



SECURING YOUR WORLD



MANUEL D'UTILISATION

ACCESS DOORBELL

Table des matières

Partie I — Prise en main

1. Présentation et description du produit	5
2. Connexion de l'appareil	10
3. Configuration de l'adresse IP	11
4. Connexion Web	12

Partie II — Visionnement en direct, lecture et événements

5. Écran de prévisualisation	19
6. Lecture	21
7. Recherche d'événements	24

Partie III — Configuration de la caméra

8. Image et encodage	30
9. Enregistrement, stockage et FTP	35
10. Alarmes, I/O et dissuasion	41
11. Événements et détection IA	45
12. Réseau et services	52

Partie IV — Contrôle d'accès et système

13. Système de contrôle d'accès	66
14. Système, utilisateurs et maintenance	82

Prise en main

Connexion, adressage IP et connexion web

Chapitre 1 Présentation et description du produit

La caméra de contrôle d'accès OCTAVUE de GSD Group combine la vérification d'identité et la vidéosurveillance haute définition dans un seul appareil intelligent, offrant une sécurité intégrée et une gestion des entrées adaptées à un vaste éventail d'environnements.

1.1 Domaine d'application

La caméra de contrôle d'accès intègre la vérification d'identité et la vidéosurveillance dans une plateforme intelligente unifiée. Sa valeur fondamentale consiste à améliorer l'efficacité, la commodité et la sécurité de la gestion des entrées. Les scénarios de déploiement typiques couvrent les environnements commerciaux, résidentiels, de bureau et de service public.

Dans les locaux commerciaux et les bureaux, où le flux de personnel est élevé et mixte (employés, visiteurs et sous-traitants), la caméra concilie l'efficacité du débit et le contrôle de la sécurité : sa fonction principale est de distinguer les niveaux d'autorité du personnel et de tenir un registre vérifiable de chaque entrée et sortie.

Dans les scénarios résidentiels, l'objectif premier est de protéger la vie privée des résidents et d'empêcher l'accès non autorisé d'étrangers tout en préservant la commodité au quotidien. La reconnaissance faciale sans carte est particulièrement précieuse pour les personnes âgées et les enfants, éliminant le désagrément bien connu des cartes d'accès oubliées ou perdues.

NOTE Tout au long de ce manuel, les termes **caméra IP** et **caméra réseau** sont utilisés de façon interchangeable pour désigner la caméra de contrôle d'accès OCTAVUE.

1.2 Description du produit

Comparée aux équipements de contrôle d'accès traditionnels, la caméra de contrôle d'accès visuel OCTAVUE offre trois avantages principaux :

- **Sécurité renforcée** : les algorithmes d'AI déjouent l'usurpation d'identité et le talonnage, tandis que la vidéo haute définition et les fonctions d'alerte précoce assurent la prévention en amont et la traçabilité après un événement.
- **Efficacité accrue** : les autorisations hiérarchiques et la gestion à distance réduisent l'intervention manuelle et simplifient la liaison entre les dispositifs de contrôle.
- **Expérience optimisée** : la reconnaissance faciale sans carte et une plateforme d'exploitation légère répondent aux besoins de groupes d'utilisateurs variés.

Ensemble, ces capacités rehaussent la sécurité, réduisent les coûts de gestion et offrent une solution de gestion des entrées et des sorties tout-en-un.

La caméra intègre également une technologie audio et vidéo de pointe dans un appareil unique et compact, utilisant une compression vidéo moderne pour conserver des images nettes et de haute qualité sans saturer la

bande passante réseau disponible. La surveillance est simple : saisissez l'adresse web de la caméra dans n'importe quel navigateur pris en charge pour visionner le flux en direct en temps réel. Les administrateurs peuvent créer plusieurs comptes d'utilisateurs avec des niveaux d'autorisation distincts pour un contrôle total de qui peut visionner ou gérer la caméra. Lorsqu'un mouvement est détecté, la caméra peut immédiatement envoyer une alerte par courriel avec des images ou des séquences vidéo capturées, et elle enregistre automatiquement une copie de sauvegarde de l'événement sur la carte mémoire locale.

1.2.1 Apparence

L'extérieur de la caméra de contrôle d'accès visuel est illustré ci-dessous.

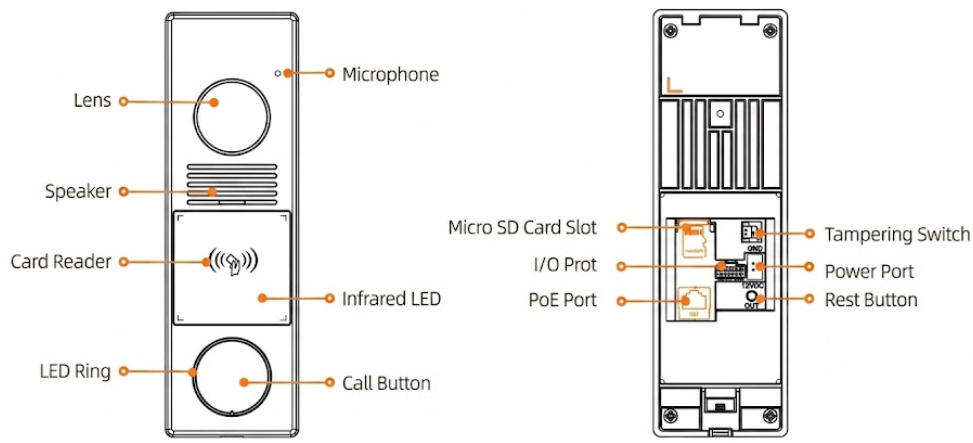


Figure 1-1. Apparence de la caméra de contrôle d'accès

1.2.2 Ports I/O et définitions des fils de queue

Le port I/O prend en charge le raccordement d'un lecteur de cartes Wiegand, d'un lecteur de cartes RS-485, de dispositifs d'alarme et de périphériques connexes. Les différents fils de queue sont décrits dans la figure et le tableau suivants.

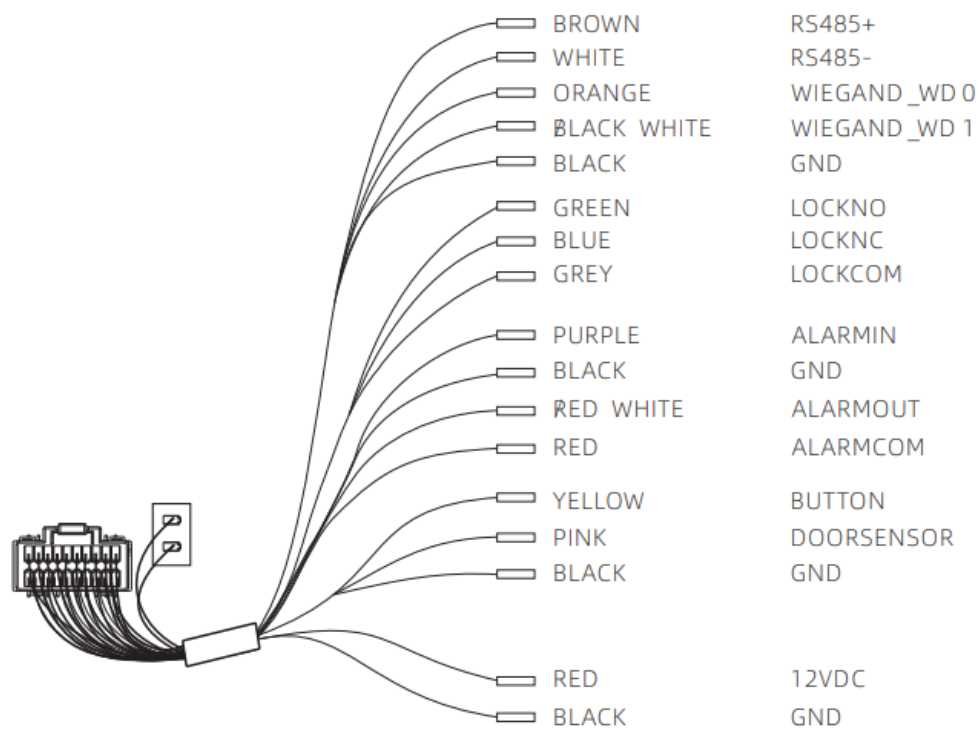


Figure 1-2. Disposition des fils de queue du port I/O

Nom du fil de queue	Couleur du fil	Port	Description
RS-485	Brun	RS-485+	Lecteur de cartes RS-485 externe
	Blanc	RS-485-	
Wiegand	Orange	WIEGAND_WD0	Lecteur de cartes Wiegand externe
	Noir/Blanc	WIEGAND_WD1	
	Noir	GND	
Serrure de porte	Vert	LOCKNO	Serrure de porte externe
	Bleu	LOCKNC	
	Gris	LOCKCOM	
Entrée/sortie d'alarme	Violet	ALARMIN	Entrée d'alarme
	Noir	GND	
	Rouge/Blanc	ALARMOUT	Alarme externe
	Rouge	ALARMCOM	
Bouton de sortie et capteur de porte	Jaune	BUTTON	Bouton de sortie et capteur de porte externes
	Rose	DOORSENSOR	
	Noir	GND	
Alimentation électrique	Rouge	12VDC	Raccordement de l'alimentation 12 VDC
	Noir	GND	

1.2.3 Schémas de câblage

Reportez-vous aux schémas suivants pour raccorder les lecteurs de cartes, les serrures de porte, les boutons de sortie, les capteurs de porte et les dispositifs d'alarme à la caméra.

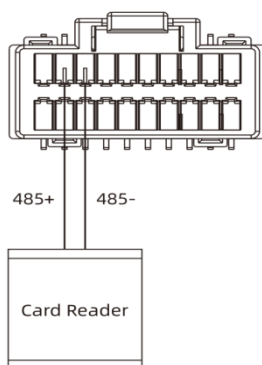


Figure 1-3. Schéma de câblage du lecteur de cartes RS-485

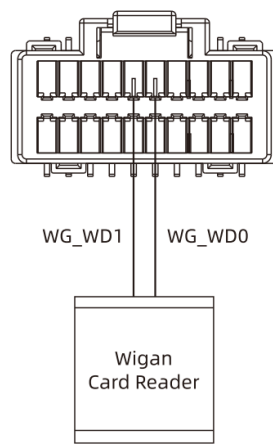


Figure 1-4. Schéma de câblage du lecteur de cartes Wiegand

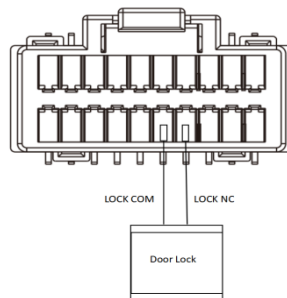


Figure 1-5. Schéma de câblage de la serrure de porte normalement fermée (NC)

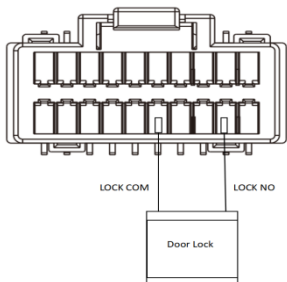


Figure 1-6. Schéma de câblage de la serrure de porte normalement ouverte (NO)

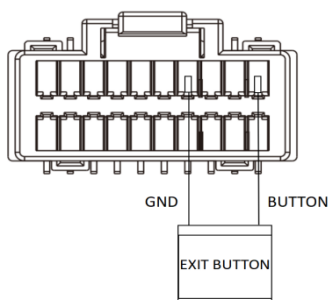


Figure 1-7. Schéma de câblage du bouton de sortie

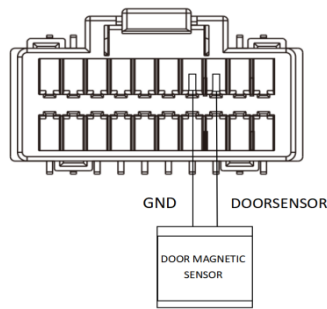


Figure 1-8. Schéma de câblage du capteur de porte (contact magnétique)

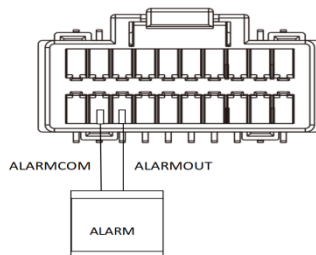


Figure 1-9. Schéma de câblage de l'alarme

1.3 Environnement d'installation

La caméra de contrôle d'accès peut être installée à l'intérieur ou à l'extérieur. Lorsque vous installez l'appareil à l'extérieur, ne le placez pas en plein soleil. Lorsque vous l'installez à l'intérieur, maintenez une distance appropriée par rapport aux lumières et aux fenêtres, comme illustré dans la figure ci-dessous.

CAUTION Une exposition prolongée à la lumière directe du soleil ou à un fort contre-jour peut dégrader la qualité de l'image et réduire la durée de vie de l'appareil. Choisissez un emplacement de montage qui évite ces conditions.

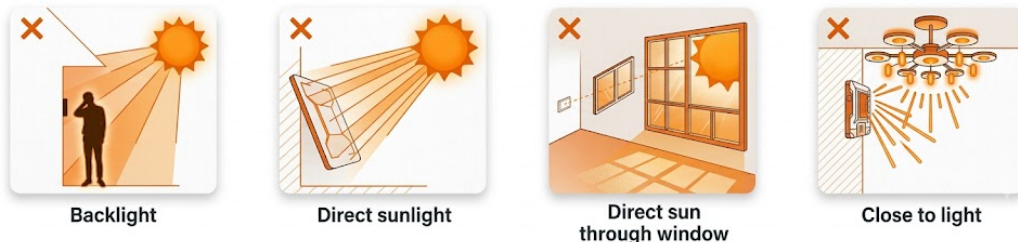


Figure 1-10. Positionnement d'installation recommandé

1.4 Environnement d'exploitation

Pour accéder à la caméra et la gérer au moyen d'un navigateur web, l'ordinateur client doit satisfaire aux exigences minimales suivantes.

- **Système d'exploitation** : Windows XP / Windows 7 / Windows 8 / Windows 10 / Windows 11, ou MacOS 10 ou supérieur.
- **CPU** : Intel i3 ou supérieur.
- **Mémoire** : 2 Go ou plus.
- **Mémoire vidéo** : 1 Go ou plus.
- **Affichage** : résolution 1024×768 ou supérieure.
- **Navigateur** : IE 10 et supérieur, Chrome 57 et supérieur, Firefox 52 et supérieur, Edge 41 et supérieur, ou Safari 12 et supérieur.

1.5 Configuration par défaut et connexion initiale

Avant l'installation, passez en revue les paramètres réseau, les identifiants et les options de connectivité par défaut suivants.

1.5.1 Paramètres réseau

Par défaut, la caméra obtient automatiquement une adresse IP auprès d'un serveur DHCP. Si aucun serveur DHCP n'est actif sur le réseau, la caméra revient à l'adresse IP statique **10.0.0.6**.

NOTE Le port web par défaut est le **80**. ONVIF est activé par défaut pour permettre une intégration immédiate avec des systèmes tiers, et le port ONVIF par défaut est synchronisé avec le port web.

1.5.2 Connexion initiale et sécurité

Le nom d'utilisateur administrateur par défaut est **admin** (sensible à la casse, tout en minuscules). Pour des raisons de sécurité, la caméra est livrée sans mot de passe par défaut.

CAUTION Lors de la première connexion, vous devez créer un mot de passe robuste en suivant les invites à l'écran. Conservez ce mot de passe en lieu sûr ; il est requis pour tous les accès ultérieurs. Consultez la section 4.2 pour plus de détails.

TIP Si le mot de passe administrateur est ultérieurement perdu, **Super Code** est la méthode de récupération de mot de passe recommandée. Activé par défaut dans les microprogrammes récents, il rétablit l'accès avec l'aide du soutien technique.

Chapitre 2 Connexion de l'appareil

La caméra de contrôle d'accès OCTAVUE prend en charge deux méthodes de connexion physique. Choisissez la méthode qui correspond à votre déploiement : une connexion directe à un seul ordinateur pour la configuration initiale et les essais sur banc, ou une connexion par l'entremise d'un routeur, d'un commutateur ou d'un NVR pour l'exploitation quotidienne et l'accès à distance.

NOTE Avant de connecter la caméra, notez son adresse IP par défaut, son masque de sous-réseau et ses identifiants de connexion tels qu'imprimés sur l'étiquette de l'appareil ou dans la documentation de démarrage rapide fournie. Ces valeurs sont nécessaires pour joindre la caméra pour la première fois.

2.1 Connexion directe à un PC

Cette méthode relie la caméra directement à un ordinateur sans routeur ni connexion Internet. Elle convient particulièrement à la configuration initiale, à la maintenance des microprogrammes et au diagnostic sur place.

1. Branchez une extrémité d'un câble Ethernet au port réseau de la caméra et l'autre extrémité directement au port réseau de votre ordinateur.
2. Mettez la caméra sous tension à l'aide de l'**adaptateur d'alimentation 12V** fourni.
3. Ajustez les paramètres réseau de votre ordinateur de sorte que son adresse IP se trouve sur le même sous-réseau que l'adresse IP par défaut de la caméra.

4. Patientez environ une minute. Une fois que la caméra a terminé sa séquence de démarrage, elle commencera à communiquer automatiquement avec votre ordinateur.

TIP Si votre ordinateur et la caméra se trouvent sur des sous-réseaux différents, la caméra ne répondra pas. Attribuez à l'ordinateur une adresse IP statique dans la même plage que celle de la caméra avant de tenter la connexion.

2.2 Connexion par routeur, commutateur ou NVR

Cette méthode connecte la caméra à votre réseau domestique ou professionnel local, permettant l'accès depuis d'autres appareils du réseau et, une fois configuré, par Internet. Il s'agit de la méthode recommandée pour l'usage quotidien et le visionnement à distance.

1. Connectez à la fois la caméra et votre ordinateur aux ports **LAN** de votre routeur, de votre commutateur réseau ou de votre NVR.
2. Branchez la caméra à son adaptateur d'alimentation.
3. Configurez le paramètre **Passerelle** de la caméra pour qu'il corresponde à l'adresse IP de votre routeur. Cela permet à la caméra d'acheminer son flux vidéo à travers le routeur et, là où c'est permis, vers Internet.

NOTE Lorsque la caméra est alimentée par un commutateur PoE ou un NVR, un adaptateur d'alimentation distinct n'est pas nécessaire. Vérifiez que le commutateur ou le NVR fournit une puissance PoE suffisante pour la caméra avant de vous y fier comme unique source d'alimentation.

Chapitre 3 Configuration de l'adresse IP

Avant que la caméra de contrôle d'accès OCTAVUE puisse être jointe depuis un navigateur web ou ajoutée à un NVR, elle doit posséder une adresse IP valide pour votre réseau local. L'outil de découverte fourni localise chaque caméra du même sous-réseau et vous permet d'attribuer ou de corriger ses paramètres réseau sans accès préalable à l'interface web.

3.1 Utilisation de l'outil de découverte

Installez et lancez l'**outil de découverte** sur un ordinateur connecté au même réseau local que la caméra. Lorsque l'application s'ouvre, elle affiche la liste des appareils et les commandes de recherche servant à analyser le réseau.

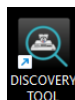


Figure 3-1. Fenêtre principale de l'outil de découverte

Cliquez sur **Rechercher** pour actualiser la liste des caméras détectées sur le réseau local. Chaque appareil qui répond est affiché avec ses détails d'identification, de sorte que vous pouvez repérer la caméra cible grâce à son identifiant P2P ou à son adresse MAC.

No.	IP	Media Port	Web Port	Channel	Device Name	Device Type	Device Version	Net Mask	Gateway	MAC	Network Mode	P2P ID	Initialized	Status
1	192.168.2.1	0	80	1	192.168.2.1	192.168.2.1	192.168.2.1	255.255.255.0	192.168.2.1	98:FA:60:08:80:00	Static	192.168.2.1	true	OK
2	192.168.2.2	0	80	1	192.168.2.2	192.168.2.2	192.168.2.2	255.255.255.0	192.168.2.1	98:FA:60:08:80:01	Static	192.168.2.1	true	OK
3	192.168.2.3	0	80	1	192.168.2.3	192.168.2.3	192.168.2.3	255.255.255.0	192.168.2.1	98:FA:60:08:80:02	Static	192.168.2.1	true	OK
4	192.168.2.4	0	80	1	192.168.2.4	192.168.2.4	192.168.2.4	255.255.255.0	192.168.2.1	98:FA:60:08:80:03	Static	192.168.2.1	true	OK
5	192.168.2.5	0	80	1	192.168.2.5	192.168.2.5	192.168.2.5	255.255.255.0	192.168.2.1	98:FA:60:08:80:04	Static	192.168.2.1	true	OK
6	192.168.2.6	0	80	32	192.168.2.6	192.168.2.6	192.168.2.6	255.255.255.0	192.168.2.1	98:FA:60:08:80:05	Static	192.168.2.1	true	OK
7	192.168.2.7	0	80	1	192.168.2.7	192.168.2.7	192.168.2.7	255.255.255.0	192.168.2.1	98:FA:60:08:80:06	Static	192.168.2.1	true	OK
8	192.168.2.8	0	80	1	192.168.2.8	192.168.2.8	192.168.2.8	255.255.255.0	192.168.2.1	98:FA:60:08:80:07	Static	192.168.2.1	true	OK
9	192.168.2.9	0	80	1	192.168.2.9	192.168.2.9	192.168.2.9	255.255.255.0	192.168.2.1	98:FA:60:08:80:08	Static	192.168.2.1	true	OK
10	192.168.2.10	0	80	1	192.168.2.10	192.168.2.10	192.168.2.10	255.255.255.0	192.168.2.1	98:FA:60:08:80:09	Static	192.168.2.1	true	OK
11	192.168.2.11	0	80	1	192.168.2.11	192.168.2.11	192.168.2.11	255.255.255.0	192.168.2.1	98:FA:60:08:80:0A	Static	192.168.2.1	true	OK
12	192.168.2.12	0	80	1	192.168.2.12	192.168.2.12	192.168.2.12	255.255.255.0	192.168.2.1	98:FA:60:08:80:0B	Static	192.168.2.1	true	OK
13	192.168.2.13	0	80	1	192.168.2.13	192.168.2.13	192.168.2.13	255.255.255.0	192.168.2.1	98:FA:60:08:80:0C	Static	192.168.2.1	true	OK
14	192.168.2.14	0	80	1	192.168.2.14	192.168.2.14	192.168.2.14	255.255.255.0	192.168.2.1	98:FA:60:08:80:0D	Static	192.168.2.1	true	OK
15	192.168.2.15	0	80	2	192.168.2.15	192.168.2.15	192.168.2.15	255.255.255.0	192.168.2.1	98:FA:60:08:80:0E	Static	192.168.2.1	true	OK
16	192.168.2.16	0	80	32	192.168.2.16	192.168.2.16	192.168.2.16	255.255.255.0	192.168.2.1	98:FA:60:08:80:0F	Static	192.168.2.1	true	OK
17	192.168.2.17	0	80	64	192.168.2.17	192.168.2.17	192.168.2.17	255.255.255.0	192.168.2.1	98:FA:60:08:80:10	Static	192.168.2.1	true	OK
18	192.168.2.18	0	80	1	192.168.2.18	192.168.2.18	192.168.2.18	255.255.255.0	192.168.2.1	98:FA:60:08:80:11	Static	192.168.2.1	true	OK
19	192.168.2.19	0	80	1	192.168.2.19	192.168.2.19	192.168.2.19	255.255.255.0	192.168.2.1	98:FA:60:08:80:12	Static	192.168.2.1	true	OK
20	192.168.2.20	0	80	2	192.168.2.20	192.168.2.20	192.168.2.20	255.255.255.0	192.168.2.1	98:FA:60:08:80:13	Static	192.168.2.1	true	OK
21	192.168.2.21	0	80	1	192.168.2.21	192.168.2.21	192.168.2.21	255.255.255.0	192.168.2.1	98:FA:60:08:80:14	Static	192.168.2.1	true	OK
22	192.168.2.22	0	80	1	192.168.2.22	192.168.2.22	192.168.2.22	255.255.255.0	192.168.2.1	98:FA:60:08:80:15	Static	192.168.2.1	true	OK
23	192.168.2.23	0	80	1	192.168.2.23	192.168.2.23	192.168.2.23	255.255.255.0	192.168.2.1	98:FA:60:08:80:16	Static	192.168.2.1	true	OK
24	192.168.2.24	0	80	1	192.168.2.24	192.168.2.24	192.168.2.24	255.255.255.0	192.168.2.1	98:FA:60:08:80:17	Static	192.168.2.1	true	OK
25	192.168.2.25	0	80	1	192.168.2.25	192.168.2.25	192.168.2.25	255.255.255.0	192.168.2.1	98:FA:60:08:80:18	Static	192.168.2.1	true	OK
26	192.168.2.26	0	80	16	192.168.2.26	192.168.2.26	192.168.2.26	255.255.255.0	192.168.2.1	98:FA:60:08:80:19	Static	192.168.2.1	true	OK
27	192.168.2.27	9000	80	8	192.168.2.27	192.168.2.27	192.168.2.27	255.255.255.0	192.168.2.1	98:FA:60:08:80:1A	Static	192.168.2.1	true	OK

Figure 3-2. Caméras détectées sur le réseau local

1. Cliquez sur **Rechercher** pour analyser le réseau local à la recherche de caméras OCTAVUE connectées.
2. Repérez la caméra cible dans les résultats en faisant correspondre son identifiant P2P ou son adresse MAC à l'étiquette figurant sur l'appareil.
3. Sélectionnez la caméra pour afficher sa configuration réseau actuelle, puis saisissez l'adresse IP, le masque de sous-réseau et la passerelle requis.
4. Appliquez les modifications pour écrire la nouvelle adresse IP dans la caméra.

TIP Si la caméra n'apparaît pas après la première analyse, cliquez de nouveau sur **Rechercher** pour actualiser la liste. Un appareil récemment mis sous tension peut prendre quelques instants avant de répondre sur le réseau.

NOTE L'adresse IP attribuée doit appartenir au même sous-réseau que l'ordinateur exécutant l'outil de découverte ; sinon, la caméra ne sera pas joignable depuis un navigateur web.

Chapitre 4 Connexion Web

La caméra de contrôle d'accès OCTAVUE offre un client Web accessible par navigateur pour la configuration et l'exploitation quotidienne. Ce chapitre décrit comment accéder au client Web, activer la caméra lors de la première utilisation, se connecter et récupérer le mot de passe administrateur s'il est perdu.

4.1 Accès au client Web

Il existe deux façons d'ouvrir le client Web de la caméra.

Exécutez l'**Outil de configuration de l'appareil** pour rechercher les caméras présentes sur le réseau actuel. Une fois la recherche terminée, cliquez sur l'adresse IP de la caméra cible dans la liste des résultats pour ouvrir directement son client Web.

No.	IP	Media Port	Web Port	Channel	Device Name	Device Type	Device Version	Net Mask	Gateway	MAC	Network Mode	P2P ID	Initialized	Status
1	192.168.2.25	0	80	1			VC21.45.1.3-200	255.255.255.0	192.168.2.1		Static		true	
2	192.168.2.26	0	80	1			VC21.45.1.3-200	255.255.255.0	192.168.2.1		Static		true	
3	192.168.2.27	0	80	1			VC21.45.1.3-200	255.255.255.0	192.168.2.1		Static		true	
4	192.168.2.28	0	80	1			VC21.45.1.3-200	255.255.255.0	192.168.2.1		Static		true	
5	192.168.2.29	0	80	1			VC21.45.1.3-200	255.255.255.0	192.168.2.1		DHCP		true	
6	192.168.2.30	0	80	32			VC1.3.0-200701	255.255.255.0	192.168.0.0/01		Static		true	
7	192.168.2.31	0	80	1			VC31.35.1.3-200	255.255.255.0	192.168.2.1		DHCP		true	
8	192.168.2.32	0	80	1			VC51.57.1.2-200	255.255.255.0	192.168.2.1		Static		true	
9	192.168.2.33	0	80	1			VC51.57.1.2-200	255.255.255.0	192.168.2.1		Static		true	
10	192.168.2.34	0	80	1			VC51.57.1.2-200	255.255.255.0	192.168.2.1		Static		true	
11	192.168.2.35	0	80	1			VC51.57.1.2-200	255.255.255.0	192.168.2.1		Static		true	
12	192.168.2.36	0	80	1			VC30.85.1.3-200	255.255.255.0	192.168.2.1		Static		true	
13	192.168.2.37	0	80	1			VC21.25.1.3-200	255.255.255.0	192.168.2.1		DHCP		true	
14	192.168.2.38	0	80	1			VC50.25.1.3-200	255.255.255.0	192.168.2.1		DHCP		true	
15	192.168.2.173	0	80	2			VC50.57.1.3-200	255.255.255.0	192.168.2.1		Static		true	
16	192.168.2.39	0	80	32			VC1.3.0-200701	255.255.255.0	192.168.0.0/01		DHCP		true	
17	192.168.2.39	0	80	64			VC1.3.0-200530	255.252.252.0	192.168.0.0/01		DHCP		true	
18	192.168.2.204	0	80	1			VC21.45.1.3-200	255.255.255.0	192.168.2.1		Static		true	
19	192.168.2.214	0	80	1			VC49.57.1.3-200	255.255.255.0	192.168.2.1		Static		true	
20	192.168.2.216	0	80	2			VC47.55.1.3-200	255.255.255.0	192.168.2.1		Static		true	
21	192.168.2.217	0	80	1			V1.0.2_240420	255.255.255.0	192.168.2.1		Static		true	
22	192.168.2.218	0	80	1			VC30.85.1.3-200	255.255.255.0	192.168.2.1		Static		true	
23	192.168.2.219	0	80	1			VC48.55.1.3-200	255.255.255.0	192.168.2.1		Static		true	
24	192.168.2.220	0	80	1			VC30.85.1.3-200	255.255.255.0	192.168.2.1		Static		true	
25	192.168.2.221	0	80	1			VC48.55.1.3-200	255.255.255.0	192.168.2.1		Static		true	
26	192.168.2.222	0	80	16			VC1.3.0-200701	255.255.255.0	192.168.0.0/01		Static		true	
27	192.168.2.234	8000	80	8			V8.2.4.1-20240627	255.255.255.0	192.168.0.0/01		DHCP		true	
28	192.168.2.235	0	80	1			VC49.57.1.3-200	255.255.255.0	192.168.2.1		Static		true	
29	192.168.2.254	0	80	1			VC21.45.1.3-200	255.255.255.0	192.168.2.1		Static		true	

Figure 4-1. Recherche de caméras avec l'Outil de configuration de l'appareil

Vous pouvez aussi saisir **http://<IP>:<port Web>** dans la barre d'adresse de votre navigateur. Par exemple, si l'adresse IP de la caméra est 192.168.2.173 et que le port Web est 80, saisissez **http://192.168.2.173:80** pour atteindre l'appareil. En utilisation normale, l'accès HTTP utilise par défaut le port 80.

NOTE Avant la connexion, assurez-vous que la caméra et le PC se trouvent sur le même segment de réseau; sinon le client Web ne peut pas être atteint.

4.2 Première connexion

Lorsque vous accédez au client Web pour la première fois, vous devez définir un mot de passe pour terminer l'activation de la caméra. Le nom d'utilisateur par défaut est **admin**, que vous pouvez modifier après vous être connecté.

CAUTION Pour protéger l'appareil, le mot de passe doit comporter de 8 à 16 caractères et combiner au moins deux des types de caractères suivants : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux. Le mot de passe ne doit pas être identique au nom d'utilisateur.

