 digit, at least 1 special character, and a minimum of 13 to a maximum of 16 characters. There is a 'Confirmer le mot de passe' field below. An 'Enregistrer' (Save) button is at the bottom. Below the button, there is a note about connecting to the web interface using the local IP address and the created password. A final 'Attention' note states that if a message about a private connection appears, it is normal, and that accepting the connection will allow access to the camera settings.

Consentement mode Expert

En parallèle, l'utilisateur est informé de l'activation du mode Expert dans les réglages de sa caméra :

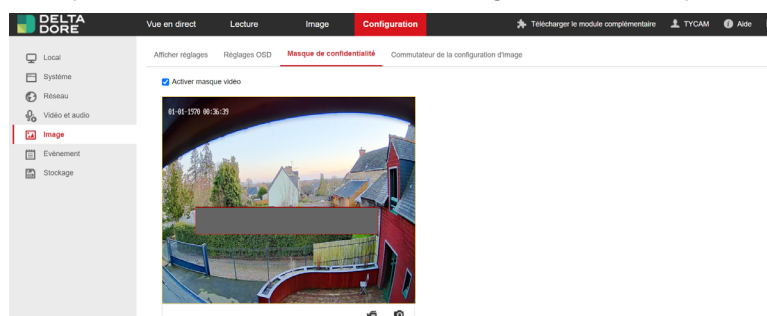


Page d'accueil de l'interface web :

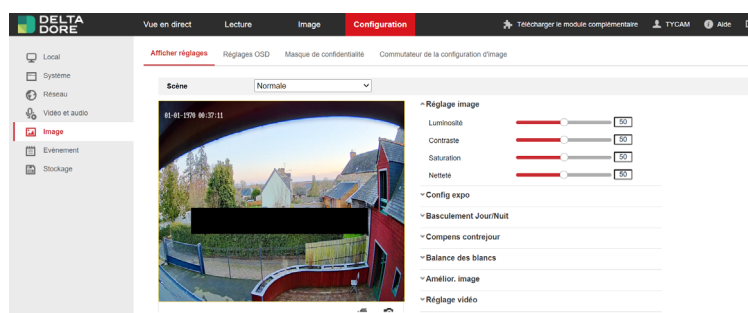


N.B. : afin que le live s'affiche, il est nécessaire dans certains cas de “Télécharger le module complémentaire” en haut à droite de l'écran.

Masque de confidentialité (dans Configuration > Masque de confidentialité) :



Paramétrage de l'image : luminosité, contraste, saturation, netteté, durée d'exposition, compensation contre-jour/ fortes lumières, désembuage, réduction du bruit, balance des blancs... (dans Configuration > Afficher réglages) :



1. Une compatibilité universelle pour une installation pérenne et évolutive

ONVIF (Open Network Video Interface Forum) est une norme internationale qui garantit l'interopérabilité des dispositifs de surveillance et de sécurité.

ONVIF fournit un **protocole de communication commun** et un **ensemble de normes** permettant à des produits de différentes marques de fonctionner ensemble de manière transparente au sein d'un environnement réseau (par exemple, centralisé dans un NVR). Elle permet ainsi de construire des systèmes de surveillance/sécurité flexibles et évolutifs.

Par ailleurs, la norme ONVIF permet d'accéder à diverses fonctionnalités telles que le streaming vidéo, le contrôle PTZ (Pan-Tilt-Zoom), la découverte de dispositifs, la gestion d'événements, et bien plus encore.

Quelques exemples d'utilisation de la compatibilité ONVIF :

- Pour associer différentes marques et modèles de caméras dans un même système de sécurité.
- Pour des usages plus avancés, tels que la récupération de flux de caméra sur des vidéophones.
- Dans le cas où il serait nécessaire d'ajouter un NVR avec des caméras Tycam pour bénéficier d'une capacité de stockage plus élevée.

Recommandations ONVIF sur les meilleures pratiques en matière de cybersécurité pour les produits de sécurité physique basés sur IP disponibles à l'adresse internet suivante :

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

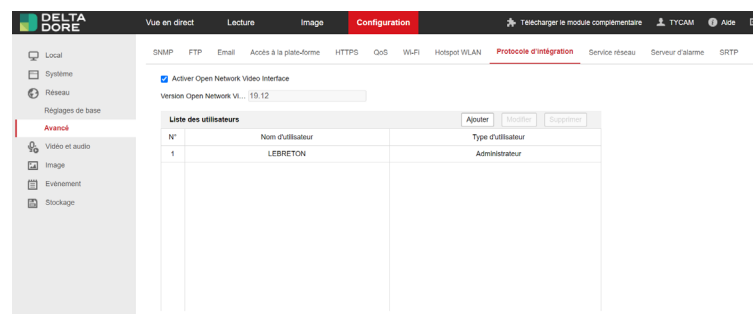
2. Configuration en ONVIF des caméras Tycam Home et Guard

N.B. : la configuration en ONVIF des caméras Tycam Home et Tycam Guard requiert l'installation d'une box maison connectée Delta Dore (Tydom 1.0, Tydom Home/Pro/Tywell, Tydom 2.0).

Afin d'accéder à la configuration du ONVIF sur la caméra (par défaut inactif), il est nécessaire d'activer le mode Expert sur l'application Tydom, puis de se rendre dans l'interface web.

Le ONVIF est configurable dans : Réseau > Avancé > Protocole d'intégration.

Au travers de cette page, il est possible d'activer l'ONVIF et de créer des utilisateurs ONVIF à raccorder au système de surveillance centralisé.



Un paramétrage des réglages de l'authentification en local peut être nécessaire afin d'être compatible avec votre solution d'enregistrement centralisée (Système > Sécurité > Authentification).

The screenshot shows the DELTA DORE configuration interface. The top navigation bar includes 'Vue en direct', 'Lecture', 'Image', and 'Configuration' (highlighted in red). To the right of the navigation bar are links for 'Télécharger le module complémentaire', 'TYCAM', and 'Aide'. On the left, a sidebar menu lists various system settings: Local, Système, Config. système, Maintenance, Sécurité (highlighted in red), Gestion des utilisateurs, Réseau, Vidéo et audio, Image, Evénement, and Stockage. The 'Sécurité' section is expanded, showing sub-tabs: 'Authentification' (highlighted in red), 'Filtre d'adresse IP', 'Filtre d'adresse MAC', 'Service de sécurité', 'Sécurité avancée', and 'Gestion des certificats'. The 'Authentification' sub-tab contains four settings, each with a dropdown menu: 'Authentication RTSP' set to 'digest', 'RTSP Digest Algorithm' set to 'SHA256', 'Authentication WEB' set to 'digest/basic', and 'WEB Digest Algorithm' set to 'SHA256'. Below these settings is a red button labeled 'Enregistrer'.

Paramètre	Valeur
Authentication RTSP	digest
RTSP Digest Algorithm	SHA256
Authentication WEB	digest/basic
WEB Digest Algorithm	SHA256

L'URL ONVIF est la suivante : **https://[adresse ip de la caméra]/onvif/device_service**