Password

Default Username: admin

New Password: [Input field]

Password Strength: [Progress bar]

Confirm Password: [Input field]

OK

1.Length must be 8 ~ 16;
2.The password cannot be the same as the username;
3.Only uppercase letters,lowercase letters,digit,special characters allowed. Must contain 2 of them;
4.Special characters include ~!@#\$%^&*()-_+=~\|{};:~'~<~>~?

Figure 4-2. Définition du mot de passe pour activer la caméra

Après avoir saisi un nouveau mot de passe, cliquez sur **OK** pour l'enregistrer. Le client Web affiche alors l'écran de configuration de la récupération du mot de passe illustré ci-dessous, où vous pouvez configurer à l'avance une ou plusieurs méthodes de récupération afin que le mot de passe administrateur puisse être réinitialisé s'il venait à être oublié.

Recover Password

☐ Security Question Configuration

Security Question 1 Your father's name?

Answer

Security Question 2 Your mother's name?

Answer

Security Question 3 Your head teacher's name in senior high school?

Answer

☐ Certificate of authorization ?

Figure 4-3. Configuration de la récupération du mot de passe à la première connexion

Trois méthodes de récupération sont disponibles :

- **Configuration des questions de sécurité** — Utilisée pour réinitialiser le mot de passe administrateur en répondant à des questions prédéfinies. Choisissez 3 des 15 questions disponibles et fournissez une réponse à chacune. Chaque réponse peut comporter jusqu'à 64 caractères.
- **Certificat d'autorisation** — Utilisé pour réinitialiser le mot de passe administrateur à l'aide d'un fichier de clé. Lorsque cette méthode est activée, cliquez sur **Exporter** pour télécharger le fichier de clé, certificate.txt, et conservez-le dans un endroit sûr.
- **Super code** — La méthode de récupération recommandée, activée par défaut dans les micrologiciels récents. Un super code à usage unique est dérivé de l'adresse MAC de la caméra et de l'heure système de la caméra et, une fois vérifié, permet de réinitialiser le mot de passe administrateur. Comme le super code est généré par le soutien technique de GSD Group, cette méthode offre un moyen fiable de retrouver l'accès lorsque les autres méthodes ne sont pas disponibles.

NOTE Lorsque vous activez une méthode de récupération de mot de passe, conservez en lieu sûr et à jour les informations de vérification associées.

4.3 Connexion générale

Lors des visites suivantes du client Web, l'écran de connexion illustré ci-dessous s'affiche. Saisissez le nom de compte et le mot de passe, puis cliquez sur **Connexion** pour ouvrir l'interface d'exploitation de la caméra. Vous pouvez également sélectionner la langue de l'interface sur l'écran de connexion.

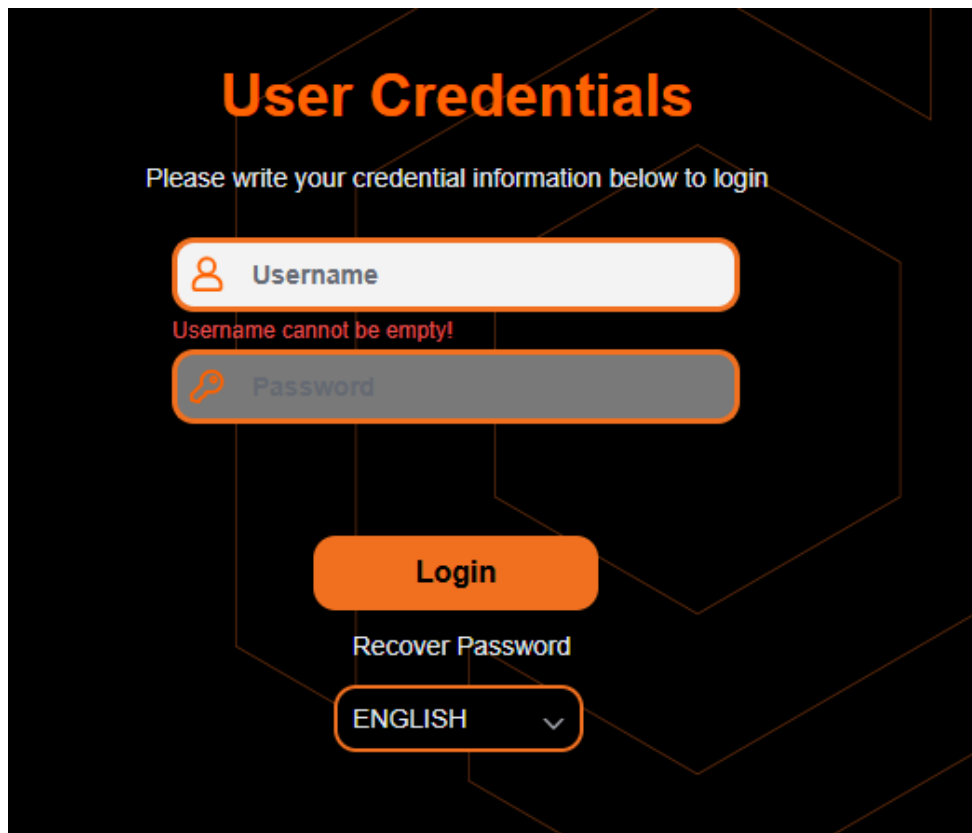


Figure 4-4. Écran de connexion du client Web

4.4 Récupération d'un mot de passe

Lorsque la récupération du mot de passe a été activée, vous pouvez retrouver l'accès si vous oubliez vos identifiants de connexion. Sur l'écran de connexion, cliquez sur **Récupérer le mot de passe** pour ouvrir l'écran de récupération, puis utilisez la question de sécurité, le certificat d'autorisation ou la méthode du super code que vous avez configurés lors de la première connexion.

4.4.1 Question de sécurité

Sur l'écran **Récupérer le mot de passe**, répondez aux questions de sécurité que vous avez configurées précédemment. Une fois les réponses vérifiées, vous pouvez définir directement un nouveau mot de passe administrateur.

The screenshot shows a 'Recover Password' dialog box with a dark background and orange borders. At the top, the title 'Recover Password' is centered. Below it, the 'Verification Mode' is set to 'Security Question Verification' in a dropdown menu. The dialog contains three security questions, each with a label and a corresponding text input field for the answer:

- Security Question 1:** 'Your father's name?' with an empty text box labeled 'Answer'.
- Security Question 2:** 'Your mother's name?' with an empty text box labeled 'Answer'.
- Security Question 3:** 'Your head teacher's name in senior high school?' with an empty text box labeled 'Answer'.

Below the questions, there is a 'New Password' text box, a 'Password Strength' indicator showing three segments, and a 'Confirm Password' text box. At the bottom, there are 'OK' and 'Cancel' buttons.

Figure 4-5. Récupération du mot de passe à l'aide des questions de sécurité

4.4.2 Certificat d'autorisation

Sur l'écran de connexion, cliquez sur **Récupérer le mot de passe** et passez à la méthode **Certificat d'autorisation**. Chargez le fichier de clé (certificate.txt) que vous avez exporté précédemment pour vérifier votre identité, puis définissez un nouveau mot de passe administrateur.

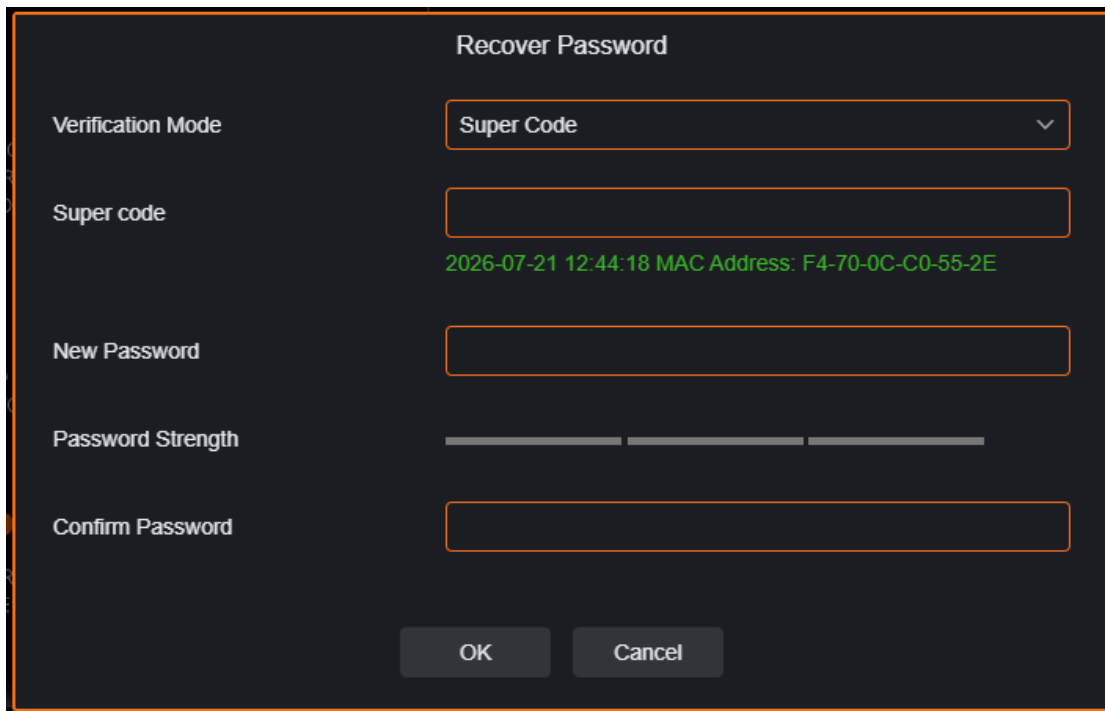
The screenshot shows a 'Recover Password' dialog box with a dark background and orange borders. At the top, the title 'Recover Password' is centered. Below it, the 'Verification Mode' is set to 'Certificate of authorization' in a dropdown menu. The dialog contains a 'Certificate of authorization' text box and an 'Import' button. At the bottom, there are 'OK' and 'Cancel' buttons.

Figure 4-6. Récupération du mot de passe à l'aide du certificat d'autorisation

NOTE Une fois le mot de passe réinitialisé avec cette méthode, le fichier de clé existant devient invalide. Reconnectez-vous et exportez un nouveau fichier de clé lorsque vous y êtes invité.

4.4.3 Super code

Sur l'écran de connexion, cliquez sur **Récupérer le mot de passe** et passez à la méthode **Super code**. L'écran change comme illustré ci-dessous. Saisissez le code de vérification correct pour réinitialiser le mot de passe administrateur. Le code de vérification est calculé par le soutien technique de GSD Group à l'aide d'un outil dédié, en fonction de l'adresse MAC de la caméra et de l'heure système de la caméra.



The screenshot shows a 'Recover Password' interface with a dark background. It includes the following elements:

- Verification Mode:** A dropdown menu currently set to 'Super Code'.
- Super code:** A text input field. Below it, a green message reads: '2026-07-21 12:44:18 MAC Address: F4-70-0C-C0-55-2E'.
- New Password:** A text input field.
- Password Strength:** A progress bar consisting of three segments, with the first two filled.
- Confirm Password:** A text input field.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

Figure 4-7. Récupération du mot de passe à l'aide d'un super code

TIP Le super code est la méthode de récupération recommandée et est activé par défaut dans les micrologiciels récents. Pour obtenir un code de vérification, communiquez avec le soutien technique de GSD Group en fournissant l'adresse MAC de la caméra et l'heure système.

Visionnement en direct, lecture et événements

Aperçu en direct, vidéo enregistrée et recherche d'événements

Chapitre 5 Écran de prévisualisation

5.1 Menu en direct

Une fois connecté, le client Web OCTAVUE by GSD Group ouvre l'interface de prévisualisation en direct, illustrée ci-dessous. La vue en direct est l'espace de travail par défaut pour surveiller la caméra et exploiter ses fonctions de contrôle d'accès.

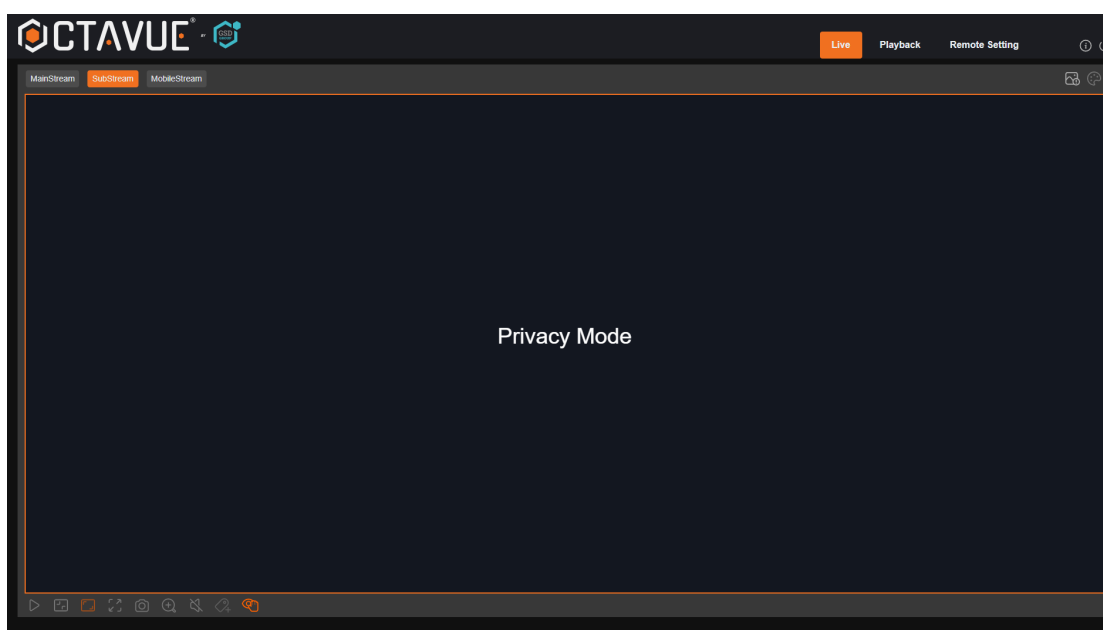


Figure 5-1. Interface de prévisualisation en direct du client Web

NOTE Les fonctions disponibles varient selon le modèle de caméra. Les commandes décrites ici peuvent différer de celles affichées sur votre appareil; reportez-vous toujours à l'interface réelle.

Le coin supérieur gauche de la fenêtre offre les commandes de flux et de navigation :

- **Menu de commutation de flux** — Sélectionne le flux utilisé pour la vue en direct actuelle, vous permettant d'équilibrer la qualité d'image par rapport à la charge du réseau et du PC.
- **Flux principal** — Fournit une image haute définition, mais impose des exigences plus élevées sur la bande passante et les performances du PC.
- **Flux secondaire** — Impose des exigences modérées sur la bande passante et les performances du PC, avec une qualité d'image inférieure à celle du flux principal.

- **Barre de commutation principale** — Bascule entre les écrans de fonction du client Web. Le client Web offre quatre menus : Direct, Lecture, Réglage à distance et Paramètres locaux.

La barre d'outils en direct offre les commandes suivantes :

-  **Infos** — Affiche l'utilisateur actuellement connecté, la version du client Web et la version du module d'extension.
-  **Alarme IA** — Ouvre la barre de notification d'alarmes sur le côté droit de la fenêtre, qui affiche les images capturées transmises par des fonctions telles que la détection de visage, de silhouette humaine et de véhicule.
-  **Couleur** — Ajuste les paramètres d'image tels que la saturation et la netteté.
- **Quitter** — Ferme la session actuelle.
- **État d'alarme vidéo** — Indique l'état d'alarme et d'enregistrement de la caméra actuelle. Pour plus de détails, voir État vidéo, plus loin dans ce chapitre.
-  **Arrêter / Lire** — Démarre ou arrête la prévisualisation du flux actuel.
-  **Proportions d'origine** — Affiche la prévisualisation actuelle dans son rapport d'aspect d'origine.
-  **Étirer** — Met à l'échelle la prévisualisation actuelle pour remplir toute la zone d'affichage.
-  **Plein écran** — Affiche la prévisualisation actuelle en plein écran. Double-cliquez sur l'image pour activer ou désactiver le plein écran, et appuyez sur Esc pour quitter.
-  **Enregistrer** — Enregistre manuellement le flux de prévisualisation actuel.
-  **Capturer** — Capture manuellement une image fixe à partir du flux actuel.
-  **Zoom numérique** — Agrandit électroniquement une zone sélectionnée de l'affichage.
-  **Audio** — Active ou désactive l'audio de la prévisualisation et ajuste son volume.
-  **Interphone vocal** — Établit une communication audio bidirectionnelle avec la caméra.
-  **Sirène** — Active ou désactive manuellement la sirène.
-  **Compteur de pixels** — Trace une zone de sélection pour indiquer les dimensions en pixels de la zone sélectionnée dans le flux.
- **Informations de la fenêtre contextuelle** — Lorsque certaines alarmes sont déclenchées, un message décrivant l'alarme en cours apparaît dans le coin inférieur droit de la fenêtre.
-  **Mode confidentialité** — Active ou désactive le mode confidentialité.
-  **Porte** — Ouvre et ferme le menu de contrôle de porte.
-  **Déverrouiller / Verrouiller** — Dans le menu de porte, cliquez sur Déverrouiller pour libérer la serrure de la porte ou sur Verrouiller pour la sécuriser.

5.2 État vidéo

Les indicateurs d'état vidéo sont des notifications à l'écran qui indiquent l'état d'alerte et d'enregistrement actuel de la caméra. Plusieurs alarmes peuvent être actives en même temps, de sorte que plusieurs indicateurs peuvent apparaître ensemble.

Indicateur	Signification
------------	---------------

(aucun)	La carte SD est normale, mais aucun enregistrement n'est en cours.
R	La caméra enregistre normalement.
H	La carte SD est dans un état anormal. Vérifiez et confirmez la carte SD.
M	Une alarme de mouvement est active, mais l'enregistrement sur alarme de mouvement n'est pas activé.
M	Une alarme de mouvement est active et l'enregistrement sur alarme de mouvement est en cours.
I	Une alarme I/O est active, mais l'enregistrement sur alarme I/O n'est pas activé.
I	Une alarme I/O est active et l'enregistrement sur alarme I/O est en cours.
S	Une alarme intelligente est active, mais l'enregistrement sur alarme intelligente n'est pas activé.
S	Une alarme intelligente est active et l'enregistrement sur alarme intelligente est en cours.
D	Une alarme d'accès (échecs d'authentification atteignant le nombre défini, dépassement du délai d'ouverture de porte ou alarme d'altération) est active, mais l'enregistrement sur alarme n'est pas activé.
D	Une alarme d'accès est active et l'enregistrement sur alarme est en cours.

NOTE Les alarmes intelligentes comprennent la détection de visage, la détection de silhouette humaine et d'autres détections basées sur l'IA.

Chapitre 6 Lecture

La surveillance en direct ne suffit pas à elle seule pour un déploiement de contrôle d'accès : les vidéos enregistrées doivent être conservées afin que les événements puissent être examinés après coup. La caméra de contrôle d'accès OCTAVUE de GSD Group enregistre les vidéos sur sa carte SD/TF et offre deux modes de récupération complémentaires — la lecture générale pour parcourir les enregistrements continus et sur événement, et la lecture intelligente pour repérer les séquences dans lesquelles une personne a été détectée.

6.1 Lecture générale

La lecture générale combine une recherche vidéo classique avec une recherche d'images assistée par l'IA. Ouvrez la page de lecture et utilisez la vue de recherche vidéo illustrée ci-dessous pour repérer et examiner les séquences stockées sur la carte SD/TF.

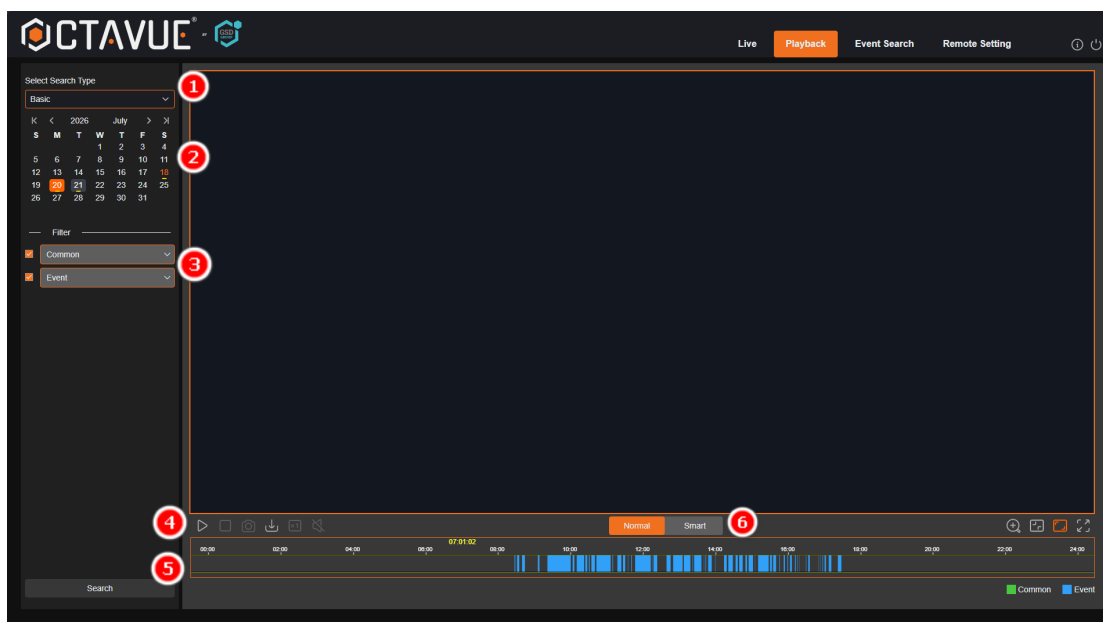


Figure 6-1. Interface de recherche vidéo générale

La vue de recherche présente les commandes suivantes :

- **Sélecteur de mode de recherche** — Bascule la fonction de recherche active. Le mode par défaut est la recherche générale, qui récupère les fichiers vidéo standard. Basculez cette commande pour passer à la recherche d'images par IA, décrite plus loin dans cette section.
- **Date de recherche** — Définit la date à rechercher. Cliquez sur **Rechercher** pour interroger la carte SD/TF ; les dates contenant des enregistrements sont indiquées sur le calendrier.
- **Type de recherche** — Répertorie les types d'enregistrement pris en charge par la caméra afin que seules les séquences requises soient affichées. Sur la barre chronologique, les enregistrements généraux (continus) apparaissent en vert et les enregistrements sur événement apparaissent en bleu.
- **Zoom de la barre de progression de lecture** — La barre de progression affiche une plage de 24 heures par défaut. Effectuez un zoom avant ou arrière sur la barre pour vous positionner plus précisément à un point de lecture. La molette de la souris effectue la même action de zoom.
- **Rechercher** — Affiche la vidéo stockée sur la carte SD/TF selon les paramètres de recherche actuels.
- **Recherche normale / intelligente** — Bascule entre la recherche normale et la recherche intelligente. Après avoir sélectionné la recherche intelligente, cliquez sur les boutons de type personne et de type véhicule dans le coin inférieur gauche ; la barre d'enregistrement marque alors en bleu la vidéo d'alarme déclenchée par le type sélectionné pour cette journée. Cette vidéo d'alarme comprend les séquences ayant déclenché la détection de piétons et la détection de mouvement.

6.1.1 Barre d'outils de commande de lecture

La barre d'outils située sous la fenêtre vidéo commande le flux de lecture actif.

- ▶ **Pause / Lecture** — Met en pause ou reprend le flux de lecture.
- **Arrêter** — Ferme le flux de lecture.
- ▶ **Avancer d'une image** — Avance la lecture d'une image à chaque clic.
- 📁 **Enregistrer** — Enregistre manuellement le flux de lecture actuel.
- 📷 **Capture** — Capture manuellement une image fixe à partir du flux actuel.
- ⬇️ **Télécharger** — Télécharge la vidéo renvoyée par la recherche actuelle.

NOTE Lorsqu'une vidéo est téléchargée au format AVF, la caméra demande si le fichier doit être chiffré, comme illustré ci-dessous. Les formats AVI et MP4 n'affichent pas cette invite.

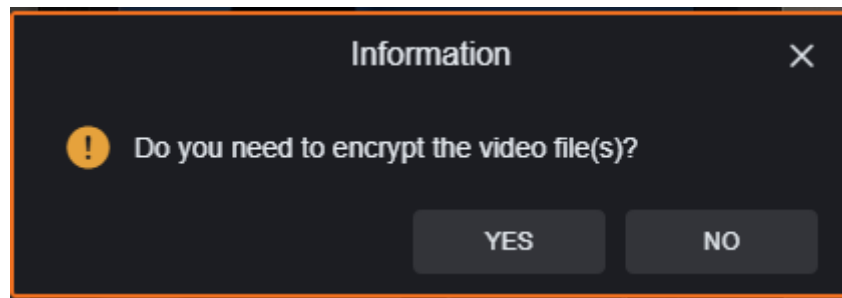


Figure 6-2. Invite de chiffrement affichée lors du téléchargement d'une vidéo au format AVF

- Vitesse** — Change la vitesse de lecture. Les vitesses prises en charge sont 1/8, 1/4, 1/2, 1, X2, X4, X8 et X16.
- Audio** — Active ou désactive le son du flux de lecture et règle son volume.
- Zoom numérique** — Agrandit une zone sélectionnée du flux de lecture.
- Taille d'origine** — Affiche l'image de lecture à son échelle d'origine.
- Étirer** — Met l'image de lecture à l'échelle pour remplir la zone d'affichage disponible.
- Plein écran** — Double-cliquez sur la fenêtre pour entrer en mode plein écran ou en sortir. Appuyez sur Échap pour quitter le plein écran.

6.2 Lecture intelligente

La lecture intelligente est disponible lorsque vous vous connectez au moyen de la vue de navigateur sans module d'extension. Elle détermine si une alarme a été déclenchée par une personne et marque ces périodes en bleu sur la barre chronologique ci-dessous, ce qui vous permet de passer directement aux séquences pertinentes.

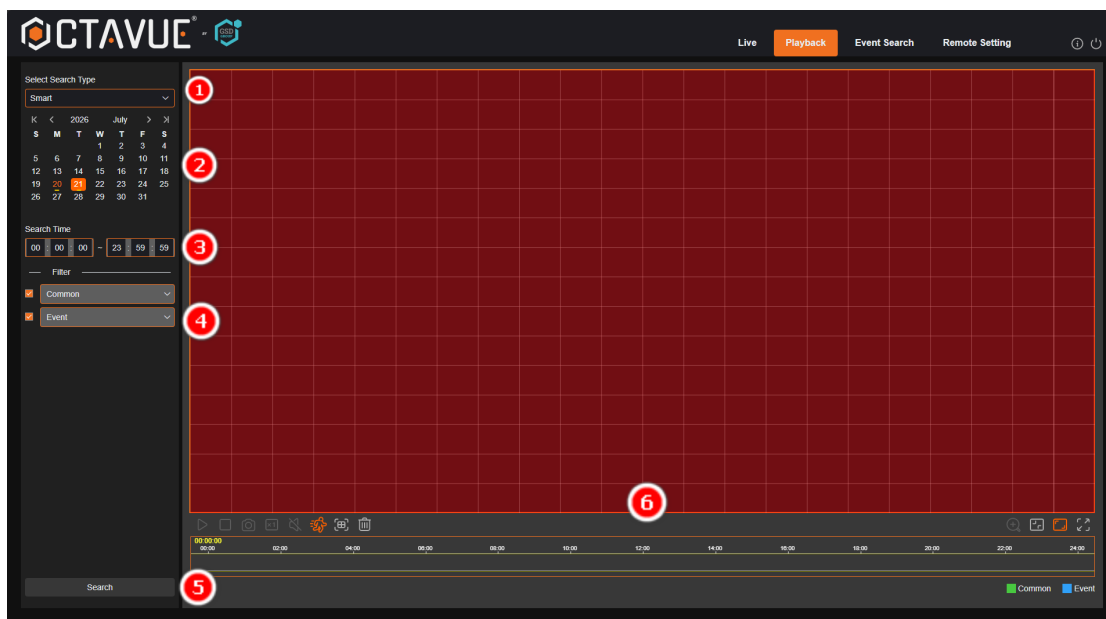


Figure 6-3. Interface de lecture intelligente

La vue de recherche intelligente présente les commandes suivantes :

- **Sélecteur de mode de recherche** — Bascule la fonction de recherche active ; ici, elle est réglée sur Intelligent.
- **Date de recherche** — Définit la date de l'événement intelligent à rechercher. Cliquez sur **Rechercher** pour interroger la carte ; les dates contenant des enregistrements sont indiquées.
- **Heure de recherche** — Définit la plage horaire des événements à rechercher, ce qui facilite le repérage d'une période précise.
- **Type de recherche** — Répertorie les types de recherche pris en charge par la caméra afin que seules les séquences requises soient affichées.
- **Rechercher** — Cliquez pour lancer la recherche.
- **Zone d'affichage des résultats de recherche** — Affiche les séquences renvoyées par la recherche.

6.2.1 Barre d'outils de commande de lecture

La barre d'outils située sous la fenêtre vidéo commande le flux de lecture actif et la zone de détection intelligente.

-  **Pause / Lecture** — Met en pause ou reprend le flux de lecture.
-  **Arrêter** — Ferme le flux de lecture.
-  **Capture** — Capture manuellement une image fixe à partir du flux actuel.
-  **Vitesse** — Change la vitesse de lecture. Les vitesses prises en charge sont 1/8, 1/4, 1/2, 1, X2, X4, X8 et X16.
-  **Audio** — Active ou désactive le son du flux de lecture et règle son volume.
-  **Intelligent** — Ouvre l'écran de configuration de la zone intelligente.
-  **Tout** — Définit l'ensemble du champ de la caméra comme zone de détection intelligente.
-  **Supprimer** — Efface l'ensemble de la zone de détection intelligente.
-  **Zoom numérique** — Agrandit une zone sélectionnée du flux de lecture.
-  **Taille d'origine** — Affiche l'image de lecture à son échelle d'origine.
-  **Étirer** — Met l'image de lecture à l'échelle pour remplir la zone d'affichage disponible.
- **Plein écran** — Double-cliquez sur la fenêtre pour entrer en mode plein écran ou en sortir. Appuyez sur Échap pour quitter le plein écran.

Chapitre 7 Recherche d'événements

La caméra de contrôle d'accès OCTAVUE de GSD Group enregistre chaque événement d'authentification, chaque image capturée et chaque instantané de détection par IA sur la carte SD/TF installée, avec la vidéo associée. L'interface de recherche d'événements vous permet de récupérer ces enregistrements selon des critères précis et de lire l'enregistrement lié à n'importe quel résultat.

Les fonctions de recherche sont regroupées par type. Utilisez le **sélecteur** de mode de recherche situé en haut de l'interface pour passer d'Événement de contrôle d'accès à Image et à Recherche IA sans quitter la page. Chaque mode présente les champs de filtre pertinents pour ce type d'enregistrement ; définissez les champs, cliquez sur **Rechercher**, et les résultats correspondants apparaissent dans la zone d'affichage de droite.

7.1 Événement de contrôle d'accès

Cette interface répertorie chaque événement d'authentification d'accès et vous permet de lire l'enregistrement associé à chacun.

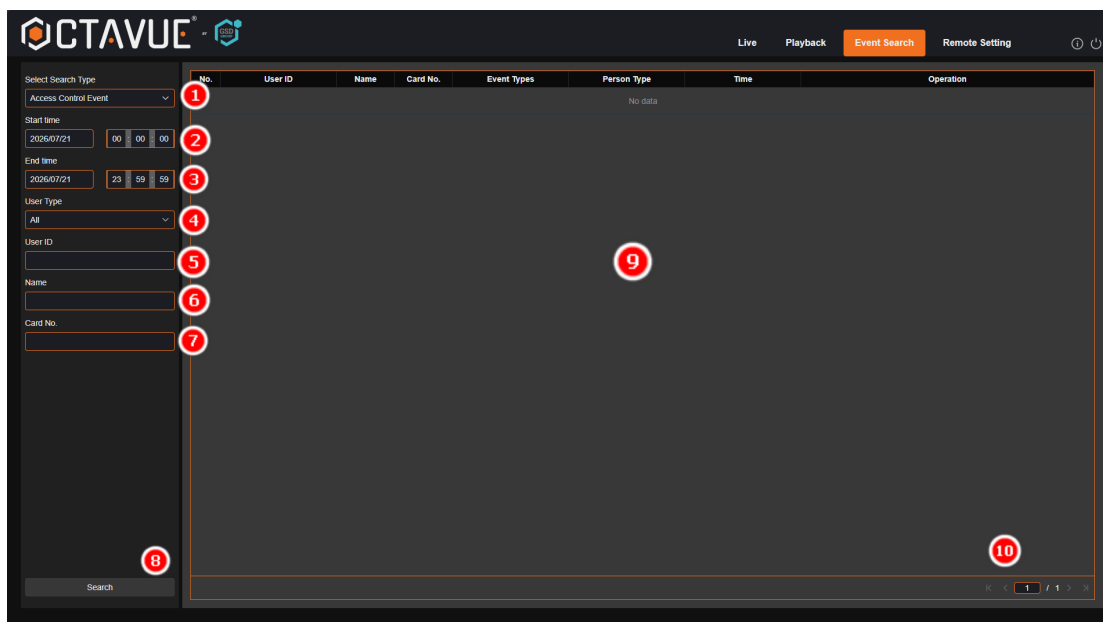


Figure 7-1. Interface de recherche d'événements de contrôle d'accès

Configurez les champs suivants, puis cliquez sur **Rechercher** pour lancer la requête :

- **Sélecteur de mode de recherche** — sélectionne la fonction de recherche active. Événement de contrôle d'accès est le mode par défaut ; dans ce mode, la requête renvoie les fichiers vidéo liés aux événements d'authentification d'accès.
- **Heure de début** — définit le début de la période de recherche.
- **Heure de fin** — définit la fin de la période de recherche.
- **Type d'utilisateur** — restreint les résultats à un ou plusieurs types d'utilisateur. Tous les types sont sélectionnés par défaut : administrateur, ordinaire, invité et utilisateurs personnalisés.
- **Nom** — saisissez un mot-clé de nom d'utilisateur pour filtrer les résultats.
- **N° de carte** — saisissez un mot-clé de numéro de carte d'accès pour filtrer les résultats.
- **Rechercher** — lance la requête à l'aide des critères ci-dessus.
- **Zone d'affichage des résultats de recherche** — répertorie les événements qui correspondent aux critères. Chaque ligne correspond à un événement d'authentification et à son enregistrement.

Dans une ligne de résultat, cliquez sur le bouton de lecture pour ouvrir l'enregistrement de cet événement :



Lit l'enregistrement associé à l'événement sélectionné.

- **Page des résultats de recherche** — le pageur situé dans le coin inférieur droit vous permet de parcourir plusieurs pages de résultats.

7.2 Image

Utilisez cette interface pour rechercher des images capturées et lire la vidéo qui les entoure.

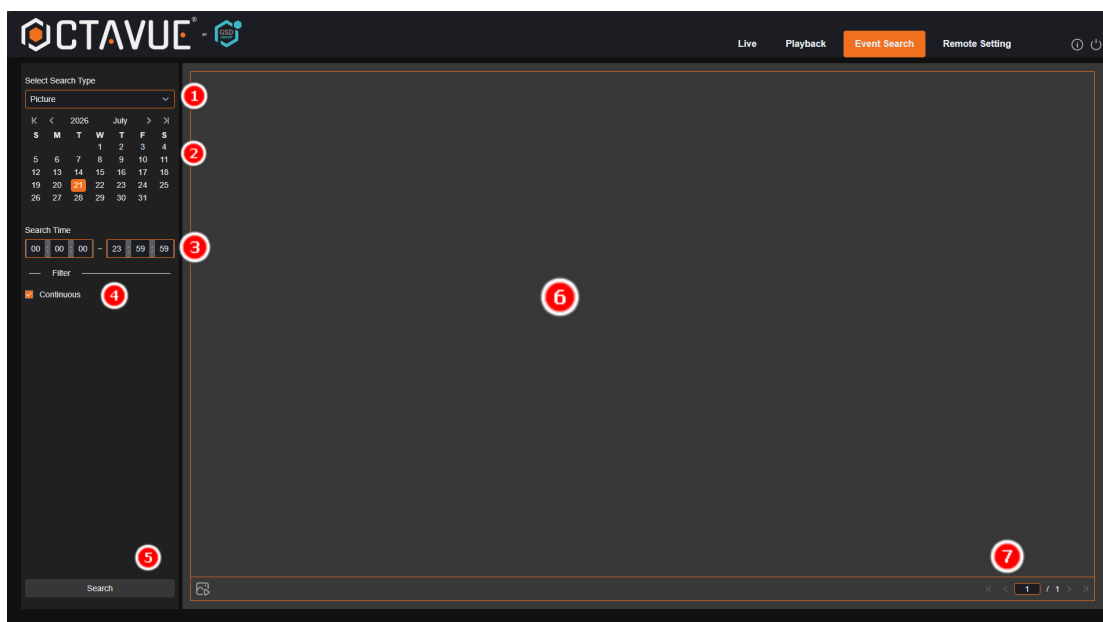


Figure 7-2. Interface de recherche d'images

Définissez les champs suivants, puis cliquez sur **Rechercher** :

- **Sélecteur de mode de recherche** — réglé sur Image pour rechercher des images capturées.
- **Date de recherche** — définit la date à rechercher. Après avoir cliqué sur Rechercher, les dates contenant des fichiers capturés sont indiquées.
- **Heure de recherche** — définit la plage horaire afin que vous puissiez récupérer les images d'une période précise.
- **Type de recherche** — sélectionne le type de capture d'image à rechercher. Tous les types sont sélectionnés par défaut.
- **Rechercher** — lance la recherche d'images.
- **Zone d'affichage des résultats de recherche** — affiche les images qui correspondent aux critères. Double-cliquez sur une image pour lire la vidéo de la période située immédiatement avant et après celle-ci.
- **Page des résultats de recherche** — le pageur situé dans le coin inférieur droit vous permet de parcourir les résultats.

7.3 IA

La recherche IA récupère les instantanés de visages et de piétons produits par les fonctions de reconnaissance de la caméra, ce qui vous permet de repérer l'enregistrement correspondant à partir d'un instantané.

7.3.1 Détection de visages

Lorsque la caméra effectue la reconnaissance de visages, elle stocke chaque visage capturé et les informations d'image associées sur la carte SD/TF. Lors d'une recherche, vous pouvez rapidement récupérer un instantané de visage répondant à vos critères et accéder à l'enregistrement qui lui est associé. L'interface de lecture de la détection de visages est illustrée ci-dessous.

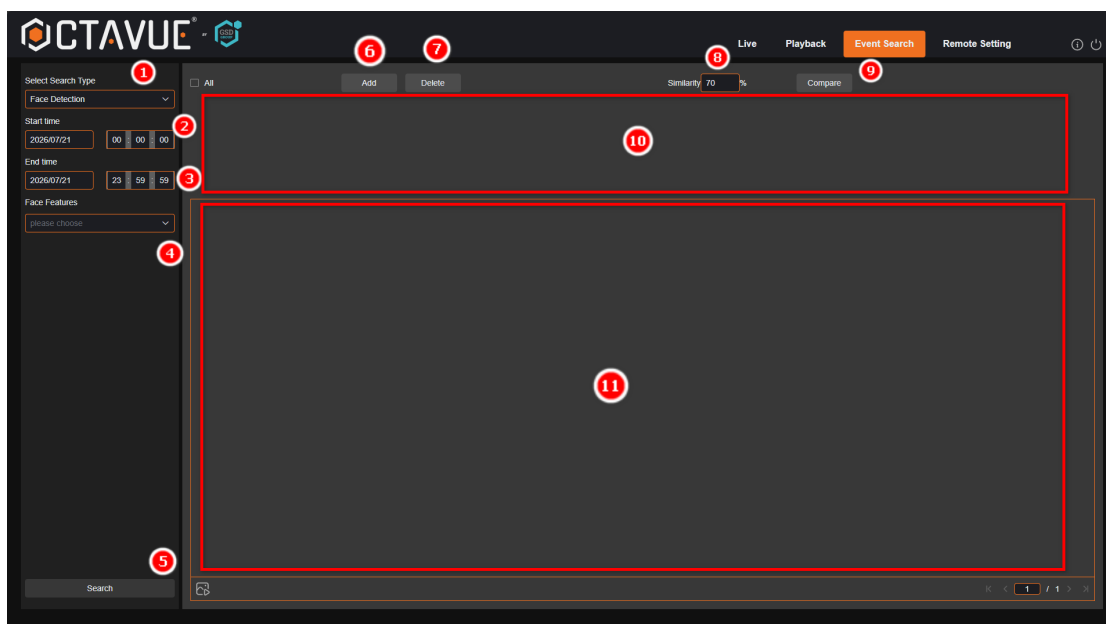


Figure 7-3. Interface de recherche de détection de visages

Configurez les commandes de recherche et de comparaison selon vos besoins :

- **Sélecteur de mode de recherche** — réglé sur Détection de visages.
- **Heure de début** — définit le début de la période de recherche des visages capturés.
- **Heure de fin** — définit la fin de la période de recherche des visages capturés.
- **Attribut de visage** — désactivé par défaut. Lorsqu'elle est activée, la recherche renvoie uniquement les visages capturés pendant que la détection des caractéristiques du visage était active. Le micrologiciel reconnaît cinq attributs de visage : le sexe, l'âge, le masque, les lunettes et l'expression.
- **Rechercher** — recherche les données de visage selon les paramètres actuels.
- **Ajouter** — ajoute une image de référence à la zone de comparaison. Vous pouvez ajouter à la fois des images locales et des images capturées.
- **Supprimer** — retire les images actuellement ajoutées.
- **Similarité** — définit la similarité minimale de valeur caractéristique qu'un visage doit atteindre pour être considéré comme une correspondance lors de l'utilisation de la fonction Comparer.
- **Comparer** — recherche les visages capturés à l'aide de l'heure de recherche sélectionnée, du groupe dans lequel se trouvent les images capturées et de l'image de visage de référence sélectionnée.
- **Zone d'affichage des images ajoutées** — affiche les images de référence actuellement ajoutées et disponibles pour la comparaison.
- **Zone d'affichage des résultats de recherche** — à droite, affiche les images renvoyées par Rechercher et Comparer. Double-cliquez sur une image pour lire la vidéo d'avant et d'après.

NOTE Comparer met en correspondance les visages capturés avec vos images de référence selon la similarité de valeur caractéristique. Abaisser le seuil de **Similarité** renvoie davantage de correspondances candidates mais augmente le risque de faux résultats ; augmentez-le pour privilégier la précision.

7.3.2 Piéton

Lorsque la caméra effectue la reconnaissance de piétons, elle stocke chaque piéton capturé et les informations d'image associées sur la carte SD/TF. Lors d'une recherche, vous pouvez rapidement récupérer un instantané de piéton répondant à vos critères et accéder à l'enregistrement qui lui est associé. L'interface de lecture de la recherche de piétons est illustrée ci-dessous.

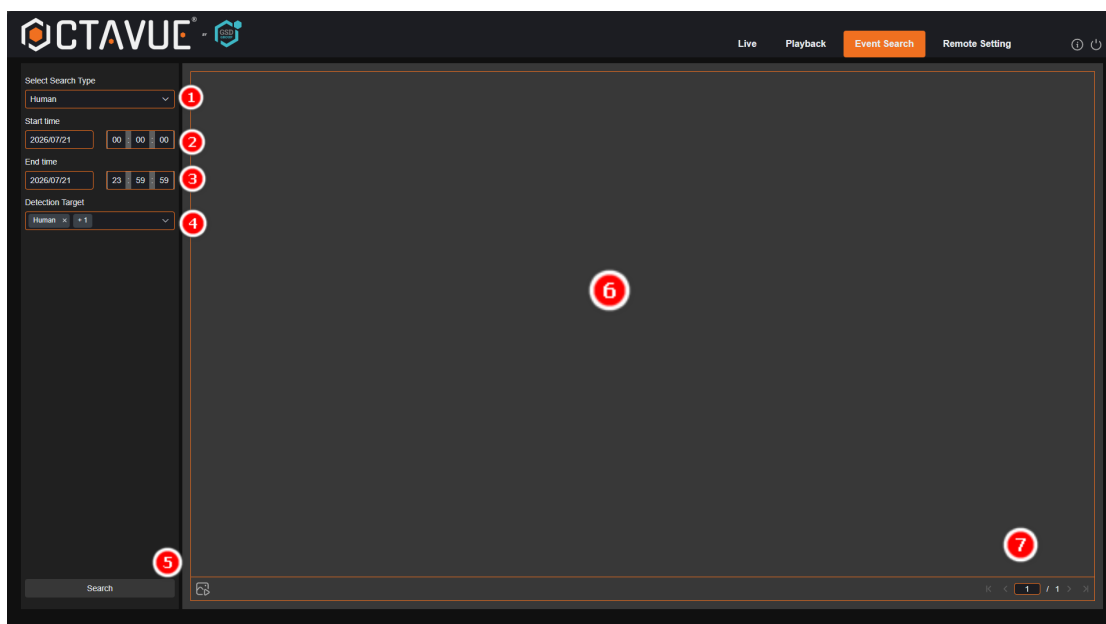


Figure 7-4. Interface de recherche de piétons

Définissez les champs suivants, puis cliquez sur **Rechercher** :

- **Sélecteur de mode de recherche** — réglé sur Piéton.
- **Heure de début** — définit le début de la période de recherche des images de piétons.
- **Heure de fin** — définit la fin de la période de recherche des images de piétons.
- **Cible de détection** — sélectionne les images humaines à inclure selon les besoins.
- **Rechercher** — recherche les images de piétons selon les paramètres actuels.
- **Zone d'affichage des résultats de recherche** — affiche les résultats correspondants. Double-cliquez sur une image pour lire la vidéo d'avant et d'après.
- **Page des résultats de recherche** — le pageur situé dans le coin inférieur droit vous permet de faire défiler les résultats.

Configuration de la caméra

Image, enregistrement, alarmes, événements et réseau

Chapitre 8 Image et encodage

Ce chapitre décrit les paramètres d'image et d'encodage disponibles dans le menu de configuration à distance de la caméra de contrôle d'accès OCTAVUE. À partir de ces pages, vous pouvez ajuster l'incrustation de l'aperçu en direct, régler le pipeline de traitement de l'image, définir les flux d'enregistrement et d'encodage, gérer l'audio et configurer la capture d'image automatique.

8.1 Aperçu

La page En direct configure le nom du canal et la position de l'affichage à l'écran (OSD) de la caméra, comme illustré ci-dessous.

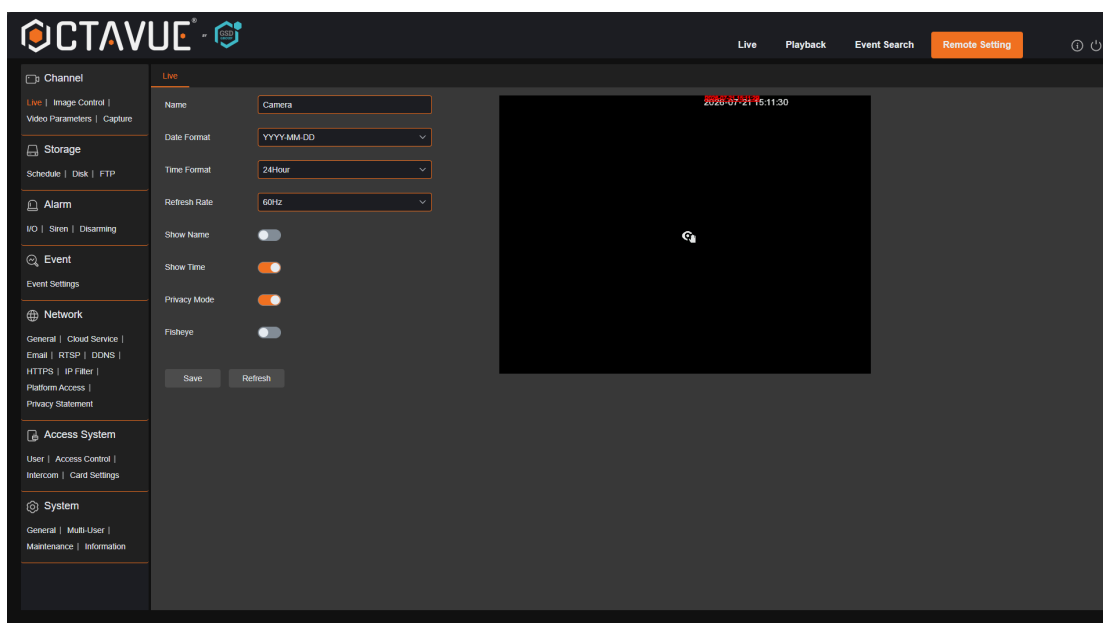


Figure 8-1. Configuration de l'aperçu en direct et de l'OSD

Configurez les paramètres suivants :

- **Nom du canal** : définit le nom du canal de la caméra.
- **Format de date** : définit le format de date affiché dans l'OSD de la caméra. Les options disponibles sont MM/DD/YYYY, YYYY-MM-DD et DD/MM/YYYY.
- **Format d'heure** : définit le format d'heure affiché dans l'OSD de la caméra, soit 12 heures, soit 24 heures.
- **Fréquence de rafraîchissement** : définit la fréquence de rafraîchissement de la caméra. Deux options sont disponibles, 60Hz et 50Hz, correspondant respectivement aux modes N et P.
- **Afficher le nom** : affiche le nom du canal de la caméra dans l'aperçu. Désactivé par défaut.
- **Afficher l'heure** : affiche l'heure de la caméra dans l'aperçu.

- **Mode confidentialité** : lorsqu'il est activé, aucune image n'est affichée dans l'aperçu ni dans la lecture, et les pages de paramètres n'affichent pas d'image d'aperçu.
- **Distorsion de l'objectif** : lorsqu'elle est activée, l'image est affichée en mode aperçu fisheye. Lorsqu'elle est désactivée, la distorsion est corrigée et l'image remplit toute la zone d'affichage. Désactivée par défaut.
- **Position d'affichage du nom du canal** : définit l'endroit où apparaît le nom du canal en faisant glisser sa position sur l'image.
- **Position d'affichage de l'heure** : définit l'endroit où apparaît l'heure en faisant glisser sa position sur l'image.
- **Enregistrer** : enregistre les modifications en cours.
- **Actualiser** : recharge les paramètres de la page en cours.

CAUTION L'activation du **Mode confidentialité** supprime toute la vidéo en direct et enregistrée, y compris sur les pages de configuration. Utilisez-le uniquement lorsque vous avez l'intention de désactiver entièrement la capture d'image.

8.2 Commandes d'image

La page Commandes d'image modifie directement les paramètres de traitement de l'image, notamment le mode couleur/noir et blanc, la plage dynamique étendue et la compensation de contre-jour, comme illustré ci-dessous.

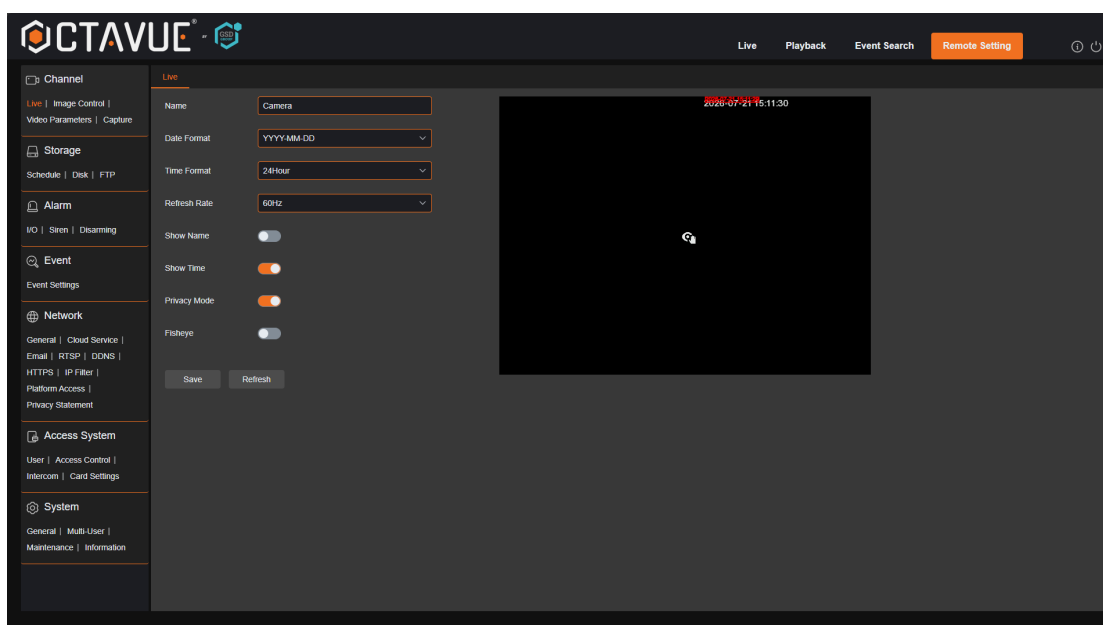


Figure 8-2. Paramètres de commande d'image

- **Mode IR-CUT** : définit le mode d'image de la caméra. Quatre modes sont disponibles :
- **Mode couleur** : l'image reste en couleur et ne passe pas en noir et blanc.
- **Mode noir et blanc** : l'image reste en noir et blanc et ne passe pas en couleur.
- **Mode image** : bascule entre la couleur et le noir et blanc selon l'image elle-même.
- **Programmation** : bascule entre la couleur et le noir et blanc selon une programmation. Pour utiliser ce mode, définissez les heures de début et de fin d'entrée en vision nocturne.
- **Commande de la DEL IR** : définit le comportement de vision nocturne de l'éclairage d'appoint infrarouge de la caméra. Trois modes sont disponibles :
- **IR intelligent** : ajuste dynamiquement l'intensité de l'éclairage infrarouge en fonction de facteurs tels que la distance focale et la surexposition éventuelle de l'image.
- **Manuel** : règle manuellement la luminosité de l'éclairage d'appoint infrarouge.

- **Feux de croisement** : ajuste manuellement la luminosité de la lampe infrarouge (0 à 100). Une valeur de 0 éteint la lampe et 100 règle la luminosité maximale.
- **Anti-surexposition** : lorsqu'elle est activée, empêche la surexposition de l'image dans les environnements très lumineux, dans tous les modes d'image.
- **Compensation d'exposition** : définit le comportement de la caméra en conditions de contre-jour. Quatre modes sont disponibles :
 - **WDR** : la plage dynamique étendue équilibre l'image uniformément selon le réglage de sorte que les zones claires et sombres restent clairement distinguables. Appelée DWDR sur certains modèles.
 - **HLC** : la compensation des hautes lumières rend les objets des zones très éclairées plus nets selon le niveau HLC configuré. Non pris en charge sur certains modèles.
 - **Contre-jour** : rend les zones sombres de l'image plus nettes selon le niveau BLC et la zone BLC configurés.
 - **Désactiver** : aucune compensation d'exposition n'est appliquée à l'image.
- **Balance des blancs** : définit la balance des blancs. Deux modes sont disponibles. **Automatique** ajuste la lumière blanche selon les paramètres par défaut, tandis que **Manuel** vous permet de régler directement le gain combiné du rouge, du vert et du bleu.
- **Obturbateur** : définit la durée d'exposition de l'obturateur. Sur les modèles qui prennent en charge la commande d'ouverture, **Automatique** sélectionne une durée d'exposition et une valeur d'ouverture appropriées dans les plages Durée d'exposition et Iris configurées, tandis que **Manuel** utilise directement les valeurs configurées. **Priorité obturbateur** dérive la valeur d'ouverture d'un obturbateur défini manuellement, et **Priorité iris** dérive la valeur d'obturateur d'une ouverture définie manuellement. Les modèles sans prise en charge de l'ouverture n'offrent que les modes automatique et manuel.

NOTE En mode obturbateur manuel, la durée d'exposition supprime l'option sans scintillement, alors qu'en mode obturbateur automatique, l'option sans scintillement est activée. Si vous revenez en mode manuel, la durée d'exposition est automatiquement réglée à 1/100 ou 1/120.

- **Durée d'exposition** : définit la durée d'exposition de la caméra, utilisée conjointement avec l'**Obturbateur**. Une durée d'exposition longue surexpose l'image, tandis qu'une durée d'exposition courte l'assombrit.
- **Mode antibrouillard** : lorsqu'il est activé, rend l'image plus nette par temps pluvieux ou brumeux.
- **Réduction de bruit 3D** : réduit le bruit de l'image pour une image plus nette. Trois modes sont disponibles : **Automatique** sélectionne le niveau de réduction de bruit de manière algorithmique, **OFF** désactive la réduction de bruit, et **Manuel** applique un coefficient de réduction de bruit défini manuellement.
- **Enregistrer** : enregistre les paramètres de commande d'image.
- **Par défaut** : rétablit les paramètres de commande d'image à leurs valeurs par défaut.
- **Actualiser** : recharge les paramètres d'image.

8.3 Paramètres vidéo

Ce menu configure les paramètres utilisés pour l'aperçu à l'écran et l'enregistrement.

8.3.1 Paramètres d'enregistrement

Cette section configure les paramètres liés à l'enregistrement du système.

- **Mode de flux** : sélectionne le flux qui est enregistré sur la carte SD. Par défaut, il s'agit du flux principal.
- **Enregistrement** : sélectionnez pour activer l'enregistrement.
- **Pré-enregistrement** : lorsqu'il est activé, la caméra commence à enregistrer quelques secondes avant un événement d'alarme. Cette option est recommandée lorsque l'enregistrement est principalement déclenché par la détection de mouvement ou les alarmes I/O.
- **Coupure réseau** : lorsqu'elle est activée, les événements continuent d'être enregistrés même lorsque le réseau est hors service ou que la connexion échoue.

8.3.2 Paramètres d'encodage

Cette section configure les paramètres de qualité d'image pour la vidéo enregistrée et la transmission réseau. Le flux principal définit généralement la qualité de la vidéo enregistrée sur le HDD. Le sous-flux définit la qualité de la vidéo d'aperçu accessible à distance, par exemple par les clients Web et le VMS. Le flux mobile, qui peut éventuellement être désactivé, définit la qualité de l'aperçu visualisé à distance depuis un appareil mobile.

The screenshot shows a configuration panel for video encoding. The 'MainStream' tab is active. The settings are as follows:

Parameter	Value
Resolution	3072 x 1728
FPS	30
Video Code Type	H.264
Video Code Level	Main Profile
Bitrate Control	VBR
Video Quality	Highest
Bitrate Mode	Predefined
Bitrate	4096 Kbps
I Frame Interval	60 (1 ~ 120)
Audio	Enabled (toggle switch)

Buttons at the bottom: Save, Default, Refresh.

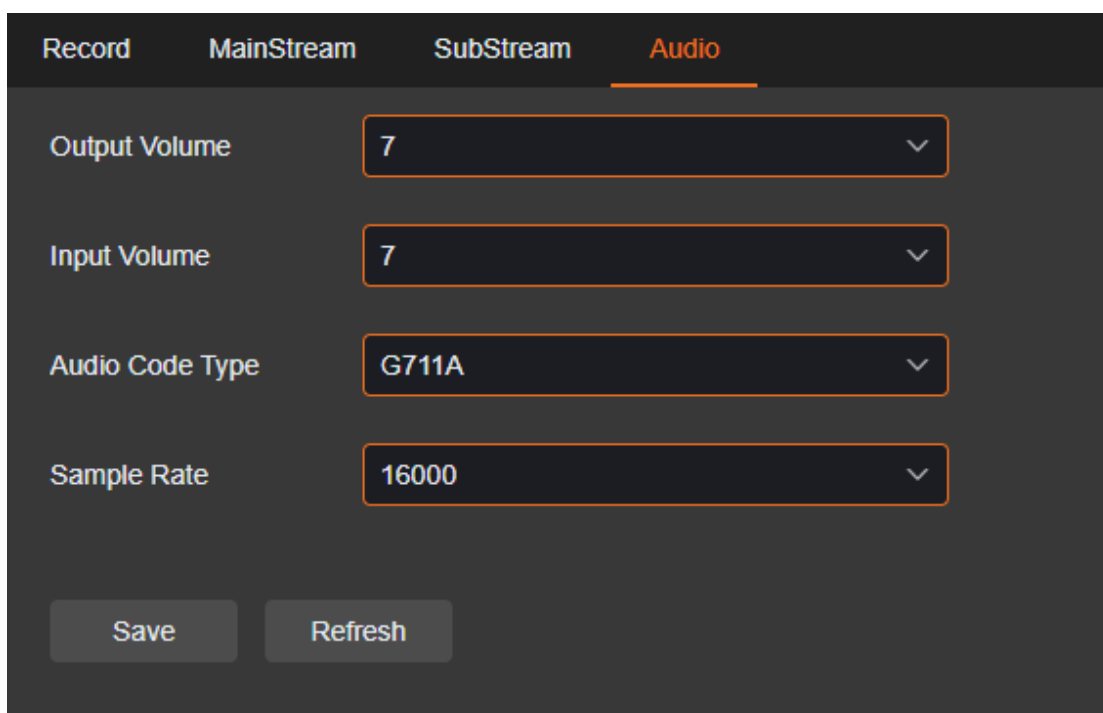
Figure 8-3. Paramètres d'encodage pour les flux principal, secondaire et mobile

- **Résolution** : indique la résolution de l'image enregistrée.
- **Fréquence d'images** : indique le nombre d'images par seconde enregistrées par la caméra.
- **Format d'encodage** : définit le type d'encodage du canal. Les options sont H.264, H.265, H.264+, H.265+ et MJPEG. MJPEG n'est disponible qu'en mode sous-flux.
- **Niveau de code vidéo** : définit le niveau de qualité vidéo : Baseline, Main Profile ou High Profile. Main Profile n'est disponible qu'avec H.265.
- **Mode d'encodage** : sélectionne la méthode de contrôle du débit. Le débit binaire constant (CBR) convient aux scènes simples comme un mur uni, tandis que le débit binaire variable (VBR) convient aux scènes plus complexes comme des rues animées.

- **Mode de configuration** : sélectionnez **Défini par l'utilisateur** pour régler le débit manuellement, ou **Mode prédéfini** pour choisir un débit prédéfini.
- **Débit binaire** : correspond au débit de transfert de données utilisé par la caméra pour enregistrer la vidéo. Un débit binaire plus élevé donne une meilleure qualité vidéo.
- **Intervalle d'images I** : définit l'intervalle d'images I de la caméra.
- **Audio** : activez cette option pour enregistrer l'audio et la vidéo simultanément. Elle nécessite un microphone connecté à la caméra ou une caméra dotée d'un audio intégré.
- **Enregistrer** : enregistre les paramètres d'encodage.
- **Par défaut** : rétablit les paramètres d'encodage à leurs valeurs par défaut.
- **Actualiser** : recharge les paramètres d'encodage.

8.3.3 Gestion de l'audio

Cette section configure l'entrée et la sortie audio de la caméra.



Record	MainStream	SubStream	Audio
			Output Volume: 7
			Input Volume: 7
			Audio Code Type: G711A
			Sample Rate: 16000
Save Refresh			

Figure 8-4. Paramètres de gestion de l'audio

- **Volume de sortie** : définit le volume de la sortie audio.
- **Volume d'entrée** : définit le volume de l'entrée audio.
- **Type de code audio** : définit le type d'encodage audio. G.711A et G.711U sont pris en charge.
- **Fréquence d'échantillonnage** : définit la fréquence d'échantillonnage audio. 8000 et 16000 sont pris en charge.

8.4 Paramètres de capture

Ce menu configure les paramètres de la fonction de capture d'image automatique.

The screenshot shows a dark-themed settings window titled 'Capture'. It contains three main settings: 'Normal Interval' and 'Alarm Interval', both set to '5 S' with dropdown arrows indicating more options are available. Below these is the 'Auto Capture' toggle switch, which is currently turned off. At the bottom of the window are two buttons: 'Save' and 'Refresh'.

Figure 8-5. Paramètres de capture automatique

- **Intervalle normal** : l'intervalle entre les captures pendant l'enregistrement normal.
- **Intervalle d'alarme** : l'intervalle entre les captures lorsqu'une alarme de détection de mouvement ou I/O est déclenchée.
- **Capture automatique** : active ou désactive la capture automatique.

Chapitre 9 Enregistrement, stockage et FTP

Ce chapitre explique comment contrôler le moment où la caméra de contrôle d'accès OCTAVUE enregistre de la vidéo et capture des images fixes, comment gérer les supports de stockage qui contiennent ces fichiers, et comment transférer les médias d'alarme vers un serveur FTP externe. Ensemble, ces réglages déterminent ce que la caméra enregistre, où c'est enregistré et comment c'est livré.

9.1 Réglages de programmation

Les programmations définissent les périodes durant lesquelles la caméra exécute des actions en continu, déclenchées par le mouvement ou déclenchées par les E/S. L'enregistrement et la capture d'images sont chacun régis par leur propre programmation indépendante.

9.1.1 Programmation d'enregistrement

Utilisez la programmation d'enregistrement pour configurer l'enregistrement régulier et d'alarme sur une période hebdomadaire définie. L'enregistrement est désactivé par défaut; une programmation doit être activée avant que la caméra ne stocke de la vidéo.

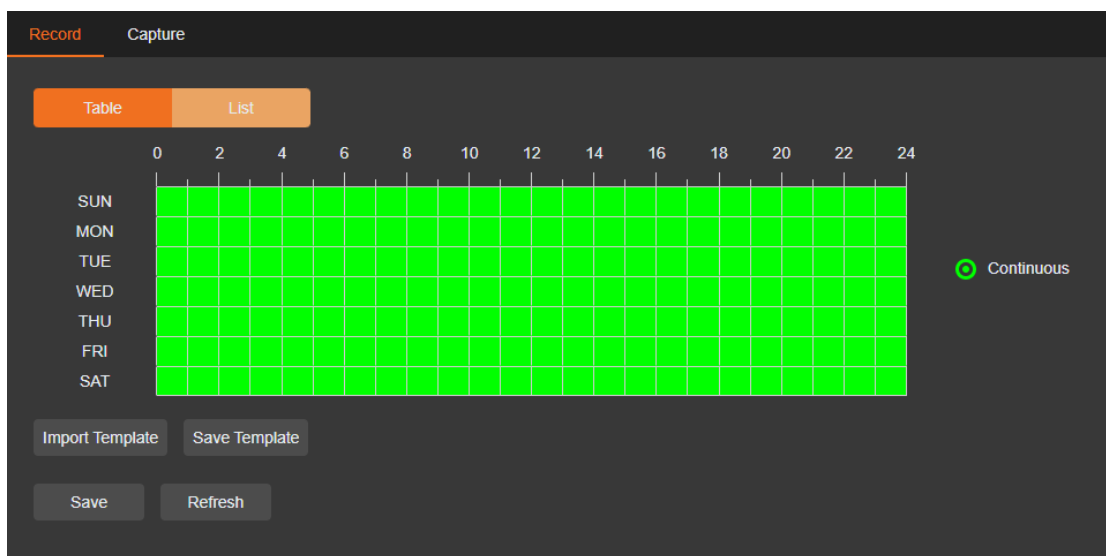


Figure 9-1. Programmation d'enregistrement en vue tableau

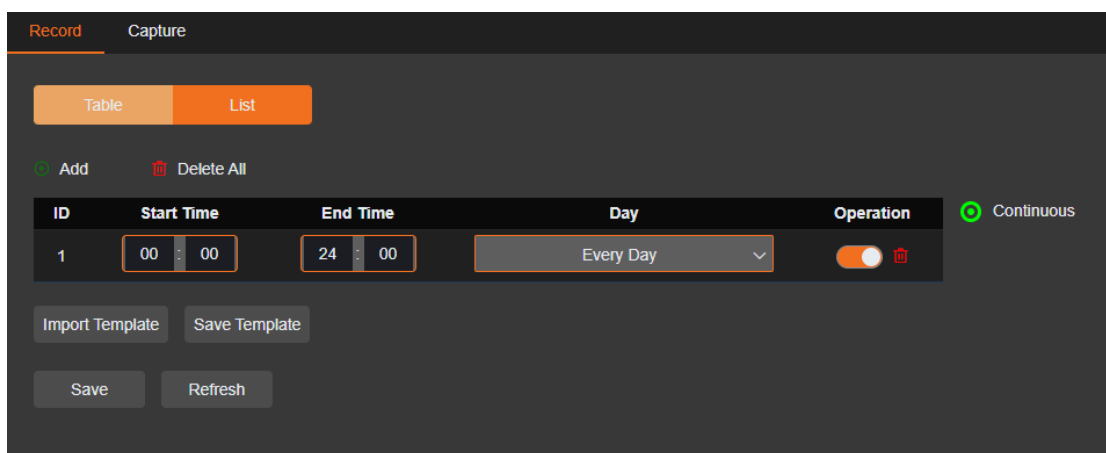


Figure 9-2. Programmation d'enregistrement en vue liste

La programmation peut être définie en vue **Tableau** ou **Liste**. Utilisez le sélecteur à droite des entrées **Normal**, **Mouvement** et **E/S** pour changer le type de vidéo dont vous modifiez la programmation.

- **Vue tableau** : glissez sur la grille, ou sélectionnez les cellules horaires individuelles, pour marquer les périodes durant lesquelles le type d'enregistrement choisi est actif.
- **Vue liste** : ajoutez des règles manuellement et saisissez une heure de début et de fin pour chacune, définissant explicitement la période active.

Les commandes suivantes sont disponibles lors de la création d'une programmation :

- **Ajouter** : créer une nouvelle règle de programmation.
- **Tout supprimer** : retirer toutes les règles de programmation.
- **Heure de début** : régler l'heure à laquelle la règle prend effet.
- **Heure de fin** : régler l'heure à laquelle la règle se termine.
- **Jour** : sélectionner le ou les jours auxquels la règle s'applique.
- **Importer un modèle** : appliquer un modèle de programmation personnalisé ou par défaut du système aux réglages actuels.

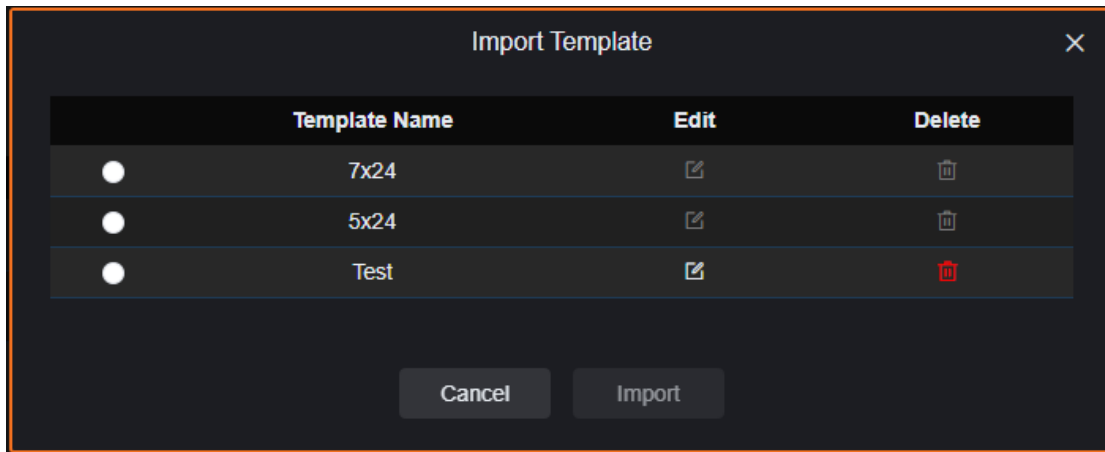


Figure 9-3. Importation d'un modèle de programmation

Les modèles vous permettent de réutiliser une programmation sur plusieurs pages et canaux. Les commandes de modèle suivantes sont disponibles :

- **Modifier** : modifier un modèle, y compris son nom et ses règles individuelles.
- **Supprimer** : retirer un modèle.

NOTE Le système fournit deux modèles intégrés, **7×24** et **5×24**. Ces modèles par défaut peuvent être modifiés mais non supprimés.

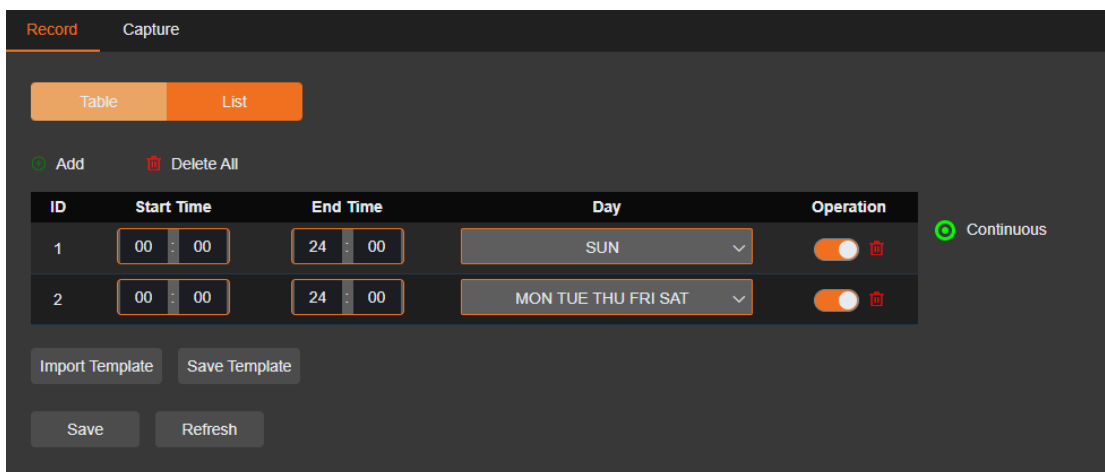


Figure 9-4. Sélection d'un modèle de programmation intégré

Utilisez **Enregistrer le modèle** pour stocker l'ensemble actuel de règles comme modèle personnalisé. Une fois enregistré, le modèle peut être importé sur d'autres pages de réglages, comme la programmation de capture.

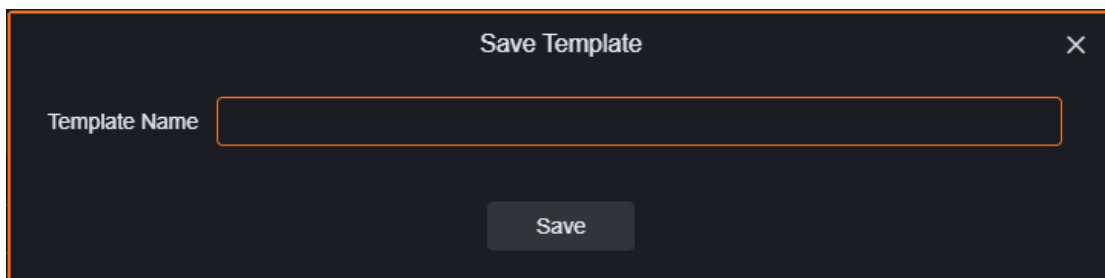


Figure 9-5. Enregistrement d'un modèle de programmation personnalisé

Lorsque la programmation est complète, utilisez les commandes suivantes pour la stocker et la distribuer :

- **Enregistrer** : enregistrer les paramètres modifiés.

- **Copier** : copier les paramètres vers un ou plusieurs autres canaux.
- **Actualiser** : recharger les paramètres actuels depuis la caméra.

9.1.2 Programmation de capture

La programmation de capture contrôle le moment où la caméra enregistre des images fixes. Configurez les périodes de capture régulière et d'alarme de sorte que la caméra n'effectue des actions de capture que durant les moments que vous définissez. La programmation de capture se configure de la même façon que la programmation d'enregistrement décrite ci-dessus, en utilisant les mêmes vues tableau et liste, les mêmes modèles et les mêmes commandes.

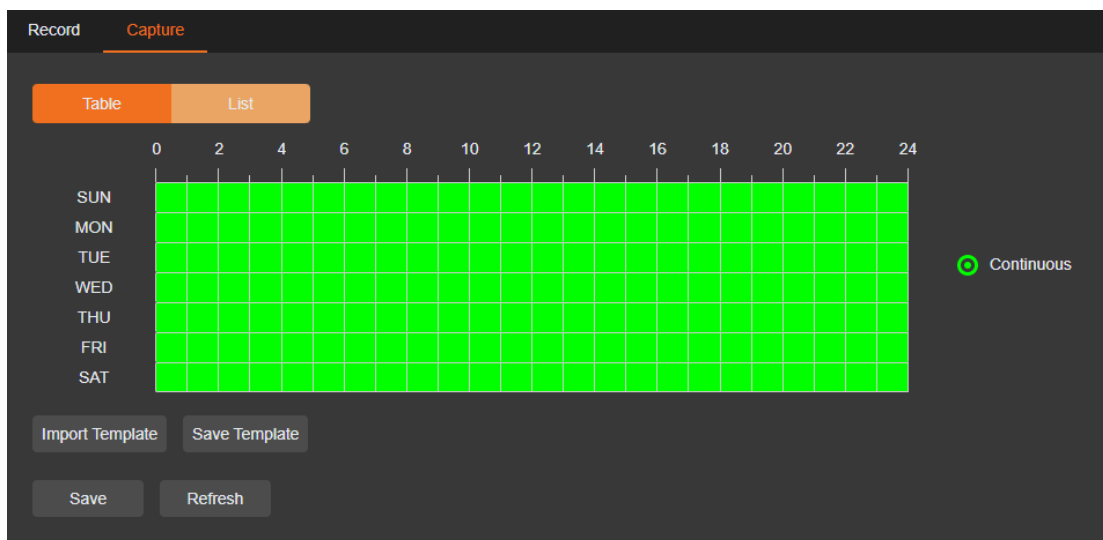


Figure 9-6. Programmation de capture en vue tableau

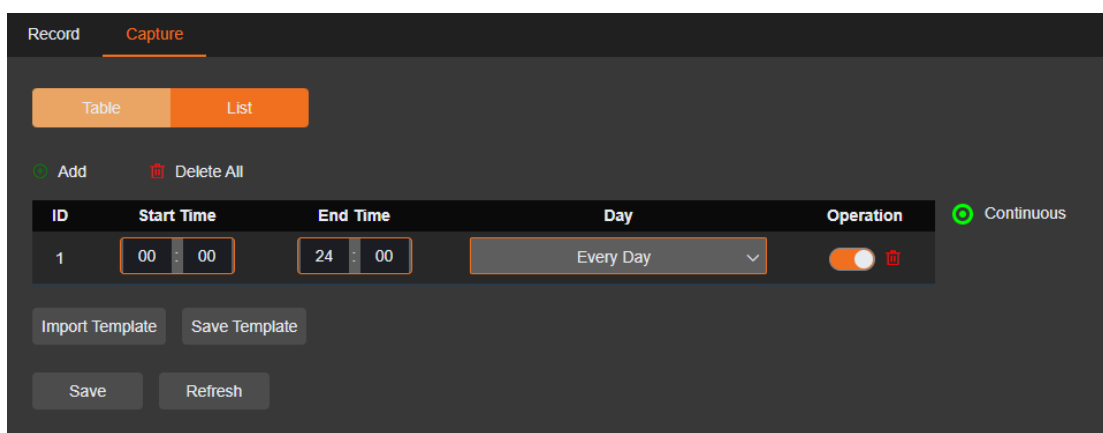


Figure 9-7. Programmation de capture en vue liste

9.2 Gestion des disques

La gestion des disques vous permet d'inspecter et de configurer le stockage qui contient la vidéo enregistrée et les images capturées, y compris la carte TF interne et un disque dur réseau optionnel.

La carte TF interne doit être formatée avant la première utilisation et de nouveau chaque fois qu'elle est remplacée par une nouvelle carte. Depuis ce menu, vous pouvez examiner l'état de la carte et la formater au besoin.

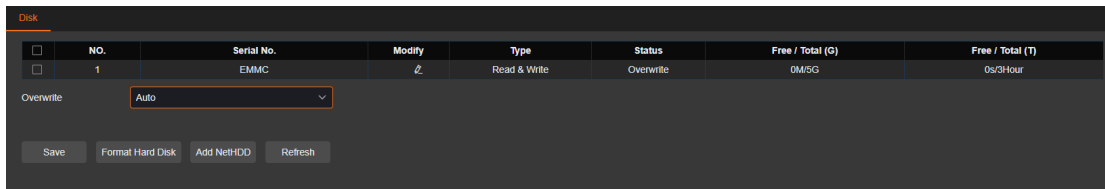


Figure 9-8. Page de gestion des disques

Sélectionnez **Formater le disque dur** pour formater la carte TF. Une fenêtre apparaît vous invitant à choisir quelle partition ou quelles partitions formater; faites votre sélection, saisissez votre nom d'utilisateur et votre mot de passe, puis confirmez pour commencer.

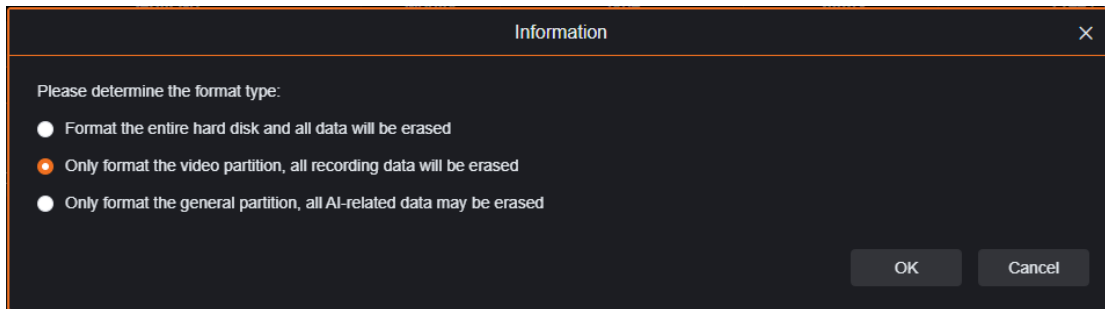


Figure 9-9. Sélection de la partition à formater

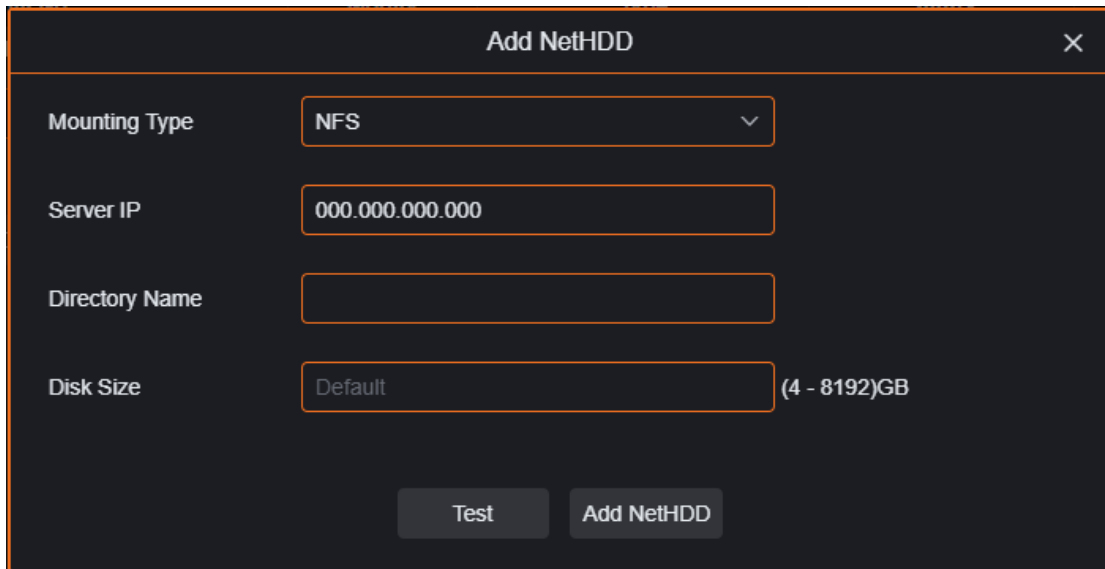
CAUTION Le formatage efface définitivement les données et ne peut être annulé. Formater le disque entier retire toutes les partitions et efface tout le contenu vidéo et de base de données, y compris la base de données de visages IA; formater seulement la partition vidéo efface toutes les données d'enregistrement. Sauvegardez tous les fichiers dont vous avez besoin avant de formater.

Les options de formatage suivantes sont disponibles :

- **Formater le disque dur et toutes les données seront effacées** : formate chaque partition, y compris la partition vidéo et la partition générale, effaçant toute la vidéo et tout le contenu de base de données.
- **Formater seulement la partition vidéo** : efface toutes les données d'enregistrement tout en laissant la partition générale intacte.
- **Formater seulement la partition générale** : formate la partition générale et efface la base de données, laissant la vidéo enregistrée intacte.

Le réglage **Écraser** contrôle ce qui se passe lorsque la carte TF devient pleine. Réglé sur **Auto**, les données les plus anciennes sont écrasées automatiquement à mesure que de l'espace est nécessaire. Réglé sur **Désactivé**, aucune vidéo existante n'est écrasée; dans ce cas, vérifiez périodiquement l'état de la carte pour vous assurer qu'elle ne se remplit pas.

Utilisez **Ajouter NetHDD** pour ajouter un disque dur réseau (NAS). Une fois qu'un NAS est configuré et connecté au réseau, la caméra peut y enregistrer la vidéo des canaux et y capturer des images. La base de données de visages IA ne peut être stockée que sur un disque dur.



The screenshot shows a dark-themed window titled "Add NetHDD". It contains the following fields and controls:

- Mounting Type:** A dropdown menu with "NFS" selected.
- Server IP:** A text input field containing "000.000.000.000".
- Directory Name:** An empty text input field.
- Disk Size:** A dropdown menu with "Default" selected, and a range "(4 - 8192)GB" displayed to its right.
- Buttons:** Two buttons at the bottom: "Test" and "Add NetHDD".

Figure 9-10. Ajout d'un disque dur réseau (NAS)

Configurez le disque dur réseau à l'aide des champs suivants :

- **Type de montage :** sélectionner le protocole, soit **NFS** ou **SMB/CIFS**. NFS ne nécessite pas de nom d'utilisateur ni de mot de passe; SMB/CIFS en nécessite.
- **Nom d'utilisateur :** le nom d'utilisateur du NAS (non utilisé en mode NFS).
- **Mot de passe :** le mot de passe du NAS (non utilisé en mode NFS).
- **IP du serveur :** l'adresse IP du NAS.
- **Nom du répertoire :** le dossier du NAS dans lequel les données sont stockées.
- **Taille du disque :** la taille du disque dur réseau.
- **Test :** vérifier la connectivité au NAS.
- **Ajouter NetHDD :** ajouter le NAS à la caméra.

9.3 Réglages du serveur FTP

Activez la fonction FTP pour téléverser des images et des vidéos depuis la caméra vers un serveur FTP, où elles peuvent être visualisées et archivées.

Figure 9-11. Page des réglages du serveur FTP

Configurez les téléversements FTP à l'aide des champs suivants :

- **Activation FTP** : activer la fonction FTP.
- **Protocole FTP** : sélectionner le protocole de transfert, soit **FTP** ou **SFTP**.
- **Serveur** : saisir l'adresse IP ou le nom de domaine de votre serveur FTP.
- **Port** : saisir le port FTP.
- **Nom d'utilisateur / Mot de passe** : saisir les identifiants de votre serveur FTP.
- **Transférer les images** : téléverser les images d'alarme vers le serveur FTP.
- **Transférer les vidéos** : téléverser la vidéo d'alarme vers le serveur FTP.

TIP Utilisez **SFTP** lorsque votre serveur le prend en charge. SFTP chiffre la connexion, protégeant vos identifiants et vos médias téléversés durant le transit.

Chapitre 10 Alarmes, I/O et dissuasion

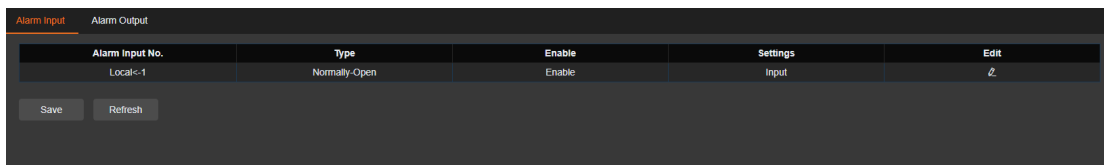
La caméra de contrôle d'accès OCTAVUE associe ses bornes d'alarme physiques à une sirène de dissuasion intégrée et à une programmation de désarmement configurable. Ce chapitre explique comment câbler et configurer les entrées d'alarme I/O, définir les réponses de liaison, régler la sirène intégrée et suspendre temporairement les actions d'alarme grâce à la fonction de désarmement.

10.1 Paramètres I/O

Le menu I/O configure les bornes d'alarme physiques de la caméra. Un détecteur externe connecté à l'entrée d'alarme peut déclencher un ensemble coordonné de réponses, tandis que le relais de sortie d'alarme peut piloter un appareil externe tel qu'un stroboscope, une serrure ou une sirène auxiliaire.

10.1.1 Paramètres d'entrée d'alarme

Cliquez sur **Paramètres** → **Événement** → **Paramètres I/O** et ouvrez l'onglet **Entrée d'alarme**. La liste affiche chaque canal d'entrée disponible ainsi que son type d'alarme et son état d'activation.

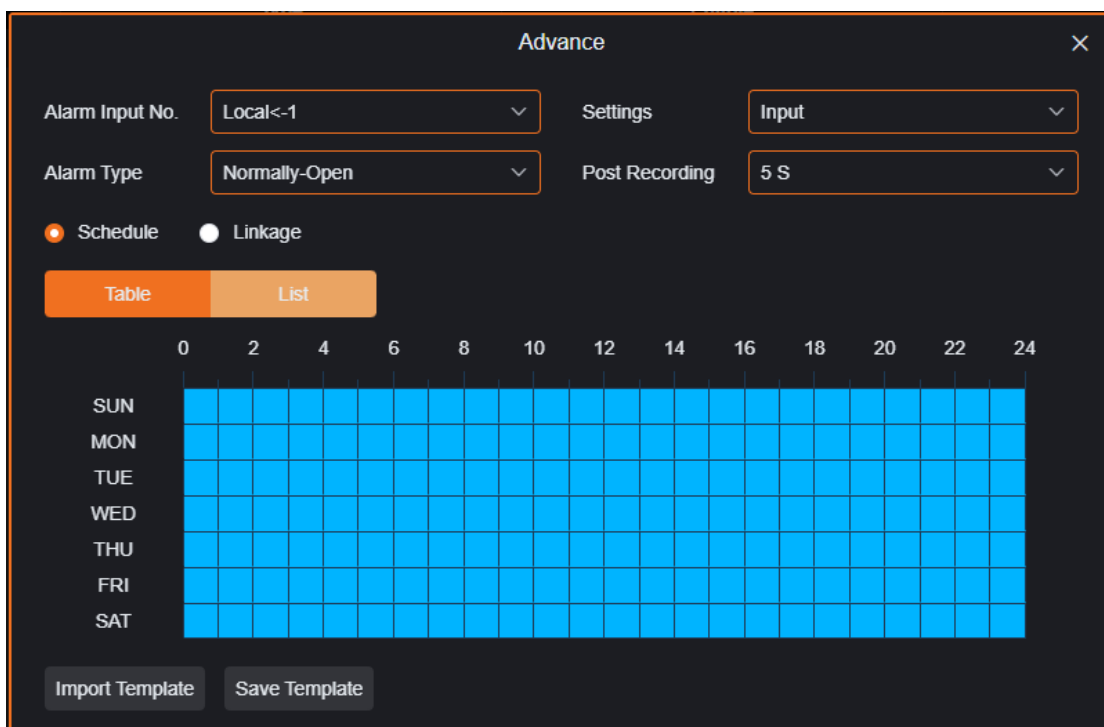


Alarm Input No.	Type	Enable	Settings	Edit
Local<-1	Normally-Open	Enable	Input	

Save Refresh

Figure 10-1. Liste des canaux d'entrée d'alarme

Cliquez sur l'icône **Modifier** dans la ligne du canal que vous voulez modifier pour ouvrir la boîte de dialogue de configuration **Avancé**, puis réglez les paramètres suivants.



Advance

Alarm Input No. Local<-1 Settings Input

Alarm Type Normally-Open Post Recording 5 S

☒ Schedule ☐ Linkage

Table List

	0	2	4	6	8	10	12	14	16	18	20	22	24
SUN													
MON													
TUE													
WED													
THU													
FRI													
SAT													

Import Template Save Template

Figure 10-2. Paramètres d'entrée d'alarme et programmation effective

- **N° d'entrée d'alarme** — Sélectionnez la source d'entrée de l'alarme I/O.
- **Paramètres** — Activez ou désactivez la fonction d'entrée d'alarme I/O pour le canal sélectionné.
- **Type d'alarme** — Sélectionnez le type de contact d'entrée correspondant au détecteur connecté : Normalement ouvert ou Normalement fermé.
- **Post-enregistrement** — Poursuit l'enregistrement pendant l'intervalle défini après que la condition de déclenchement disparaît. La valeur par défaut est de 5 secondes.
- **Programmation** — Définissez la période d'armement pendant laquelle l'alarme d'entrée I/O est active. Consultez la section Paramètres de programmation pour plus de détails sur la modification de la grille horaire hebdomadaire.

10.1.1.1 Liaison d'alarme

Sélectionnez l'option **Liaison** dans la boîte de dialogue **Avancé** pour définir les actions que la caméra effectue lorsque cette entrée est déclenchée.

The screenshot shows the 'Advance' dialog box with a dark theme. At the top, there's a title bar 'Advance' with a close button. Below it, there are four dropdown menus: 'Alarm Input No.' set to 'Local<-1', 'Settings' set to 'Input', 'Alarm Type' set to 'Normally-Open', and 'Post Recording' set to '5 S'. Below these are two radio buttons: 'Schedule' (unselected) and 'Linkage' (selected). The main area is divided into two columns. The left column is titled 'Normal Linkage' and contains a list of options: 'Email' (checkbox), 'FTP Picture Upload' (checkbox), 'FTP Video Upload' (checkbox), 'Event Push Platform' (checkbox with a checkmark), 'Record Channel' (checkbox with a checkmark), and 'Siren' (checkbox). The right column is titled 'Alarm Output' and contains one option: 'Local->1' (checkbox).

Figure 10-3. Actions de liaison d'entrée d'alarme

- **Courriel** — Envoie un courriel de notification à la boîte de courriel configurée lorsque l'alarme est déclenchée.
- **Téléversement d'image FTP** — Téléverse une capture de l'événement d'alarme vers le serveur FTP.
- **Téléversement vidéo FTP** — Téléverse un clip vidéo de l'événement d'alarme vers le serveur FTP.
- **Sirène** — Fait retentir la sirène intégrée à des fins de dissuasion lorsque l'alarme est déclenchée.

NOTE Les liaisons Courriel et FTP n'agissent qu'après la configuration des serveurs Courriel et FTP correspondants dans les menus réseau. Utilisez le bouton **Paramètres** à côté des options FTP pour confirmer quel serveur reçoit les images et la vidéo téléversées.

10.2 Paramètres de la sirène

Sur les modèles équipés d'une sirène, ce menu configure le dissuasif sonore qui retentit lorsqu'une liaison d'alarme le requiert. Une fois déclenchée, la sirène s'active automatiquement pour dissuader les intrus.

Figure 10-4. Page de configuration de la sirène

- **Sirène** — Active ou désactive la sirène.
- **Type de sirène** — Sélectionnez le fichier audio que la sirène joue. Deux tonalités intégrées sont fournies.
- **Volume de la sirène** — Réglez le niveau de sortie, ajustable de 1 à 10.
- **Durée de la sirène(s)** — Réglez la durée pendant laquelle la sirène retentit par déclenchement, ajustable de 5 à 180 secondes.
- **Programmation** — Définissez la période pendant laquelle la sirène est autorisée à retentir. Consultez la section Paramètres de programmation.

TIP En plus des tonalités intégrées, certains modèles prennent en charge l'importation d'un maximum de trois fichiers de sirène personnalisés au format PCM ou WAV. Chaque fichier importé doit utiliser une fréquence d'échantillonnage ne dépassant pas 8000 Hz et ne doit pas dépasser 256 KB. Pour supprimer une tonalité personnalisée, sélectionnez-la et cliquez sur le bouton **Supprimer** à côté d'elle.

10.3 Désarmement

Le désarmement suspend temporairement la réponse de la caméra aux liaisons d'alarme, ce qui est utile pendant la maintenance ou une activité autorisée qui déclencherait autrement des alertes. Ce menu définit le commutateur de désarmement, les types de liaison à supprimer et la programmation pendant laquelle la suppression s'applique.

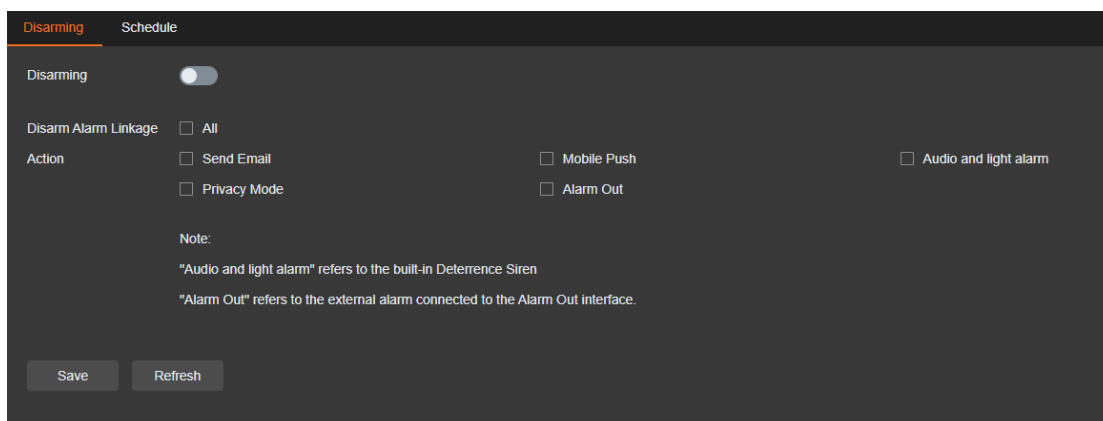


Figure 10-5. Page de configuration du désarmement

- **Désarmement** — Active ou désactive la fonction de désarmement.
- **Action** — Sélectionnez les réponses de liaison d'alarme locales qui sont supprimées lorsque le désarmement est actif. Utilisez **Tout** pour sélectionner ou effacer chaque type d'un seul coup.
- **Envoyer un courriel** — Lorsque cette option est sélectionnée, les alarmes déclenchées n'envoient pas de courriels de notification.
- **Notification poussée mobile** — Lorsque cette option est sélectionnée, la caméra n'envoie pas de messages d'alarme aux applications mobiles RXCam View et CybVu.
- **Alarme sonore et lumineuse** — Lorsque cette option est sélectionnée, la sirène de dissuasion intégrée ne répond pas aux alarmes déclenchées.
- **Sortie d'alarme** — Lorsque cette option est sélectionnée, l'appareil externe connecté à l'interface de sortie d'alarme ne répond pas aux alarmes déclenchées.
- **Mode confidentialité** — Lorsque cette option est sélectionnée, l'unité visuelle de contrôle d'accès entre en mode confidentialité une fois le commutateur de désarmement en un clic activé.
- **Programmation** — Définissez la période pendant laquelle le désarmement est en vigueur. Consultez la section Paramètres de programmation.

CAUTION Lorsque le désarmement est actif, les liaisons d'alarme sélectionnées sont entièrement supprimées et la caméra ne vous informera pas des événements qu'elles signaleraient normalement. Assurez-vous que le désarmement est désactivé, ou que sa programmation est terminée, avant de compter sur la caméra pour la surveillance de sécurité.

Chapitre 11 Événements et détection IA

La caméra de contrôle d'accès OCTAVUE utilise des alarmes intelligentes basées sur l'IA pour reconnaître les visages, les piétons et les mouvements dans la scène surveillée et pour déclencher les réponses liées que vous configurez. Chaque type de détection doit d'abord être activé depuis les réglages **Événement** avant que ses alarmes ne prennent effet.

Chaque fonction de détection IA consomme de la puissance de traitement de la caméra. Comme la performance sur l'appareil est limitée, certaines fonctions IA ne peuvent pas fonctionner en même temps. Les combinaisons disponibles sur un appareil donné dépendent du modèle; suivez toujours les invites à l'écran et les spécifications de votre modèle de caméra précis.

NOTE Activer des fonctions IA supplémentaires augmente la charge de traitement de la caméra. Si une fonction ne peut être activée en même temps qu'une autre, l'interface indique quels types de détection sont mutuellement exclusifs sur votre modèle.

11.1 Détection de visage

La détection de visage localise d'abord une cible de visage dans le champ de la caméra et capture une image qui répond aux exigences configurées. L'algorithme du modèle de visage calcule ensuite les données de caractéristiques faciales à partir de l'image capturée et les compare à la base de données de visages pour déclencher une alarme. La fonction de détection de visage doit être activée avant qu'aucune de ces étapes ne puisse se produire.

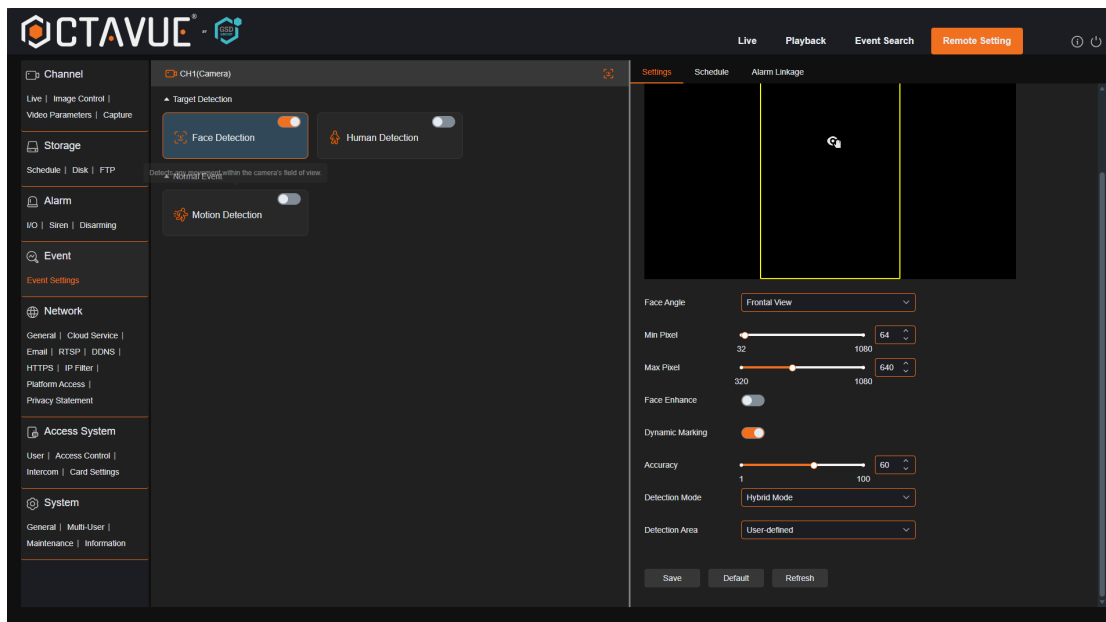


Figure 11-1. Réglages de détection de visage

Configurez les paramètres suivants pour contrôler la façon dont les visages sont capturés, filtrés et détectés :

- **Détection de visage** — Active ou désactive la fonction de détection de visage.
- **Angle du visage** — Filtre les images capturées de sorte que seules les images correspondant au réglage d'angle sélectionné soient poussées. Trois modes sont disponibles.
- **Vue frontale** — Pousse uniquement les vues frontales du sujet.
- **Multi-angle** — Pousse les images qui contiennent des visages de côté (profil).
- **Personnalisé** — Personnalise la plage d'angles pour lesquels les images peuvent être poussées. Une fois activé, les options **Plage de roulis**, **Plage de tangage**, **Plage de lacet** et **Qualité d'image**, ainsi que les boutons **Défaut frontal** et **Défaut multi**, deviennent disponibles.
- **Plage de roulis** — Règle le roulis permis du visage capturé dans le modèle 3D. Lorsque l'angle dépasse la limite, la détection de visage a tout de même lieu mais l'image n'est pas poussée.
- **Plage de tangage** — Règle le tangage permis du visage capturé dans le modèle 3D. Lorsque l'angle dépasse la limite, la détection de visage a tout de même lieu mais l'image n'est pas poussée.
- **Plage de lacet** — Règle le lacet permis du visage capturé dans le modèle 3D. Lorsque l'angle dépasse la limite, la détection de visage a tout de même lieu mais l'image n'est pas poussée.
- **Qualité d'image** — Règle la qualité d'image minimale. Une qualité plus élevée aide à filtrer les images détectées qui ne sont pas des visages utilisables.
- **Défaut frontal** — Lorsque le mode d'application est réglé sur **Personnalisé**, applique les valeurs par défaut de capture frontale : Plage de roulis 30, Plage de tangage 30, Plage de lacet 45 et Qualité d'image 100.
- **Défaut multi** — Lorsque le mode d'application est réglé sur **Personnalisé**, applique les valeurs par défaut de capture multi-angle : Plage de roulis 180, Plage de tangage 180, Plage de lacet 180 et Qualité d'image 100.
- **Pixels min** — Règle le cadre de pixels de reconnaissance minimal; un visage doit être plus grand que cette valeur pour être reconnu. Le survol du curseur affiche le cadre de pixels réel dans l'aperçu à droite, et glisser

le cadre ajuste directement la valeur. Le cadre disparaît de l'aperçu cinq secondes après que la souris s'en éloigne.

- **Pixels max** — Règle le cadre de pixels de reconnaissance maximal; un visage doit être plus petit que cette valeur pour être reconnu. Le survol du curseur affiche le cadre de pixels réel dans l'aperçu à droite, et glisser le cadre ajuste directement la valeur. Le cadre disparaît de l'aperçu cinq secondes après que la souris s'en éloigne.
- **Amélioration du visage** — Améliore la capture des cibles en mouvement et ajuste la luminosité selon le visage le plus proche de la caméra pour optimiser le résultat de capture (pris en charge par certains modèles).
- **Cadre englobant** — Affiche le cadre de détection de visage et la ligne de règle de détection (pris en charge par certains modèles).
- **Sensibilité** — Une sensibilité plus élevée réduit les alarmes manquées mais augmente la probabilité de fausses alarmes.
- **Mode de détection** — Filtre les objets que la caméra évalue. Deux modes sont disponibles.
- **Toujours** — Effectue la détection de visage sur tous les objets du champ.
- **Mouvement seulement** — Filtre les visages immobiles, comme les portraits et les statues dans la scène.
- **Zone de détection** — Définit la zone utilisée pour reconnaître les objets. Deux modes sont disponibles.
- **Plein écran** — Détecte sur toute la zone que la caméra peut surveiller.
- **Personnalisé** — Détecte uniquement dans les zones que vous délimitez manuellement.

11.2 Détection de piéton

La détection de piéton identifie la forme humaine dans la scène selon vos réglages, déclenche une alarme et enregistre la capture correspondante.

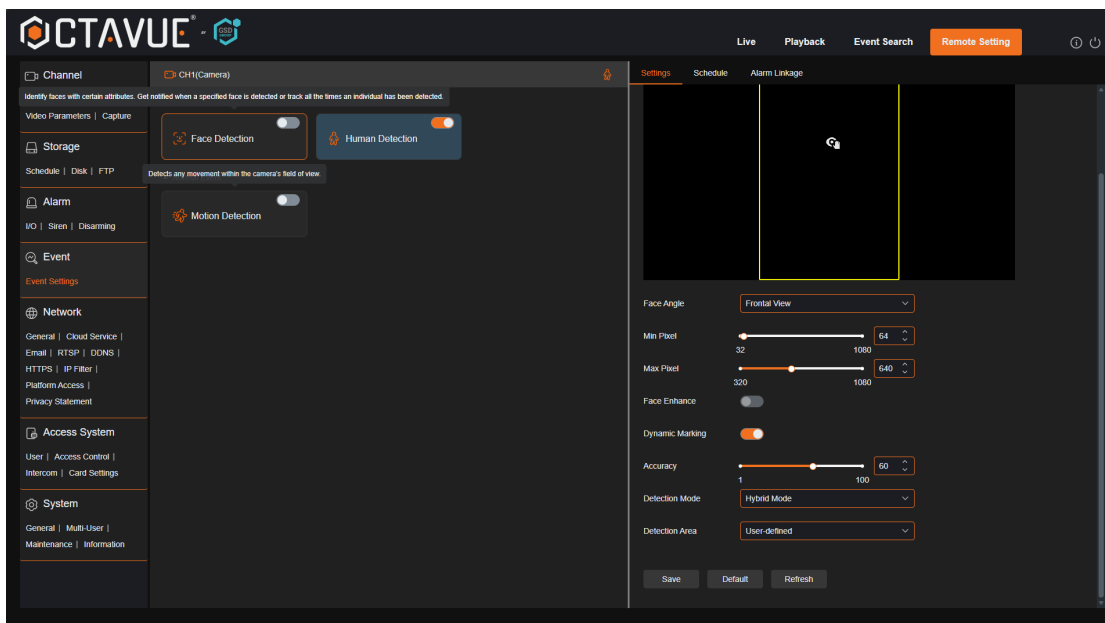


Figure 11-2. Réglages de détection de piéton

- **Activer** — Active ou désactive la détection de forme piétonne.
- **Mode de capture** — Règle le comportement d'instantané. Les images capturées peuvent être reçues comme notifications poussées en vue en direct ou examinées via un NVR connecté. Trois modes de capture sont pris en charge.
- **Défaut** — La caméra pousse une seule image du piéton ou du véhicule détecté, du moment où l'objet est détecté jusqu'à sa disparition.

- **Mode temps réel** — En détectant un objet, la caméra pousse immédiatement une image, puis pousse une autre image lorsque l'objet disparaît.
- **Mode intervalle** — Pousse les images un nombre défini de fois selon l'intervalle configuré. Ce mode expose les réglages **Qté d'instantanés** et **Intervalle de capture**.
- **Qté d'instantanés** — Règle le nombre de fois qu'une image est poussée pour ce que la caméra considère comme la même cible : 1, 2, 3 ou illimité, à l'intervalle défini par **Intervalle de capture**.
- **Intervalle de capture** — Règle le temps entre les poussées, mesuré depuis l'apparition de la cible ou depuis la poussée précédente.
- **Pixel min** — Règle le cadre de pixels de reconnaissance minimal; le piéton ou le véhicule doit être plus grand que cette valeur pour être reconnu. Le survol du curseur affiche le cadre de pixels réel dans l'aperçu à droite, et glisser le cadre ajuste directement la valeur. Le cadre disparaît de l'aperçu cinq secondes après que la souris s'en éloigne.
- **Pixel max** — Règle le cadre de pixels de reconnaissance maximal; le piéton ou le véhicule doit être plus petit que cette valeur pour être reconnu. Le survol du curseur affiche le cadre de pixels réel dans l'aperçu à droite, et glisser le cadre ajuste directement la valeur. Le cadre disparaît de l'aperçu cinq secondes après que la souris s'en éloigne.
- **Cadre englobant** — Affiche le cadre de détection du piéton ou du véhicule et la ligne de règle de détection.
- **Zone de détection** — Définit la zone de détection. Deux modes sont disponibles.
- **Plein écran** — Détecte sur toute la zone que la caméra peut surveiller.
- **Personnalisé** — Détecte uniquement dans la zone que vous délimitez manuellement.
- **Sensibilité** — Une sensibilité plus élevée rend les objets piétons ou véhicules plus faciles à détecter mais peut générer plus de fausses alarmes.
- **Mode de détection** — Filtre le comportement des objets dans la zone de détection. Deux modes sont disponibles.
- **Toujours** — Détecte tous les piétons dans le champ.
- **Mouvement seulement** — Filtre les piétons immobiles.

11.3 Détection de mouvement

Sur cette page, vous configurez les paramètres de détection de mouvement. Lorsque la caméra détecte le mouvement d'une cible dans l'image, elle déclenche une série de réponses d'alarme.

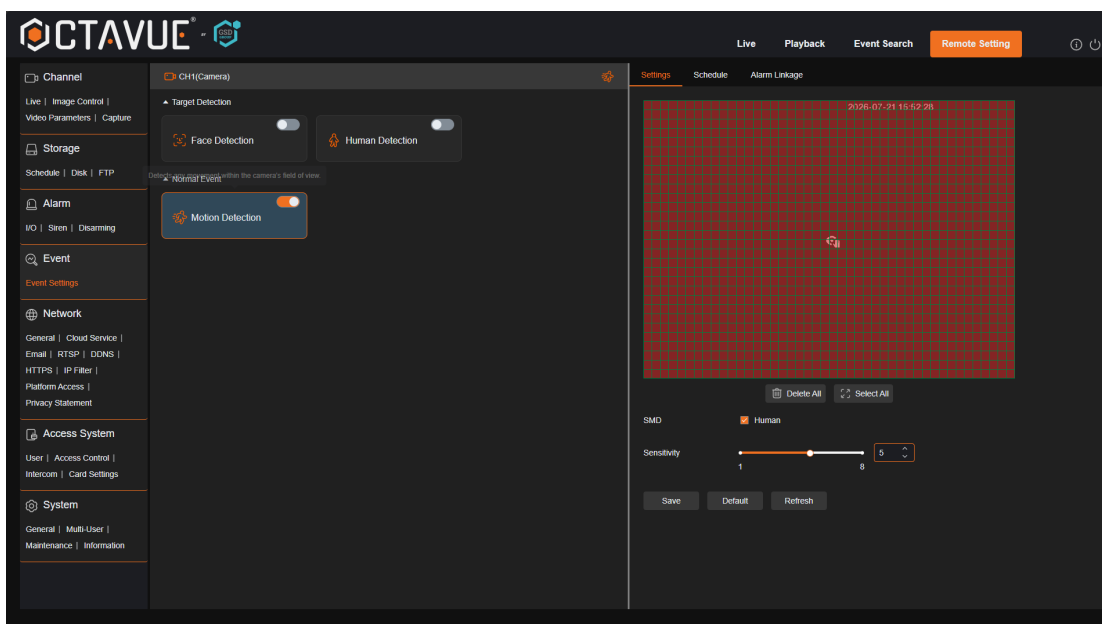


Figure 11-3. Réglages de détection de mouvement

Par exemple, une alarme de mouvement déclenchée peut envoyer un courriel à une adresse spécifiée par l'utilisateur avec une image de la caméra en pièce jointe (lorsque cette option est activée), ou livrer une notification poussée via l'application mobile.

Glissez le bouton gauche de la souris sur la fenêtre de droite pour définir la zone de détection. Seul le mouvement dans cette zone déclenche une alarme.

- **Détection de mouvement** — Active ou désactive la détection de mouvement.
- **SMD** — Configure les cibles de détection pour la détection de mouvement.
- **Piéton** — Détecte et alerte uniquement pour les cibles de forme humaine.
- **Sensibilité** — Ajuste la sensibilité de détection de mouvement; des valeurs plus élevées augmentent la sensibilité.

11.4 Réglages de liaison d'alarme

La liaison d'alarme définit les actions que la caméra exécute lorsqu'un événement déclenche une alarme. Configurez chaque liaison de sorte que les réponses appropriées s'exécutent automatiquement.

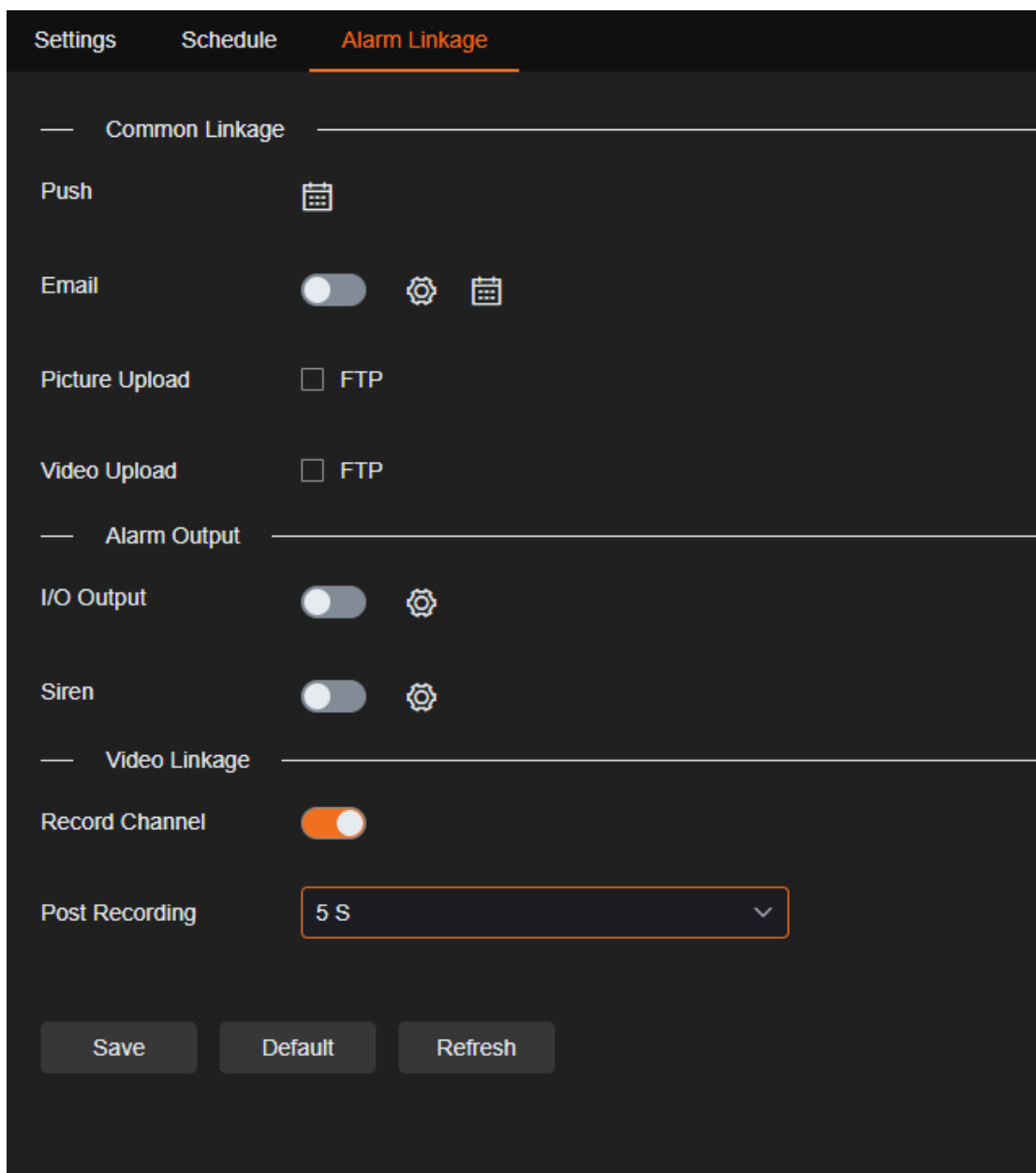


Figure 11-4. Réglages de liaison d'alarme

- **Plateforme de poussée d'événement** — Pousse les événements vers des plateformes de services tierces après qu'une alarme E/S se produit. Cette option est sélectionnée par défaut.
- **Courriel** — Détermine si la caméra envoie un courriel lorsqu'une alarme d'événement est déclenchée. Cliquez sur **Configurer** ou **Programmation** à droite pour configurer les paramètres de courriel.
- **Téléversement d'image** — Lorsque **FTP** est sélectionné, la caméra envoie une image au serveur FTP associé lorsqu'une alarme d'événement est déclenchée. Le serveur FTP doit d'abord être associé; reportez-vous à la section Réglages du serveur FTP. Cliquez sur **Configurer** à droite pour sélectionner quelles images d'alarme de canal sont téléversées vers le serveur FTP.
- **Téléversement de vidéo** — Lorsque **FTP** est sélectionné, la caméra envoie une vidéo au serveur FTP associé lorsqu'une alarme d'événement est déclenchée. Le serveur FTP doit d'abord être associé à la caméra. Cliquez sur **Configurer** à droite pour sélectionner quel canal est téléversé vers le serveur FTP.
- **Sirène** — Un interrupteur de dissuasion. Lorsqu'une alarme est déclenchée, la caméra répond selon les paramètres de la page de réglages de dissuasion par sirène. Cliquez sur **Configurer** à droite pour régler ces paramètres directement.

- **Canal d'enregistrement** — Un interrupteur de liaison de canal d'enregistrement. Cliquez sur **Configurer** à droite pour sélectionner les canaux liés. Lorsqu'une alarme est déclenchée, les canaux sélectionnés enregistrent le type d'alarme correspondant.
- **Délai d'enregistrement** — La durée pendant laquelle la caméra continue d'enregistrer après la fin de l'alarme.

11.4.1 Poussée d'alarme personnalisée (Notification)

La poussée d'alarme personnalisée livre les informations d'alarme du côté de l'appareil à un ou plusieurs serveurs spécifiés. Cette fonction exige que chaque serveur ait terminé l'intégration et le débogage avec la caméra.



Figure 11-5. Liaison d'alarme avec notification personnalisée

Pour configurer la poussée d'alarme personnalisée du côté de l'appareil, cliquez sur **Notification** (réglages de poussée d'alarme personnalisée) pour ouvrir la page de réglages.

Figure 11-6. Réglages de poussée d'alarme personnalisée

- **URL de notification** — Sélectionne le serveur cible. Jusqu'à trois serveurs sont pris en charge, qui peuvent être identiques ou différents.
- **Activer** — Active la poussée du serveur sélectionné.
- **Protocole** — Règle le mode de protocole. HTTP et HTTPS sont pris en charge pour pousser les informations d'alarme vers le serveur.

- **Intervalle de déclenchement** — L'intervalle de poussée, de 0 à 900 s; la valeur par défaut est 30 s.
- **Méthode** — La méthode de poussée. POST et GET sont pris en charge; la méthode POST prend en charge la poussée d'une image.
- **URL** — L'URL de poussée personnalisée.
- **Authentification** — Lorsqu'elle est désactivée, aucune authentification n'est requise pour accepter les notifications poussées.
- **Nom d'utilisateur** — Le nom d'utilisateur d'authentification du serveur.
- **Mot de passe** — Le mot de passe d'authentification du serveur.

CAUTION Envoyez les notifications d'alarme uniquement à des serveurs que vous contrôlez et en qui vous avez confiance. Lorsque vous utilisez le protocole HTTP ou désactivez l'authentification, les données d'alarme et les identifiants sont transmis sans protection; utilisez HTTPS avec l'authentification activée dans la mesure du possible.

Chapitre 12 Réseau et services

Ce chapitre décrit la configuration réseau et les options de services connectés offertes sur la caméra de contrôle d'accès OCTAVUE. À partir de ces menus, vous définissez la façon dont la caméra obtient son adresse, les protocoles et les ports qu'elle utilise, ainsi que la manière dont elle rejoint les plateformes infonuagiques, de courriel, de diffusion et de gestion tierces.

12.1 Paramètres réseau

Le menu Paramètres réseau est l'endroit où vous configurez les paramètres réseau principaux de la caméra, notamment la méthode d'adressage (DHCP ou statique), la connexion PPPoE et le SNMP. Pour la plupart des installations, le DHCP est l'option recommandée et la plus courante; n'utilisez une adresse IP statique que lorsque votre déploiement exige un adressage fixe. Si votre connexion Internet nécessite un nom d'utilisateur et un mot de passe d'authentification, sélectionnez PPPoE.

12.1.1 Paramètres généraux

Ouvrez **Paramètres** → **Réseau** → **Général** pour configurer l'adressage IP de la caméra. Si la caméra est connectée à un routeur qui prend en charge le DHCP, activez l'option **DHCP** et le routeur attribuera automatiquement tous les paramètres réseau à l'appareil. Désactivez le DHCP pour saisir les paramètres manuellement.

General PPPoE SNMP IEEE802.1X Port Configuration

DHCP ☐

IP Address

Subnet Mask

Gateway

IPv6 DHCP ☐

IPv6 Address

Subnet Prefix Length (1 ~ 128)

IPv6 Gateway

DNS 1

DNS 2

IPv6 DNS 1

IPv6 DNS 2

Multicast

Multicast ☒

Multicast Address (224.0.0.0~239.255.255.255)

Stream Encryption

Audio-Video Encrypted Transmission ☒

Intercom Encrypted Transmission ☒

Figure 12-1. Paramètres réseau généraux

Lorsque l'adressage est configuré manuellement, réglez les paramètres suivants :

- **Adresse IP** — l'identifiant de la caméra sur le réseau. Elle est composée de quatre nombres compris entre 0 et 255 séparés par des points, par exemple « 192.168.001.100 ».
- **Masque de sous-réseau** — un paramètre réseau qui définit la plage d'adresses IP pouvant être utilisées sur le réseau. Si l'adresse IP est comparée à la rue où vous habitez, le masque de sous-réseau représente le quartier environnant. Il est lui aussi composé de quatre nombres séparés par des points, par exemple « 255.255.000.000 ».
- **Passerelle** — l'adresse qui permet à la caméra de rejoindre d'autres réseaux. Son format est le même que celui d'une adresse IP, par exemple « 192.168.001.100 ».

- **Adresse IPv6** — l'identifiant IPv6 de la caméra sur le réseau. Il est composé de huit groupes de valeurs hexadécimales comprises entre 0 et FFFF, séparés par des deux-points, par exemple « ABCD:EF01:2345:6789:ABCD:EF01:2345:6789 ».
- **DNS1 / DNS2** — DNS1 est le serveur DNS actif et DNS2 est le serveur DNS de secours. Dans la plupart des cas, seule l'adresse DNS1 doit être saisie.
- **Multidiffusion** — lorsque cette option est activée, le flux principal peut être livré par multidiffusion.
- **Adresse de multidiffusion** — précise l'adresse de multidiffusion. Un lecteur tiers peut demander un flux multimédia en multidiffusion à la caméra au moyen du protocole RTSP.
- **Transmission audio-vidéo chiffrée** — active la transmission chiffrée des flux audio et vidéo.



Figure 12-2. Paramètres d'adresse IP manuelle

La caméra peut détecter les adresses IP en double au sein du même segment réseau. Si l'adresse que vous appliquez est déjà utilisée, un message d'avertissement s'affiche afin que vous puissiez attribuer une adresse différente avant l'enregistrement.

Figure 12-3. Message d'avertissement d'adresse IP en double

12.1.2 PPPoE

La caméra prend en charge la connexion réseau commutée au moyen du PPPoE. Ouvrez **Paramètres** → **Réseau** → **PPPoE** pour la configurer.

Figure 12-4. Paramètres PPPoE

1. Cochez la case **Activer PPPoE**.
2. Saisissez le nom d'utilisateur et le mot de passe PPPoE fournis par votre fournisseur de services.
3. Cliquez sur **Enregistrer** pour appliquer les paramètres.

NOTE Une fois les paramètres PPPoE enregistrés, la caméra redémarre pour activer la connexion.

12.1.3 SNMP

Le protocole SNMP (Simple Network Management Protocol) permet la surveillance à distance de la caméra sur le réseau. Ouvrez **Paramètres** → **Réseau** → **SNMP** pour configurer les paramètres suivants.

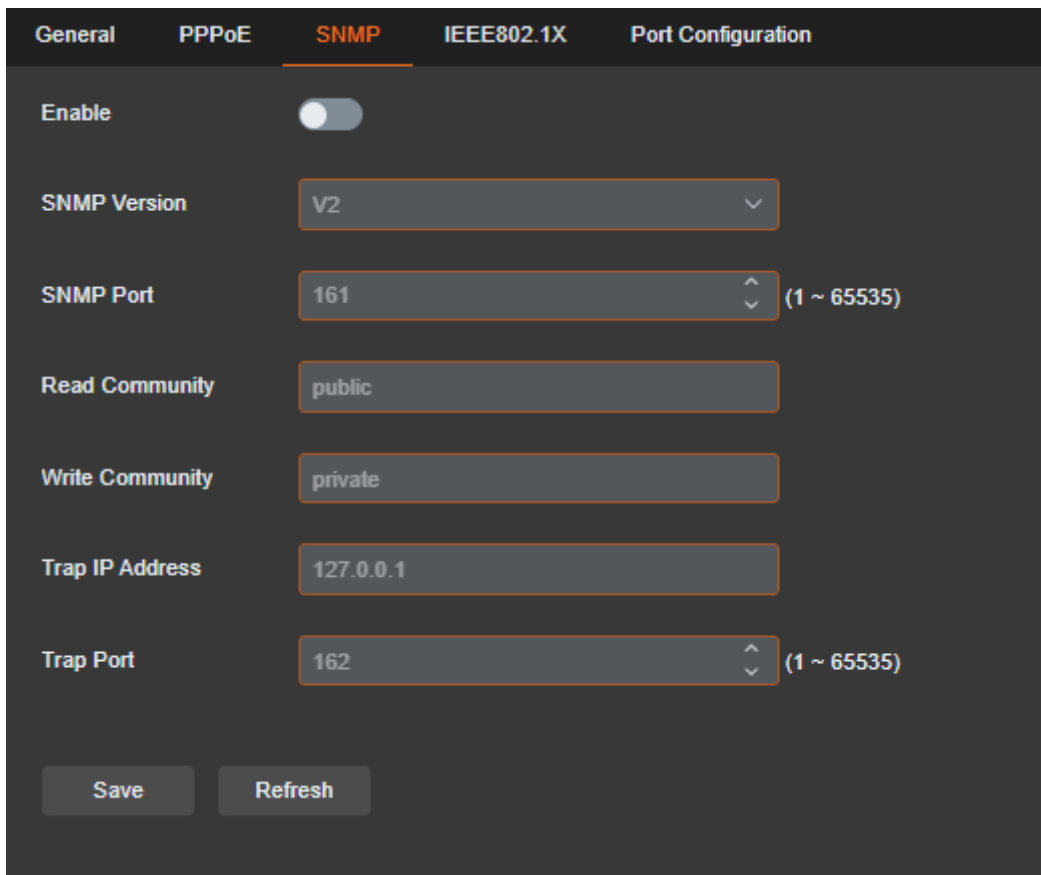


Figure 12-5. Paramètres SNMP

- **Activer** — active ou désactive le SNMP.
- **Version SNMP** — définit la version du serveur SNMP. Les versions V1, V2 et V3 sont offertes.
- **Port SNMP** — définit le port utilisé par le serveur SNMP.
- **Communauté de lecture** — définit la chaîne de communauté de lecture du serveur SNMP.
- **Communauté d'écriture** — définit la chaîne de communauté d'écriture du serveur SNMP.
- **Adresse IP des interruptions** — définit l'adresse IP de destination des interruptions SNMP.
- **Port des interruptions** — définit le port de destination des interruptions SNMP.

12.1.4 IEEE 802.1X

IEEE 802.1X est un protocole de contrôle d'accès réseau basé sur les ports, utilisé principalement dans les environnements de réseau local pour renforcer la sécurité du réseau en vérifiant l'identité des utilisateurs et en contrôlant les autorisations d'accès au niveau du port. Un appareil réseau connecté à un port de commutateur ne peut accéder aux ressources du réseau local qu'après avoir réussi l'authentification; si l'authentification échoue, l'accès à ces ressources est refusé.

Figure 12-6. Paramètres IEEE 802.1X

- **Activer IEEE 802.1X** — active ou désactive l'authentification IEEE 802.1X.
- **Méthode d'authentification** — définit le mode d'authentification IEEE 802.1X.
- **Version EAPOL** — sélectionne la version du protocole EAPOL.
- **Nom d'utilisateur** — définit le nom d'utilisateur de l'authentification IEEE 802.1X.
- **Mot de passe** — définit le mot de passe de l'authentification IEEE 802.1X.
- **Certificat CA** — importe le certificat CA.
- **Certificat client** — importe le certificat client.
- **Clé privée client** — importe la clé privée du client.
- **Mot de passe de la clé privée client** — saisit le mot de passe de la clé privée du client.
- **Installer** — le bouton d'importation. Après avoir sélectionné un fichier de certificat ou de clé, cliquez sur ce bouton pour l'enregistrer sur la caméra.

12.1.5 Paramètres des ports

Ouvrez **Paramètres** → **Réseau** → **Port** pour configurer les ports de protocole et les services réseau connexes.

Server	Internal Port	External Port	Protocol	UPnP Status	Mapping Strategy	UPnP
HTTP Port	80	80	TCP	Inactive	Auto	☐
HTTPS Port	443	443	TCP	Inactive	Auto	☐
RTSP Port	554	554	TCP	Inactive	Auto	☐

Multicast Port: 10000 (1024-65535)

P2P Switch: ☒

Auto Redirect to HTTPS: ☐

Figure 12-7. Paramètres des ports

- **Port HTTP** — le port utilisé pour accéder à la caméra à partir d'un navigateur Web au moyen du protocole HTTP. Valeur par défaut : 80.
- **Port HTTPS** — le port utilisé pour accéder à la caméra à partir d'un navigateur Web au moyen du protocole HTTPS. Valeur par défaut : 443.
- **Port RTSP** — le port utilisé pour accéder à la caméra au moyen du protocole RTSP. Valeur par défaut : 554.
- **UPnP** — pour vous connecter à distance à la caméra avec le client Web, la redirection de ports doit être configurée sur le routeur. Si votre routeur prend en charge l'UPnP, activez cette option et les ports requis

sont mappés automatiquement; vous n'avez pas besoin de configurer la redirection de ports manuellement. Si votre routeur ne prend pas en charge l'UPnP, configurez la redirection de ports manuellement.

- **Port de multidiffusion** — définit le port de multidiffusion.
- **Commutateur P2P** — active ou désactive le P2P. Lorsqu'il est désactivé, la connectivité P2P ne prend pas effet.

12.2 Service infonuagique

L'activation du service infonuagique génère un code QR dynamique pour la région sélectionnée. La numérisation de ce code avec l'application mobile ajoute la caméra à l'application pour la gestion à distance. Lorsqu'un identifiant infonuagique est préprogrammé avec une région fixe, seules les informations de liaison sont affichées; le commutateur du service infonuagique et le code dynamique ne sont pas affichés.

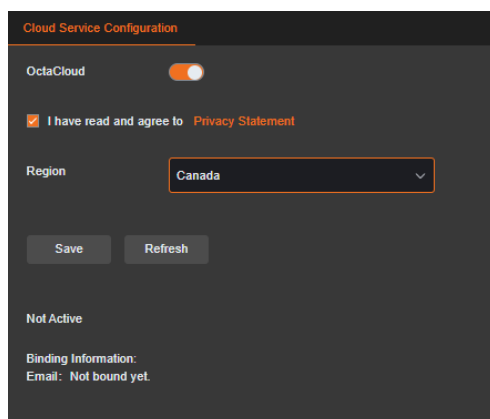


Figure 12-8. Paramètres du service infonuagique

- **Service infonuagique** — active ou désactive le service infonuagique.
- **Déclaration de confidentialité** — avant de pouvoir activer le service infonuagique, vous devez lire et accepter la déclaration de confidentialité.
- **Région** — sélectionne la région du service infonuagique. Elle doit correspondre à la région utilisée lors de l'inscription du compte de l'application.
- **Affichage du code QR** — une fois le service infonuagique activé et une région définie, un code QR dynamique est généré automatiquement. Le code est valide pendant 300 s, après quoi il expire et doit être actualisé. Numérisez le code avec l'application pour ajouter la caméra.
- **Dissocier** — supprime la liaison entre la caméra et le compte de l'application. Après la dissociation, l'appareil apparaît hors ligne dans l'application et n'y est plus accessible.

NOTE Le service infonuagique communique avec le serveur infonuagique; la caméra doit donc disposer d'un accès à Internet pour que cette fonction fonctionne.

12.3 Courriel

Configurez les paramètres de courriel afin que la caméra puisse envoyer des notifications système — par exemple, lorsqu'une alarme est déclenchée ou que le stockage est plein — à un ou plusieurs destinataires.

12.3.1 Paramètres

Ouvrez **Paramètres** → **Réseau** → **Courriel** pour configurer le serveur de messagerie et les destinataires.

Figure 12-9. Paramètres de courriel

- **Courriel** — cochez la case pour activer les notifications par courriel.
- **Type** — le type de boîte aux lettres. Deux types sont offerts : Outlook et Autre.
- **Chiffrement** — activez cette option si votre serveur de messagerie exige une authentification SSL ou TLS. Si vous n'êtes pas certain, réglez-la à Automatique.
- **Port SMTP** — le port SMTP du serveur de messagerie.
- **Serveur SMTP** — l'adresse du serveur SMTP.
- **Nom d'utilisateur** — l'adresse de courriel de l'expéditeur.
- **Mot de passe** — le mot de passe du compte de courriel de l'expéditeur.
- **Destinataire 1 à 3** — les adresses de courriel qui recevront les notifications d'événements de la caméra.
- **Intervalle** — l'intervalle de temps minimal entre les courriels de notification.

TIP Pour confirmer que tous les paramètres sont corrects, cliquez sur **Tester le courriel**. Un message de test est envoyé à l'adresse du destinataire; s'il arrive, la configuration est correcte.

12.3.2 Paramètres d'horaire

Définissez un horaire pendant lequel la fonction de courriel est active. Les notifications ne sont envoyées que pendant les périodes de temps planifiées. Pour en savoir plus sur la définition d'un horaire, consultez la section de configuration de l'horaire.

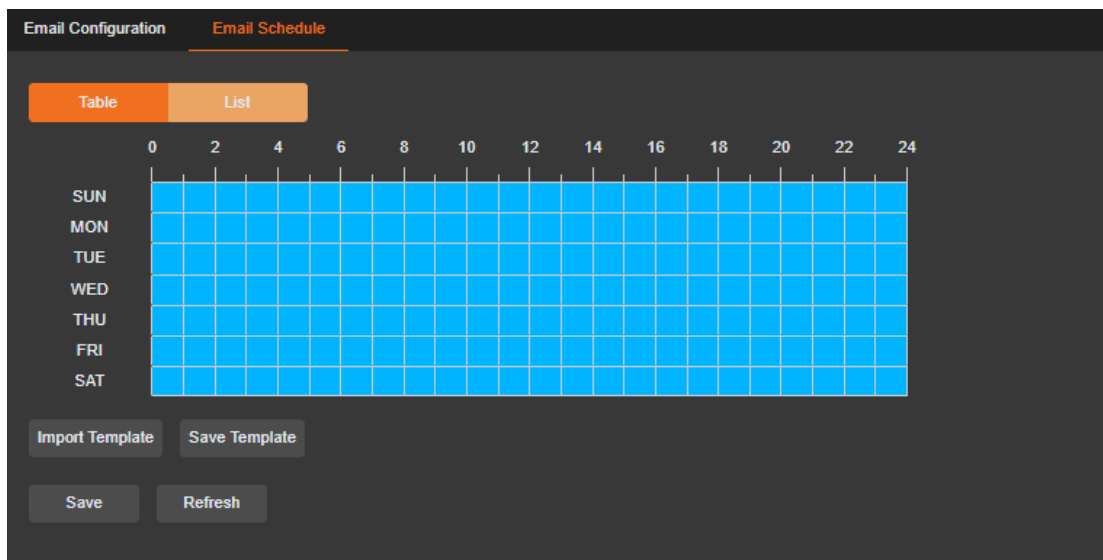


Figure 12-10. Paramètres d'horaire de courriel

12.4 RTSP

Le RTSP (Real Time Streaming Protocol) contrôle la transmission du flux multimédia. Ouvrez **Paramètres** → **Réseau** → **RTSP** pour configurer les paramètres suivants.

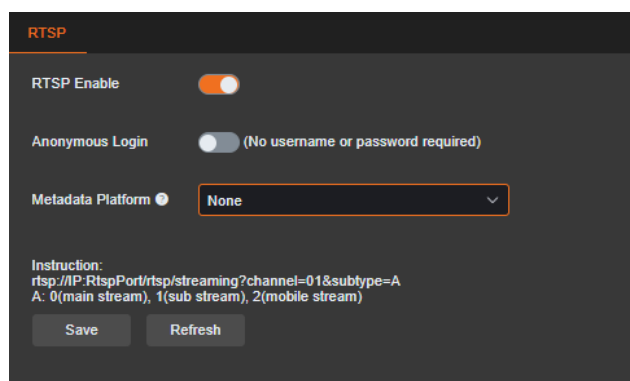


Figure 12-11. Paramètres RTSP

- **Activer RTSP** — active ou désactive le RTSP. Le protocole n'est offert que lorsque cette option est activée.
- **Connexion anonyme** — lorsque cette option est activée, le flux RTSP est accessible sans authentification.
- **Plateforme de métadonnées** — lorsque la caméra est connectée à une plateforme de surveillance tierce au moyen du protocole ONVIF, ce paramètre contrôle le format des métadonnées d'événements et d'alarmes poussées vers cette plateforme :
 - **Aucune** — aucune métadonnée n'est poussée.
 - **Général** — pousse les métadonnées dans un format commun convenant aux plateformes tierces sans exigences particulières.
 - **Milestone** — pousse les métadonnées formatées pour la plateforme Milestone.

12.5 DDNS

Le service DNS dynamique (DDNS) vous permet de rejoindre la caméra au moyen d'un nom de domaine plutôt que d'une adresse IP changeante. Ouvrez **Paramètres** → **Réseau** → **DDNS** pour le configurer.

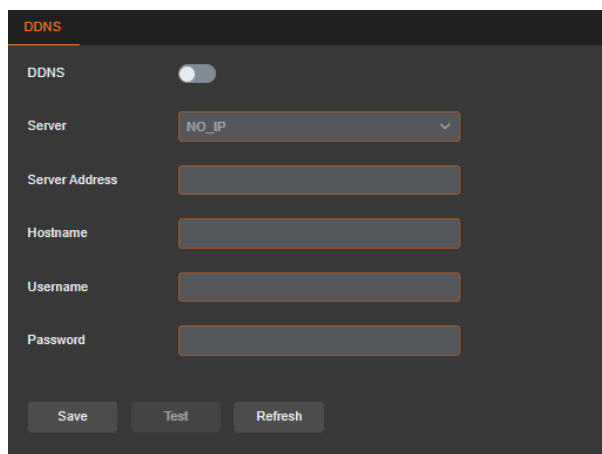


Figure 12-12. Paramètres DDNS

- **DDNS** — cochez la case pour activer le DDNS.
- **Serveur** — sélectionne le serveur DDNS préféré. DYNDNS et NO_IP sont pris en charge, avec une prise en charge partielle de CHANGEIP et DNSEXIT.
- **Nom d'hôte** — le nom de domaine que vous avez créé sur la page Web du fournisseur DDNS. Il s'agit de l'adresse saisie dans le navigateur pour vous connecter à distance à la caméra à partir d'un PC.
- **Utilisateur / Mot de passe** — le nom d'utilisateur et le mot de passe obtenus lors de la création d'un compte auprès du fournisseur DDNS.

NOTE Après avoir saisi tous les paramètres, cliquez sur **Tester** pour vérifier les paramètres DDNS. Si le résultat est « Réseau inaccessible ou erreur DNS », confirmez que la connexion réseau fonctionne et que les informations DDNS sont correctes.

12.6 HTTPS

Ce menu configure l'accès sécurisé à la caméra au moyen du protocole HTTPS. Ouvrez **Paramètres** → **Réseau** → **HTTPS** pour sélectionner le certificat.

Figure 12-13. Paramètres HTTPS

- **Type de certificat** — le type d'authentification. Par défaut et Personnalisé sont offerts. Sélectionnez Personnalisé pour vous connecter à l'aide de votre propre certificat.
- **Certificat** — sous le type Personnalisé, sélectionnez le fichier de certificat personnalisé.
- **Clé** — sous le type Personnalisé, sélectionnez le fichier de clé personnalisé.

12.7 Filtre IP

La fonction Filtre IP vous permet de définir une liste noire ou une liste blanche d'adresses autorisées à se connecter à la caméra. Ouvrez **Paramètres** → **Réseau** → **Filtre IP** pour la configurer.

Figure 12-14. Paramètres du filtre IP

- **Activer** — active ou désactive la fonction de filtrage. Lorsqu'elle est activée, vous pouvez choisir d'appliquer une liste noire ou une liste blanche.
- **Modifier la liste de filtrage** — sélectionne la liste à configurer (liste noire ou liste blanche).
- **Ajout unique** — ajoute une seule adresse IP.
- **Ajout par segment réseau** — ajoute une plage d'adresses.
- **Adresse de début** — l'adresse de début de la plage.
- **Adresse de fin** — l'adresse de fin de la plage.
- **Supprimer** — retire une adresse IP ajoutée de la liste noire ou de la liste blanche.

CAUTION Soyez prudent lorsque vous appliquez une liste blanche. Si votre propre adresse n'y figure pas, vous risquez de vous verrouiller hors de la caméra et de devoir établir une connexion locale pour rétablir l'accès.

12.8 Accès aux plateformes

La caméra peut pousser ses flux audio et vidéo ainsi que ses notifications d'événements vers des plateformes externes, soit par diffusion en direct RTMP, soit par la plateforme de poussée d'événements.

12.8.1 RTMP

Sur la page RTMP, activez la fonction et saisissez une adresse de serveur valide pour pousser le flux audio et vidéo de la caméra vers un serveur de diffusion en direct, comme YouTube.

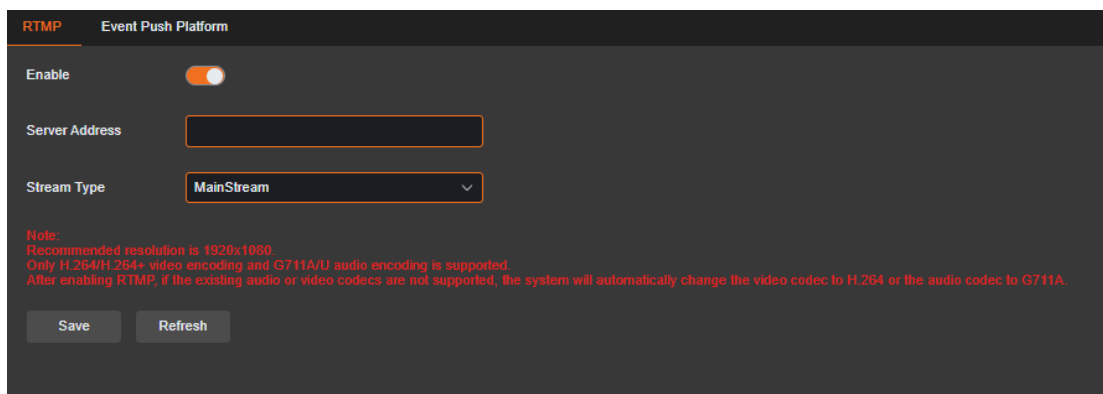


Figure 12-15. Paramètres RTMP

- **Activer** — active ou désactive la fonction RTMP.
- **Adresse du serveur** — l'adresse du serveur vers lequel le flux est poussé.
- **Type de flux** — sélectionne le flux audio et vidéo qui est poussé vers le serveur.

12.8.2 Plateforme de poussée d'événements

La poussée d'événements livre les notifications d'alarme à une plateforme externe au moyen de la méthode HTTP, HTTPS ou UDP. La méthode HTTP/HTTPS prend en charge les requêtes POST et GET; la méthode UDP prend en charge la monodiffusion, la multidiffusion et la diffusion générale.

NOTE La fonction de poussée d'événements n'est prise en charge que sur certains modèles.

12.8.2.1 Poussée HTTP/HTTPS

The screenshot shows the 'Event Push Platform' configuration page. The 'Enable' toggle is turned on. The 'Precise' toggle is turned off. The 'Name' field is empty. The 'Push Way' is set to HTTP. The 'Username' and 'Password' fields are empty. The 'Server Address' field contains '192.168.1.168 or example.com'. The 'Port' field contains '123'. The 'URL' field contains 'API/AlarmEvent/EventPush'. The 'Method' dropdown is set to 'POST'. The 'Interval' dropdown is set to 'OFF'. The 'Save' and 'Refresh' buttons are at the bottom.

Figure 12-16. Paramètres de poussée d'événements HTTP/HTTPS

- **Activer** — active ou désactive la fonction de poussée d'événements.
- **Précise** — active ou désactive la poussée précise. Lorsqu'elle est activée, la caméra pousse une fois au déclenchement d'une alarme et une autre fois à la fin de l'alarme. Lorsqu'elle est désactivée, elle ne pousse qu'une seule fois, au début de l'alarme.
- **Nom** — définit le nom du canal. Les caractères chinois ne sont pas pris en charge.
- **Méthode de poussée** — sélectionne la poussée HTTP, la poussée HTTPS ou la poussée UDP.
- **Nom d'utilisateur** — définit le nom d'utilisateur. Il peut être laissé à NULL s'il n'est pas requis.
- **Mot de passe** — définit le mot de passe. Il peut être laissé à NULL s'il n'est pas requis.
- **Adresse du serveur** — définit l'adresse du serveur.
- **Port** — définit le port du serveur. Plage : 1–65535.
- **URL** — définit le chemin de l'API du serveur. Il peut être laissé à NULL s'il n'est pas requis.
- **Méthode** — le type de requête HTTP/HTTPS. POST et GET sont pris en charge. Seule la méthode POST HTTP/HTTPS peut pousser des images; les autres méthodes ne poussent que des messages, sans image d'accompagnement. Le type d'alarme d'une image poussée doit correspondre à la barre d'alarme de prévisualisation de l'interface Web.
- **Intervalle** — définit l'intervalle de maintien de connexion. Le mécanisme de maintien de connexion pousse périodiquement une notification au client à l'intervalle prédéfini sans affecter la poussée d'alarme normale. Le mode UDP ne dispose d'aucun mécanisme de maintien de connexion.

12.8.2.2 Poussée UDP

The screenshot shows the 'Event Push Platform' configuration window. The 'RTMP' tab is active. The 'Enable' toggle is turned on. The 'Precise' toggle is turned off. The 'Name' field is empty. The 'Push Way' section has three radio buttons: 'HTTP' (off), 'HTTPS' (off), and 'UDP' (on). The 'UDP Method' dropdown is set to 'Broadcast'. The 'UDP Address' field contains '255.255.255.255'. The 'UDP Port' dropdown is set to '5000', with a range '(1 ~ 65535)' indicated. At the bottom are 'Save' and 'Refresh' buttons.

Figure 12-17. Paramètres de poussée d'événements UDP

- **Activer** — active ou désactive la fonction de poussée d'événements.
- **Précise** — active ou désactive la poussée précise. Lorsqu'elle est activée, la caméra pousse une fois au déclenchement d'une alarme et une autre fois à la fin de l'alarme. Lorsqu'elle est désactivée, elle ne pousse qu'une seule fois, au début de l'alarme.
- **Nom** — le nom du canal. Les caractères chinois ne sont pas pris en charge.
- **Méthode de poussée** — sélectionne la méthode de poussée. Sélectionnez HTTP pour la poussée HTTP ou UDP pour la poussée UDP.
- **Méthode UDP** — le type de poussée UDP. La monodiffusion, la multidiffusion et la diffusion générale sont prises en charge :
- **Monodiffusion** — saisissez l'adresse IP et le port du serveur UDP du client. Seule cette adresse reçoit les messages poussés.
- **Multidiffusion** — les serveurs UDP clients sur le même segment réseau qui partagent la même adresse et le même port UDP reçoivent tous le message; les autres adresses ne le reçoivent pas.
- **Diffusion générale** — tous les serveurs UDP sur le même segment réseau reçoivent le message.
- **Adresse UDP** — l'adresse du serveur UDP.
- **Port UDP** — le port du serveur UDP. Plage : 1–65535.

Contrôle d'accès et système

Utilisateurs, portes, cartes, interphone et administration

Chapitre 13 Système de contrôle d'accès

Le système de contrôle d'accès est le cœur de la caméra de contrôle d'accès OCTAVUE par GSD Group. Il réunit tout ce qui est nécessaire pour gérer qui peut ouvrir une porte et de quelle façon : l'inscription des utilisateurs avec identifiants de visage et de carte d'accès, les paramètres d'authentification et du matériel de porte, l'intégration de lecteurs tiers par RS-485 et Wiegand, la liaison d'alarme, un interphone SIP intégré et les réglages de format de carte. Ce chapitre décrit chaque domaine à tour de rôle.

Tous les réglages ci-dessous sont accessibles depuis l'interface Web de la caméra. Les fonctions de contrôle d'accès sont regroupées sous **Réglages** → **Système d'accès**; par exemple, les fiches d'utilisateur se gèrent sous **Réglages** → **Système d'accès** → **Utilisateur**.

13.1 Utilisateur

La zone **Utilisateur** est l'endroit où les opérateurs consultent l'état d'inscription d'un coup d'œil et créent, modifient, filtrent, importent et exportent les personnes autorisées à utiliser la porte. La caméra prend en charge jusqu'à **3 000 utilisateurs**, **3 000 visages** et **30 000 cartes d'accès**.

13.1.1 Informations sur l'utilisateur

La page **Informations sur l'utilisateur** est un tableau de bord qui résume l'état d'inscription actuel du système. Elle indique le nombre total d'utilisateurs inscrits, combien d'entre eux disposent d'identifiants de visage et de carte d'accès, et quelle part de la capacité de l'appareil en utilisateurs, visages, cartes et événements a été utilisée.

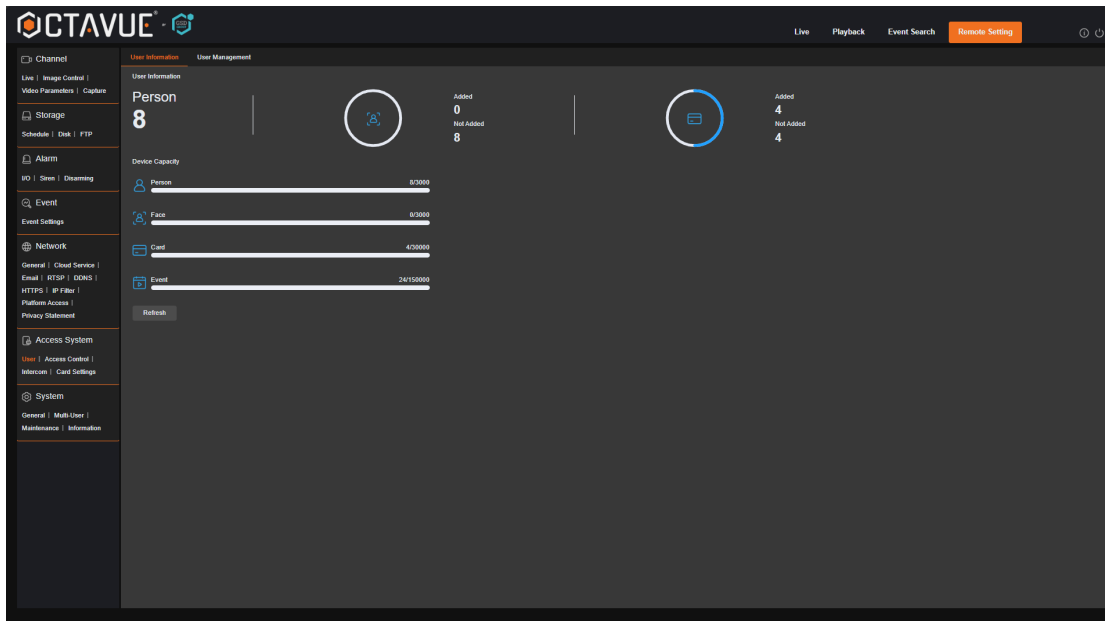


Figure 13-1. Tableau de bord des informations sur l'utilisateur

Le tableau de bord présente les compteurs suivants :

- **Nombre total d'utilisateurs** — le nombre total d'utilisateurs qui ont été ajoutés.
- **Reconnaissance faciale ajoutée / non ajoutée** — le nombre d'utilisateurs qui ont, et qui n'ont pas, un visage inscrit. Cliquez sur l'un ou l'autre chiffre pour accéder à la page Gestion des utilisateurs filtrée selon les utilisateurs correspondants.
- **Cartes d'accès ajoutées / non ajoutées** — le nombre d'utilisateurs qui ont, et qui n'ont pas, une carte d'accès inscrite. Cliquez sur l'un ou l'autre chiffre pour ouvrir la page Gestion des utilisateurs filtrée en conséquence.
- **Personne** — le nombre d'utilisateurs actuellement inscrits par rapport au nombre maximal d'utilisateurs pouvant être ajoutés.
- **Visage** — le nombre de visages inscrits par rapport au nombre maximal de visages pouvant être ajoutés.
- **Carte** — le nombre de cartes d'accès inscrites par rapport au nombre maximal de cartes pouvant être ajoutées.
- **Événement** — le nombre d'événements d'accès enregistrés par rapport au nombre maximal d'événements pouvant être stockés.

13.1.2 Gestion des utilisateurs

La page **Gestion des utilisateurs** sert à ajouter et à modifier les fiches d'utilisateur et à repérer rapidement un utilisateur donné. Les utilisateurs peuvent être filtrés par ID d'utilisateur, nom d'utilisateur ou numéro de carte d'accès, puis affinés par état des identifiants et type d'utilisateur. La base de données complète des utilisateurs peut aussi être importée et exportée à des fins de sauvegarde ou d'approvisionnement en lot.

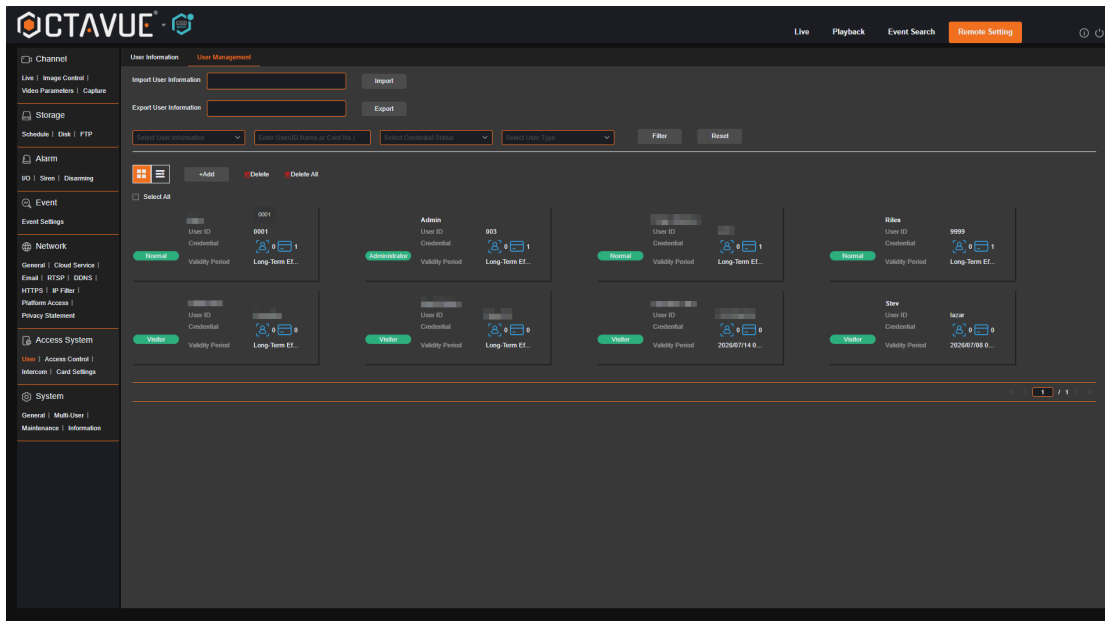


Figure 13-2. Page Gestion des utilisateurs

Les commandes suivantes gèrent la base de données des utilisateurs dans son ensemble :

- **Importer les informations sur l'utilisateur** — cliquez sur le champ pour ouvrir la boîte de dialogue de sélection de fichier, choisissez le fichier de paramètres, puis cliquez sur **Importer** pour charger la base de données des utilisateurs.
- **Exporter les informations sur l'utilisateur** — saisissez un nom de fichier pour les paramètres exportés et cliquez sur **Exporter** pour enregistrer la base de données actuelle des utilisateurs.

Utilisez la barre de filtres pour repérer des utilisateurs précis :

- **Sélectionner les informations sur l'utilisateur** — choisissez de filtrer par ID d'utilisateur, nom d'utilisateur ou numéro de carte.
- **Saisir l'utilisateur (ID, nom ou n° de carte)** — tapez le mot-clé qui correspond au champ sélectionné ci-dessus.
- **Sélectionner l'état des identifiants** — filtrez par état des identifiants : tous, aucun identifiant ajouté, visage ajouté, visage non ajouté, carte ajoutée ou carte non ajoutée.
- **Sélectionner le type d'utilisateur** — filtrez par rôle : administrateur, utilisateur régulier, visiteur ou utilisateur personnalisé.
- **Filtrer** — appliquez les conditions de filtre sélectionnées à la liste des utilisateurs.
- **Réinitialiser** — effacez toutes les conditions de filtre.

Les fiches d'utilisateur peuvent s'afficher selon deux dispositions. Utilisez les icônes de mode d'affichage pour passer de l'une à l'autre :

 **Mode Carte de visite** — affiche les utilisateurs sous forme de cartes visuelles.

 **Mode Liste** — affiche les utilisateurs dans une liste compacte.

Les commandes restantes agissent sur des utilisateurs individuels ou sélectionnés :

- **Ajouter** — créez une nouvelle fiche d'utilisateur.
- **Supprimer** — sélectionnez un utilisateur et cliquez pour supprimer cette fiche d'utilisateur.
- **Tout supprimer** — supprimez toutes les fiches d'utilisateur. Une invite de confirmation doit être acceptée avant que l'opération se poursuive.
- **Tout sélectionner** — sélectionnez tous les utilisateurs de la page actuelle afin que la même opération puisse leur être appliquée à tous.

- **Zone d'affichage des informations sur l'utilisateur** — montre chaque utilisateur inscrit, y compris le visage, l'ID d'utilisateur, le nom d'utilisateur, l'identifiant, la date d'expiration et le type d'utilisateur.
- **Modifier** — survolez une carte d'utilisateur pour faire apparaître le bouton de modification, puis cliquez dessus pour ouvrir la page de détails de l'utilisateur.
- **Pagination** — les commandes situées dans le coin inférieur droit permettent de parcourir la liste des utilisateurs.

CAUTION Tout supprimer efface l'ensemble de la base de données des utilisateurs et est irréversible. Exportez d'abord les informations sur l'utilisateur pour que l'inscription puisse être restaurée au besoin.

13.1.2.1 Ajouter et modifier un utilisateur

Cliquez sur **Ajouter** ou sur le bouton **Modifier** d'une carte d'utilisateur pour ouvrir la page de détails de l'utilisateur, où les informations et les identifiants de l'utilisateur sont saisis ou modifiés.

Figure 13-3. Page de détails de l'utilisateur

Saisissez l'identité et les règles d'accès de l'utilisateur :

- **ID d'utilisateur** — un identifiant personnalisable. Ce champ est obligatoire lors de l'ajout d'un utilisateur.
- **Nom** — le nom d'utilisateur. Facultatif et modifiable.
- **N° d'étage** — le numéro d'étage. Facultatif et modifiable.
- **N° de local** — le numéro de local. Facultatif et modifiable.
- **Sexe** — Homme, Femme ou Inconnu. La valeur par défaut est Homme.
- **Type d'utilisateur** — administrateur, utilisateur régulier, invité ou utilisateur personnalisé. La valeur par défaut est utilisateur régulier.

- **Utilisateur valide à long terme** — lorsqu'elle est activée, l'utilisateur n'a aucune expiration. Les administrateurs ont cette option activée en permanence et ne peuvent pas la modifier; les invités n'ont pas ce commutateur.
- **Période de validité** — la plage de dates active pour l'utilisateur. Les utilisateurs réguliers et personnalisés peuvent la définir une fois que **Utilisateur valide à long terme** est désactivée.
- **Nombre d'accès illimité** — lorsqu'elle est activée, l'utilisateur peut s'authentifier pour ouvrir la porte un nombre illimité de fois. Ce commutateur est offert aux invités et aux utilisateurs personnalisés.
- **Nombre de visites** — le nombre d'entrées autorisé. Chaque authentification réussie réduit le compte de un; lorsqu'il atteint 0, l'utilisateur ne peut plus ouvrir la porte. Cette valeur peut être définie une fois que **Nombre d'accès illimité** est désactivé.

NOTE L'ID d'utilisateur ne peut être attribué que lors de la création initiale d'un utilisateur. Il ne peut pas être modifié une fois la fiche enregistrée.

Sous **Configuration du certificat**, attribuez les identifiants de l'utilisateur :

- **Visage** — le visage de référence inscrit. Lors de l'authentification, le visage détecté est comparé à cette image; une similarité de 70 % ou plus est acceptée. Les images de visage téléversées ne doivent pas dépasser 200 Ko et doivent être au format JPG, JPEG ou PNG.
- **Carte** — saisissez le numéro de carte manuellement ou présentez la carte d'accès à la zone du lecteur pour le capturer automatiquement. Chaque utilisateur peut détenir jusqu'à 10 cartes d'accès, et chaque carte peut être désignée comme carte normale, carte de contrainte, carte de patrouille ou carte désactivée (accessibilité).
- **Code QR** — pour les invités, un code QR peut être généré pour l'authentification. Le code généré peut être exporté sous forme d'image et se voir attribuer une période de validité.
- **Authentification** — la méthode d'authentification acceptée pour l'utilisateur. Les options comprennent visage ou carte ou code QR, carte, carte et visage, visage, et code QR. La valeur par défaut est visage ou carte ou code QR.

TIP Une carte de contrainte permet à un utilisateur d'ouvrir la porte sous la menace tout en déclenchant silencieusement une alarme. Réservez au moins une carte de contrainte pour les emplacements à risque élevé et gardez son attribution confidentielle.

13.2 Contrôle d'accès

La zone **Contrôle d'accès** régit le comportement de l'authentification, la façon dont le matériel de porte est piloté, la manière dont les lecteurs externes sont connectés par RS-485 et Wiegand, ainsi que les actions liées aux alarmes de contrôle d'accès.

13.2.1 Réglages d'authentification

Cette page définit l'intervalle d'authentification pour un même utilisateur et configure les alarmes d'échec d'authentification et d'effraction. Pendant l'intervalle configuré, un utilisateur donné ne peut s'authentifier avec succès qu'une seule fois; si des tentatives répétées sont faites en succession rapide, seule la première réussit. Un seuil d'échecs maximal peut être défini afin qu'une fois le nombre de tentatives échouées atteint, une alarme d'échec d'authentification soit déclenchée et ses actions de liaison configurées activées.

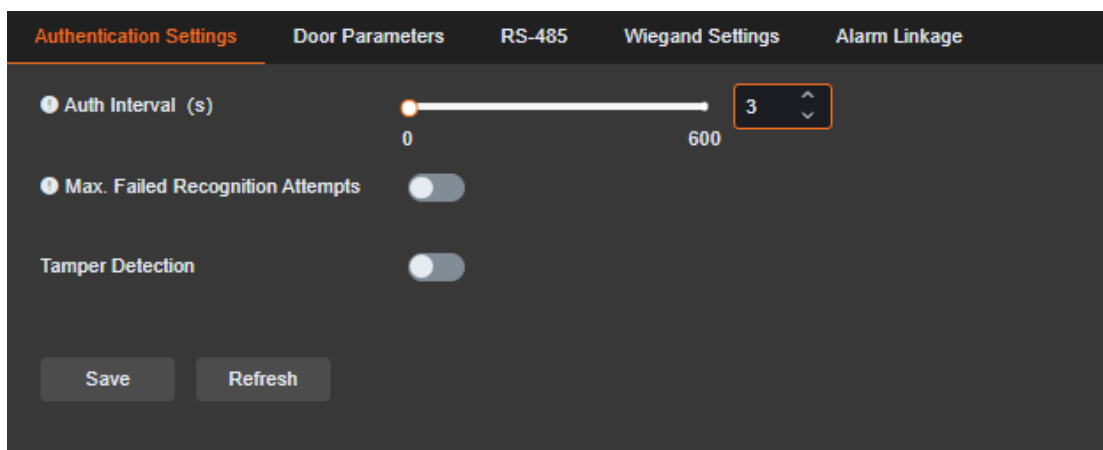


Figure 13-4. Réglages d'authentification

- **Intervalle d'authentification** — le temps minimal qui doit s'écouler entre deux authentifications réussies par le même utilisateur. Plage de 0 à 600 s; par défaut 3 s.
- **Tentatives de reconnaissance échouées max.** — le commutateur qui active l'alarme d'échecs maximal.
- **Tentatives d'authentification échouées max.** — le nombre d'échecs consécutifs qui déclenche l'alarme. Plage de 1 à 10.
- **Détection d'effraction** — le commutateur d'alarme d'effraction. Lorsqu'il est activé, une alarme d'effraction est déclenchée si la caméra est retirée de force après l'installation, et les actions de liaison configurées sont amorcées.

CAUTION Activez la **Détection d'effraction** sur toute porte où la caméra est physiquement accessible. Sans elle, le retrait de l'appareil de son support ne générera aucune alarme.

13.2.2 Paramètres de porte

Cette page définit la durée pendant laquelle la porte reste déverrouillée, le délai d'ouverture de porte et les caractéristiques électriques du matériel de porte connecté. Une durée d'ouverture distincte, plus longue, peut être accordée aux utilisateurs d'accessibilité. Lorsqu'un capteur de contact de porte (contact magnétique) est utilisé, la caméra déclenche une alarme de délai d'ouverture de porte si la porte n'est pas fermée dans le temps configuré, et amorce les actions liées.

Figure 13-5. Paramètres de porte

- **Durée d'ouverture de porte** — la durée pendant laquelle la porte reste déverrouillée après une authentification réussie ou une ouverture manuelle. Plage de 0 à 255 s; par défaut 5 s.
- **Durée d'ouverture avec carte d'accessibilité** — la durée d'ouverture accordée lorsqu'une carte d'accessibilité est utilisée, donnant à l'utilisateur plus de temps pour passer. Plage de 5 à 255 s; par défaut 20 s.
- **Alarme de délai d'ouverture de porte** — le temps après lequel une alarme est déclenchée si la porte n'a pas été fermée. Utilisé conjointement avec le capteur de contact de porte. Plage de 1 à 255 s; par défaut 30 s.
- **Type de capteur de contact de porte** — réglez sur normalement ouvert ou normalement fermé pour correspondre au contact de porte installé. Si cela ne correspond pas au type de capteur réel, l'état de porte rapporté sera inversé.
- **Type de bouton de sortie** — réglez sur normalement ouvert ou normalement fermé pour correspondre au bouton de sortie (demande de sortie) installé. Appuyer sur le bouton de sortie ouvre la porte directement, sans authentification.
- **État de la serrure** — réglez sur normalement ouvert ou normalement fermé pour correspondre à la serrure installée. Si cela ne correspond pas au type de serrure réel, le comportement de la serrure sera inversé. Après une authentification réussie, un déverrouillage manuel ou un verrouillage manuel, la serrure connectée réagit en conséquence.

WARNING Les réglages **Type de capteur de contact de porte**, **Type de bouton de sortie** et **État de la serrure** doivent correspondre au câblage du matériel installé. Une incohérence inverse le comportement de la porte et peut la laisser déverrouillée alors qu'elle devrait être sécurisée.

13.2.3 RS-485

Un lecteur de carte RS-485 externe peut lire les informations de carte d'accès afin qu'une carte inscrite puisse être passée à ce lecteur pour ouvrir la porte.

Figure 13-6. Réglages RS-485

- **Activer** — le commutateur d'activation RS-485.
- **Protocole** — Pelco-D ou Pelco-P sur RS-485. La caméra de contrôle d'accès est fixée à Pelco-D.
- **Débit en bauds** — le débit de signalisation de la liaison RS-485. La caméra de contrôle d'accès est fixée à 9600.
- **Bit de données / Bit d'arrêt** — le nombre de bits de données par caractère et le nombre de bits d'arrêt qui marquent la fin d'un paquet. Les options de Bit de données sont 8, 7, 6 ou 5; les options de Bit d'arrêt sont 1 ou 2. La caméra de contrôle d'accès est fixée à 8 bits de données et 1 bit d'arrêt.
- **Code d'adresse** — l'adresse de réception des commandes. Elle est obtenue automatiquement par la caméra de contrôle d'accès et n'est pas modifiable.

NOTE Sur la caméra de contrôle d'accès OCTAVUE, le protocole RS-485, le débit en bauds, les bits de données/d'arrêt et l'adresse sont pré-réglés; seul le commutateur **Activer** est configurable. Ces valeurs fixes sont affichées à titre de référence lors du câblage d'un lecteur compatible.

13.2.4 Réglages Wiegand

Activez ce commutateur pour connecter un lecteur de carte Wiegand et ouvrir la porte en passant une carte. La caméra de contrôle d'accès prend en charge les lecteurs à protocole Wiegand 26 et Wiegand 34.

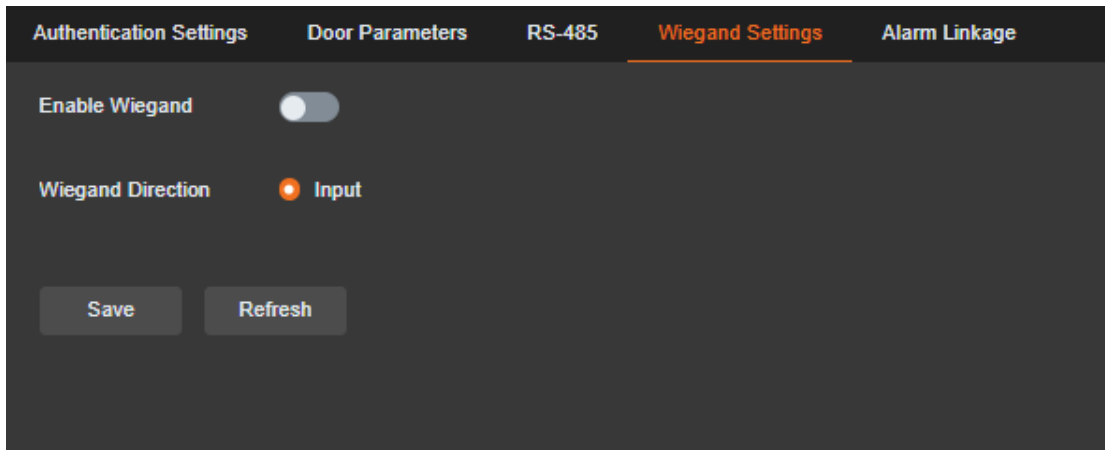


Figure 13-7. Réglages Wiegand

- **Activer Wiegand** — le commutateur d'activation du lecteur de carte Wiegand.

13.2.5 Liaison d'alarme

Les alarmes de contrôle d'accès peuvent déclencher un ensemble de réponses liées. Trois sources d'alarme sont disponibles : échec d'authentification, délai d'ouverture de porte et effraction. Chaque source possède sa propre configuration de liaison, et les actions disponibles sont les mêmes pour les trois.

Les actions de liaison sont les suivantes :

- **Poussée d'événement vers la plateforme** — pousse l'événement vers la plateforme de gestion configurée.
- **Courriel** — envoie un courriel lorsque l'événement est déclenché. Cliquez sur le bouton de réglages ou de calendrier pour configurer les paramètres de courriel et la période active.
- **Téléversement d'image** — téléverse les instantanés d'alarme vers le serveur FTP lié. Le serveur FTP doit d'abord être configuré; cliquez sur le bouton de réglages pour sélectionner les canaux dont les instantanés sont téléversés.
- **Téléversement vidéo** — téléverse la vidéo d'alarme vers le serveur FTP lié. Le serveur FTP doit d'abord être configuré; cliquez sur le bouton de réglages pour sélectionner les canaux dont la vidéo est téléversée.
- **Sirène** — le commutateur de liaison de la sirène de dissuasion. Lorsque l'alarme est déclenchée, la sirène réagit selon les paramètres de la page des réglages de dissuasion. Cliquez sur le bouton de réglages pour les configurer directement.
- **Canal d'enregistrement** — le commutateur de liaison d'enregistrement. Cliquez sur le bouton de réglages pour sélectionner les canaux qui enregistrent le type d'alarme correspondant lorsque l'alarme est déclenchée.
- **Délai d'enregistrement** — la durée pendant laquelle l'enregistrement se poursuit après la fin de l'alarme.
- **Notification** — le commutateur de poussée personnalisée. Cliquez sur le bouton de réglages pour ouvrir la page de notification personnalisée, où une URL de poussée personnalisée et les options connexes sont définies.

13.2.5.1 Échec d'authentification

Déclenchée lorsque l'authentification faciale échoue. Les liaisons disponibles sont Poussée d'événement vers la plateforme, Courriel, Téléversement d'image, Téléversement vidéo, Sirène, Canal d'enregistrement, Délai d'enregistrement et Notification.

Authentication Settings
Door Parameters
RS-485
Wiegand Settings
Alarm Linkage

Authentication Failed
Door Open Timeout
Tampering Detection

Common Linkage

Email
☒
☐
☐

Picture Upload
☐ FTP

Video Upload
☐ FTP

Alarm Output

I/O Output
☒
☐

Siren
☒
☐

Video Linkage

Record Channel
☒

Post Recording
5 S

Save
Default
Refresh

Figure 13-8. Liaison d'alarme d'échec d'authentification

13.2.5.2 Délai d'ouverture de porte

Déclenchée lorsque la porte n'est pas fermée dans le délai configuré. Les liaisons disponibles sont Poussée d'événement vers la plateforme, Courriel, Téléversement d'image, Téléversement vidéo, Sirène, Canal d'enregistrement, Délai d'enregistrement et Notification.

Authentication Settings
Door Parameters
RS-485
Wiegand Settings
Alarm Linkage

Authentication Failed
Door Open Timeout
Tampering Detection

Common Linkage

Email
☒
☐
☐

Picture Upload
☐ FTP

Video Upload
☐ FTP

Alarm Output

I/O Output
☒
☐

Siren
☒
☐

Video Linkage

Record Channel
☒

Post Recording
5 S

Save
Default
Refresh

Figure 13-9. Liaison d'alarme de délai d'ouverture de porte

13.2.5.3 Effraction

Déclenchée lorsque la caméra est manipulée ou retirée. Les liaisons disponibles sont Poussée d'événement vers la plateforme, Courriel, Téléversement d'image, Téléversement vidéo, Sirène, Canal d'enregistrement, Délai d'enregistrement et Notification.

The screenshot shows the 'Alarm Linkage' configuration page. The top navigation bar includes 'Authentication Settings', 'Door Parameters', 'RS-485', 'Wiegand Settings', and 'Alarm Linkage'. The sub-navigation bar includes 'Authentication Failed', 'Door Open Timeout', and 'Tampering Detection'. The main content area is divided into three sections: 'Common Linkage', 'Alarm Output', and 'Video Linkage'. 'Common Linkage' includes 'Email' (toggle on), 'Picture Upload' (checkbox off), and 'Video Upload' (checkbox off). 'Alarm Output' includes 'I/O Output' (toggle on) and 'Siren' (toggle on). 'Video Linkage' includes 'Record Channel' (toggle on) and 'Post Recording' (dropdown set to '5 S'). At the bottom are 'Save', 'Default', and 'Refresh' buttons.

Figure 13-10. Liaison d'alarme d'effraction

13.3 Interphone

L'interphone intégré permet à la caméra de contrôle d'accès de passer et de recevoir des appels audio et vidéo, soit directement entre appareils (Poste à poste), soit par l'intermédiaire d'un serveur SIP. Cette zone couvre le comportement des appels, la configuration du compte et du destinataire SIP, ainsi que les règles DTMF pour le contrôle à distance de la porte pendant un appel.

13.3.1 Configuration des appels

Cette page contrôle le comportement général des appels. Un appel sans réponse est automatiquement terminé une fois le délai d'appel atteint. Pour effectuer des appels SIP, activez le commutateur SIP, puis configurez un compte de serveur SIP sur la page Configuration du compte SIP et un destinataire sur la page Destinataire SIP. Lorsque les appels SIP entrants sont autorisés, un téléphone SIP peut appeler la caméra de contrôle d'accès; lorsque la réponse automatique est activée, la caméra répond automatiquement à ces appels. Les appels vidéo peuvent être lancés lorsque le client SIP les prend en charge.

Figure 13-11. Configuration des appels

- **Délai d'appel** — la durée pendant laquelle l'appareil sonne avant qu'un appel sans réponse soit automatiquement terminé. Plage de 10 à 180 s; par défaut 60 s.
- **Voyant d'état** — le mode du voyant lumineux : automatique, allumé en permanence ou éteint.
- **Activer SIP** — active les appels SIP sortants.
- **Autoriser les appels SIP entrants** — permet à la caméra de recevoir des appels SIP.
- **Réponse automatique** — répond automatiquement à un appel SIP entrant.
- **Port SIP** — le port de signalisation SIP.
- **Port de départ RTP** — le port de départ du flux média RTP.

NOTE Lorsqu'un appel vidéo est établi, le format d'encodage est forcé à H.264 pour la compatibilité avec le client appelant.

13.3.2 Configuration du compte SIP

Cette page définit le compte d'appel SIP. Par défaut, la caméra utilise un compte Poste à poste, pour lequel seul le nom peut être modifié. Jusqu'à 7 comptes de serveur SIP peuvent être ajoutés, mais un seul compte peut être activé à la fois; le compte activé apparaît comme disponible et les comptes restants apparaissent comme indisponibles.

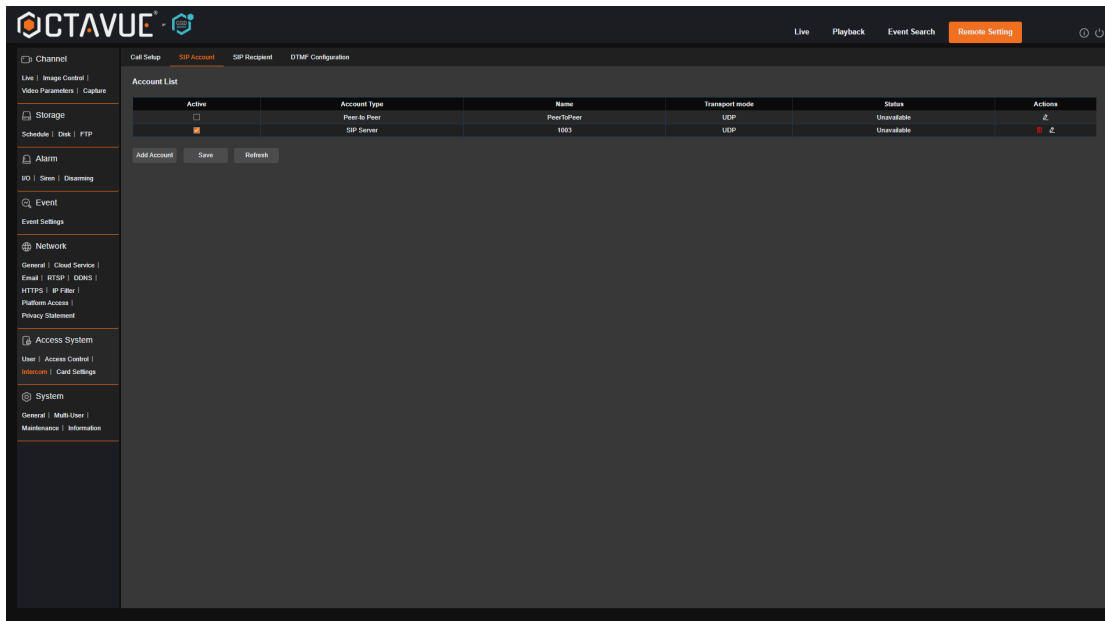


Figure 13-12. Configuration du compte SIP

Cliquez sur ajouter pour créer un compte de serveur SIP et saisir ses paramètres :

Figure 13-13. Ajout d'un compte de serveur SIP

- **Type de compte** — réglé sur le type Serveur SIP.
- **Nom** — le nom du compte.
- **IP du serveur** — l'adresse IP du serveur SIP.
- **Port** — le port du serveur SIP.
- **Mot de passe** — le mot de passe du compte.
- **Identifiant de l'appelant** — l'identification de l'appelant présentée pour le compte.
- **Mode de transport** — le protocole de transport : UDP, TCP ou TLS.

TIP Utilisez **TLS** comme mode de transport lorsque le serveur SIP le prend en charge, afin que la signalisation entre la caméra et le serveur soit chiffrée.

13.3.3 Destinataire SIP

Cette page gère les contacts que la caméra peut appeler. Les types de destinataire Poste à poste et Serveur SIP peuvent être ajoutés, jusqu'à un maximum de 16 destinataires dans la liste de contacts.

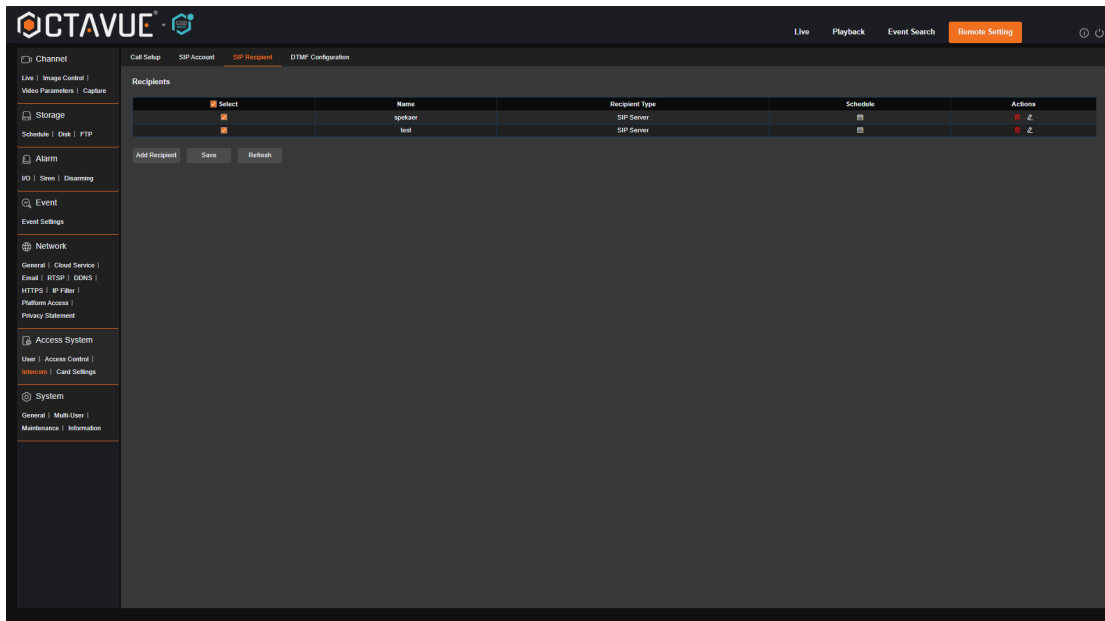


Figure 13-14. Liste des destinataires SIP

Pour un destinataire **Serveur SIP**, saisissez :

Figure 13-15. Ajout d'un destinataire de serveur SIP

- **Type de destinataire** — réglé sur Serveur SIP.
- **Nom** — le nom du compte du destinataire.
- **Identifiant de l'appelant** — l'identification de l'appelant pour le destinataire.

Pour un destinataire **Poste à poste**, saisissez :

Figure 13-16. Ajout d'un destinataire Poste à poste

- **Type de destinataire** — réglé sur Poste à poste.
- **Nom** — le nom du compte du destinataire.
- **IP du destinataire** — l'adresse IP de l'appareil destinataire.

13.3.4 Configuration DTMF

Les règles DTMF permettent à la personne en appel SIP d'actionner la porte à distance à partir du clavier d'appel. Une fois qu'une règle est activée, la saisie du code de clavier correspondant suivi de # pendant un appel SIP exécute l'action associée, comme ouvrir ou fermer la porte. Jusqu'à 16 règles peuvent être ajoutées, et deux règles ne peuvent pas partager le même code de clavier.

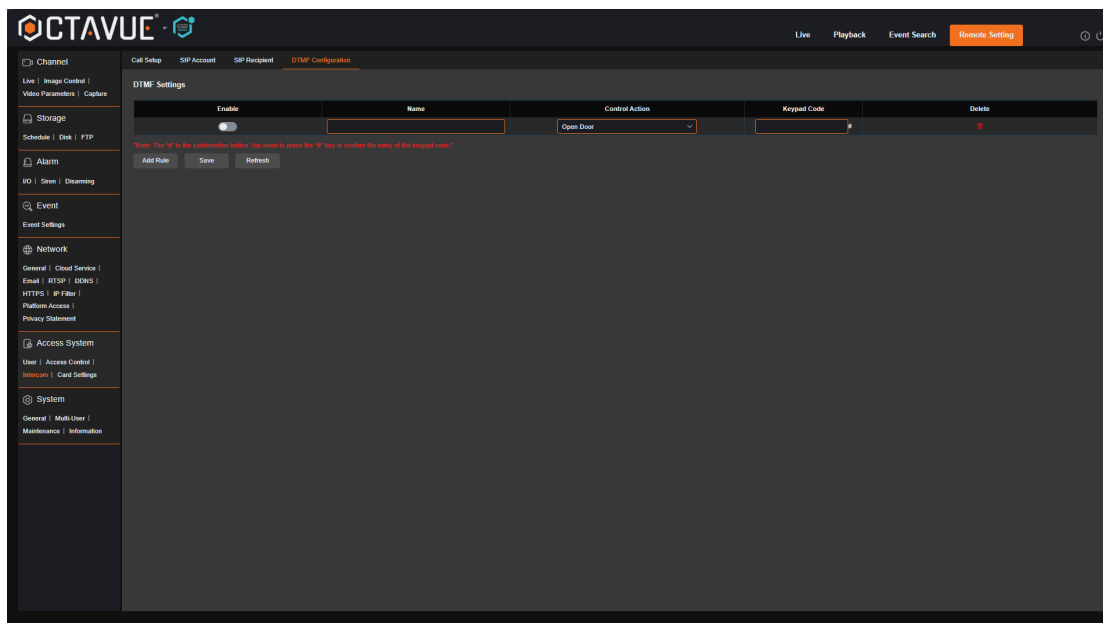


Figure 13-17. Configuration DTMF

- **Activer** — le commutateur qui active la règle.
- **Nom** — le nom de la règle.
- **Action de contrôle** — l'action exécutée par la règle : ouvrir ou fermer.
- **Code de clavier** — la commande de clavier qui invoque la règle.
- **Supprimer** — supprime la règle correspondante.
- **Ajouter une règle** — crée une nouvelle règle.

CAUTION Une règle DTMF permet d'ouvrir la porte à distance à partir d'un clavier d'appel. Restreignez les destinataires qui peuvent joindre la caméra et gardez les codes de clavier confidentiels pour empêcher toute entrée non autorisée.

13.4 Réglages de carte

La zone **Réglages de carte** sélectionne quelles technologies de carte sans contact la caméra lit et comment les numéros de carte sont interprétés lorsqu'un lecteur tiers est utilisé.

13.4.1 Type de carte

Sélectionnez quelles technologies de carte sont activées. NFC, Mifare et Desfire sont pris en charge. Les trois types sont contrôlés indépendamment et ne sont pas mutuellement exclusifs, de sorte que n'importe quelle combinaison peut être activée à la fois.

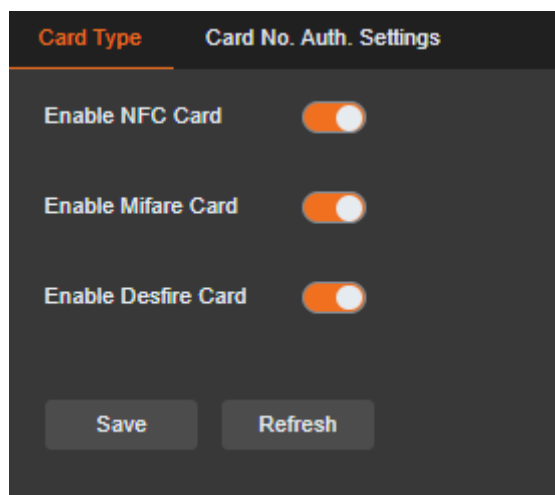


Figure 13-18. Type de carte

- **Activer la carte NFC** — active ou désactive les cartes NFC.
- **Activer la carte Mifare** — active ou désactive les cartes Mifare.
- **Activer la carte Desfire** — active ou désactive les cartes Desfire.

13.4.2 Authentification du numéro de carte

Sélectionnez comment les numéros de carte sont lus : le protocole Numéro de carte complet, le protocole Wiegand 26 ou le protocole Wiegand 34. Du moment que le contrôleur d'accès prend en charge le protocole Numéro de carte complet et peut détecter automatiquement le format Wiegand, il est compatible avec les lecteurs Wiegand 26 et Wiegand 34. Lorsque Numéro de carte complet est sélectionné, les lecteurs utilisant le protocole Wiegand 26 ou Wiegand 34 sont reconnus normalement.

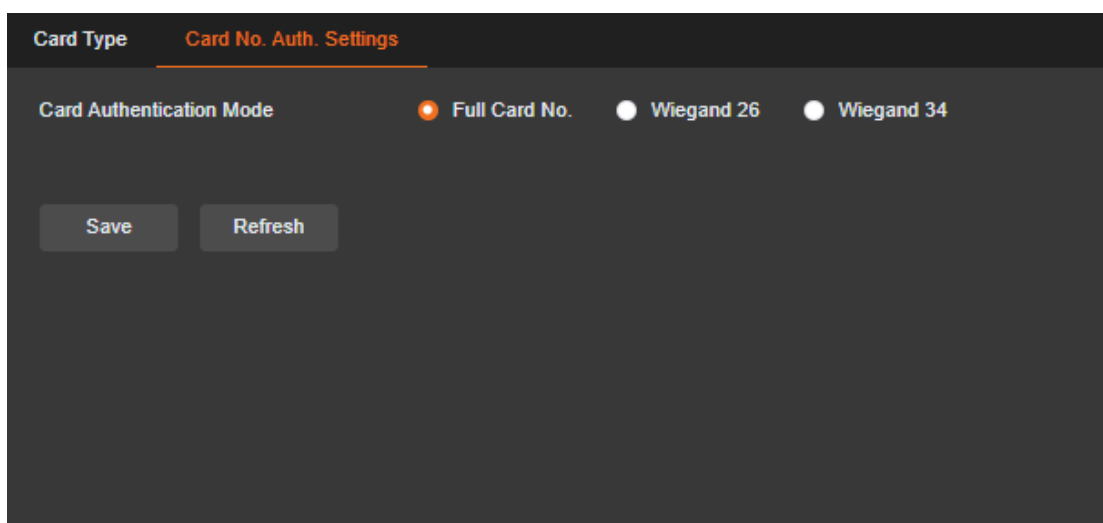


Figure 13-19. Authentification du numéro de carte

- **N° de carte complet** — le protocole de numéro de carte complet. Lorsqu'il est sélectionné, les lecteurs à numéro de carte complet et les lecteurs compatibles sont pris en charge.
- **Wiegand 26** — lorsqu'il est sélectionné, seuls les lecteurs à protocole Wiegand 26 sont pris en charge.
- **Wiegand 34** — lorsqu'il est sélectionné, seuls les lecteurs à protocole Wiegand 34 sont pris en charge.

NOTE Ces options s'appliquent uniquement aux lecteurs de carte tiers. Le lecteur de carte intégré à la caméra de contrôle d'accès n'est pas affecté par ce réglage.

Chapitre 14 Système, utilisateurs et maintenance

Ce chapitre porte sur les paramètres administratifs qui permettent de garder la caméra de contrôle d'accès OCTAVUE exacte, sécurisée et à jour : l'horloge système et l'heure avancée, les comptes multiutilisateurs et les autorisations, les tâches de maintenance courantes telles que l'examen des journaux, la mise à niveau du micrologiciel et la sauvegarde des paramètres, ainsi que les pages en lecture seule qui affichent les renseignements sur l'appareil et la confidentialité.

14.1 Configuration générale du système

Les paramètres généraux du système définissent la façon dont la caméra tient l'heure. Une horloge exacte est essentielle pour obtenir des entrées de journal utiles, des enregistrements programmés et des événements d'accès cohérents; configurez donc la source de temps, le fuseau horaire et les règles de l'heure avancée avant de mettre la caméra en service.

14.1.1 Date et heure

Ouvrez la page de la date et de l'heure pour définir la façon dont la caméra obtient et affiche l'heure actuelle.

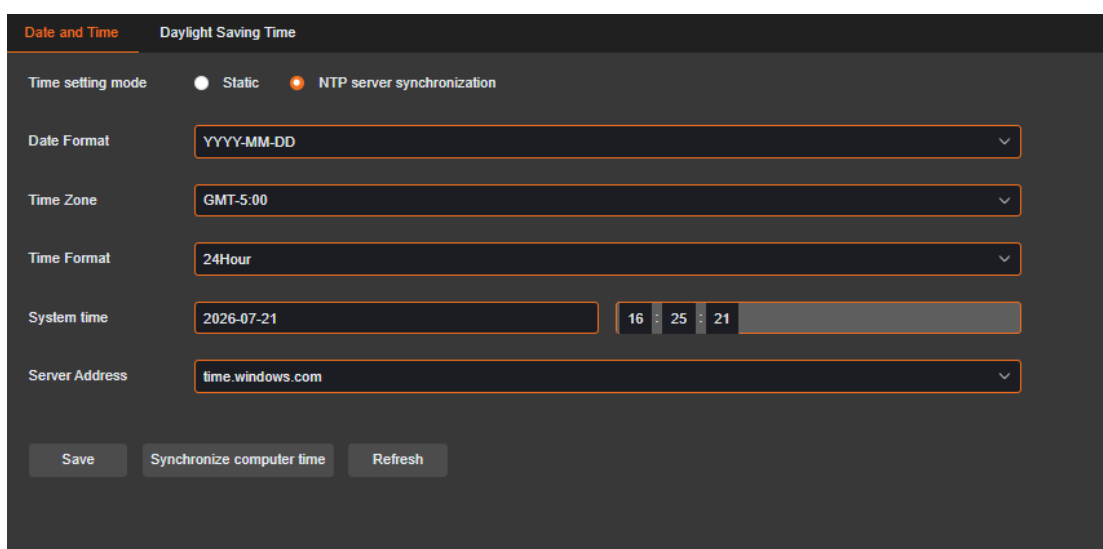


Figure 14-1. Paramètres de date et d'heure

Configurez les options suivantes :

- **Mode de réglage de l'heure** — choisissez **Manuel** ou **NTP**. En mode manuel, vous saisissez l'heure vous-même; en mode NTP, la caméra se synchronise automatiquement avec un serveur de temps réseau.
- **Format de date** — sélectionnez l'ordre préféré pour le jour, le mois et l'année.
- **Fuseau horaire** — sélectionnez le fuseau horaire qui correspond à la région ou à la ville de la caméra.
- **Format d'heure** — choisissez entre l'horloge de 24 heures et celle de 12 heures.
- **Heure système** — cliquez sur le champ pour régler la date et l'heure actuelles manuellement.
- **Synchroniser avec l'heure de l'ordinateur** — applique à la caméra l'horloge de l'ordinateur que vous utilisez.
- **Adresse du serveur** — en mode NTP, sélectionnez le serveur de temps utilisé pour la synchronisation.

NOTE Lorsque la synchronisation **NTP** est sélectionnée, l'heure système ne peut pas être réglée manuellement; la caméra obtient l'heure du serveur configuré.

14.1.2 Heure avancée

L'heure avancée (DST) fait avancer l'horloge d'un décalage fixe pendant une partie de l'année. Activez cette fonction si le fuseau horaire ou la région de la caméra observe l'heure avancée.

The screenshot shows the 'Daylight Saving Time' configuration page. At the top, there's a toggle switch for 'Daylight Saving Time' which is currently turned on. Below it are two radio buttons: 'Set by week' (selected) and 'Set by date'. The 'Start Time' section has three dropdowns: 'March', 'The 2nd', and 'SUN', followed by a time field '12 : 00 : 00'. The 'End Time' section has three dropdowns: 'November', 'The 1st', and 'SUN', followed by a time field '12 : 00 : 00'. The 'Time Offset' section has a dropdown menu showing '1Hour'. At the bottom, there are 'Save' and 'Refresh' buttons.

Figure 14-2. Paramètres de l'heure avancée

- **Heure avancée** — activez cette option si le fuseau horaire de la caméra observe l'heure avancée.
- **Régler par semaine** — définissez le début et la fin de la période de l'heure avancée par mois, semaine et heure de la journée (par exemple, le premier dimanche du mois à 2 h 00).
- **Régler par date** — définissez les dates et heures exactes du calendrier auxquelles l'heure avancée commence et se termine.
- **Heure de début / Heure de fin** — définissez les moments auxquels l'heure avancée commence et se termine.
- **Décalage horaire** — sélectionnez la durée ajoutée pendant la période de l'heure avancée. Il s'agit de la différence entre le temps universel coordonné (UTC) et l'heure locale.

14.2 Gestion multiutilisateur

Ce menu permet à l'administrateur de créer et de configurer des comptes supplémentaires, chacun ayant son propre nom d'utilisateur, mot de passe et droits d'accès.

Le système prend en charge les types d'utilisateurs suivants :

- **Administrateur (ADMIN)** — l'administrateur du système a le contrôle total de la configuration et peut modifier à la fois le mot de passe de l'administrateur et celui de l'utilisateur, ainsi qu'activer ou désactiver la protection par mot de passe.
- **Utilisateur normal (USER)** — un compte standard limité à des fonctions telles que l'aperçu, la recherche et la lecture. L'administrateur peut créer plusieurs utilisateurs, chacun se voyant accorder des droits d'accès différents.

NO.	Username	Level	Status	Password	Policy
1	admin	ADMIN	Enable	ℹ	
2	user1	USER	Disable	ℹ	⊗
3	user2	USER	Disable	ℹ	⊗
4	user3	USER	Disable	ℹ	⊗
5	user4	USER	Disable	ℹ	⊗
6	user5	USER	Disable	ℹ	⊗
7	user6	USER	Disable	ℹ	⊗

Refresh

Figure 14-3. Liste des comptes d'utilisateurs

Figure 14-4. Modification d'un compte d'utilisateur

Pour créer ou activer un compte d'utilisateur :

1. Sélectionnez l'un des utilisateurs actuellement inactifs et cliquez sur l'icône **Modifier le mot de passe**.
2. Sélectionnez **Activer** pour activer le compte.
3. Cliquez sur **Nom d'utilisateur** pour modifier le nom du compte.
4. Cliquez sur le champ à côté de **Mot de passe** et saisissez le mot de passe souhaité.
5. Cliquez sur le champ à côté de **Confirmer** et saisissez de nouveau le même mot de passe.
6. Cliquez sur **OK**. Vous serez invité à saisir le mot de passe de l'administrateur à des fins d'authentification.



Figure 14-5. Invite d'authentification par mot de passe

Pour définir les autorisations d'un sous-utilisateur, cliquez sur le compte pour ouvrir la page **Stratégie**, puis cochez la case à côté de chaque fonction que vous souhaitez accorder. Cliquez sur **Tout** pour sélectionner toutes les autorisations ou sur **Effacer** pour supprimer toutes les sélections.

Figure 14-6. Page de stratégie d'autorisations du sous-utilisateur

14.3 Maintenance du système

À partir du menu de maintenance du système, vous pouvez rechercher et examiner les journaux système, rétablir les réglages d'usine, mettre à niveau le micrologiciel, exporter et importer les

paramètres de configuration, programmer des redémarrages automatiques et activer le mode développeur.

14.3.1 Gestion des journaux

Le journal système enregistre les événements importants tels que les alertes de mouvement et les avertissements système. Vous pouvez rechercher dans le journal par type et par période et exporter un fichier de sauvegarde vers votre ordinateur.

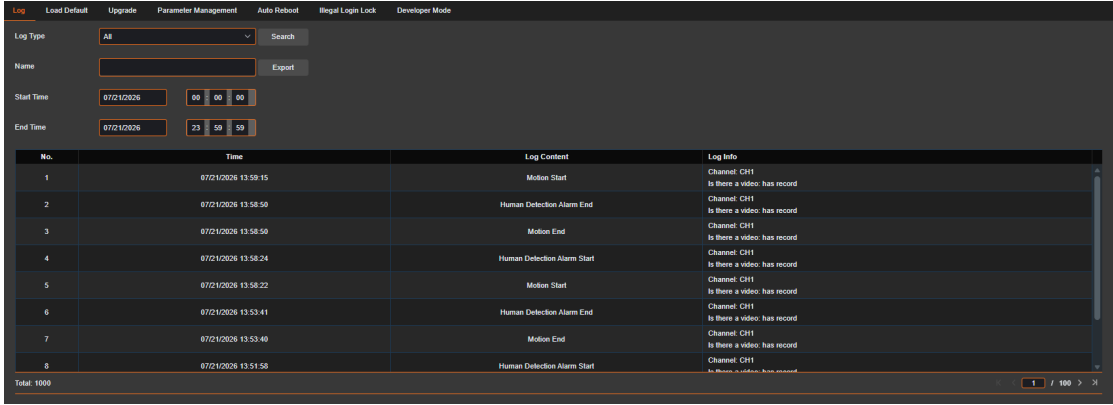


Figure 14-7. Recherche et sauvegarde du journal

Sélectionnez une catégorie dans la liste **Type de journal**, ou choisissez **Tout** pour afficher tous les événements de la période sélectionnée. Les catégories disponibles sont :

- **Système** — paramètres système, redémarrage, redémarrage automatique, mise à niveau, réglage de l'heure et étalonnage NTP.
- **Configuration** — modifications du contrôle en direct, du masquage de confidentialité, du mode et de l'horaire d'enregistrement, du flux principal et secondaire, du réseau, du courriel, de la couleur, de la détection de mouvement, du stockage, du multiutilisateur, du NTP, du contrôle d'image, du flux mobile, du RTSP, du filtre IP, du rétablissement des réglages d'usine, de la détection sonore, de l'importation et de l'exportation, de la notification d'événements, de la capture, de la dissuasion, de l'IA, du FTP, du DDNS, du HTTPS, de l'audio, de la sirène, de la maintenance du système, du masquage vidéo, de l'alarme I/O et des paramètres du service infonuagique.
- **Alarme** — début et fin de la détection de mouvement, alarme I/O, détection de piéton, détection de visage, échec d'authentification et délai d'expiration d'ouverture de porte, ainsi que les événements de détection de sabotage.
- **Compte** — connexion, déconnexion, verrouillage de compte et modifications d'utilisateur.
- **Enregistrement** — recherche, lecture et sauvegarde.
- **Stockage** — formatage du disque, disque plein et erreur de disque.
- **Réseau** — réseau déconnecté, réseau en ligne, erreurs réseau et changements de mode réseau.

Pour rechercher et exporter le journal :

1. Dans la liste **Type mineur**, sélectionnez le type d'événement précis à rechercher. (Cette liste n'est pas disponible lorsque le type de journal est réglé sur **Tout**.)
2. Dans le champ **Nom**, saisissez un nom de fichier pour le journal exporté. Cliquez sur **Exporter** pour créer une sauvegarde du journal système.
3. Cliquez sur le champ **Heure de début** et sélectionnez la date et l'heure de début dans le calendrier à l'écran.
4. Cliquez sur le champ **Heure de fin** et sélectionnez la date et l'heure de fin dans le calendrier.
5. Cliquez sur **Rechercher** pour exécuter la requête.

6. Examinez les entrées du journal pour la période sélectionnée.



Figure 14-8. Entrées du journal système



Figure 14-9. Entrées du journal des alarmes



Figure 14-10. Entrées du journal des comptes



Figure 14-11. Entrées du journal réseau

Utilisez les boutons de navigation dans le coin inférieur droit du menu pour passer d'une page d'événements de journal à l'autre.

14.3.2 Chargement des réglages par défaut

Cette page offre plusieurs méthodes de réinitialisation qui rétablissent les paramètres de configuration de la caméra à leurs valeurs d'usine. Le rétablissement des réglages d'usine ne formate pas les données stockées sur la carte TF.

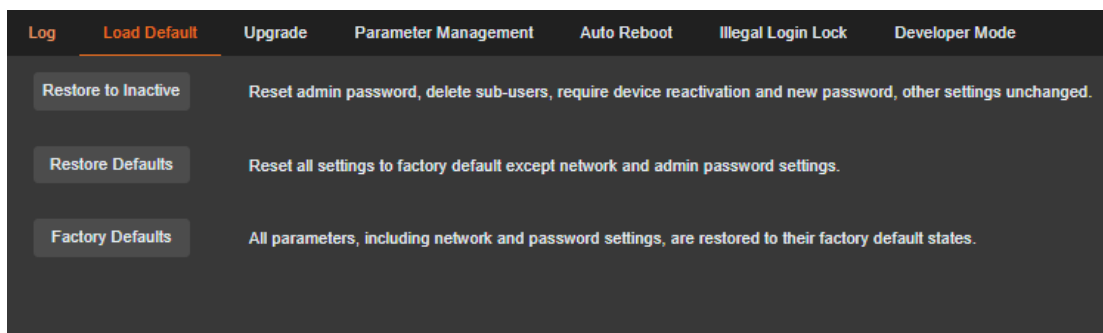


Figure 14-12. Chargement des réglages par défaut

- **Rétablir à l'état inactif** — réinitialise le mot de passe de l'administrateur et supprime tous les sous-utilisateurs. La caméra doit être réactivée, mais tous les autres paramètres des pages restent inchangés.
- **Rétablir les valeurs par défaut** — rétablit tous les paramètres des pages à leurs valeurs d'usine, à l'exception des paramètres réseau et du mot de passe de l'administrateur.
- **Réglages d'usine** — rétablit chaque paramètre de la caméra à sa valeur d'usine.

CAUTION Le rétablissement des réglages par défaut est irréversible et efface votre configuration. Selon la méthode sélectionnée, les sous-utilisateurs, le mot de passe de l'administrateur et les paramètres réseau peuvent être supprimés, ce qui oblige à réactiver et à reconfigurer la caméra. Exportez une sauvegarde des paramètres avant de continuer.

14.3.3 Mise à niveau du système

Ce menu vous permet de mettre à niveau le micrologiciel de la caméra, soit à partir d'un fichier sur votre ordinateur, soit en détectant une mise à niveau en ligne.

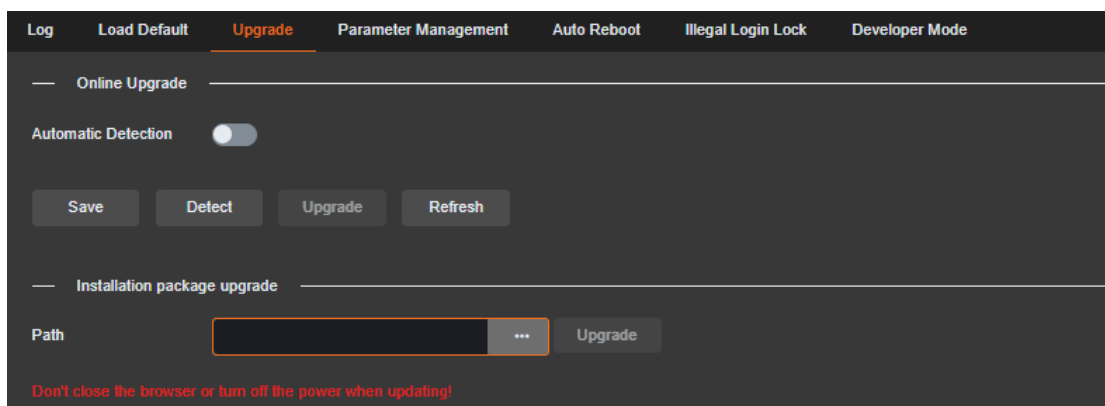


Figure 14-13. Mise à niveau du système

- **Détection automatique** — activez cette option pour vérifier automatiquement la présence de fichiers de mise à niveau en ligne.
- **Enregistrer** — enregistre les paramètres actuels.
- **Détecter** — après avoir défini le chemin de mise à niveau, cliquez pour vérifier manuellement la présence d'un fichier de mise à niveau en ligne. Une invite s'affiche lorsqu'une nouvelle version est disponible.

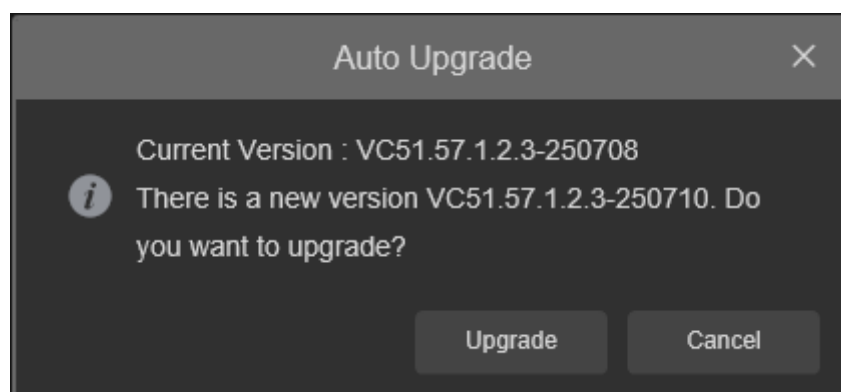


Figure 14-14. Nouvelle version de micrologiciel détectée

Pour mettre à niveau le micrologiciel à partir d'un fichier local :

1. Enregistrez le fichier de micrologiciel (un fichier **.bin**) sur le disque dur de votre ordinateur.
2. Cliquez sur ... à côté de **Chemin** et sélectionnez le fichier de micrologiciel sur votre ordinateur.
3. Cliquez sur **Mettre à niveau** pour commencer. La mise à niveau prend environ 3 à 4 minutes.

CAUTION Ne mettez pas la caméra hors tension et ne fermez pas l'interface Web à aucun moment pendant la mise à niveau du micrologiciel. L'interruption du processus peut rendre l'appareil inutilisable.

NOTE Si la caméra doit vérifier la présence de la dernière version du micrologiciel sur le serveur infonuagique, activez le commutateur du service infonuagique pour lier l'application et effacer les paramètres de configuration de mise à niveau en ligne de cette page.

14.3.4 Gestion des paramètres

La gestion des paramètres vous permet d'exporter les réglages configurés du menu principal vers un ordinateur, ou d'importer un fichier de configuration précédemment enregistré sur la caméra.

The screenshot shows the 'Parameter Management' tab in a web interface. It features two input fields: 'Import File' and 'Export file name', each followed by a button labeled 'Import' and 'Export' respectively. The interface has a dark theme with orange accents.

Figure 14-15. Importation et exportation des paramètres

- **Importer un fichier** — cliquez sur le champ pour ouvrir la fenêtre de chemin, sélectionnez le fichier de paramètres, puis cliquez sur **Importer** pour lancer l'importation.
- **Nom du fichier d'exportation** — cliquez sur le champ pour saisir un nom pour le fichier exporté, puis cliquez sur **Exporter** pour enregistrer les paramètres.

14.3.5 Redémarrage automatique

Le redémarrage automatique permet à la caméra de se redémarrer selon un horaire régulier, ce qui contribue à maintenir la stabilité à long terme. Il est recommandé de garder cette fonction activée.

The screenshot shows the 'Auto Reboot' tab. It includes a toggle for 'Auto-maintenance', a dropdown for 'Maintenance Interval' (set to '7 Day'), and a dropdown for 'Maintenance Time' (set to '00:00-02:00'). Below these is a red informational message: 'Auto Maintenance helps to keep your device healthy and optimized by running all maintenance tasks automatically at the time you choose. Your device will reboot when maintenance completed.' At the bottom are 'Save', 'Refresh', and 'Reboot' buttons.

Figure 14-16. Paramètres du redémarrage automatique

- **Maintenance automatique** — active ou désactive la fonction de maintenance automatique.
- **Intervalle de maintenance** — définit la fréquence à laquelle la caméra effectue la maintenance automatique.
- **Heure de maintenance** — définit la période pendant laquelle la maintenance automatique a lieu. La caméra se redémarre à un moment aléatoire à l'intérieur de cette plage.

14.3.6 Mode développeur

Le mode développeur permet au personnel technique de collecter et d'enregistrer des informations de journal pour le débogage de l'appareil.

The screenshot shows the 'Developer Mode' tab. It features a 'Camera Debug' toggle (which is turned on), a 'Mode' dropdown (set to 'NVR'), and buttons for 'Export debug info' and 'Pack Log'. Below these is a 'Device Status Reporting' toggle (also turned on), followed by 'Save' and 'Refresh' buttons. At the bottom, there is an 'Export Search Log' input field and an 'Export' button.

Figure 14-17. Paramètres du mode développeur

- **Débogage de la caméra** — sélectionnez pour activer le mode développeur.
- **Mode** — sélectionnez la méthode de collecte et d'enregistrement des informations de débogage : **NVR**, **SD_Card** ou **FTP**.
- **Télécharger les journaux de débogage** — en mode **SD_Card**, cliquez sur ce bouton et saisissez le mot de passe correct pour exporter les informations de débogage vers votre ordinateur.
- **Empaqueter le journal** — en mode **NVR** ou **FTP**, cliquez sur ce bouton pour téléverser les informations de journal empaquetées vers le serveur FTP.
- **Signalement de l'état de l'appareil** — activez pour téléverser l'état du stockage, l'état des canaux et les informations sur l'appareil vers le serveur P2P.
- **Exporter le journal de recherche** — saisissez un nom de fichier et cliquez sur **Exporter** pour exporter tous les fichiers de journal stockés sur l'appareil vers votre ordinateur.

14.3.7 Verrouillage des connexions illégales

Le verrouillage des connexions illégales protège la caméra contre les tentatives répétées de découverte de mot de passe en bloquant temporairement l'accès après un trop grand nombre d'échecs consécutifs.

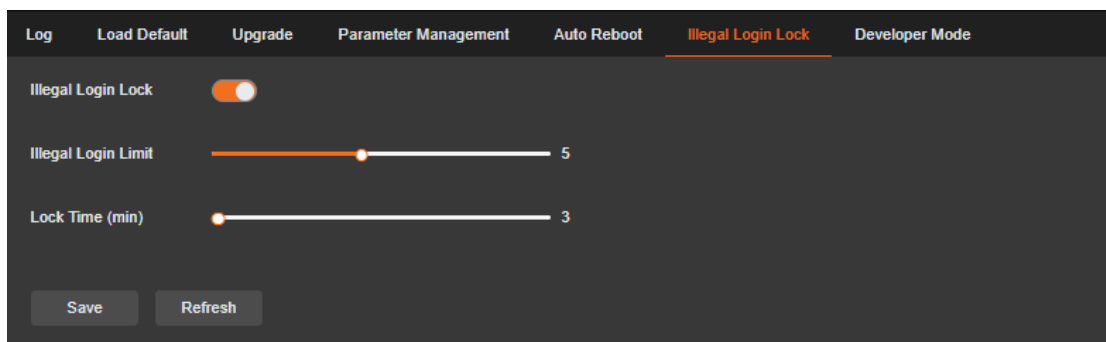


Figure 14-18. Paramètres du verrouillage des connexions illégales

- **Verrouillage des connexions illégales** — sélectionnez pour activer la fonction.
- **Limite de connexions illégales** — définit le nombre de tentatives de connexion échouées consécutives autorisées avant le verrouillage du compte. Faites glisser le curseur pour ajuster la valeur.
- **Durée de verrouillage (min)** — définit la durée, en minutes, pendant laquelle la connexion est bloquée une fois la limite atteinte. Les tentatives de connexion sont de nouveau autorisées après l'expiration de cette période. Faites glisser le curseur pour ajuster la valeur.

14.4 Informations système

Les pages d'informations système présentent des renseignements en lecture seule sur la caméra et son accord de confidentialité.

14.4.1 Informations sur l'appareil

Cette page affiche des informations système telles que l'identifiant de l'appareil, le nom du modèle, l'adresse MAC et la version du micrologiciel.

Figure 14-19. Informations sur l'appareil

14.4.2 Déclaration de confidentialité

Cette page présente le texte intégral de l'accord de confidentialité de l'appareil pour votre examen.

Figure 14-20. Déclaration de confidentialité